UTEG
UNIVERSIDAD TECNOLÓGICA EMPRESARIAL DE GUAYAQUIL

Tesis en Opción al Título de:

INGENIERO EN GESTION EMPRESARIAL MENCION GESTION INFORMATICA

Título de la Tesis:

PROCESO DE TRANSICION DE REDES IPV4 A IPV6

Autores:

Ernesto Paúl Morán Villalva

Marcos Paúl Benítes Donoso

TUTOR:

Ing. José Townsend

OCTUBRE 2007

Guayaquil - Ecuador

Agradecimiento *Marcos*

Primero quiero agradecer a Dios, porque me ha dado la fortaleza para poder culminar etapa muy importante en mi vida profesional. También quiero agradecer infinitamente a mis padres, ellos me han brindado su apoyo incondicional para todo, siempre, y han sido un pilar esencial para este logro, a todos los profesores que me han inculcado buenas costumbres y me han transmitidos sus conocimientos. De manera especial también mi amigo y compañero de tesis Paúl Morán.

Este trabajo lo dedico a todas las personas que de alguna forma han ayudado a que este logro se haga realidad.

Agradecimiento *Paul*

Detrás de toda culminación de una meta hay un gran equipo de trabajo. Agradezco infinitamente a todas esas personas que supieron aportar en mi vida todo su esfuerzo para lograr este objetivo. Sobre todo y de manera muy especial a Dios a mi madre Nora Villalva Cabrera, seguida de un gran maestra de mi infancia mi tía Melva Villalva Cabrera y a mi abuelita que siempre fue la gran madre de todos en la familia Julia Rebeca Cabrera.

A mi compañero y amigo de tesis Marcos Benites.

Dedico este trabajo a Dios todo poderoso quien nos da el poder de la sabiduría y la inteligencia.

A mi madre Nora Villalva dedico este trabajo de manera muy especial ya que sin su talento sus ejemplos su disciplina y sobre todo su amor; yo no seria nadie en esta vida.

A mi tía Melva Villalva

A mi abuelita Julia Cabrera

A mis tíos que están siempre cerca de mí

A mi compañera idónea

A mis amigos y amigas

INDICE

1. RESUMEN

Este trabajo de tesis pretende ofrecer una guía practica que permita migrar y/o permitir cohexistir la interoperabilidad de redes y aplicaciones IPv4 e IPv6, en al caso de las aplicaciones sin cambiar el código fuente de las mismas. En muchos casos no se dispone del código fuente, o existe un problema de licencias que impide modificarlo.

Además, existen casos en los que, aunque se dispone del código, portarlo a la nueva interfaz de IPv6, distribuirlo e instalarlo puede resultar un trabajo costoso que requiera demasiado tiempo. Por estos motivos, la presente propuesta tiene relevancia durante el período de transición, permitiendo convivencia de aplicaciones, o partes de una aplicación, ya portadas a IPv6 con aplicaciones IPv4 existentes.

Las ventajas que nos aportará el uso de IPv6 en nuestras redes, aplicaciones y servicios, previsiblemente irán más allá de nuestros objetivos primarios, permitiéndonos obtener resultados que no se podrían conseguir de otro modo.

El proceso de migración también nos ayudará a crear el conocimiento base a partir del cual podremos desarrollar proyectos de implantación de esta tecnología.

La migración ha de verse como un proceso evolutivo que comenzará con la implantación del nuevo protocolo en las infraestructuras de comunicaciones, para continuar luego con la modificación de aplicaciones, servicios y sistemas de gestión de las mismas, acabando con la extensión del protocolo a la mayor parte de los dispositivos interconectados a la red de redes.

Durante la implantación del nuevo protocolo los sistemas han de verse afectados lo menos posible, con el fin de que la migración en la capa de red se pueda realizar de forma escalonada y según las necesidades que vayan surgiendo.

HIPOTESIS

Al final de esta tesis el lector estará familiarizado con los conceptos básicos de este protocolo y podrá diseñar un proceso de migración adecuado.

OBJETIVO GENERAL

Precisar los fundamentos de IPv6 y mostrar las posibilidades de las implementaciones actuales de este protocolo así como también mostrar algunos temas relacionados con la seguridad y los servicios para IPv6, así como una metodología y los pasos necesarios para implantar IPv6 en una red en producción.

OBJETIVOS ESPECIFICOS

Analizar los siguientes tópicos:

- Describir las diferentes técnicas para la
  - migración de IPv4 a IPv6
  - transición de IPv4 a IPv6
  - convivencia entre IPv4 e IPv6
- Mostrar que sucede con las aplicaciones desarrolladas para IPv4 y las implicaciones para la migración a IPv6
- Identificar escenarios de seguridad para la operación de IpnG (IPv6)
- Mostrar un banco de prueba replicable sobre el cual las organizaciones interesadas en la migración puedan utilizar para sus pruebas
- Mostrar como instalar el protocolo IPv6 en MS Windows y Linux

3. INTRODUCCION/EVOLUCION [1] [2] [3] [4] [5] [6] [7]

En 1992, el IETF llego a la conclusión de que haría falta un sustituto del IPv4 y formo un grupo de trabajo con el nombre de IPNG que tendrá la misión de desarrollar la siguiente generación del protocolo IP. De las distintas propuestas, el IETF escogió el Protocolo IP versión 6, que mas tarde será Draft Standard.[8]

El protocolo IPv6 tiene sus orígenes en la RFC 1752, "The Recommendation for the IP Next Generation Protocol", publicada en enero de 1995, y que ponía fin a un concurso de propuestas para un nuevo protocolo que sustituyera al protocolo IPv4. Este concurso fue suscitado a partir de una primera decisión, en junio de 1992, del entonces Internet Activities Board (IAB), en la que se tomaba el protocolo CLNP de ISO como punto de partida para este nuevo protocolo. Esta decisión recibió una muy mala acogida en la comunidad Internet, lo que llevó al IAB a retirarla y a abrir el citado concurso que concluyó con la publicación de la RFC 1752[9]

"En un impresionante corto período de tiempo, se han conectado las PC a LAN, se han conectado las LAN entre sí, y a las WAN, y todo ello, a menudo, se ha conectado con el mundo externo. El resultado es una Internet extraordinariamente diversa con millones de usuarios."[10]

El diseño del sistema original de direcciones de IP no era el apropiado para un entorno como éste. El espacio de números resultaba pequeño. Al contrario que con el sistema telefónico, que utiliza un código de país y de área, la numeración no era jerárquica. Los bloques de números se asignaban a las organizaciones de manera muy ineficiente, desperdiciándose gran parte del espacio de números.[11]

---

[1] http://www.microsoft.com
[2] IPv6 UJI - Luis Peralta, Febrero 19 del 2002
[3] Comunicaciones de Telefónica I+D (Telefónica Investigación y Desarrollo) Marzo 2005
[4] Cisco IPv6 Implementations and Transitions, June 2006
[5] Estudio de la problemática de la implantación de IPv6 en la RECETGA (Andrés Gómez, José Carlos Pérez, Juan Villasuso, Natalia Costas) Enero 28 del 2005
[6] Deploying IPv6 Networks (By Ciprian Popoviciu, Eric Levy-Abegnoli, Patrick Grossetete)
[7] Understanding IPv6 - Joseph Davies, Microsoft 2004
[8] http://www.ietf.org
[9] Una breve historia de Internet (Primera Parte) Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Lawrence G. Roberts, Stephen Wolff
[10] Cisco Networking Academy Program
[11] Internet Architecture Board

El resultado es qué el espacio de números se ha agotado. Además, como los números no se asignan jerárquicamente las tablas de routing crecen muy rápidamente.[12]

No se espera una reducción de la expansión de Internet. Hay un crecimiento continuado en la expansión de las computadoras personales y su conectividad a la red global. Además, aparecen nuevos desafíos:

- La comunicación de las nuevas generaciones de computadoras personales móviles, la evolución de los actuales asistentes personales digitales.
- La anticipación en la demanda de audio y vídeo en tiempo real, que pondrá la actual tecnología en sus límites.[13]

De lo anterior se puede inferir que la sociedad de consumo tiene en Internet una herramienta y plataforma de mercadeo, operaciones (logística y distribución) y mejora de los procesos de negocios.

El desarrollo de la versión 6 de IP, IPv6, llamada también IP de siguiente generación, se ha visto estimulado por la urgente necesidad de resolver los problemas de direcciones de Internet, routing, rendimiento, seguridad y congestión.

IPv6 está definido en el documento RFC 2460, "Internet Protocol, Versión 6 (IPv6) Specification" [Especificación del Protocolo Internet, versión 6 (IPv6)]. IPv6 es un protocolo de **datagramas** sin conexión no confiable, que se utiliza principalmente para el direccionamiento y routing de paquetes entre hosts.

Sin conexión significa que no se establece una sesión antes de intercambiar datos. No confiable significa que la entrega no está garantizada. IPv6 siempre intenta por todos los medios entregar los paquetes. Un paquete IPv6 se puede perder, entregar fuera de secuencia, duplicar o retrasar. IPv6 no intenta recuperarse de estos tipos de errores. La confirmación de paquetes entregados y la recuperación de paquetes perdidos se efectúan mediante un protocolo de nivel superior, como TCP.[14]

---

[12] Designing Internetworks with IPv6, Henrik Lund Kramshøj, April 28, 2002
[13] Driscol & Associates, 1.995
[14] Designing Internetworks with IPv6, Henrik Lund Kramshøj, April 28, 2002

Las características de IPv6 son las siguientes:[15]

- Dispone de direcciones de 128 bits, 16 octetos, que se pueden estructurar jerárquicamente para simplificar la delegación de direcciones y el routing.
- Simplifica la cabecera principal de IP, pero define muchas cabeceras de extensión opcionales. De esta forma se pueden incorporar las nuevas funciones de intercomunicación cuando se necesiten.

3.1. Los Motivos de IPv6

La versión actual del Protocolo Internet (denominada IP versión 4 o IPv4) no ha cambiado de forma significativa desde la publicación del documento RFC 791 en 1981[16]. IPv4 ha demostrado ser un protocolo robusto, de fácil implementación e interoperable, y ha superado la prueba de ampliar un conjunto de redes interconectadas para un uso global del tamaño que Internet tiene en la actualidad. Éstas son las virtudes de su diseño inicial.

Sin embargo, el diseño inicial no previó las siguientes circunstancias:[17]

- El reciente crecimiento exponencial de Internet y el agotamiento inminente del espacio de direcciones IPv4. Las direcciones IPv4 han empezado a escasear relativamente, lo que ha obligado a algunas organizaciones a utilizar un traductor de direcciones de red (NAT, Network Address Translator) para asignar múltiples direcciones privadas a una única dirección IP pública. Si bien NAT fomenta la reutilización del espacio de direcciones privadas, no admiten la seguridad de nivel de red basada en estándares o la asignación correcta de todos los protocolos de nivel superior y pueden crear problemas al conectar dos redes que utilizan el espacio de direcciones privadas. Además, la importancia cada vez mayor de los dispositivos y aparatos conectados a Internet garantiza que acabará por agotarse el espacio de direcciones IPv4 públicas.

- El crecimiento de Internet y la capacidad de los routers de la red troncal de Internet para mantener tablas de routing grandes. Debido a la forma en que los ids. de red de IPv4 se han asignado y se siguen asignando, lo normal es que existan más de 70.000 rutas en las tablas de routing de los routers de **red troncal** de Internet. La

---

[15] RFC 2460
[16] Internet Engineering Task Force http://www.ietf.org
[17] IPv6 - La Internet de nueva generación (2005) Latif Laid

infraestructura actual de routing de la red Internet IPv4 es una combinación de routing plano y jerárquico.

- La necesidad de una configuración más sencilla. La mayoría de las implementaciones actuales de IPv4 se deben configurar manualmente o mediante un protocolo de configuración de direcciones con estado como el Protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol). Al existir más equipos y dispositivos que utilizan IP, surge la necesidad de una configuración de direcciones más sencilla y automática y otras opciones de configuración que no dependan de la administración de una infraestructura DHCP.

- El requisito de seguridad en el nivel de IP. La comunicación privada a través de un medio público como Internet requiere servicios de cifrado que impidan que los datos enviados se puedan ver o modificar durante el tránsito. Aunque en la actualidad existe un estándar que proporciona seguridad para los paquetes IPv4 (denominado seguridad de Protocolo Internet o IpSec), este estándar es opcional y prevalecen las soluciones propietarias. [18]

- La necesidad de mayor compatibilidad con la entrega de datos en tiempo real (denominado también calidad de servicio). Aunque existen estándares de calidad de servicio (QoS, Quality of Service) para IPv4, la compatibilidad con el tráfico en tiempo real depende del campo Tipo de servicio (TOS, Type of Service) de IPv4 y la identificación de la carga, que suele utilizar un puerto UDP o TCP. El campo TOS de IPv4 tiene una funcionalidad limitada y diferentes interpretaciones. Además, la identificación de la carga que utiliza un puerto TCP o UDP no es posible cuando la carga del paquete IPv4 está cifrada.

Para solucionar estos problemas, el Grupo de trabajo de ingeniería de Internet (IETF, Internet Engineering Task Force) ha desarrollado un conjunto de protocolos y estándares denominados IP versión 6 (IPv6). Esta nueva versión, anteriormente llamada IP La siguiente generación (IPng, IP-The Next Generation), incorpora los conceptos de muchos métodos propuestos para la actualización del protocolo IPv4. IPv6 está diseñado con la

[18] RFC 2401: Security Architecture for the Internet Protocol

intención de reducir al mínimo el impacto en los protocolos de nivel superior e inferior al evitar la adición arbitraria de nuevas características[19]

El motivo básico por el que surge, en el seno del IETF (Internet Engineering Task Force), la necesidad de crear un nuevo protocolo, que en un primer momento se denominó IPng (Internet Protocol Next Generation, o "Siguiente Generación del Protocolo Internet"), fue la evidencia de la falta de direcciones.[20]

- IPv4 tiene un espacio de direcciones de 32 bits, es decir, (4'294.967.296).
- En cambio, IPv6 ofrece un espacio de 2128 340.282.366.920.938.463.463.374.607.431'768.211.456) (RFC2373)
- Sin embargo, IPv4 tiene otros problemas o "dificultades" que IPv6 soluciona o mejora.

Los creadores de IPv4, a principio de los años 70, no predijeron en ningún momento, el gran éxito que este protocolo iba a tener en muy poco tiempo, en una gran multitud de campos, no sólo científicos y de educación, sino también en innumerables facetas de la vida cotidiana.[21]

Desde ese momento, y debido a la multitud de nuevas aplicaciones en las que IPv4 ha sido utilizado, ha sido necesario crear "añadidos" al protocolo básico.

Entre los "parches" más conocidos, se puede citar medidas para permitir la Calidad de Servicio (QoS), Seguridad (IpSec), y Movilidad, fundamentalmente.[22]

El inconveniente más importante de estas ampliaciones de IPv4, es que utilizar cualquiera de ellos es notablemente sencillo, pero no tanto cuando se pretende usar al mismo tiempo dos "añadidos", y no se convierte en casi imposible o muy poco práctico el uso simultáneo de tres o más, haciendo de la administración notablemente compleja.

---

[19] OReilly.IPv6.Essentials.2nd.Edition.May.2006
[20] Cisco Networking Academy Program
[21] Una breve historia de Internet (Primera Parte) Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Lawrence G. Roberts, Stephen Wolff
[22] Sacando partido a IPv6 con redes IPv4, Palet Jordi, CTO Consulitel

3.2. ¿Porqué IPv6? [23]

Un único motivo lo impulso: Más direcciones!

- Para miles de millones de nuevos dispositivos, como teléfonos celulares, PDAs, dispositivos de consumo, vehículos, etc
- Para miles de millones de nuevos usuarios, como China, India, etc.
- Para tecnologías de acceso "always-on", como xDSL, cable, ethernet, etc.

Pero, ¿No es Verdad que aún Quedan Muchas Direcciones IPv4?

- La mitad del espacio de direcciones IPv4 aún no ha sido utilizado; El tamaño de Internet se duplica cada año[24], ¿significa esto que sólo quedan unos pocos años?; No, debido a que hoy se niega direcciones IPv4 públicas a la mayoría de los nuevos hosts para ello se emplean mecanismos como NAT, PPP, etc. para compartir direcciones
- Nuevos tipos de aplicaciones y nuevos mecanismos de acceso, requieren direcciones únicas

El protocolo IPv6 ha sido designado por los organismos de estandarización de protocolos IP/Internet como la nueva versión del protocolo IP empleado actualmente en Internet (IPv4).[25]

En este sentido, Vinton G. Cerf, chairman del ICANN y considerado como padre de la Internet actual, participa activamente en distintos eventos y foros de discusión sobre IPv6.

El objetivo es instaurar IPv6 antes de llegar a una situación crítica en Internet y en las redes IP actuales, debido a la falta de direccionamiento público (estimado hacia 2009-2011).

Los sistemas de acceso a redes IP, denominados always-on, en los que el usuario residencial y/o remoto está permanentemente conectado con una dirección IP pública, son cada vez más frecuentes. Estas redes incrementan la demanda de las direcciones IP públicas a un ritmo mayor del esperado, pues el acceso permanente impide una concentración de recursos (las direcciones IP públicas) basado en la división por tiempo de uso de las mismas (asignación dinámica).

---

[23] Tomado y adaptado de A. Chaudhry, B. Crosby, A. Zinin
[24] Internet Architecture Board
[25] Internet Corporation for Assigned Names and Numbers (ICANN) http://www.icann.org/announcements/IPv6-report-06sep05.htm

El fuerte crecimiento actual de las redes de acceso de banda ancha, especialmente ADSL y las redes de cable, augura una anticipación de la fecha límite en la que podrían agotarse las direcciones IPv4 públicas.

Por tanto, se considera que éste puede ser un factor que desencadene el uso de direcciones y, por tanto, del protocolo IPv6.

Estos nuevos servicios y aplicaciones de banda ancha demandan de la Red, no solamente una elevada capacidad en los enlaces, sino unos requisitos de temporización y conformación del tráfico. Los equipos que prestan servicio en las redes públicas no están en condiciones de ofrecer con garantías de éxito dichas prestaciones.

Por otra parte, la comunidad de usuarios de Internet y los fabricantes de equipos y operadores de servicios de telecomunicación no pueden abordar drásticamente el rediseño de una gran cantidad de redes, protocolos y servicios. Por lo tanto, se plantea el problema de implantar un nuevo protocolo, como el IPv6, o bien introducir innumerables mejoras en el actual IPv4, con objeto de satisfacer las necesidades de los usuarios.

Esta problemática, sin embargo, se puede abordar bajo otros puntos de vista. No se trata de eliminar la infraestructura IPv4 para dar paso a IPv6.

3.3. IPv6, ¡SÌ! NAT ¡NO! [26]

No todos son defensores de IPv6, la proverbial y ancestral "resistencia al cambio". Los antagonistas (en su derecho) sostienen que los problemas de asignación de dirección y de routing pueden ser controlados con otros mecanismos. Uno de estos mecanismos que ha demostrado ser especialmente polémico es la translación de dirección de red. Los que apoyan a NAT afirman que es la solución completa a los problemas de dirección IPv4.

Sus adversarios, por otro lado, ven a NAT como un computador no fiable que es activamente perjudicial a la interoperabilidad, ya que incapacita las redes verdaderas de punto a punto, un criterio para seguridad cada datagrama que pasa por una red NAT tiene que ser convertido, lo que hace que sea imposible usar los protocolos de arquitectura de seguridad IP (IpSec) para encriptar o firmar las transmisiones de forma

[26] IPv6 - La Internet de nueva generación (2005) Latif Laid

digital. Por otro lado, NAT hace posible ocultar redes enteras detrás de una sola dirección IP, lo que es una forma de seguridad por derecho propio.

3.3.1. ¿Porqué NAT no es Adecuado?

- No funciona con gran número de "servidores", es decir, dispositivos que son "llamados" por otros (ejemplo, Teléfonos IP, P2P)
- Inhiben el desarrollo de nuevos servicios y aplicaciones (creatividad)
- Comprometen las prestaciones, robustez, seguridad y manejabilidad de Internet
- Usa una única dirección IPv4 para que una red completa pueda acceder a Internet.
- Incrementa la complejidad de la configuración.
- Crea puntos únicos de fallo (cuellos de botella) en las conexiones a redes.
- Dificulta la escalabilidad.
- Algunos protocolos son incapaces de atravesar los dispositivos NAT, por ejemplo RTP y RTCP.
- No se emplea Multicast porque es muy compleja (nivel de detalle) su configuración.
- Dificulta la movilidad.
- Resta flexibilidad.
- Perjudica la operación y gestión de la red.
- NAT es una solución temporal frente a los problemas de IPv4, pero no es la solución definitiva.

El actual protocolo Internet, IPv4, desarrollado a últimos de los setenta y primeros de los ochenta [27], atiende más de 4.000 millones de hosts, pero no todas las direcciones están disponibles. Más de 500 millones de direcciones IPv4 se reservan como direcciones experimentales[28], privadas o para multidifusión. El esquema original IPv4 de direccionamiento basado en clases también dio como resultado una distribución de direcciones muy ineficaz, que se mitigó parcialmente con la introducción de CIDR (classless inter domain routing) en 1993 [29]. Sin embargo, debido a la naturaleza jerárquica del espacio de direccionamiento y requisitos de agregación de dirécción,

---

[27] J. Postel (Editor): "Internet Protocol," IETF Standard RFC 791/STD 5, septiembre 1981 (ftp://ftp.rfceditor.org/innotes/rfc791.txt).
[28] Internet Engineering Task Force http://www.ietf.org
[29] V. Fuller y otros: "Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy," IETF Proposed Standard RFC 1519, septiembre 1993

ambos extremos funciones vitales para gestionar el tamaño de la tabla de routing Internet, sólo puede usarse una fracción del número teórico de direcciones [30].

Además se introdujo la tecnología NAT (traducción de dirección de red)[31] [32] para ralentizar la velocidad a la que se agotan las direcciones IPv4, permitiendo a varios hosts compartir una única dirección IP. NAT es fenomenal para mejorar el uso de espacio de dirección, pero rompe el paradigma de comunicación extremo a extremo, crítico para la aparición de aplicaciones del tipo par a par, máquina a máquina, siempre en marcha. Algunos argumentan que NAT siempre ofrece seguridad escondiendo la estructura de direccionamiento interna y en algunos casos incluyendo software firewall. De todas formas, el software adicional aumenta la complejidad y sigue sin ofrecer una completa seguridad de servicio.

Las direcciones IPv4 han sido distribuidas muy desigualmente entre los distintos Regional Internet Registries (RIR) por la Internet Corporation for Assigned Names and Numbers (ICANN): 74% a American Registry for Internet Numbers (ARIN), 17% al Centro de coordinación de redes IP europeas (RIPE NCC), y 9% a Asia Pacific Network Information Center (APNIC). Esta distribución desigual queda dramáticamente ejemplificada cuando se observa que ¡grandes universidades estadounidenses como Stanford y MIT [tienen asignadas un número de direcciones IPv4 de similar magnitud al de toda China!

Por ello, a finales de los noventa, IAB (Comisión de Arquitectura de Internet) de IETF (Grupo de Tareas sobre Ingeniería de Internet) presentó un trabajo para desarrollar un sucesor de IPv4. Los directores de área de IETF IP Next Generation Area enumeraron sus recomendaciones finales en RFC 1752 en julio de 1994 [33].

Había nacido una nueva generación de Internet Protocol: IPv6. El conjunto central de protocolos IPv6 se plasmó en un IETF Draft Standard en agosto de 1998.

---

[30] Durand y otros: "The H-Density Ratio for Address Assignment Efficiency An Update on the H ratio", IETF Informational RFC, RFC 3194, noviembre de 2000

[31] P. Srisuresh y otros: "IP Network Address Translator (NAT) Terminology and Considerations," IETF Informational RFC, RFC 2663, agosto de 1999

[32] B. Dutcher: "The NAT Handbook: Implementing and Managing Network Address Translation," John Wiley & Sons,352 páginas, ISBN 0471390895, noviembre de 2000.

[33] S. Bradner y otros: "The Recommendation for the IP Next Generation Protocol," IETF Proposed Standard RFC 1752, enero de 1995

El desarrollo de CIDR, NAT y DHCP (dynamic host configuration protocol)[34] ha mejorado significativamente IPv4, y puede restar fuerza a algunas de las ventajas clave de IPv6. Sin embargo, la inhabilidad para anticipar áreas de crecimiento económico y la resultante distribución desigual de direcciones IPv4 alrededor del mundo ha ocasionado fuertes presiones geopolíticas que están impeliendo urgentemente a la adopción de IPv6. Este ímpetu ha sido particularmente visible en Asia, seguida de Europa, y reflejado más recientemente en la decisión de las autoridades de EE.UU. de desplegar IPv6 en redes gubernamentales no más tarde de 2008.[35]

Como se menciono anteriormente, la ventaja fundamental de IPv6 es el espacio de direcciones.

El reducido espacio de IPv4, a pesar de disponer de cuatro mil millones de direcciones (4'294.967.296), junto al hecho de una importante falta de coordinación, durante la década de los 80, en la delegación de direcciones, sin ningún tipo de optimización, dejando incluso grandes espacios discontinuos, esta llevando a límites no sospechados en aquel momento.[36]

Por supuesto, hay una solución que puede considerarse como evidente, esta sería la renumeración, y reasignación de dicho espacio de direccionamiento.

Sin embargo, no es tan sencillo, es incluso impensable en algunas redes, ya que requiere unos esfuerzos de coordinación, a escala mundial, absolutamente impensables.

Además, uno de los problemas de IPv4 permanecería: la gran dimensión de las tablas de routing en el **troncal** de Internet, que la hace ineficaz, y perjudica enormemente los tiempos de respuesta (request time).

La falta de direcciones no es apreciable por igual en todos los puntos de la red, de hecho, no es casi apreciable, por el momento, en Norte América. Sin embargo, en zonas geográficas como Asia (en Japón la situación esta llegando a ser crítica), y Europa, el problema se agrava.[37]

---

[34] R. Droms: "Dynamic Host Configuration Protocol," IETF Draft Standard RFC 2131, March 1997
[35] National Security Agency (NSA) http://www.nsa.org
[36] Driscol &Associates 2002
[37] Driscol &Associates 2002

Como ejemplos, podemos citar el caso de China que ha pedido direcciones para conectar 60.000 escuelas, tan sólo ha obtenido una clase B (65.535 direcciones), o el de muchos países Europeos, Asiáticos y Africanos, que solo tienen una clase C (255 direcciones) para todo el país.

Tanto en Japón como en Europa el problema es creciente, dado al importante desarrollo de las redes de telefonía celular, inalámbricas, módems de cable, xDSL, etc., que requieren direcciones IP fijas para aprovechar al máximo sus posibilidades e incrementar el número de aplicaciones en las que pueden ser empleados.
La razón de utilización de las direcciones IP por parte de los usuarios, esta pasando en pocos meses de 10:1 a 1:1, y la tendencia se invertirá. En pocos meses, podrá verse dispositivos "siempre conectados", con lo que fácilmente un usuario podría tener, en un futuro no muy lejano, hasta 50 o 100 IP's (1:50 o 1:100).[38]

Algunos Proveedores de Servicios Internet se ven incluso obligados a proporcionar a sus clientes direcciones IP privadas, mediante mecanismos de NAT (traslación de direcciones, es decir, usar una sola IP pública para toda una red privada). De hecho, casi todos los ISP's (Internet Service Provider) se ven obligados a delegar tan sólo reducidos números de direcciones IP públicas para sus grandes clientes corporativos.

Como ya se ha comentado, la solución, temporalmente, es el uso de mecanismos NAT. Desafortunadamente, de seguir con IPv4, esta tendencia no sería "temporal", sino "invariablemente permanente". Ello implica la imposibilidad práctica de muchas aplicaciones, que quedan relegadas a su uso en Intranets, dado que muchos protocolos son incapaces de atravesar los dispositivos NAT:

- RTP y RTCP ("Real-time Transport Protocol" y "Real Time Control Protocol") usan UDP con asignación dinámica de puertos (NAT no soporta esta traslación).
- La autenticación Kerberos necesita la dirección fuente, que es modificada por NAT en la cabecera IP.
- Multicast, aunque es posible, técnicamente, su configuración es tan complicada con NAT, que en la práctica no se emplea.

---

[38] http://www.telefonica.com/sociedad_de_informacion/

3.4. Cuestión de tiempo [39]

En la conferencia anual de 1999 del Grupo de Interés Especial sobre Comunicación de Datos de la Asociación de Maquinaria de Computación (SIGCOMM99), Sandy Fraser, Científico Jefe de AT&T, expresó inquietud por la arquitectura de la Internet. ¿Es ésta adaptable? ¿Por qué no nos hemos desplazado todavía de IPv4 a IPv6? ¿Se ha osificado la alabada Fuerza de Tareas de Ingeniería de Internet (IETF)?

Uno de los problemas que rodea el debate IPv6 es que no hay ninguna fecha específica para la cual se habrán acabado todas las direcciones IPv4. Los optimistas afirman que a IPv4 le queda todavía unas cuantas buenas décadas. Los pesimistas avisan que sólo le quedan unos pocos años. A pesar de todo hay un gran empuje hacia adelante para IPv6. Naciones como China y Japón que no recibieron mucho espacio de direcciones en IPv4 son proponentes principales, como lo son las industrias nacientes. Los proveedores de telefonía digital móvil de próxima Generación y los vendedores de electrodomésticos conectados en redes hacen observar que necesitaran direcciones IP para millones de aparatos.

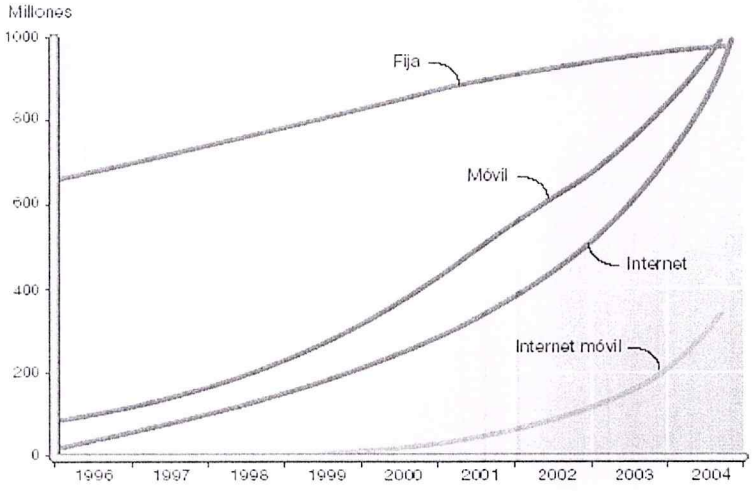


Figura 1 A la luz del crecimiento pronosticado (abonados) de telefonía fija y móvil e internet móvil, no es demasiado temprano para que los operadores de redes empiecen a planificar, instalar y probar redes IPv6, Fuente Internet Architecture Board

También hay movimiento por parte de la IETF, cuyo grupo de trabajo de protocolo Internet de próxima generacion (IPng) sigue estudiando mucho las especificaciones IPv6 y el IPv6 Forum recientemente[40] formado fomenta el nuevo protocolo IP, para construir la nueva Internet.

---

[39] IPv6 - La Internet de nueva generación (2005) Latif Laid
[40] http://www.IPv6.org

3.4.1. Cifras: el crecimiento de Internet

Las cifras de "internautas, usuarios de acceso a internet, cibernautas", esperadas en los próximos años, avalan lo expuesto [41]

- África: 800.000.000 (sólo 3.000.000 sin NAT)
- América Central y del Sur: 500.000.000 (sólo 10.000.000 sin NAT)
- América del Norte: 500.000.000 (sólo 125.000.000 sin NAT
- Asia: 2.500.000.000 (sólo 50.000.000 sin NAT)
- Europa Occidental: 250.000.000 (sólo 50.000.000 sin NAT)

Pero lo más importante es el imparable crecimiento de aplicaciones que necesitan direcciones IP públicas únicas, globales, válidas para conexiones extremo a extremo, y por tanto enrutables: Videoconferencia, Voz sobre IP, seguridad, e incluso juegos.

MERCADO VERTICAL	EJEMPLOS DE APLICACION	TAMAÑO DEL MERCADO
- lectura de contadores	- Lecturas de consumos de servicios básicos	242'000.000
- Seguridad	- Sistemas de alarmas de incendios, etc., residenciales como y comerciales	24'000.000
- posicionamiento de vehículos/ flotas e información de condiciones	- Seguimiento automático de vehículos - Seguimiento de inventarios - Diagnostico y seguridad de vehículos	15'000.000
- Monitorización	- Maquinas de venta automática - Buzones de correo - Gas e irrigación	7'900.000
	total	**289'900.000**

Tabla : Sólo en Estados Unidos de América, el mercado potencial de aplicaciones susceptibles de ser conectadas a la red [42]

En 1.997, el mercado de dispositivos con aplicaciones capaces de conectarse a Internet (sin incluir terminales ni computadores, tan sólo WebTV, agendas electrónicas, teléfonos con acceso a Internet, y consolas de juegos), era de 3'000.000. En el año 1.998, este se duplica hasta llegar a los 6'000.000, y las previsiones de crecimiento para el 2.002, según IDC, son de 56'000.000.[43]

---

[41] Internet Architecture Board
[42] Driscol & Associates, 1995
[43] Driscol & Associates, 2002

Sólo contabilizando el crecimiento de la nueva generación de telefonía móvil (UMTS), en el año 2.003[44] se prevén cifras del orden de los 1.000.000.000 de usuarios, la misma cifra que para la telefonía fija y que para el número de usuarios "fijos" de Internet. En ese momento, los usuarios móviles con conexión a Internet se acercarán a los 400'000.000

Se prevé unas necesidades de direcciones IP para los dispositivos de la red (no para los dispositivos de los usuarios), para el año 2.005, de 3,2 millones, y de 6,3 para el 2.010. Según el mismo informe, en el 2.005, se requerirían un total de 20.000.000.000 de direcciones IP para los dispositivos de los usuarios.[45]

Nuevas tecnologías emergentes, como Bluetooth, WAP, redes inalámbricas, redes domésticas, etc., hacen más patente esta necesidad de crecimiento, al menos, en los que al número de direcciones se refiere.

Por ejemplo, la última tendencia es la de permitir a cualquier dispositivo serial, ser conectado a una LAN o WAN, y por que no a Internet. Este tipo de "convertidores", denominados "Universal Device Server" (Servidor de Dispositivos Universal, permite que aplicaciones impensables por las limitaciones de los cableados seriales, se realicen remotamente a través de redes, o incluso que un sistema de alarmas, que antes requería un módem dedicado para la conexión con la central de recepción de alarmas, pueda ahora enviar un e-mail, ¡con todo lujo de detalles!.

Podríase pensar en la utilización, en general, de casi cualquier dispositivo tanto doméstico como industrial, integrado en la gran red, pero también en dispositivos de control médico, marcapasos, etc.

---

[44] Driscol & Associates, 2003
[45] Foro UMTS/GSM

4. HISTORIA Y FUTURO DE TCP/IP

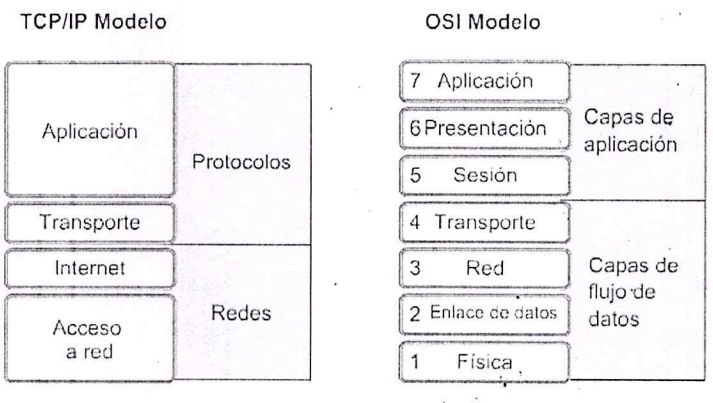
El Departamento de Defensa de EE.UU. (DoD) creó el modelo de referencia TCP/IP porque necesitaba una red que pudiera sobrevivir ante cualquier circunstancia.

La creación del modelo TCP/IP ayudó a solucionar este difícil problema de diseño de redes. Desde entonces, TCP/IP se ha convertido en el estándar en el que se basa la Internet.

Al leer sobre las capas del modelo TCP/IP, tenga en cuenta el propósito original de la Internet. Recordar su propósito ayudará a reducir las confusiones. El modelo TCP/IP tiene cuatro capas: la capa de aplicación, la capa de transporte, la capa de Internet y la capa de acceso de red. Es importante observar que algunas de las capas del modelo TCP/IP poseen el mismo nombre que las capas del modelo OSI. Resulta fundamental no confundir las funciones de las capas de los dos modelos ya que estas desempeñan diferentes funciones en cada modelo.

4.1. Diferencias entre los modelos OSI y TCP/IP:

- TCP/IP combina las capas de presentación y de sessión en una capa de aplicación
- TCP/IP combina la capas de enlace de datos y la capa física del modelo OSI en una sola capa
- TCP/IP parece ser más simple porque tiene menos capas
- La capa de transporte TCP/IP que utiliza UDP no siempre garantiza la entrega confiable de los paquetes mientras que la capa de transporte del modelo OSI sí.



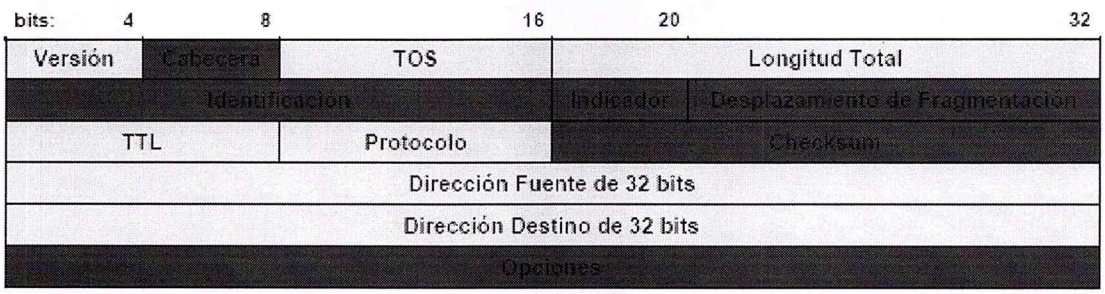
La Internet se desarrolla de acuerdo con los estándares de los protocolos TCP/IP. El modelo TCP/IP gana credibilidad gracias a sus protocolos. A diferencia, en general, las redes no se contruyen a base del protocolo OSI. El modelo OSI se utiliza como guía para comprender el proceso de comunicación.

5. EL PROTOCOLO IPv6 (RFC2460, ¿Que es IPv6?)

5.1. EL Punto de Referencia IPv4: [46]

El protocolo de Internet fue desarrollado para "proveer las funciones necesarias para enviar un paquete de bits (un datagrama de Internet) desde una fuente hasta un destino sobre un sistema interconectado de redes", y ha proveído esa función por casi 2 décadas. IP es primariamente concerniente con el envío del datagrama. Igualmente importantes, sin embargo, son las emisiones que IP no direcciona, como el envío puntual de datos de extremo a extremo o el envío de datos secuencial. IP deja estas emisiones para la capa Host-to-Host y las implementaciones del TCP y del UDP que reside allá.

En el proceso de entregar datagramas, IP debe negociar con direccionamiento y fragmentación. La dirección asegura que el datagrama llegue al destinatario correcto, sea que esté del otro lado de la ciudad o del otro lado del mundo. La fragmentación es necesaria porque las LAN y WAN que cualquier datagrama atraviese pueden tener tamaños de frames que difieren, y datagrama de IP debe siempre ajustar dentro del frame, como se muestra en la figura siguiente (Por ejemplo, un frame de Ethernet puede acomodar 46 – 1,500 octetos de datos, mientras FDI carga hasta 4,470 octetos). Campos específicos dentro del encabezado de IP manejan las funciones de fragmentación y direccionamiento. Note en la figura que cada grupo horizontal de bits (llamado una palabra) es de 32 bits de ancho.



La longitud mínima de la cabecera IPv4 es de 20 bytes (cada fila de la tabla supone 4 bytes). A ello hay que añadir las opciones, que dependen de cada caso.

En la tabla anterior se ha usado abreviaturas, en aquellos casos en los que son comunes.

- Version – Versión (4 bits)

[46] Palet Jordi, CTO Consulitel

- Header – Cabecera (4 bits)
- TOS (Type Of Service) – Tipo de Servicio (1 byte)
- Total Length – Longitud Total (2 bytes)
- Identification – Identificación (2 bytes)
- Flag – Indicador (4 bits)
- Fragment Offset – Desplazamiento de Fragmentación (12 bits – 1.5 bytes)
- TTL (Time To Live) – Tiempo de Vida (1 byte)
- Protocol – Protocolo (1 byte)
- Checksum – Código de Verificación (2 bytes)
- 32 bit Source Address – Dirección Fuente de 32 bits (4 bytes)
- 32 bit Destination Address – Dirección Destino de 32 bits (4 bytes)

En la tabla anterior, se ha marcado, mediante el color de fondo, los campos que van a desaparecer en IPv6, y los que son modificados, según el siguiente esquema:

Se ha pasado de 12 campos, en IPv4, a tan solo 8 en IPv6.

El motivo fundamental por el que los campos son eliminados, es la innecesaria redundancia. En IPv4 se tiene la misma información de varias formas. Un caso muy evidente es el checksum o verificación de la integridad de la cabecera: Otros mecanismos de encapsulado ya realizan esta función (IEEE 802 MAC, framing PPP, capa de adaptación ATM, etc.).
El caso del campo de "Fragment Offset", es ligeramente diferente, dado que el mecanismo por el que se realiza la fragmentación de los paquetes es totalmente modificado en IPv6, lo que implica la total "inutilidad" de este campo. En IPv6 los routers no fragmentan los paquetes, sino que de ser precisa, dicha fragmentación/desfragmentación se produce extremo a extremo.

- payload length → longitud de carga útil (payload length), que en definitiva, es la longitud de los propios datos, y puede ser de hasta 65.536 bytes. Tiene una longitud de 16 bits (2 bytes).
- Protocol → siguiente cabecera (next header), dado que en lugar de usar cabeceras de longitud variables se emplean sucesivas cabeceras encadenadas, de ahí que desaparezca el campo de opciones. En muchos casos ni siquiera es

procesado por los routers, sino tan sólo extremo a extremo. Tiene una longitud de 8 bits (1 byte).

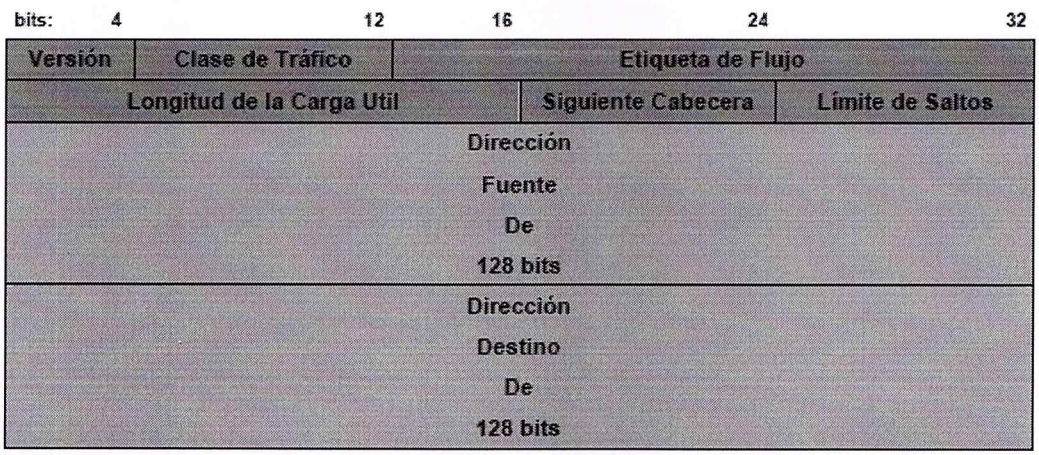
- time to live → límite de saltos (Hop Limit). Tiene una longitud de 8 bits (1 byte).Los nuevos campos son:

Los nuevos campos son:

- traffic class, también denominado Prioridad (Priority), o simplemente Clase (Class). Podría ser más o menos equivalente a TOS en IPv4. Tiene una longitud de 8 bits (1 byte).
- flow label, para permitir tráficos con requisitos de tiempo real. Tiene una longitud de 20 bits.

Estos dos campos, como se puede suponer, son los que permiten una de las características fundamentales e intrínsecas de IPv6: Quality of Service (QoS), Class of Service (CoS), y en definitiva un poderoso mecanismo de control de flujo, de asignación de prioridades diferenciadas según los tipos de servicios.

Por tanto, en el caso de un paquete IPv6, la cabecera tendría el siguiente formato:



El campo de versión, que es igual a 6, lógicamente, tiene una longitud de 4 bits.

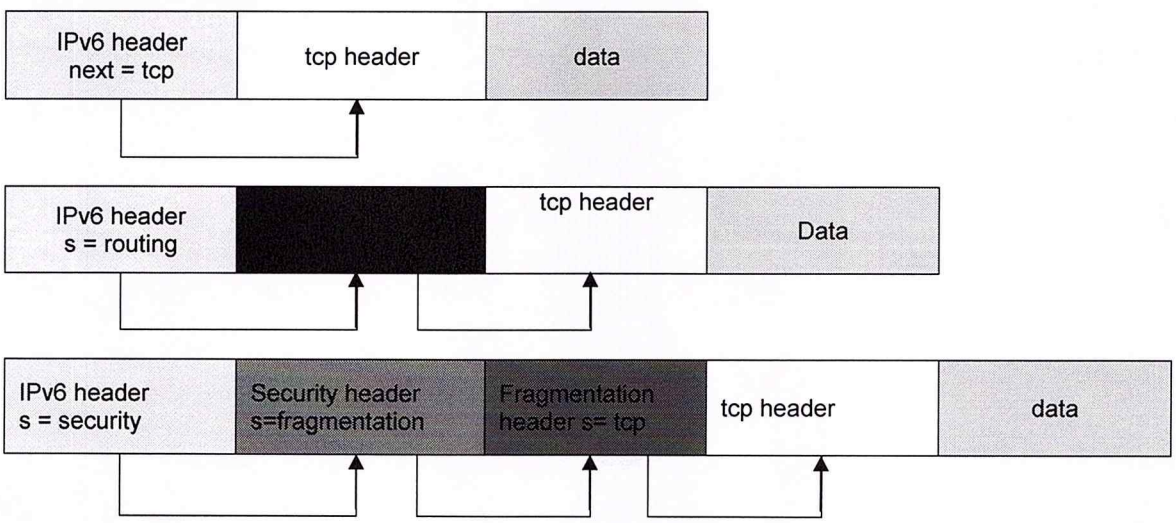
La longitud de esta cabecera es de 40 bytes, el doble que en el caso de IPv4, pero con muchas ventajas, al haberse eliminado campos redundantes.

Además, como ya hemos mencionado, la longitud fija de la cabecera, implica una mayor facilidad para su procesado en routers y switchs, incluso mediante hardware, lo que implica unas mayores prestaciones.

A este fin coadyuva, como se ha indicado anteriormente, el hecho de que los campos están alineados a 64 bits, lo que permite que las nuevas generaciones de procesadores y microcontroladores, de 64 bits, puedan procesar mucho más eficazmente la cabecera IPv6.

El valor del campo "next header", indica cual es la siguiente cabecera y así sucesivamente. Las sucesivas cabeceras, no son examinadas en cada nodo de la ruta, sino sólo en el nodo o nodos destino finales. Hay una única excepción a esta regla: cuando el valor de este campo es cero, lo que indica opción de examinado y proceso "hop-by-hop". Así, por citar algunos ejemplos, cabeceras con información de enrutado, fragmentación, opciones de destino, autenticación, encriptación, etc., que en cualquier caso, han de ser procesadas en el orden riguroso en que aparecen en el paquete.

Sin entrar en más detalles, véanse a continuación los siguientes ejemplos gráficos del uso del concepto de las "cabeceras de extensión" (definidas por el campo "siguiente cabecera"), mecanismo por el que cada cabecera es "encadenada" a la siguiente y anterior (si existen):



El MTU (Unidad Máxima de Transmisión), debe de ser como mínimo, de 1.280 bytes, aunque se recomiendan tamaños superiores a 1.500 bytes. Los nodos descubren el valor MTU a través de la inspección de la ruta. Se prevé así una optimización de los paquetes

y del número de cabeceras, dado el continuo crecimiento de los anchos de banda disponibles, así como del incremento del propio tráfico.

5.2. Los Criterios para el IPng.

En diciembre de 1993, el RFC 1550 fue distribuido, titulado "IP: Next Generation (IPng)". Este RFC invitó a cualquier interesado que sometiera comentarios con respecto a cualesquiera requisitos específicos para el IPng o cualquier factor dominante que se deban considerar durante el proceso de selección de IPng. 21 respuestas fueron sometidas que trataron una variedad de asuntos, incluyendo: seguridad (RFC 1674), opinión de un usuario corporativo grande (RFC 1686).

El área de IPng detallado en el RFC 1726, "Criterio Técnico para elegir IP, la nueva generación de direcciones IP (IPng)", para definir los sistemas de los criterios que serían utilizados en el proceso de la evaluación de IPng. Los 18 criterios son los siguientes:

- **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 routing 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 routings 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 son LAN, WAN y MAN y SAN. 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 routing 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 y la transmisión del paquete de multicast.
- **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.

5.3. La Cabecera de IPv6

El paquete de IPv6 es cargado en un frame de red local como en IPv4; sin embargo, el encabezado de IPv6 consiste en 2 partes. Estas son el encabezado base de IPv6, más encabezado de extensión opcional. Con o sin algún encabezado de extensión opcional, un constraint de tamaño fijo en uniframe de red local debe ser respetado. Por ejemplo, la mayor cantidad de datos que puede ser cargada en un frame Ethernet es 1500 octetos. Si el encabezado de extensión es añadido al paquete de IPv6, menos datos de aplicación pueden ser enviados. El host y/o su sistema operativo deben tener un mecanismo para manejar esto.

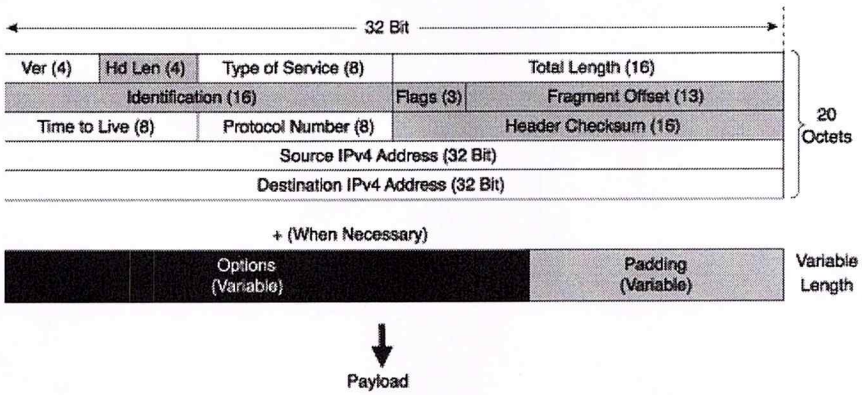
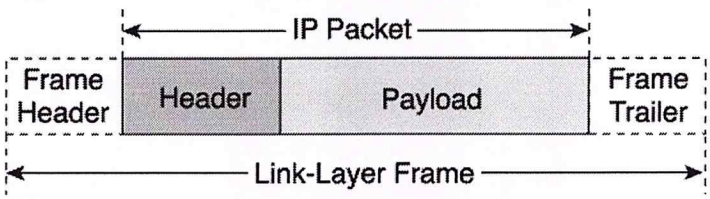


Fig. 2-3

La cabecera de un paquete IPv6 es, sorprendentemente, más sencilla que la del paquete IPv4. Y recuérdese que además la funcionalidad del protocolo IPv6 es mucho mayor.



El frame header de un paquete IPv4 es variable, por lo que necesita un campo de tamaño o longitud. Sin embargo, para simplificar la vida de los routers, IPv6 utiliza un header lenght de 40 bytes, que componen un total de ocho campos:

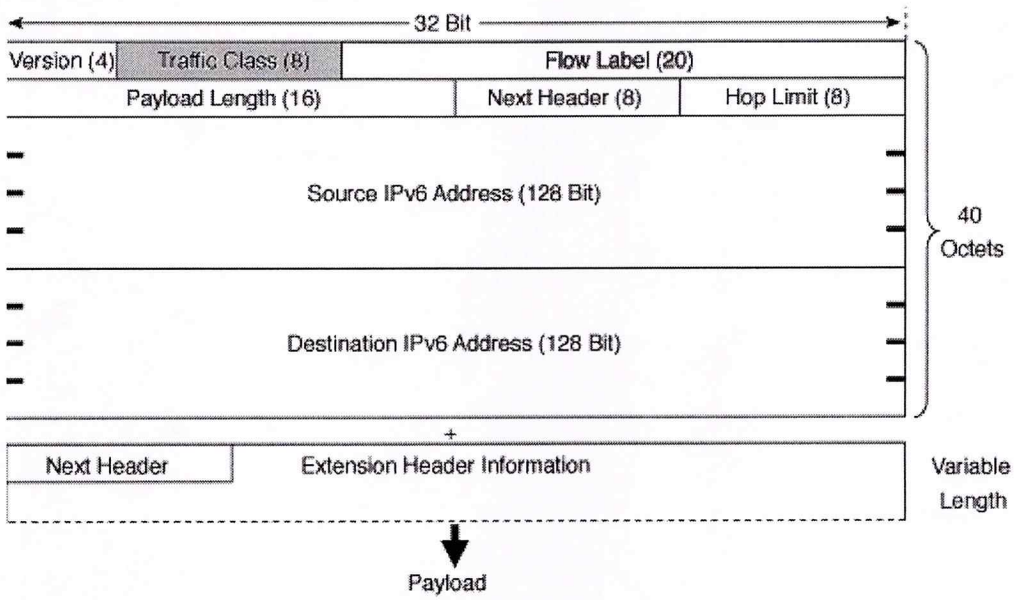
5.3.1. El Campo Versión

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.

5.3.2. El Campo Traffic Class

El campo Traffic Class es de 8 bits de largo y su intención para los nodos de origen y/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 "Diferentiation Services".

Estos 3 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.

Dos de los otros documentos, RFC 2474 y RFC 2475, discuten el concepto e implementación de servicios de diferenciación, que tienen la intención de discriminar entre varios tipos de servicio, requiriendo el estado por carga y señalización en cualquier salto. RFC 2474 define un campo Differentiated Services que reemplaza el campo Type of Service de IPv4. RFC 2475 es más general en la naturaleza, y describe una arquitectura para servicios diferenciados y las funciones a ser proveídas.

Esta arquitectura es descrita en 2 componentes: uno trata con el reenvío de paquetes, y el otro trata con las políticas que determinan los parámetros usados en la ruta de reenvío. Una analogía es dibujada desde las diferencias entre reenvío de paquetes y ruteo de paquetes. El reenvío es el proceso por paquete que determina (de una tabla de ruteo) a qué interfase un paquete debe ser enviado. (En otras palabras, si el encabezado de paquete identifica la subred en Quito, entonces envía este paquete por la interfase #5). Rutear es un proceso más complejo que determina las entradas en esa tabla de ruteo, y (posiblemente más importante) la política que determina cómo esa tabla es construida. (Por ejemplo, si el enlace a Quito se cae, entonces envía el paquete vía Manta en vez de vía Machala). Como se discutió en RFC 2474, los comportamientos de la ruta de reenvío son mejor entendidos que las políticas que configuran los parámetros que afectan la ruta de envío.

RFC 2474 se concentra en el componente de la ruta de reenvío que determina el "per hop behavior" (PHB) de los paquetes, más que en la política y parámetros de configuración del componente. Los PHB's incluirían tratamiento específico que un paquete individual recibe, con las cosas del mensaje de que son requeridas para eficientizar ese tratamiento especial. Un PHB suficientemente definido debería permitir la construcción de servicios predecibles.

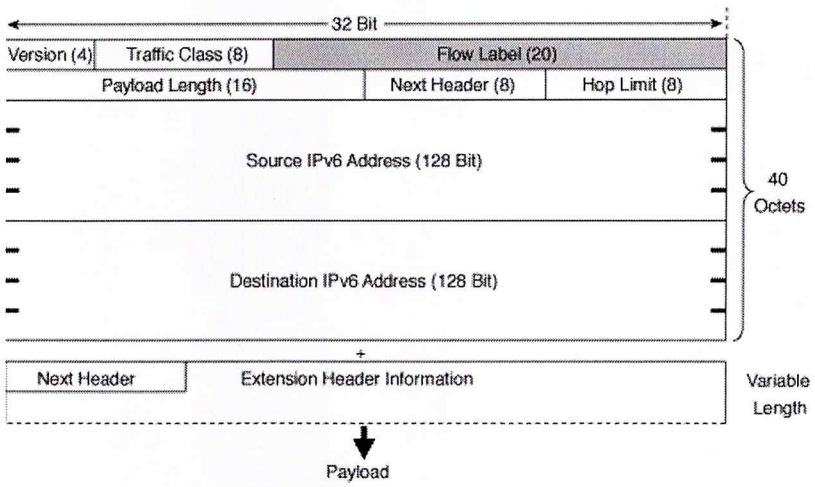
RFC 2474 define el formato para el campo Differentiated Services (DS) que contiene 2 subcampos. El subcampo Differentiated Services Codepoint (DSCP) selecciona el PHB que un paquete experimenta en cada nodo. El campo Currently Used (CU) es reservado para futuras definiciones.

El campo Type of Service de IPv4 consiste en 3 partes: un campo precedente de 3 bits, 3 bits que especifican banderas (Delay, Throughput y Reliability, o DTR) y 2 bits que son reservados. RFC 2474 define un grupo de puntos de código, el patrón de bits para el subcampo DSCP sería XXX000 (en binario, donde x sería cero o uno). Note que los 3 "X" bits corresponden con las mismas posiciones de los bits de DTR; sin embargo, RFC 2474 establece que ningún atento es hecho para mantener compatibilidad hacia atrás con esos bits de banderas. También, el punto de código con valor 000000 es asignado al PHB por default, que es definido como el comportamiento de envío "común, de más esfuerzo". (Nótese la comparación con el campo de precedencia, éste correspondería con el valor para precedencia de "rutina".)

Otros valores de punto de código han sido agrupados en pools, con un pool reservado para tareas basadas en estándares, y otros, para propósitos de uso local y experimental. RFC 2474 describe estas tareas en detalle más grande.

5.3.3. 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 4 de estos bits han sido ahora colocados en el campo Traffic Class.

Un flujo es una secuencia de paquetes enviados a un destino unicast o multicast que necesita manejo especial por los routers IPv6 que intervienen.

Todos los paquetes pertenecientes a un mismo flujo debe ser enviado con la misma dirección fuente, dirección destino y etiqueta de flujo. Un ejemplo de un flujo sería paquete que soporta un servicio en tiempo real, como audio o vídeo.

Flow Label es usado por esa fuente para etiquetar esos paquetes que requieren manejo especial por el nodo IPv6. Si un host o router no soporta funciones de Flow Label, el campo es fijado a cero en el origen e ignorado en la recepción.

Múltiples flujos de datos pueden existir entre una fuente y un destino, así como tráfico de datos que no es asociado con un flujo particular. Un flujo único es identificado por la combinación de una dirección fuente y una etiqueta de flujo que no sea cero. La etiqueta de flujo es un número seudo-aleatorio elegido del rango de 1 a FFFFFH (donde H denota notación hexadecimal). Esa etiqueta es usada como una clave hash por router para buscar el estado asociado con ese flujo.

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.

5.3.4. 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). Nótese que 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 2 medidas operan en diferentes campos. Payload Length (IPv6) mide los datos después del encabezado, mientras Total Length (IPv4) mide los datos y el Header Lenght.

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.

5.3.5. El Campo de Siguiente Cabecera (Next Header Field)

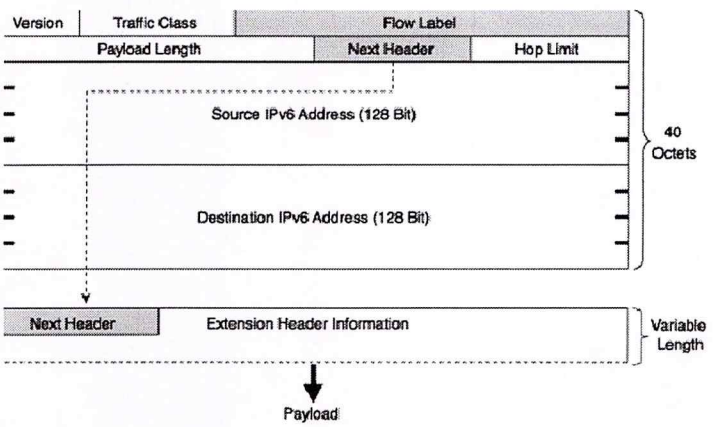
El campo Next Header tiene 8 bits de longitud e identifica el encabezado inmediatamente siguiente del header de IPv6. Este campo usa los mismos valores que el campo Protocol de IPv4. Ejemplos:

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

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.

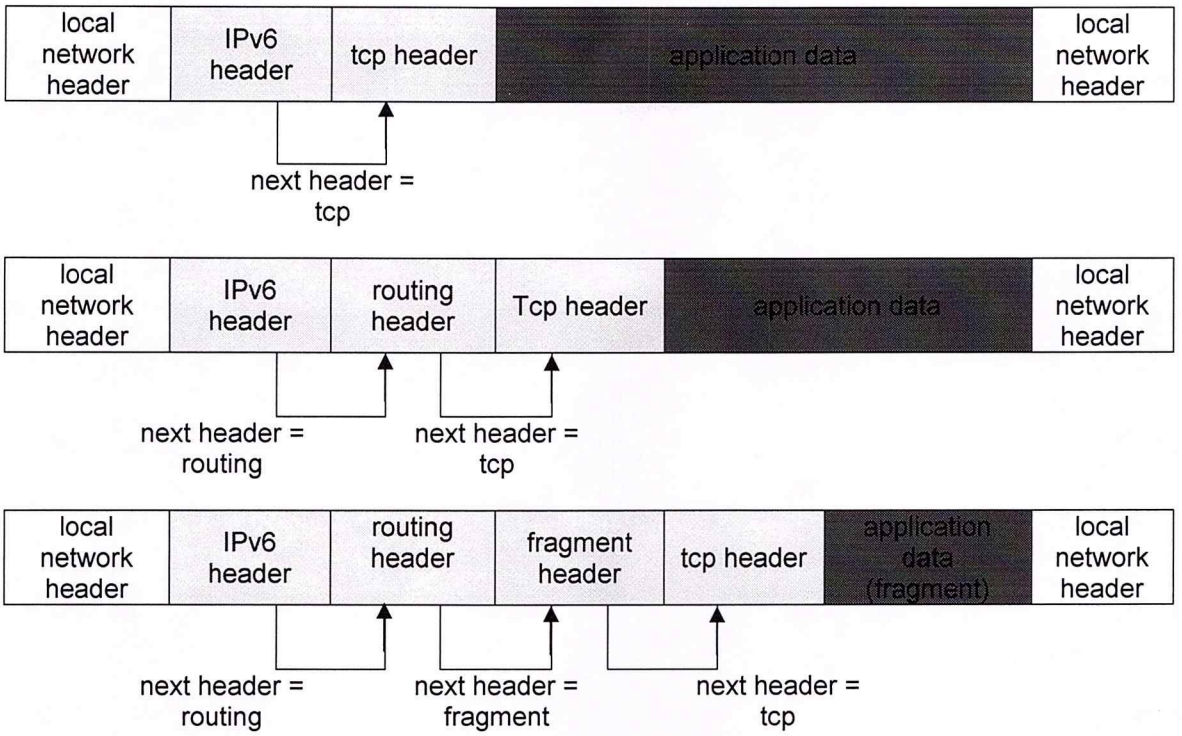
En el primer caso ningún encabezado de extensión es requerido, Next Header = TCP, y el encabezado TCP y cualquier protocolo de capa más alta le sigue[47]. En el segundo ejemplo, un header Routing es requerido. Luego, Next Header de IPv6 = Routing; en el header Routing, Next Header = TCP, y el encabezado TCP y cualquier protocolo de capa más alta le sigue.

En el tercer caso, tanto el header Routing como Fragment son requeridos, con los campos Next Header identificados acordemente.



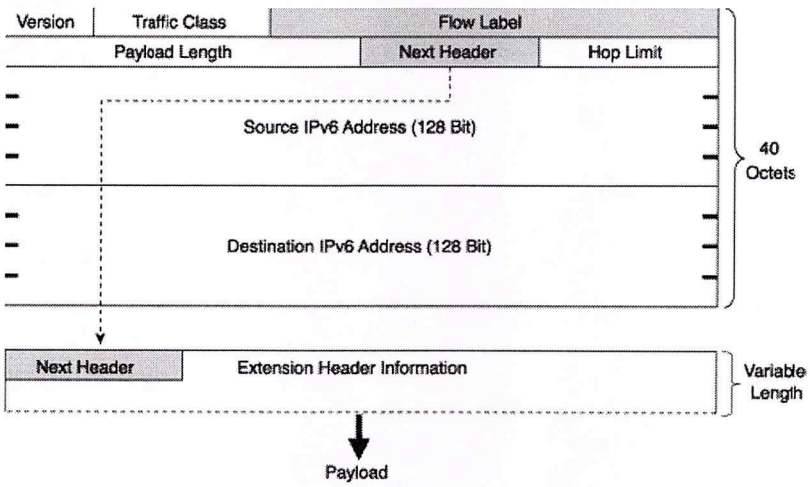
[47] CISCO Systems CCNA Curriculum V 3.1

Figura Next header field operation



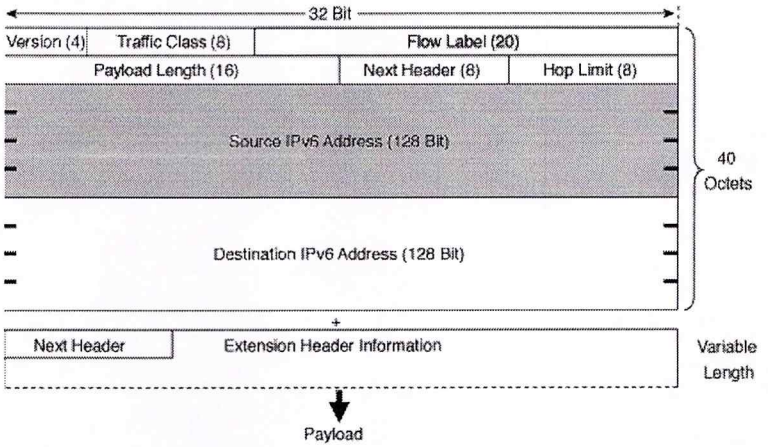
5.3.6. El Campo Hop Limit

El campo Hop Limit tiene 8 bits de longitud, y va descreciendo 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. Note que con Hop Limit usada en IPv6, la base del tiempo no está disponible más.



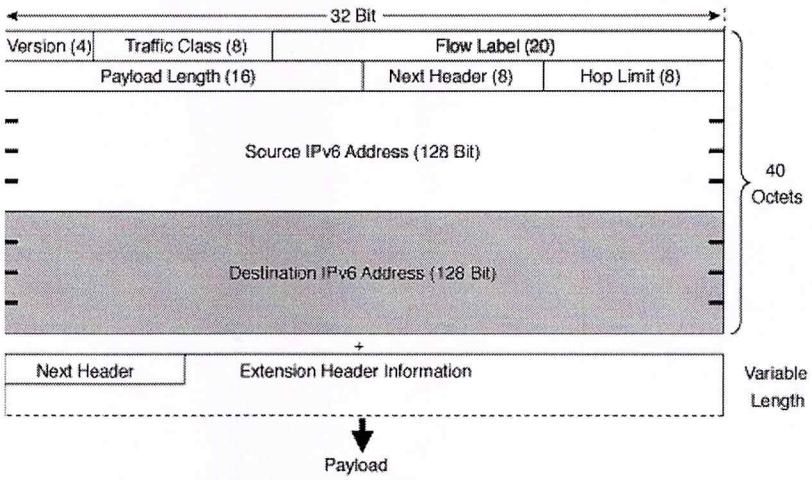
5.3.7. El Campo Source Address

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.



5.3.8. 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 la de 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.



5.4. Encabezados de Extensión

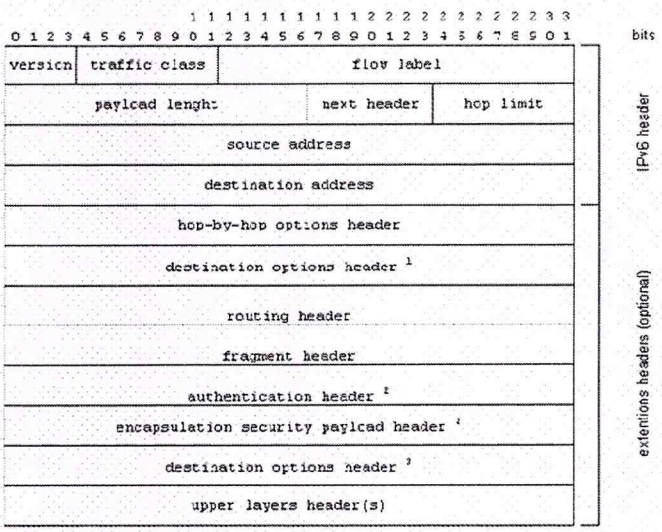
El diseño de IPv6 simplifica el encabezado existente de IPv4 colocando muchos de los campos existentes en encabezado opcionales. De esta forma, el procesamiento de paquetes ordinarios no es complicado por uso indebido de encabezados, mientras las condiciones más complejas son todavía proveídas.

Como se ha visto, un paquete IPv6, que consiste de un paquete IPv6 más su carga, puede consistir de cero, uno o más encabezados de extensión. Cada encabezado de extensión es un múltiple integral de 8 octetos de longitud para retener la alineación de 8

octetos para encabezados subsecuentes. Para óptimo desempeño del protocolo, estos encabezados de extensión son colocados en un orden específico.

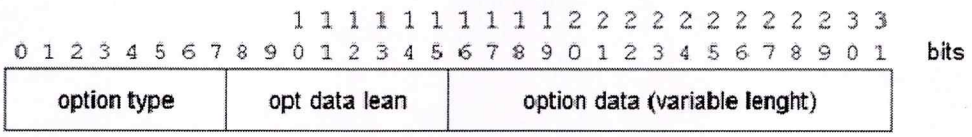
5.4.1. Orden de los Encabezados de Extensión

RFC 2460 recomienda que los encabezados de extensión sean colocados en el paquete IPv6 en un orden particular:



5.4.2. Opciones de los Encabezado de Extensión

Dos de los encabezados de extensión, Hop-by-Hop y Destination Options, pueden cargar una o más opciones que identifican más allá de los parámetros de operación de red. Estas opciones son codificadas usando el formato TLV (Tipe-Lenght-Valor) que es especificado por el lenguaje de descripción de mensajes Abstract Syntax Notation 1 (ASN.1)[48] (TLV es ampliamente usado entre protocolos de comunicación, incluyendo el Simple Network Management Protocol, SNMP.) La opción formato incluye un campo Option Type de 8 bits que identifica la longitud del campo Option Data dada en octetos; y un campo Option Data de longitud variable.



Los dos bits de orden más alto del campo Option Type, especifican como tener opciones que son irreconocibles en el nodo de procesamiento de IPv6:

[48] IPv6 Essentials, 2nd Edition (2006)

valor	Acción
00	Salta la opción y continúa procesando el encabezado
01	Descarta el paquete
01	Descarta el paquete y envía un mensaje ICMP Problema de Parámetro (Tipo de Opción irreconocible) a la fuente
11	Descarta el paquete y envía un mensaje ICMP problema de parámetro (Tipo de Opción irreconocible) a la fuente (solo si el destino no era multicast)

El tercer bit de orden más alto del campo Option Type especifica si Option Data de esa opción puede cambiar en ruta al destino final del paquete o no.

valor	acción
0	Option data no cambia su valor en ruta.
1	Option data puede cambiar en ruta.

Además, hay 2 opciones que son usadas, como necesarios, para rellenar las opciones de forma que el encabezado de extensión contenga un múltiplo de 8 octetos. Pad1 Option es usado para insertar 1 octeto de relleno en el área de opciones en el encabezado. Note que esta opción es un caso especial (notado por Type = 0) que no tiene los campos Opt Data Len ó Option Data.

PadN Option es usada para insertar 2 ó más octetos de relleno en el área Options de un encabezado. Note que esta opción tiene un campo Type = 1. Si el relleno deseado fuera n octetos, el campo Opt Data Len contendría el valor n-2 octetos de valor cero.

5.4.3. Encabezado de Extensión Hop-by-Hop

El encabezado de opción Hop-by-Hop carga información opcional que debe ser examinada por cada nodo dentro de la ruta de envío del paquete. Como resultado, el encabezado de opción Hop-by-Hop, cuando está presente, debe inmediatamente seguir al encabezado de IPv6. (Los otros encabezados de extensión no son examinados o procesados por ningún nodo en la ruta de envío del paquete hasta que el mismo alcanza su destino(s) propuesto(s).) La presencia del encabezado Hop-by-Hop es identificada por un valor de 0 en el campo Next Header del encabezado IPv6. Este encabezado posee 2 campos, más opciones.

El campo Next Header tiene 8 bits de longitud, e identifica el encabezado que inmediatamente continúa el encabezado de opción Hop-by-Hop. Este campo usa los mismos valores que el campo Protocol de IPv4.

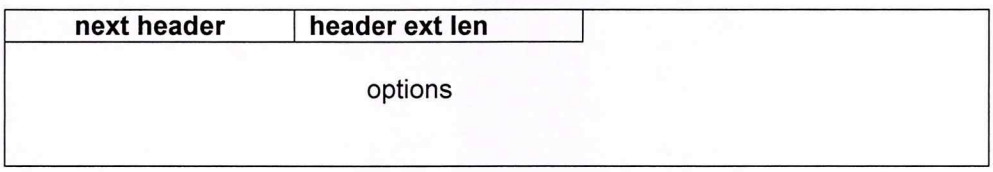
El campo Header Extension Length (Hdr Ext Len) tiene 8 bits de longitud, y mide la longitud del encabezado Hop-by-Hop Options en unidades de 8 octetos, sin contar los primeros 8 octetos.

El campo Options es variable en longitud, siempre que el encabezado Hopby-Hop Options completo sea un entero y un múltiplo de 8 octetos de longitud.

Una opción actualmente definida, la opción Jumbo Payload, que es usada para enviar paquetes de IP que son entre 65,536 y 4,294,967,295 octetos de longitud.

Esta opción es definida por Option Type = 194 (o C2H), Opt Data Len = 4 (octetos) y un campo de 4 octetos que carga la longitud del paquete jumbo en octetos (excluyendo el encabezado base de IPv6, pero incluyendo el encabezado Hop-by-Hop Options y algún otro encabezado). Jumbo Payload Length debe ser más grande que 65,535. También, el campo Payload Length = 0 (para indicar una condición especial) cuando Jumbo Payload es usado.

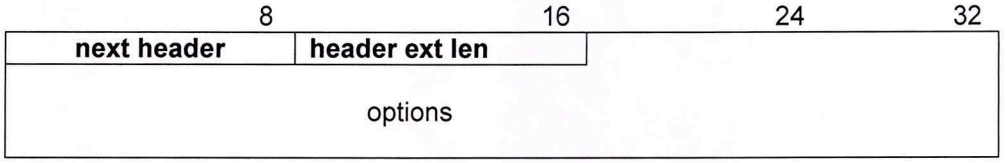
Además, esta opción no debe ser usada en un paquete que carga un encabezado fragmento (como si tuviera algún sentido el enviar un paquete muy grande –para eficiencia sólo se requiere que sea partido en varios pedazos – para la transmisión.



5.4.4. Encabezado Destination Options

El encabezado Destination Options carga información que debe ser examinada solo por el(os) nodo(s) destino(s) del paquete. La presencia del encabezado Destination Options es identificada por un valor de 60 en el campo Next Header del encabezado precedente. Este encabezado contiene 2 campos más opciones.

El campo encabezado Extension Length (Hdr Ext Len) tiene 8 bits de longitud, y mide la longitud del encabezado Destination Options en unidades de 8 octetos, sin contar los primeros 8 octetos.



El campo Options es variable en longitud, como el encabezado Destination Options, es un entero múltiple de 8 octetos de longitud. Solo 2 opciones son definidas en RFC 2460 – la opción Pad1, usada para insertar 1 octeto de relleno en el área Options de un encabezado, y PadN, usada para insertar 2 ó más octetos de relleno en el área Options de un encabezado.

5.4.5. Encabezado de Routing

El header de Routing lista uno o más nodos intermediarios que son "visitados" en la ruta desde la fuente hasta el destino. La presencia del encabezado Routing es identificada por un valor de 43 en el campo Next Header del encabezado precedente. Este encabezado contiene 4 campos, más data de tipo específico.

El campo Next Header tiene 8 bits de longitud, e identifica el encabezado que continúa inmediatamente al encabezado Routing. Este campo usa los mismos valores que el campo Protocol de IPv4.

- El campo Header Extension Length (Hdr Ext Len) tiene 8 bits de longitud, y mide la longitud del encabezado Routing en unidades de 8 octetos, sin contar los primeros 8 octetos.
- El campo Routing Type tiene 8 bits de longitud e identifica una variante particular del encabezado Routing. (RFC 2460 define una variante, Routing Type 0, que es descrita debajo.)
- El campo Segments Left tiene 8 bits de longitud, e indica el número de segmentos de ruta que quedan, o en otras palabras, el número de nodos intermedios explícitamente listados que todavía serán visitados antes de alcanzar el destino final.
- El campo Type-Specific es variable en longitud, con un formato definido por la variante particular Routing Type.
- RFC 2460 define una variante simple, el encabezado Routing Type 0, que contiene una lista ordenada de direcciones que serán visitadas durante la ruta del paquete. Para este encabezado, el campo Next Header es definido como arriba; sin embargo,

el campo Hdr Ext Len contiene un número igual a 2 veces el número de direcciones en el encabezado.

8	16	24	32
next header	**header ext len**	**routing type**	**segments left**
type-specific data			

Por ejemplo, si hubiese n direcciones en el encabezado, el campo Hdr Ext Len contendría el valor 2n. El campo Routing Type indicaría Type = 0. El campo Segments Left sería como arriba, y el campo Reserved sería configurado a cero para la transmisión e ignorado en la recepción. Una lista de direcciones de 128 bits, numerada de 1 a n, completaría el header Routing Type 0.

RFC 2460 da un ejemplo del uso del header Routing. En este ejemplo, note que los 3 nodos intermediarios (y cuatro segmentos) separan el nodo Fuente (S) del nodo Destino (D).

Para viajar del nodo Fuente al nodo Intermediario I (I1), el encabezado base de IPv6 usa Source Address (SA) = S, y Destination Address (DA) = I1. El encabezado Routing especifica un Hdr Ext Len (HEL) = 6, Segments Left = 3, y las direcciones de los 3 nodos restantes durante el camino: nodo Intermediario 2 (I2), nodo Intermediario 3 (I3) y nodo Destino (D).

Para viajar de I1 a I2, el algoritmo de ruteo intercambia la dirección Destino de IPv6 con la primera dirección en la lista de direcciones (I2). Note que Source Address (SA = S) será consistente para todos los segmentos.
Para viajar de I2 a I3, el algoritmo de ruteo intercambia la dirección Destino de IPv6 con la segunda dirección en la lista de direcciones (I3).

Para viajar de I3 al Destino final (D), el algoritmo de ruteo intercambia la dirección Destino de IPv6 con la tercera dirección en la lista de direcciones (D).

Note que el estado final de las direcciones de encabezado de IPv6 es ahora SA = S y DA = D, y el encabezado Routing lista los nodos intermediarios, I1, I2 e I3, en el orden en que fueron visitados.

5.4.6. Encabezado Fragment

El encabezado Fragment es usado por un origen IPv6 para transmitir paquetes que son más grandes de lo que cabrían en la unidad de transmisión máxima (MTU) del paquete a sus destinos. La presencia del encabezado Fragment es identificada por un valor de 44 en el campo Next Header en el encabezado precedente. Note que la fragmentación para IPv6 es sólo hecha en el nodo fuente, no en los routers intermediarios junto a la ruta de envío del paquete; este es un cambio de procedimiento desde IPv4.

El encabezado Fragment contiene 6 campos. El campo Next Header tiene 8 bits de largo e identifica el encabezado que continúa inmediatamente al header Fragment. Este campo tiene los mismos valores que el campo del Protocolo IPv4.

- El campo Reserved tiene 8 bits de largo, y está reservado para uso futuro.
- Este campo es inicializado en cero para la transmisión e ignorado en la recepción.
- El campo Fragment Offset es un entero sin signo de 13 bits que mide la compensación, en unidades de 8 octetos, de los datos que continúan este encabezado, relativo al comienzo de la parte fragmentable del paquete original.
- El campo reservado tiene 2 bits de largo, y está reservado para uso futuro.
- Este campo es inicializado en cero para la transmisión e ignorado en la recepción.

next header	**reserved**	**fragment offset**	**res**	M
identification				

La bandera M es de 1 bit de longitud y determina si más fragmentos vienen (M = 1) o si este es el último fragmento (M = 0).

El campo Identification es de 32 bits de largo y únicamente identifica el (los) paquete(s) fragmentado(s) durante el proceso de re-ensamblaje. Este campo es generado por el nodo fuente.

Un paquete requiriendo fragmentación es considerado que consiste de 2 partes: una parte no fragmentable y una parte fragmentable. La parte no fragmentable incluye el encabezado IPv6, más cualquier encabezado de extensión que debe ser procesado en ruta al destino. Este puede incluir un encabezado Hop-by-Hop y un encabezado Routing. La parte fragmentable es el balance del paquete, que puede incluir cualquier encabezado

de extensión que es procesado al final del nodo destino, los encabezado de capa más alta, y datos de aplicación.

La parte fragmentable del paquete original está dividida en fragmentos que son íntegros múltiplos de 8 octetos (excepto tal vez por el último fragmento, que puede no ser un íntegro múltiplo de 8 octetos). Cada paquete fragmentado consiste de 3 partes: la parte no fragmentable del paquete original, un encabezado Fragment y un fragmento de datos. La parte no fragmentable de cada fragmento contiene un campo Payload Length revisado (con la porción de IPv6) que hace juego con la longitud de este fragmento y un campo Next Header = 44 (indicando que un encabezado Fragment viene después).

Las longitudes de los fragmentos resultantes caben dentro del MTU de la ruta a los destinos de los paquetes. En el(los) nodo(s) destino(s), un proceso llamado reensamblaje es usado para reconstruir el paquete original de los paquetes fragmentados. El proceso de reensamblaje es también descrito en RFC 2460.

5.4.7. Encabezado de Autentificación

Asegurando las transmisiones de datos se ha convertido en un tema extremadamente importante para los manejadores de red. La comunidad de Internet ha direccionado estos temas en RFC 2401 "Security Architecture for the Internet Protocol". En el capítulo 7 se discutirá esta arquitectura en detalle.

Dos encabezado son discutidos en RFC 2401 que proveen los mecanismos de seguridad de IP. El encabezado Authentification es definido en RFC 2402.

Encapsulating Security Payload (ESP) es definido en RFC 2406. Estos dos mecanismos pueden ser usados separadamente, o conjuntamente, como las necesidades de seguridad lo dicten.

El encabezado Authentification provee integridad sin conexiones y autentificación de datos de origen para datagramas de IP, más protección original contra "replays". La presencia de este encabezado es identificada por un valor de 51 en el campo Next Header en el encabezado precedente. Este encabezado contiene 6 campos.

El campo Next Header tiene 8 bits de largo e identifica el encabezado que continúa inmediatamente al encabezado Authentification. Este campo usa los mismos valores que el campo del Protocolo IPv4.

El campo Payload Length tiene 8 bits de longitud y provee la longitud del encabezado Authentification en palabras de 32 bits, menos 2 (ejemplo: los primeros 8 octetos del encabezado Authentification no son contados).

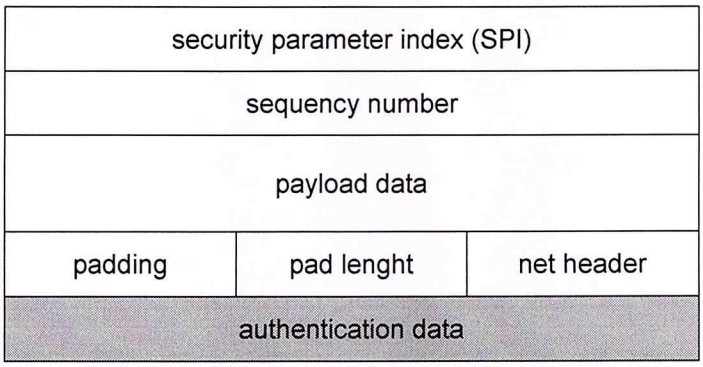
El valor mínimo es 1, que consiste en el valor de autentificación de 96 bits (3 palabras de 32 bits), menos el valor 2 (3 – 2 = 1). Este mínimo es sólo usado en el caso de un algoritmo de autentificación "nulo", empleado para procesos de depuración.

Los campos reservados tienen 16 bits de longitud y es reservado para uso futuro. Este campo es inicializado en cero para la transmisión. Está incluido en el cálculo Authentification Data, pero sino es ignorado en la recepción.

El campo Security Parameters Index (SPI) es un valor arbitrario de 32 bits que identifica la asociación de seguridad (SA) para este datagrama, relativo a la dirección contenida en el encabezado de IP al que este encabezado de seguridad es asociado, y relativo al protocolo de seguridad empleado. La asociación de seguridad, como se define en RFC 2401, es una conexión simple y lógica que es creada para propósitos de seguridad. Todo tráfico que atraviesa SA tiene el mismo proceso de seguridad. SA puede comprimir muchos parámetros, incluyendo el algoritmo Authentification, claves del algoritmo de autentificación y otros. Según RFC 2402, el valor de SPI = 0 puede ser usado para propósitos locales, de implementación específicas. Otros valores, en el rango de 1 – 255, son reservados para uso futuro por la Internet Assigned Numbers Authority (IANA).

El campo Sequence Number contiene un número de 32 bits que aumenta "monotónicamente". Tanto el contador del que envía como el contador del que recibe son inicializados en cero cuando una asociación de seguridad es establecida.

Authentification Data es un campo de longitud variable que contiene el Valor de Chequeo de Integridad - Integrity Check Value (ICV). Este campo debe ser un múltiplo integral de 32 bits de longitud.



5.4.8. Encabezado Encapsulating Security Payload

El encabezado propuesto Encapsulating Security Payload (ESP) está designado para proveer confidencialidad, autentificación de datos de origen, integridad sin conexión, un servicio anti-"replay", y confidencialidad de flujo limitado de tráfico. El(los) servicio(s) proveído(s) depende de la asociación de seguridad y su implementación. La presencia del encabezado ESP es identificada por un valor de 50 en el campo Next Header del encabezado precedente. Este encabezado contiene 7 campos, algunos obligatorios, otros opcionales dependiendo de la asociación de seguridad.

El campo Security Parameters Index (SPI) es un valor arbitrario de 32 bits que identifica la asociación de seguridad para este datagrama, relativo a la dirección IP destino contenido en el encabezado IP con el que este encabezado de seguridad es asociado, y relativo al protocolo de seguridad empleado. El campo SPI es obligatorio.

El campo Sequence Number contiene un número de 32 bits que "monotónicamente" aumenta. El contador del que envía y el contador del que recibe son inicializados en cero cuando una asociación de seguridad es establecida. El campo Sequence Number es obligatorio.
El campo Payload Data es de longitud variable que contiene datos descritos por el campo Next Header. El campo Payload Data es obligatorio.

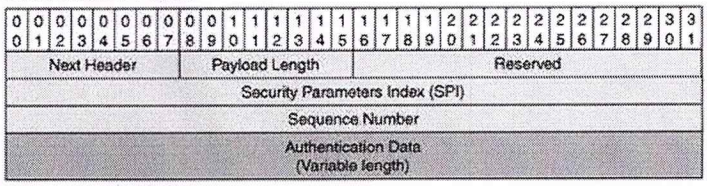
El campo Padding puede opcionalmente contener 0 – 255 octetos de información de relleno, como requerido por la implementación de seguridad. El campo Pad Length indica el número de octetos de relleno (0 – 255) que son inmediatamente precedidos.

El campo Padding es obligatorio. El campo Next Header tiene 8 bits de largo e identifica el encabezado que inmediatamente continúa al encabezado ESP.

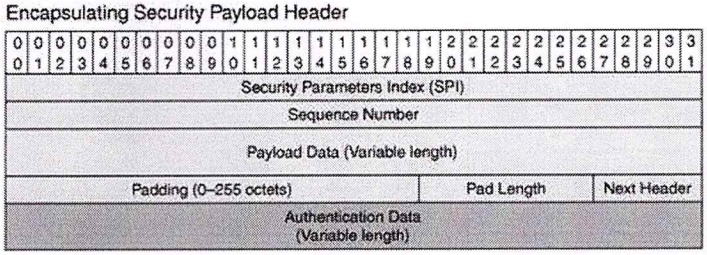
Este campo tiene los mismos valores que el campo del protocolo de IPv4. El campo Next Header es obligatorio.

Authentification Data es un campo de longitud variable que contiene un Valor de Chequeo de Integridad - Integrity Check Value (ICV). La longitud de este campo depende de la función de autentificación que es seleccionada. El campo Authentification Data es opcional, y es incluido sólo si esa asociación de seguridad ha seleccionado servicio de autentificación.

Authentication Header



Encapsulating Security Payload Header



5.4.9. Encabezado No Next

El valor de 59 en el campo Next Header de un paquete de IPv6 o cualquiera de los encabezados de extensión indica que nada continúa a ese encabezado. Por esto, éste se llama "No Next".

6. ARQUITECTURA DE DIRECCIONAMIENTO (RFC2373)

Sin interrogantes, el desarrollo más dramático proveído por IPv6 es el aumento del tamaño en el campo de direcciones – de 32 a 128 bits por dirección.

Mientras el campo de 32 bits de IPv4 produce 4,294,967,296 direcciones distintas, el campo de 128 bits de IPv6 tiene considerablemente más:
340,282,366,920,938,463,374,607,431,768,211,456 en total.

Ha sido estimado que esto iguala a 32 direcciones por pulgada cuadrada de tierra seca en la superficie de la Tierra. Pero antes de ingresar en esta estructura de direccionamiento y todos sus rigores, considérese brevemente los formatos de direccionamiento de IPv4 para comparación.

6.1. Modelos de Direccionamiento. (RFC2373)

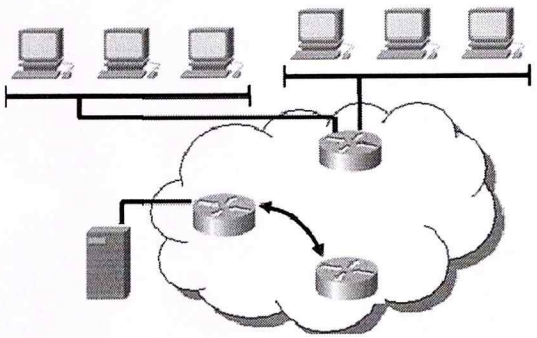
Cualquier tipo de dirección se asigna a interfaces, no nodos. Es algo importante de recordar. Todas las interfaces han de tener, por los menos, una dirección de enlace local (Link-Local) de tipo unicast.

Un mismo interfaz puede tener asignadas múltiples direcciones de cualquier tipo (unicast, anycast, multicast) o ámbito (scope). Direcciones unicast con ámbito mayor que el de enlace no son necesarias para interfaces que no son usados como origen y destino de paquetes IPv6 hacia o desde no vecinos. Esto significa que para la comunicación dentro de una LAN no hace falta direcciones IPv6 globales, suficiente con direcciones de ámbito local. De hecho, es lo aconsejable para enlaces punto a punto.

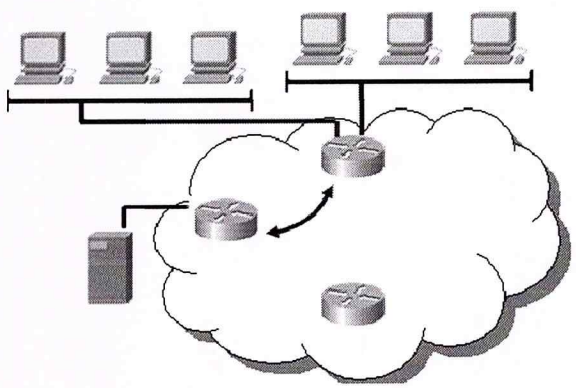
Respecto a los prefijos de subred, IPv6 sigue el mismo modelo que IPv4, es decir, un prefijo se asocia a un enlace, pudiendo haber varios prefijos en un mismo enlace.

La estructura de dirección IPv6 encuentra sus raíces en la estructura CIDR, que incluye un prefijo de dirección, un ID de Site y un ID de Host. Para IPv6, sin embargo, habrá múltiples prefijos de direcciones, y cada uno de ellos puede tener múltiples estructuras similares a ID de Site y ID de Host. Como una base, el documento de arquitectura de direccionamiento de IPv6, define 3 tipos diferentes de direcciones IPv6:

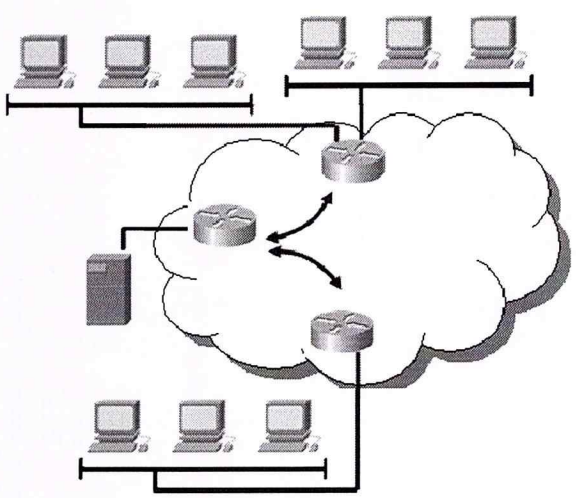
- **Unicast:** Un identificador para una interfase simple. Un paquete enviado a una dirección unicast es entregado a la interfase identificada por esa dirección.



- **Anycast:** Un identificador para un conjunto de interfases (típicamente perteneciente a nodos diferentes). Un paquete enviado a una dirección anycast es entregado por una de las interfases identificadas por esta dirección (la más cercana, según la medida de distancia del protocolo de ruteo).



- **Multicast:** Un identificador para un conjunto de interfases (típicamente perteneciendo a nodos diferentes). Un paquete enviado a una dirección multicast es entregado a todas las interfases identificadas por esta dirección.



Note que el término difusión (broadcast) no aparece, porque la función de difusión es reemplazada por la definición de multicast. También note que las direcciones de IPv6 de todo tipo son asignadas a interfases, no nodos; un nodo (como un router) puede tener múltiples interfases, y así múltiples direcciones unicast. Además, una interfase simple puede estar asignada a múltiples direcciones. Mas adelante se vera a profundidad los modos de direccionamiento

6.2. Ambitos.

Se acaba de mencionar en la sección anterior el 'ámbito' de una dirección sin saber todavía lo que era. El protocolo IPv6 añade soporte para direcciones de distintos ámbitos, lo que quiere decir que habrá direcciones globales y no globales. Si bien con IPv4 emplea direccionamiento no global con la ayuda de prefijos de red privados, con IPv6 esta noción forma parte de la propia arquitectura de direccionamiento.

Cada dirección IPv6 tiene un ámbito, que es un área dentro de la cual esta puede ser utilizada como identificador única de uno o varias interfaces. El ámbito de cada dirección forma parte de la misma dirección, con lo que va a poder diferenciarlos a simple vista.
Para las direcciones unicast se distinguen tres ámbitos:

- De enlace local (link-local), para identificar interfaces en un mismo enlace. Empiezan todas por fe80:.
- De sitio local (site-local), para identificar interfaces en un mismo 'sitio'. La definición de 'sitio' es un tanto genérica, pero en principio un 'sitio' es el área topológica de red perteneciente a un edificio o un campus, perteneciente a una misma organización. Empiezan por fec0:.
- Global, para identificar interfaces en toda Internet. Éstas comienzan por 2001: o 3ffe:.
- En lo que a ámbito se refiere, las direcciones anycast siguen la misma norma que las unicast.

Sin embargo, para las direcciones multicast se tiene catorce posibles ámbitos, que identifican desde una interfaz local a una dirección global. Nodos de un mismo ámbito y visibles entre sí definen una zona. No se permite que un router rutee tráfico entre diferentes zonas (perderían todo el sentido los ámbitos).

Una de las grandes ventajas de los ámbitos es que permitiría la renumeración de prefijos sin mucha dificultad, ya que las direcciones de ámbito no global se mantendrían. Se tiene que esperar que se produzca alguna renumeración de prefijos globales, ya que según crezca una organización su prefijo se puede quedar pequeño y necesitar más espacio de direcciones. Y como hemos dicho antes, se trataría siempre que sea posible de mantener las tablas de routing al mínimo. Lo que sólo se consigue dando un prefijo nuevo mayor e invalidando el anterior, porque lo que seguramente sucedería sería que las redes contiguas ya estén asignadas.

6.3. Nomenclatura de las Direcciones.

Hay tres formas comunes de representar direcciones IPv6 en texto:

- x:x:x:x:x:x:x:x, donde cada x es el valor en hexadecimal de cada grupo de 16 bits de la dirección.
- x:x::x, en el caso de que haya grupos contiguos de 16 bits todos cero. Es una abreviatura que serviría para hacer más "cómodo" el uso de algunas direcciones.
- x:x:x:x:x:x:d.d.d.d, donde las x son los seis grupos de 16 bits en hexadecimal de mayor peso de la dirección y las d son los valores decimales de los cuatro grupos de 8 bis de menor peso de la dirección. Esta forma es a veces más conveniente a la hora de manejar entornos mixtos IPv6 e IPv4. Por ejemplo:
  0:0:0:0:0:FFFF:129.144.52.38 y en su forma abreviada **::FFFF:129.144.52.38**

representación Normal	representación abreviada	tipo
1080:0:0:0:8:800:200C:417ª	1080::8:800:200C:417A	unicast
FF01:0:0:0:0:0:0:101	FF01::101	multicast
0:0:0:0:0:0:0:1	::1	Loopback
0:0:0:0:0:0:0:0	::	no especificada

Tabla Nomenclatura de direcciones IPv6

6.4. Nomenclatura de los Prefijos.

La representación de los prefijos de direcciones con IPv6 es similar a la CIDR con IPv4, esto es: dirección-IPv6/tamaño-prefijo.

Donde dirección-IPv6 es alguna de las notaciones vistas en la sección anterior y tamaño-prefijo es un valor decimal que especifica cuantos bits de la dirección corresponden al prefijo. Por ejemplo, el prefijo de la UJI en hexadecimal es **3FFE33300002**, que son 48 bits, se lo puede escribir como:

3FFE:3330:0002:0000:0000:0000:0000:0000/48

3FFE:3330:2:0:0:0:0:0/48

3FFE:3330:2::/48

Si se quiere escribir la dirección y el prefijo, no hace falta escribir los dos de forma explícita. Por ejemplo, una dirección IPv6 de la misma UJI con su prefijo asociado quedará **3FFE:3330:2:1:250:BAFF:FE7A:E67E/48**

6.5. Representación de Direcciones.

Las direcciones IPv4 son típicamente representadas en notación con punto decimal. Así, una dirección de 32 bits es dividida en 4 direcciones de 8 bits, y cada sección es representada por un número decimal entre 0 y 255: 128.138.213.13.

Como las direcciones IPv6 son de 128 bits de longitud, un método diferente de representación es requerido. Como se especificó en RFC 2373, la representación preferida es: x:x:x:x:x:x:x:x donde x representa 16 bits, y cada una de esas secciones de 16 bits es definida en hexadecimal.

La representación de las direcciones IPv6 sigue el siguiente esquema:

a) x:x:x:x:x:x:x:x, donde "x" es un valor hexadecimal de 16 bits, de la porción correspondiente a la dirección IPv6. No es preciso escribir los ceros a la izquierda de cada campo.

Ejemplos:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

1080:0:0:0:8:800:200C:417A

b) Dado que, por el direccionamiento que se ha definido, podrán existir largas cadenas de bits "cero", se permite la escritura de su abreviación, mediante el uso de "::", que representa múltiples grupos consecutivos de 16 bits "cero". Este símbolo sólo puede aparecer una vez en la dirección IPv6.

Ejemplos: Las direcciones:
- 1080:0:0:0:8:800:200C:417A (una dirección unicast)
- FF01:0:0:0:0:0:0:101 (una dirección multicast)
- 0:0:0:0:0:0:0:1 (la dirección loopback)
- 0:0:0:0:0:0:0:0 (una dirección no especificada)

Pueden representarse como:
- 1080::8:800:200C:417A (una dirección unicast)
- FF01::101 (una dirección multicast)
- ::1 (la dirección loopback)
- :: (una dirección no especificada)

c) Una forma alternativa y muy conveniente, cuando nos hallemos en un entorno mixto IPv4 e IPv6, es x:x:x:x:x:x:d:d:d:d, donde "x" representa valores hexadecimales de 16 bits (6 porciones de mayor peso), y "d" representa valores decimales de las 4 porciones de 8 bits de menor peso (representación estándar IPv4).

Ejemplos:	Pueden representarse como:
0:0:0:0:0:0:13.1.68.3	::13.1.68.3
0:0:0:0:0:FFFF:129.144.52.38	::FFFF:129.144.52.38

La representación de los prefijos IPv6 se realiza del siguiente modo: **dirección-IPv6/longitud-del-prefijo** donde:

- dirección-IPv6 = una dirección IPv6 en cualquiera de las notaciones válidas
- longitud-del-prefijo = valor decimal indicando cuantos bits contiguos de la parte izquierda de la dirección componen el prefijo

Por ejemplo, las representaciones válidas del prefijo de 60 bits 12AB00000000CD3, son:

12AB:0000:0000:CD30:0000:0000:0000:0000/60
12AB::CD30:0:0:0:0/60
12AB:0:0:CD30::/60

Por tanto, para escribir una dirección completa, indicando la subred, podrías hacerlo como: 12AB:0:0:CD30:123:4567:89AB:CDEF/60

Por ejemplo: una dirección IPv6 podría ser de la forma: FEDC:BA98:7654:3210:FEDC:BA98:7654:3210.

Nótese que cada una de las secciones de 16 bits es separada por ":", y que cada 4 números hexadecimales son usados para representar cada sección de 16 bits. Si alguna sección contiene ceros al principio, esos ceros no son requeridos. Por ejemplo: 1080:0000:0000:0000:0008:0800:200C:417A puede ser simplificada a: 1080:0:0:0:8:800:200C:417A.

Si largas cadenas de ceros aparecen en una dirección, "::" Puede ser usado para indicar múltiples grupos de 16 bits de ceros, que más luego simplifican la dirección de arriba a: 1080::8:800:200C:417A.
El uso de "::" es restringido a aparecer solo una vez en una dirección, aunque puede ser usado para comprimir o los ceros del principio o los subsiguientes en una dirección. Por ejemplo, una dirección 'loopback' de: 0:0:0:0:0:0:0:1 podría ser simplificada a: ::1.

Cuando las direcciones IPv6 son expresadas en texto, es común delinearlas como dirección y longitud de prefijo: IPv6-address/prefix-length donde la dirección IPv6 es expresada en una de las notaciones listadas anteriormente, y la longitud de prefijo es un valor decimal que especifica el número de los bits más a la izquierda de la dirección comprimida en el prefijo. Por ejemplo:
12AB:0000:0000:CD30:0000:0000:0000:0000/60 indica que el prefijo de 60 bits (en hexadecimal) es: 12AB00000000CD3.

6.6. Arquitectura.

Las direcciones IPv6 de 128 bits pueden ser divididas en un número de subcampos para proveer máxima flexibilidad para tanto las representaciones actuales como las futuras. Los bits líderes, llamados el Prefijo de Formato (Format Prefix), definen el tipo específico de dirección IPv6. RFC 2373 define un número de esos prefijos.

Note que el espacio de dirección ha sido asignado por NSAP, IPX, unicast global, multicast y otros tipos de direcciones. Al tiempo de este escrito, 15% del espacio de dirección ha sido asignado y el 85% restante ha sido reservado para uso futuro. [49]

Una dirección multicast comienza con el valor binario 11111111; cualquier otro prefijo identifica una dirección unicast. Las direcciones anycast son parte de la asignación de las direcciones unicast y no se les da un identificador único.

Note que RFC 2373 define 2 apremios adicionales referentes a la arquitectura de direccionamiento de IPv6. Primero, los tipos especiales de direcciones especiales son asignados fuera del prefijo de formato 0000 0000.

Estas son las direcciones No Especificadas, Loopback y de Compatibilidad que contienen direcciones IPv4 encajado. Segundo, algunas direcciones IPv6 contienen identificadores encajado en la interfaz. Los formatos de prefijo 001 hasta 111, esperan por direcciones multicast (prefijo de formato 1111 1111) requieren todos tener identificadores de interfaz de 64 bits especificados en el formato IEEE EUI-64.

IPv6 soporta direcciones cuatro veces más grandes que las utilizadas por IPv4 (128 bits contra 32 bits de IPv4). Esto proporciona un espacio de direccionamiento 296 veces el

[49] IETF http://www.ietf.org

mayor que el que brinda IPv4. Si bien el espacio de direcciones es extremadamente grande, la asignación y el routing de las mismas requieren la utilización de esquemas jerárquicos que reducen la eficiencia del espacio de direccionamiento utilizado. Así y todo, se estima que en el peor de los casos, las direcciones de 128 bits de IPv6 pueden acomodar 1018 host; esto es mas de 1500 direcciones por metro cuadrado de la superficie de la tierra.

El tipo específico de una dirección IPv6 queda determinado por los primeros bits. La asignación actual de los prefijos se muestra en la siguiente tabla.

Asignación	Prefijo (binario)	Fracción del espacio de direcciones
Reservado	00000000	1/256
No asignado	00000001	1/256
Reservado para asignación NSAP	0000001	1/128
Reservado para asignación IPX	0000010	1/128
No asignado	0000011	1/128
No asignado	00000	1/32
No asignado	00001	1/16
No asignado	001	1/8
Dirección unicast basada en proveedor	010	1/8
No asignado	011	1/8
Reservado para direcciones unicast basadas en regiones geográficas	100	1/8
No asignado	101	1/8
No asignado	110	1/8
No asignado	1110	1/16
No asignado	11110	1/32
No asignado	111110	1/64
No asignado	1111110	1/128
No asignado	111111100	1/512
Direcciones para el uso del enlace local	1111111010	1/1024
Direcciones para el uso del sitio local	1111111011	1/1024
Direcciones multicast	11111111	1/256

6.6.1. Direcciones Unicast.

Existen varios tipos de direcciones unicast en IPv6, como las globales agregables, las Site-Local, las Link-Local, las IPX jerárquicas, la NSAP, y las compatibles IPv4. Más tipos de direcciones pueden ser definidos en el futuro.

Dependiendo de la actividad/función que realice cada nodo, éste puede tener más o menos conocimiento de la estructura del paquete IPv6. Por ejemplo, un nodo puede considerar una dirección IPv6 unicast como un "todo" siendo inconsciente incluso de los prefijos; algo más complejo entendería de prefijos y, yendo un poco más lejos, podría entender la jerarquía dentro del prefijo y lo que ello implica.

Un número de formas para direcciones unicast ha sido definido para IPv6, algunas con estructuras más complejas que proveen asignaciones de dirección jerárquica. La forma más simple es una dirección unicast sin estructura interna, en otras palabras, sin jerarquía de dirección definida.

La próxima posibilidad sería especificar un prefijo de subred (Subnet Prefix) dentro de la dirección de 128 bits, así dividir la dirección en un prefijo de subred (con n bits) y un id de interfase (128 – n bits).

Algunas direcciones especiales son también definidas en RFC 2373.
La dirección 0:0:0:0:0:0:0:0 (también representada 0::0, o simplemente ::) es definida como la dirección no especificada, que indica la ausencia de una dirección. Esta dirección podría ser usada en el inicio cuando un nodo todavía no tiene una dirección asignada. La dirección no especificada puede nunca ser asignada a cualquier nodo.

La dirección 0:0:0:0:0:0:0:1 (también representada 0::1, o simplemente ::1) es definida como la dirección loopback. Esta dirección es usada por un nodo para enviar un paquete a sí mismo.

- La **dirección loopback** puede nunca ser usada a cualquier interfaz. Un paquete IPv6 con una dirección destino de la dirección loopback nunca debe ser enviado fuera de un nodo simple, y nunca debe ser reenviado por un router IPv6.
- Las direcciones unicast son direcciones bien conocidas. Un paquete que se envía a una dirección unicast deberán llegar a la interfaz identificada por dicha dirección.
- Las **direcciones anycast** son sintácticamente indistinguibles de las direcciones unicast pero sirven para identificar a un conjunto de interfaces. Un paquete destinado a una dirección anycast llega a la interfaz "más cercana" (en términos de métrica de "routers"). Las direcciones anycast sólo se pueden utilizar en "routers".

- Las **direcciones multicast** identifican un grupo de interfaces. Un paquete destinado a una dirección multicast llega a todos las interfaces que se encuentran agrupados bajo dicha dirección.

Nota: Las direcciones IPv4 de tipo broadcast (normalmente xxx.xxx.xxx.255) se expresan en IPv6 mediante direcciones multicast.

Tabla. Direcciones IPv6 reservadas

IPv6 address	Prefix length (bits)	descripción	notas
::	128	sin especificar	como 0.0.0.0 en Pv4
::1	128	dirección de bucle local (loopback)	como las 127.0.0.1 en IPv4
::00:xx:xx:xx:xx	96	direcciones IPv6 compatibles con IPv4	Los 32 bits más bajos contienen una dirección IPv4. También se denominan direcciones "empotradas."
::ff:xx:xx:xx:xx	96	direcciones IPv6 mapeadas a IPv4	Los 32 bits más bajos contienen una dirección IPv4. Se usan para representar direcciones IPv4 mediante direcciones IPv6.
fe80:: - feb::	10	direcciones link-local	equivalentes a la dirección de loopback de IPv4
fec0:: - fef::	10	direcciones site-local	Equivalentes al direccionamiento privado de IPv4
ff::	8	multicast	
001 (base 2)	3	direcciones unicast globales	Todas las direcciones IPv6 globales se asignan a partir de este espacio. Los primeros tres bits siempre son "001".

6.6.1.1. Direcciones de Compatibilidad

Dos direcciones de transición han sido definidas para las redes de transición IPv4/IPv6.

La primera dirección es llamada una dirección IPv4 compatible con IPv6.

- Es usada cuando 2 dispositivos IPv6 (como hosts o routers) necesitan comunicarse vía una infraestructura de ruteo IPv4. Los dispositivos en la punta de IPv4 usaría n esta dirección unicast especial, que carga una dirección IPv4 en el orden bajo de 32 bits. Este proceso es llamado túneles automático. Note que el prefijo es 96 bits de ceros.

- El segundo tipo de dirección de transición es llamado IPv4 tras la dirección IPv6. Esta dirección es usada por los nodos de solo IPv4 que no soportan IPv6.

Por ejemplo, un host IPv6 usaría IPv4 a través de la dirección IPv6 para comunicarse con otro host que solo soporte IPv4. Note que el prefijo es 80 bits e ceros seguido de 16 bits de unos.

6.6.1.2. Direcciones que Soportan la Arquitectura OSI

Muchas redes incorporan elementos derivados de los protocolos OSI (Open Systems Interconnection) en sus arquitecturas de direccionamiento y ruteo. Un ejemplo OSI es el Protocolo de Redes sin Conexión, ISO 8473, y su esquema de direccionamiento, que usa direcciones NSAP (Network Service Access Point).

Otros ejemplos son los protocolos de ruteo OSI, End System to Intermediate System (ES-IS), definidos en ISO 9542, o el Intermediate System to Intermediate System (IS-IS), definido en ISO 10589. Desde que las direcciones NSAP (llamadas NSAPAs) son típicamente de 20 octetos de longitud, los mecanismos deben ser proveídos para adaptar este formato al de la estructura de direcciones IPv6 de 16 bits. Las direcciones que soportan NSAPAs tienen un prefijo de formato de 7 bits de 0000001.

RFC 1888 define 4 mecanismos para soportar el direccionamiento OSI NSAP en una red IPv6:

- NSAPA restringido mapeando en direcciones IPv6 de 16 octetos.
- NSAPA truncado para ruteo, NSAPA completo en la opción IPv6
- Dirección IPv6 normal, NSAPA completo en la opción IPv6
- Direcciones IPv6 cargadas como direcciones OSI

Cuando las NSAPAs son mapeadas en direcciones IPv6 de 16 octetos, un bit cero continúa el prefijo de formato 0000001, rendimiento de un primer octeto de 00000010. Los campos subsecuentes incluyen un código del formato de la autoridad (AFcode), cuál codifica el identificador de la autoridad y del formato (AFI), un indicador inicial del dominio (IDI), un prefijo, un área, y un End System ID.

Una NSAPA truncada utilizada como una dirección IPv6 toma los octetos de orden alto de la dirección NSAP, que incluye la información de ruta que consiste de Routing Domain y

los identificadores de Área, y entonces trunca otros campos NSAP que no son requeridos.

Una tercera alternativa es cargar NSAPAs completas como una opción dentro del encabezado Destination Options. Note que Option Type = 195 (decimal) y que las NSAPAs completas (20 octetos) son entonces incluidas en el encabezado Destination Option.

La alternativa final permite a una dirección IPv6 ser fijada dentro de una dirección NSAP de 20 octetos. El primer octeto es un Authority and Format Indicator, y los dos octetos próximos son conocidos como Internet Code Point (ICP). Tomados juntos, estos 3 octetos comprenden el Initial Domain Part (IDP) de la NSAPA. Los próximos 16 octetos contienen la dirección IPv6; el octeto final, llamado un selector, está configurado en cero.

Detalles concernientes a la implementación de las direcciones NSAP son también proveídos en RFC 1888.

6.6.1.3. Direcciones IPX

Las direcciones IPX (Internetwork Packet Exchange) deberían ser mapeados en direcciones IPv6 con un formato que comienza con el formato de prefijo de 7 bits 0000010. El balance de esta dirección todavía está bajo estudio.

6.6.1.4. Direcciones Unicast Globales Agregables

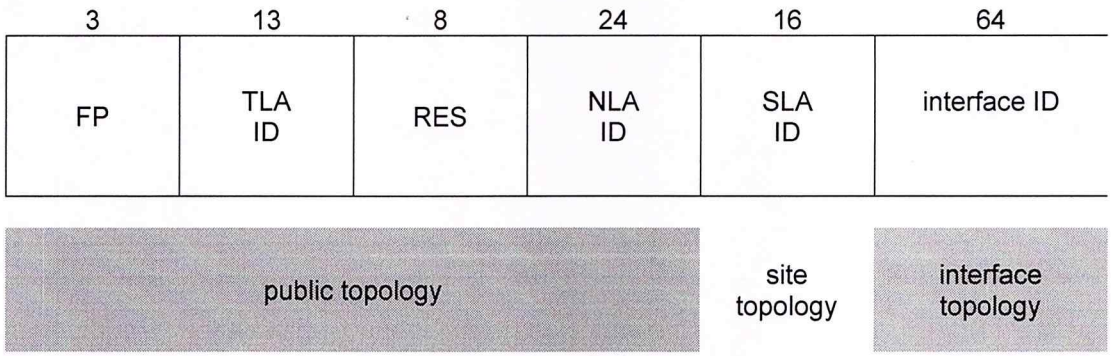
Muchas redes de comunicaciones, como la red de teléfonos global, son basadas en un esquema de direccionamiento jerárquico. Una jerarquía facilita un escalamiento y ruta más fáciles.

Para IPv6, la jerarquía para las direcciones agregables es organizada en 3 niveles: una topología pública, una topología de site y un identificador de interfase, como se documenta en RFC 2374. La topología pública es la colección de proveedores e intercambios que provee el servicio de tránsito del Internet público. La topología de site es local a un site u organización específica, pero no provee servicio de tránsito público a nodos fuera de su site. Los identificadores de interfase proveen identificación única para interfases en un link específico (Como una nota histórica, el formato de la Dirección Agregable Unicast Globales reemplazó el previamente definido formato Dirección Unicast

Basado en el Proveedor, que fue definido en RFC 2073. El formato Agregable mejora el formato Basado en el Proveedor en un número de formas. RFC 2073 es ahora considerado como 'histórico'.)

Así, una arquitectura basada en adición incluiría los proveedores intercontinentales, los intercambios y suscriptores. Los intercambios asignarán direcciones IPv6. En algunos casos, los suscriptores se conectarían directamente a un intercambio. Esto proveería acceso a múltiples proveedores intercontinentales y permitirán un cambio de proveedores ser hecho sin tener que reenumerar su organización.

La dirección agregable unicast global comienza con un formato de prefijo de 001 e incluye otros 4 campos que especifican varios niveles de jerarquía. El identificador de Agregación de Alto Nivel (TLA – Top-Level Aggregation Identifier) es un campo de 13 bits. Así, 8,192 (213) TLAs pueden ser asignados por cada valor de formato de prefijo definido. Una propuesta para la asignación de TLAs está documentada en RFC 2450.



FP format prefix (001)
TLA top–level aggregation identifier
RES reserved
NLA next level aggregation identifier
SLA site level aggregation identifier

aggregatable global unicast address

El campo Reserved, que tiene 8 bits de longitud, está proveído para permitir la expansión más amplia de campos TLA o NLA como la experiencia adicional con IPv6 es cumplida.

Cada organización a la que un TLA es asignado es proveída con 24 bits de espacio de dirección Next-Level Aggregation Identifier (NLA ID). El espacio NLA ID es entonces

usado por las organizaciones para crear una jerarquía de direccionamiento y para identificar sites. El uso de NLA está también propuesto en RFC 2450.

El espacio de 24 bits NLA ID puede ser asignado en varios niveles de sites. La organización responsable de TLA define el diseño de bit del espacio NLA. El diseño de bit del siguiente nivel NLA es la responsable del nivel previo NLA ID (como NLA1), NLA ID constituye la Topología Pública (64 bits total).

El identificador de Agregación del Nivel de Site (SLA ID – Site-Level Aggregation Identifier) es un campo de 16 bits que permite a organizaciones individuales crear una jerarquía de direccionamiento local. El campo SLA ID puede soportar 65,535 (216) subredes individuales. Jerarquías múltiples de subredes pueden ser también definidas.

El último campo es el identificador de Interfase (Interface Identifier), que identifica las interfases en un link. Cada ID de Interfase tiene 64 bits de longitud y es estructurado de acuerdo al formato IEEE EUI-64, que será discutido en una sección siguiente.

6.6.1.5. Identificadores de Interfaz

Los identificadores de interfaz en las direcciones unicast IPv6 se utilizan para identificar interfaces en un determinado enlace (una LAN, por ejemplo). Es necesario que sean únicos en el enlace, porque se deja de identificar interfaces al nivel de enlace ya no hay nada más que hacer. Pero esto último no significa que puedan seguir siendo únicos en un ámbito mayor que el de enlace.

Por norma general, los identificadores se obtendrán a partir de las direcciones de la capa de enlace.

Unos cuantos tipos de prefijos requieren identificadores de interfaz de 64 bits y, además, estar construidos en formato IEEE EUI-64. Estos identificadores pueden ser globales en el caso de que un token global esté disponible, como los 48 bits del MAC, o locales en caso de que no lo esté, como un enlace por puerto paralelo o los extremos de un túnel.

Se requiere que el bit 'u' sea invertido en caso de que el identificador se haya construido a partir del formato EUI-64. Este bit, según la terminología IEEE es el que indica la localidad o universalidad del identificador. Esto, que en un principio no tiene mucho

sentido, va a servir para que aquellas interfaces donde no es posible obtener un token global tengan una forma más sencilla. Por ejemplo, un extremo de un túnel, su identificador debería ser 0200:0:0:1 en vez de ::1 si este cambio no nos arreglase un poco la vida.

6.6.1.6. Direcciones IPv6 con Direcciones IPv4

Dentro de los mecanismos previstos de transición de IPv4 a IPv6, existe una técnica que permite a los hosts y routers entunelar dinámicamente paquetes IPv6 sobre la infraestructura IPv4 existente. Los nodos que vayan a utilizar esta técnica recibirán una dirección IPv4. A este tipo de direcciones se les llama direcciones IPv6 compatibles con IPv4.

También existen otro tipo de dirección IPv6 que contiene a una IPv4 y se utilizará para representar aquellos nodos que sólo disponen de pila IPv4 y se utilizará para representar aquellos nodos que sólo disponen de pila IPv4. En este caso los 32 bits más bajos serán iguales que en el caso anterior (la dirección IPv4), pero los 16 bits siguientes por delante serán todos 1. Este tipo de direcciones recibe el nombre de direcciones IPv6 mapeadas IPv4.

6.6.2. Direcciones de Prueba

Una asignación especial ha sido propuesta para el propósito de probar software IPv6 y es descrita en RFC 2471. (Esta asignación de direcciones de prueba tiene como intención reemplazar la asignación de prueba anterior definida en RFC 1897.) Estas direcciones son solo para ser usadas para prueba de IPv6 y no son ruteables en el internet. El formato de las direcciones de prueba está basado en la Dirección Unicast Global Agregable, con sus varios campos asignados como sigue:

- FP: 001 (Asignado a la Dirección Unicast Global Agregable).
- TLA ID: 1FFE H (Asignado para prueba 6bone).
- NLA ID: Asignado por el administrador TLA.
- SLA ID: Asignado por la organización individual.
- Interface ID: Un identificador de interfase para ese link (Ethernet, token ring, etc.)

Nótese que el formato de las Direcciones de Prueba no contiene el campo Reserved, que estaba incluido entre los campos TLA y SLA en la Dirección Unicast Global Agregable

para permitir futura expansión de cualquier espacio de dirección. El formato de las Direcciones de Prueba define una función específica de direccionamiento, y sus desarrolladores eligieron asignar los bits de Reserved a NLA ID, haciendo que el campo NLA tuviera 32 bits de longitud.

6.6.3. Direcciones de uso local

Dos direcciones están definidas para uso local solamente. La dirección Linklocal es usada por un link simple y su intención es la configuración de auto dirección, descubrimiento de vecino (Neighbor Discovery), o cuando no hay routers presentes. La dirección Link-local comienza con el Formato de Prefijo 111111101 e incluye un campo Inteface ID de 64 bits. Los routers nunca reenvían paquetes con la dirección destino o fuente Link -local hacia otros links.

La dirección Site-local es usada por las organizaciones que todavía no se han conectado al Internet. En vez de fabricar una dirección IPv6, ellos pueden usar la dirección Site-local. Los routers nunca reenvían paquetes con las direcciones fuente Site-local fuera de ese site. Esta dirección comienza con el Formato de Prefijo 1111111011 e incluye tanto un campo Subnet ID de 16 bits como un campo Interface ID de 64 bits.

6.6.4. Direcciones Anycast

Una dirección anycast es una que es asignada a múltiples interfases, típicamente en nodos diferentes. Un paquete con una dirección destino anycast es ruteado a la interfase más cercano teniendo esta dirección, como se midió en la definición de distancia del protocolo de ruteo. El concepto de hacer anycast dentro de trabajos de Internet basado en ip fue propuesto por primera vez en RFC 1546.

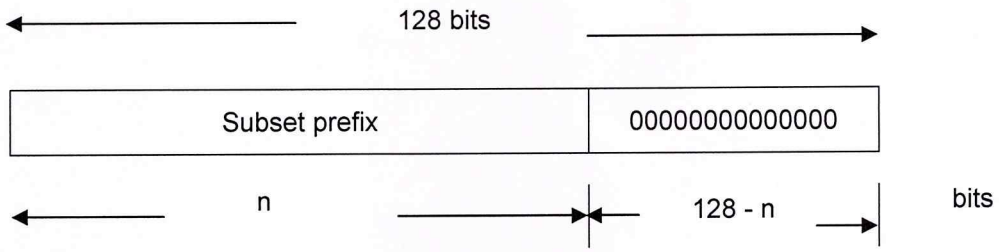
RFC 2373 nota varios usos posibles para la dirección anycast :

1- Identificar un set de routers pertenecientes a un ISP
2- Identificar el set de routers pegado (attached) a una subred particular
3- Identificar el set de routers que proveen entrada a un dominio de ruteo particular.

Dos restricciones son puestas en las direcciones anycast. Primero, ellas no deben ser usadas como direcciones fuente para un paquete IPv6. Segundo, una dirección anycast puede solo ser asignada a routers, no a hosts.

Una dirección anycast es predefinida y requerida: la dirección anycast Subnet-Router. Esta dirección comienza con un prefijo de subred de longitud variable y concluye con ceros para rellenar. Todos los routers en esa subred deben soportar esta dirección anycast. Su intención es ser usada en aplicaciones donde un nodo necesita comunicarse con un miembro de un grupo de routers en una subred remota.

Trabajo adicional ha sido propuesto que define un set de direcciones anycast reservadas dentro de cada prefijo de subred. Asignaciones de direcciones anycast adicionales se esperan a ser definidas en el futuro.

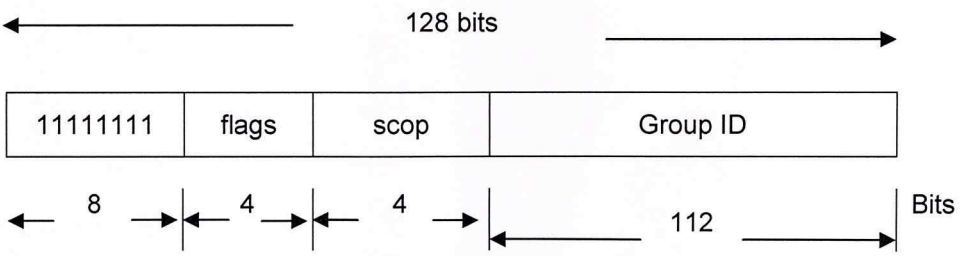


subnet-router anycast address (required)

6.6.5. Direcciones Multicast

La dirección multicast identifica un grupo de nodos, y cada uno de estos nodos puede pertenecer a múltiples grupos multicast. Las direcciones multicast son definidas en RFC 2373 y documentadas en más detalle en RFC 2375.

La dirección multicast comienza con el Formato de Prefijo 11111111 e incluye 3 campos adicionales. El campo Flags contiene cuatro flags (banderas) de 1 bit. Los 3 bits de las banderas más significantes están reservados para uso futuro y son inicializados en cero. La cuarta bandera es llamada el bit T, o transitorio. Cuando T=0, la dirección multicast es una dirección multicast permanentemente asignada (o mejor conocida), asignada por la autoridad de numeración de Internet global.
Cuando T=1, un transitorio (o asignación no permanentemente) de dirección multicast es indicada.



El campo Scop es un campo de 4 bits que es usado para limitar el alcance del grupo multicast. Los valores del campo Scop son:

valor	significado
0	Reservado
1	alcance de nodo local
2	alcance de link local
3	sin asignar
4	sin asignar
5	alcance se site local
6	sin asignar
7	sin asignar
8	alcance de organización local
9	sin asignar
A	sin asignar
B	sin asignar
C	sin asignar
D	sin asignar
E	alcance global
F	Reservado

El campo Group ID identifica el grupo multicast, sea permanente o transitorio, dentro del alcance dado. Las direcciones multicast no pueden ser usadas como direcciones fuente en los datagramas IPv6 o aparecer en ningún encabezado de ruteo. RFC 2373 documenta las siguientes direcciones multicast predefinidas:
Direcciones multicast reservadas:

FF00:0:0:0:0:0:0:0 FF01:0:0:0:0:0:0:0 FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0 FF04:0:0:0:0:0:0:0 FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0 FF07:0:0:0:0:0:0:0 FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0 FF0A:0:0:0:0:0:0:0 FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0 FF0D:0:0:0:0:0:0:0 FF03:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Las direcciones multicast de arriba están reservadas y nunca serán asignadas a ningún grupo multicast.

Todas las direcciones de los nodos: FF01:0:0:0:0:0:0:1 FF02:0:0:0:0:0:0:1

6.6.6. Direcciones Requeridas para cualquier nodo

Todos los nodos, en el proceso de identificación, al unirse a la red, deben de reconocer como mínimo, las siguientes direcciones:

- Sus direcciones locales de enlace para cada interfaz
- Las direcciones unicast asignadas
- La dirección de loopback
- Las direcciones multicast de todos los nodos
- Las direcciones multicast solicitadas para cada dirección unicast o anycast asignadas
- Las direcciones multicast de todos los grupos a los que dicho host pertenece

Además, en el caso de los routers, tienen que reconocer también:

- La dirección anycast del router de la subnet, para las interfaces en las que esta configurado para actuar como router
- Todas las direcciones anycast con las que el router ha sido configurado
- Las direcciones multicast de todos los routers
- Las direcciones multicast de todos los grupos a los que el router pertenece

Además, todos los dispositivos con IPv6, deben de tener, predefinidos, los prefijos siguientes:

- Dirección no especificada
- Dirección de loopback
- Prefijo de multicast (FF)
- Prefijos de uso local (local de enlace y local de sitio)
- Direcciones multicast predefinidas
- Prefijos compatibles IPv4

Se debe de asumir que todas las demás direcciones son unicast a no ser que sean específicamente configuradas (por ejemplo las direcciones anycast).

6.6.7 Direcciones Unicast Globales Agregables (RFC2374)

Dado que uno de los problemas que IPv6 resuelve es la mejor organización jerárquica del routing en las redes públicas (globales), es indispensable el concepto de direccionamiento "agregable".

En la actualidad ya se emplea este tipo de direcciones, basadas en la agregación por parte de los proveedores del troncal Internet, y los mecanismos adoptados para IPv6, permiten su continuidad. Pero además, se incorpora un mecanismo de agregación basado en "intercambios".

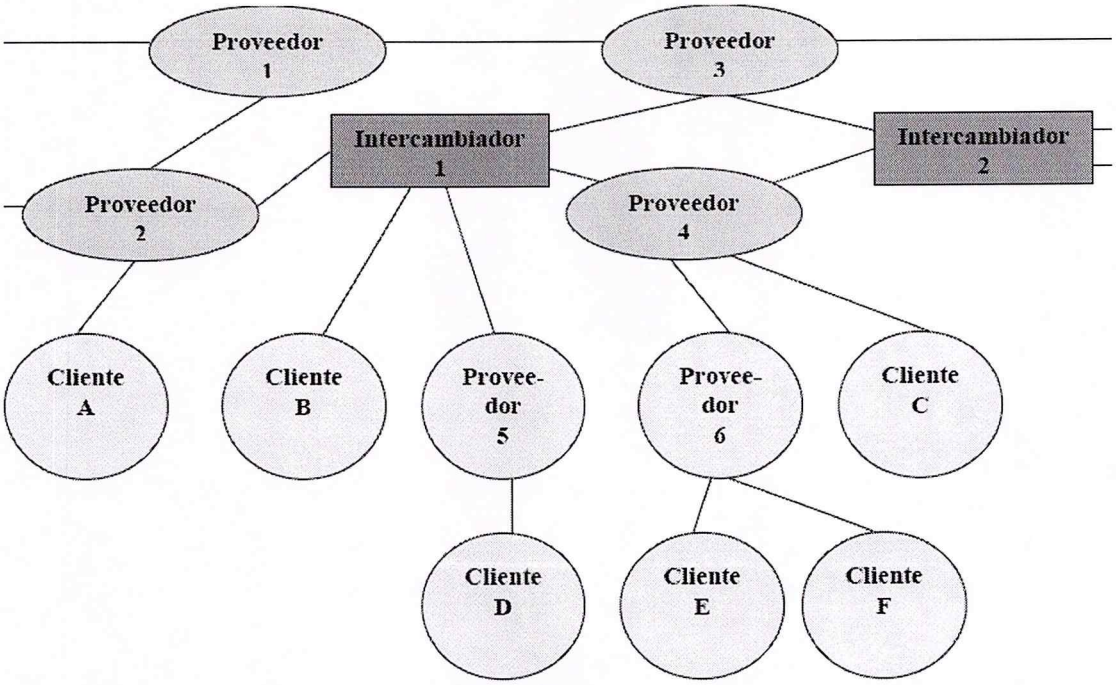
La combinación de ambos es la que permite un enrutamiento mucho más eficiente, dando dos opciones de conectividad a unas u otras entidades de agregación.
Se trata de una organización basada en tres niveles:

- Topología Pública: conjunto de proveedores e "intercambiadores" que proporcionan servicios públicos de tránsito Internet.
- Topología de Sitio: redes de organizaciones que no proporcionan servicios públicos de tránsito a nodos fuera de su propio "sitio".
- Identificador de Interfaz: identifican interfaces de enlaces.

En la figura adjunta, el formato de direcciones agregables ha sido diseñado para soportar proveedores de larga distancia (identificados como Proveedor 1-4), intercambiadores (Intercambiador 1 y 2), proveedores de niveles inferiores (podrían ser ISP's, identificados como Proveedor 5 y 6), y Clientes (Cliente A-F).

A diferencia de lo que ocurre actualmente, los intercambiadores también proporcionarán direcciones públicas IPv6. Las organizaciones conectadas a dichos intercambiadores también recibirán servicios de conectividad directos, indirectamente a través del intercambiador, de uno o varios proveedores de larga distancia.

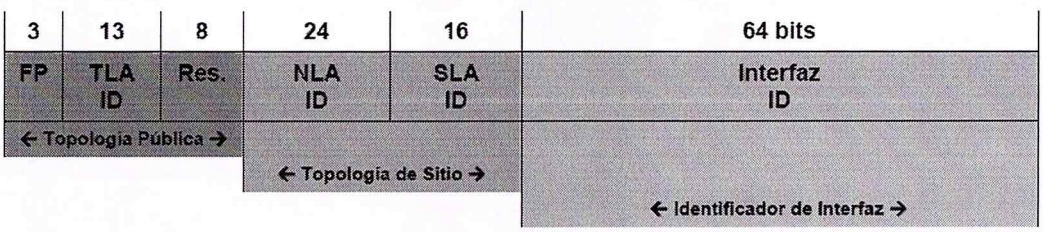
De esta forma, su direccionamiento es independiente de los proveedores de tráfico de larga distancia, y pueden, por tanto, cambiar de proveedor sin necesidad de renumerar su organización. Este es uno de los objetivos de IPv6.



Además, una organización puede estar suscrita a múltiples proveedores (multi-homing o "multi-localización"), a través de un intercambiador, sin necesidad de tener prefijos de direcciones de cada uno de los proveedores.

6.6.8 Estructura de Direcciones Unicast Globales Agregables

El formato de las direcciones unicast globales agregables es el siguiente:



Donde:

FP	Prefijo de Formato (001) - Format Prefix
TLA ID	Identificador de Agregación de Nivel Superior - Top-Level Aggregation Identifier
Res.	Reservado para uso futuro
NLA ID	Identificador de Agregación de Siguiente Nivel - Next-Level Aggregation Identifier
SLA ID	Identificador de Agregación de Nivel de Sitio - Site-Level Aggregation Identifier
Interfaz ID	Identificador de Interfaz

El campo Reservado permitirá, en el futuro, ampliaciones "organizadas" del protocolo, por ejemplo ampliar el número de bits de los campos TLA y NLA. Por el momento contiene ceros.

6.6.9 Identificador de Agregación de Nivel Superior

Se trata del nivel superior en la estructura jerárquica de enrutado. Los routers situados en este nivel tienen, en la tabla de enrutamiento, una entrada para cada TLA ID activo, y probablemente entradas adicionales relativas al propio TLA ID donde están físicamente situados.

Podrían tener otras entradas, para su optimización, dependiendo de su topología, pero siempre pensando en que se minimice la tabla.

Esta estructura de direccionamiento permite 8.192 (213) identificadores de TLA. Se prevé su crecimiento haciendo que este campo crezca hacia la derecha en el espacio reservado para el futuro, o usando este mismo formato/estructura para prefijos de formato (FP) adicionales.

Resumiendo:

Puede parecer un esquema muy complejo, pero en realidad es muy simple y sobre todo, muy eficiente. Los resultados de este esquema son:

a) Las direcciones siguen siendo asignadas por el proveedor, pero al cambiar de proveedor, sólo cambia el prefijo, y la red se "renumera" automáticamente (routers, sitios y nodos finales – dispositivos – servidores).
b) Las interfaces pueden tener múltiples direcciones.
c) Las direcciones tienen ámbito (Global, Sitio, Enlace).
d) Las direcciones, al estar compuestas por un prefijo y un identificador de interfaz, nos permiten separar "quién es" de "donde esta conectado":
e) Además, las direcciones tienen un período de vida (de validez).

6.7. Calidad de Servicio (Quality of Service – QoS)

Los campos de la etiqueta de la prioridad y del flujo en el encabezado IPv6 son utilizados por una fuente para identificar los paquetes que necesitan la dirección especial por los routers de la red. El concepto de un flujo en el IP es una salida importante de IPv4 y de la mayoría de los otros protocolos sin conexión; algunos han llamado flujos que una forma de circuitos virtuales sin conexión desde todos los paquetes con la misma etiqueta del flujo se trata semejantemente y la red lo visualiza como entidades asociadas.

La dirección especial para quality-of-service que no están por defecto, es los usos de una ayuda importantes de la capacidad para que requieran rendimiento de procesamiento garantizado, end-to-end retrasado, e inquietud, por ejemplo multimedia o comunicación en tiempo real. Estos parámetros de QOS son una extensión del tipo de IPv4's de capacidad del servicio (TOS).

El campo de prioridad permite que la fuente identifique la prioridad deseada de un paquete. Los valores 0-7 se utilizan para controlar el tráfico congestionado, o el tráfico que retrocede en respuesta a la congestión de red, tal como segmentos del TCP. Para este tipo de tráfico, se recomiendan los valores siguientes de la prioridad:

1) Tráfico sin Caracterizar.
2) Tráfico "relleno".
3) Transferencia de datos desatendida. (Ejemplo: E-mail)
4) Reservado
5) Transferencia a Granel Atendida. (Ejemplo: FTP, HTTP, NFS)
6) Reservado
7) Tráfico Interactivo. (Ejemplo: Telnet, SSH, X)
8) Tráfico del control del Internet (Ejemplo: SNMP)

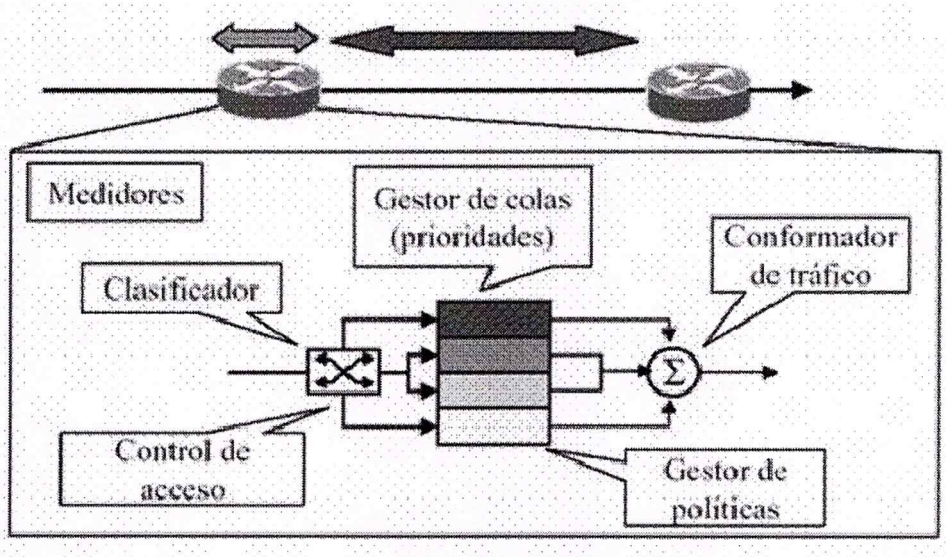
Los valores 8-15 se definen para controlar el tráfico de no-congestión, o el tráfico que no retrocede en respuesta a la congestión de red, tal como paquetes en tiempo real que son enviados en una tarifa constante. Para este tipo de tráfico, el valor más bajo de la prioridad (8) se debe utilizar para los paquetes que el remitente está el más dispuesto a haber desechado bajo condiciones de la congestión (Ejemplo: tráfico video de alta fidelidad) y el valor más alto (15) se debe utilizar para esos paquetes que el remitente está lo más menos posible dispuesto a haber desechado (Ejemplo: Voz sobre IP).

La etiqueta del flujo es utilizada por una fuente para identificar los paquetes que necesitan el QOS no están por defecto. La naturaleza de la dirección especial se pudo transportar a los routers de la red por un protocolo del control, tal como el protocolo de la reservación del recurso (RSVP), o por la información dentro de los paquetes del flujo ellos mismos, tales como una opción del salto-por-salto. Puede haber flujos activos múltiples de una fuente a una destinación, así como el tráfico que no se asocia a ningún flujo (es decir, etiqueta del flujo = 0). Un flujo es identificado únicamente por la combinación de una dirección de la fuente y de una etiqueta distinta a cero del flujo.

Este aspecto de IPv6 todavía está en la etapa experimental y la definición del futuro espera.

la **latencia de encolado** puede ser controlada por los mecanismos de QoS

la **latencia de propagación** viene dada por el medio: no se puede cambiar



Versión	clase de trabajo	etiqueta de flujo
longitud carga útil	next header	Limite saltos
Source address		
target address		

6.7.1. Origenes del QoS

A finales de los 90, con el advenimiento de las redes IP como ganadoras en la carrera por la supremacía de la Convergencia de Voz, Video y Datos, se volvió trascendental el término Calidad de Servicio (QoS Quality of Service). Es debido a que las redes IP eran invariablemente "redes del mejor esfuerzo" y carecían de la QoS necesaria para las nuevas aplicaciones de "real time". El desafío será entonces, convertir, las redes IP, en modelos de redes de servicios diferenciados. La calidad de servicio es un término a menudo mal utilizado y que tiene una variedad de significados. En este trabajo QoS hace referencia tanto a la clase de servicio (CoS Class of Service) como, al tipo de servicio (ToS Type of Service).

El objetivo básico de CoS y ToS es conseguir el ancho de banda y la latencia necesarios para una aplicación determinada. Una CoS permite al administrador de la red agrupar diferentes flujos de paquetes, teniendo cada uno requisitos de latencia y ancho de banda diferentes. Un ToS es un campo en una cabecera de Protocolo Internet (IP) que permite que tenga lugar una clase de servicio. Adicionalmente, en el diseño del nuevo protocolo de Internet, IPv6, se incluyeron características de "Calidad de Servicio". Los campos "Clase de Tráfico" y "Etiqueta de Flujo" se usan específicamente para dicha función. En este trabajo se mostrará las necesidades de QoS de las aplicaciones más comunes y en consecuencia cuales son los modelos que compiten para satisfacerlas, tales como DiffSere IntServ. También se hará una mención del soporte de IPv6 para diseñar redes con Calidad de Servicio.

6.7.1.1. Antecedentes de QoS

- Las redes IP en la mitad de los 90 fueron "redes del mejor esfuerzo"
- Con el rápido crecimiento de nuevas aplicaciones se necesita la provisión de recursos de calidad
- Mejor comprensión que ciertas aplicaciones son más "importantes" que otras y demandan un tratamiento preferencial de la red (Tiempo Real (Voz y Video)2 Expectativas de QoS

6.7.2 Expectativas del usuario final

- Percepción de QoS eminentemente subjetiva.
- No es fácilmente mensurable.
- Solo se interesa cuando la red se degrada o se pierde por completo.

- Apreciación de la QoS por comparación con otro servicio similar y por el costo
- Expectativas de la administración de redes
- Percepción la calidad de la red mediante estadísticas: Velocidad, desempeño, pérdida de paquetes y satisfacción del cliente.
- Expectativas y "problemas de calidad" son más absolutos y mensurables.
- Proveedores de servicio formalizan las expectativas con acuerdos de niveles de servicio (SLA),
- Establece los límites aceptables del desempeño de la red.
- Contrato de servicio entre el cliente y el proveedor
- Describe la clase de servicio que deberá ser provisto
- El proveedor es responsable de asegurar los recursos adecuados para soportar la SLA.

6.7.3. ¿Qué es Calidad de Servicio?

- Calidad: proceso de entrega de datos en forma fiable y/o mejor de lo normal
- Servicio: algo ofrecido al usuario final de la red(

QoS) Calidad de Servicio es el efecto colectivo del rendimiento de la red, que determina el grado de satisfacción del usuario y está caracterizada por la combinación de aspectos tales como: soporte, operabilidad, seguridad y otros factores específicos de cada servicio.

6.7.4. ¿Que es Clase de Servicio?

Clase de Servicio (CoS) es un esquema de clasificación con que son agrupados los tráficos que tienen requerimientos de rendimiento similares.

- Una manera de diferenciar diferentes tipos de tráficos y por ende poder priorizarlos.
- Los rasgos de la QoS son especificados mediante los números de las clases de servicio.

El protocolo Ipv6 fue diseñado para mejor la cualidad de Calidad de Servicio. Se crean dos nuevos campo y se mejora el rendimiento general del protocolo. La mejora de rendimiento se basa en que los paquetes pudieran ser tratados de manera eficiente por los routers. Para ello Ipv6 tiene menos campos; la etiqueta de flujos está antes de las direcciones, permitiendo el ruteado por flujos, donde se calcula la ruta una vez; ICMPv6 es un protocolo más ligero y conciso; se permite la Autoconfiguración y el campo TTL se

cambia por número de saltos. Ipv6 soporta Calidad de Servicio a través de dos campos nuevos.

En IPv6 aparecen nuevos campos respecto a IPv4 y otros son renombrados, dando lugar a la nueva cabecera:

Clase de Tráfico (Traffic Class): también denominado Prioridad (Priority), o simplemente Clase (Class). Podría ser más o menos equivalente a TOS en IPv4. Tiene una longitud de 8 bits. (1 byte).
Que también se denomina Prioridad o simplemente Clase. Este campo debería ser usado por los nodos que originan trafico y/o por los router que re-enrutan para identificar y distinguir entre diferentes clases y prioridades de los paquetes Ipv6, los cuales deben recibir un tratamiento particular, en cada nodo. Este campo fue diseñado para soportar Servicios Diferenciados (DiffServ) y se aconseja que se siga la semántica del campo DS.

Etiqueta de flujo (Flow Label): sirve para permitir tráfico con requisitos de tiempo real. Tiene una longitud de 20 bits.

Este campo puede ser usado en el origen para etiquetar los paquetes, aun mismo destino, que requieran un tratamiento especial por los routers Ipv6, tales como servicios de QoS no habituales o "real time". Esta herramienta es todavía experimental y sujeta a cambios hasta que sean claro los requerimientos de soporte de flujo en Internet. Este campo fue diseñado para soportar Servicios Integrados (IntServ)

Estos dos campos son los que nos permiten una de las características fundamentales e intrínsecas de IPv6: Calidad de Servicio (QoS) y Clase de Servicio (CoS), y en definitiva un poderoso mecanismo de control de flujo, de asignación de prioridades diferenciadas según los tipos de servicio.

La longitud de esta cabecera es de 40 bytes, el doble que en IPv4, pero con muchas ventajas al haberse eliminado campos redundantes. Debido a que la longitud de la cabecera es fija, implica numerosas ventajas ya que facilita el procesado en router y conmutadores. Los nuevos procesadores y microcontroladores de 64 bits pueden procesar de forma más eficazmente este tipo de cabecera, ya que los campos están alineados a 64 bits.

El formato de paquetes en IPv6 contiene un nuevo campo de identificación de flujo de tráfico de 24 bits que tendrá un gran valor para vendedores que implementan funciones de red de calidad de servicio.

Las etiquetas de flujo en IPv6 pueden ser usadas para identificar en la red un conjunto de paquetes que necesitan un manejo especial durante y después de una falla. El enrutamiento basado en flujo podría mejorar algunas de las características determinísticas asociadas con la tecnología de conmutación orientada a conexión y los circuitos virtuales telefónicos.

El flujo es una secuencia de paquetes desde un origen a un destino que necesita de cierto tratamiento especial, por lo tanto la etiqueta de flujo se utiliza para identificar un flujo de datos que tiene un mecanismo de –manejo especial (p.e. reserva de ancho de banda).

Dos peculiaridades del IPv6 lo diferencian de la versión 4 en la cuestión calidad de servicio (QoS): las etiquetas de flujo y el campo prioridad. Las mismas son particularmente importantes en las denominadas aplicaciones Internet2, donde la calidad del servicio es fundamental.

La QoS (Quality of Service, Calidad de Servicio) garantiza que se transmitirá cierta cantidad de datos en un tiempo dado (throughput). Una de las grandes ventajas de ATM (Asynchronous Transfer Mode – Modo de Transferencia Asíncrona) respecto de técnicas como el Frame Relay y Fast Ethernet, es que soporta niveles de QoS. Esto permite que los proveedores de servicios ATM garanticen a sus clientes que el retardo de extremo a extremo no excederá un nivel específico de tiempo. Además que en los servicios satelitales da una nueva perspectiva en la utilización del ancho de banda, dando prioridades a las aplicaciones de extremo a extremo con una serie de reglas.

Una red IP esta basada en paquetes de datos, estos paquetes de datos tienen una cabecera que contiene información sobre el resto del paquete. Existe una parte del paquete que se llama TOS, en realidad esta parte esta pensada para llevar banderas o marcas. Lo que se puede hacer para darle prioridad a un paquete sobre el resto es marcar una de esas banderas.

Para ellos el equipo que genera el paquete, por ejemplo un gateway de vozip, coloca una de esas banderas en un estado determinado y los dispositivos por donde pasa ese paquete luego de ser transmitido deben tener la capacidad para poder discriminar los paquetes para darle prioridad sobre los que no fueron marcados. Y además son de plastilina.

7. AUTOCONFIGURACIÓN Y RED LOCAL

7.1. Objetivo del Diseño.

Como se ha visto hasta ahora, IPv6 tiene algunas capacidades (y algunas complejidades) que van más allá de lo que IPv4 ofrece en el presente.

Afortunadamente, los arquitectos de IPv6 desarrollaron protocolos y procesos adicionales que mejoran esas complejidades.

En este capítulo, se revisara uno de los protocolos más importantes, Stateless Address Autoconfiguration, que permite a una workstation entrar a una red IPv6 al inicio automáticamente. El proceso de autoconfiguración es también muy útil para administradores de red que están migrando de sus redes IPv4 existentes a IPv6, pues elimina muchos de los requerimientos para configuración humana de direcciones, parámetros de ruteo, y así. Si el proceso de autoconfiguración falla, o es inadecuado para una situación particular, el DHCP para IPv6 (DHCPv6) también ha sido definido. Además, hay temas únicos para topologías de LAN o WAN particulares que tienen como factor el tema de implementación.

7.2. Stateless Address Autoconfiguration (RFC2462)

La palabra auto configuración se describe mejor por sus 2 raíces: auto, que significa "mismo", y configuración, que significa "arreglo funcional". De acuerdo a RFC 2462, el proceso de auto configuración incluye crear direcciones de linklocal y verificar su unicidad en el link, así como determinar qué información debe ser auto configurada (direcciones, otra información, o ambas). Note que el proceso de auto configuración especificado en RFC 2462 se aplica solo a los hosts; es asumido que los routers están configurados de alguna otra manera.

Hay 3 métodos para obtener direcciones: **un mecanismo sin estado, un mecanismo con estado, o ambos**. Tanto la autoconfiguración sin estado como con estado pueden ser usadas simultáneamente. Que tipo de autoconfiguración está en uso es especificado por el mensaje Router Advertisement.

En un modelo de autoconfiguración con estado, los hosts obtienen direcciones, información de configuración, parámetros, y así, desde un servidor.

Ese servidor mantiene una base de datos conteniendo la información necesaria y guarda control firme sobre las asignaciones de dirección. El modelo de autoconfiguración con estado para IPv6 es definido por el protocolo DHCP para IPv6 (DHCPv6), que consideraremos en la próxima sección.

En contraste, autoconfiguración sin estado no requiere manual configuración de los hosts, mínima (o ninguna) configuración de routers, y ningún servidor adicional. El acercamiento sin estado es usado cuando un site no se concierne acerca de las direcciones específicas que son usadas, mientras ellas sean únicas y ruteables.

Con la auto configuración sin estado, un host genera su propia dirección usando 2 elementos de información: Información disponible localmente (por Ej.: disponible desde el host mismo) más información publicitada por routers. La parte del host es llamada un identificador de interfase, que identifica una interfase en una subred. La parte del router viene de un prefijo de dirección que identifica la subred asociada con un link. La dirección derivada es una combinación de estos 2 elementos. Si un router no existe en una subred, el host todavía puede generar un tipo especial de dirección llamada la dirección linklocal.

La dirección link-local puede ser usada solo para comunicación entre nodos unidos al mismo link.
Note que el proceso de autoconfiguración sin estado, como se define en RFC 2462, se aplica solo a los hosts, no a los routers. (Porque los hosts obtienen alguna información de sus direcciones de los routers, estos routers deben ser configurados usando algún otro medio.) La sola excepción de esta regla es que los routers pueden generar sus propias direcciones link-local, y pueden verificar la unicidad de estas direcciones en el link, cuando son booteadas o reiniciadas.

Las direcciones IPv6 son "arrendadas" a una interfase por un particular periodo de tiempo, que puede ser indefinido. Asociado con la dirección es un tiempo de vida indicando que tan largo puede ser limitado a esa interfase. Con la expiración del tiempo de vida, tanto el atascamiento como la dirección se vuelven inválidas, y la dirección puede ser reasignada a otra interfase en el internet. Para soporte de estos atascamientos, la dirección asignada puede tener 2 fases: preferida, que significa que el

uso de esta dirección es sin restricciones; y desaprobada, indicando que el uso adicional de esa dirección es desalentado, en anticipación de un atascamiento inválido.

El proceso de autoconfiguración sin estado comienza con la generación de una dirección link-local para esa interfase:

La dirección de link -local es generada combinando el prefijo de dirección linklocal (1111 1110 10) con un identificador de interfase de 64 bits. El identificador de interfase es específico para una topología LAN o WAN en uso. En muchos casos, es derivado de la dirección del hardware que reside en el ROM en la tarjeta de interfase de red. Nosotros miraremos los varios identificadores de interfase en las secciones subsecuentes de este capítulo. (Como nota histórica, los documentos anteriores de IPv6 RFC e Internet Draft usaron el término "token de interfase" en vez del término usado actualmente "identificador de interfase".)

El próximo paso determina la unicidad de la dirección tentativa que ha sido derivada de combinar el prefijo de link -local y el identificador de interfase. En este paso, un mensaje Neighbord Solicitation es transmitido con la dirección tentativa como la dirección target. Si otro nodo está usando esta dirección, un mensaje Neighbor Advertisement se retorna. En este evento, la autoconfiguración se para y alguna intervención manual es requerida. Si ninguna respuesta Neighbor Advertisement es retornada, la dirección tentativa es considerada única y la conectividad al nivel de IP con los nodos vecinos es ahora posible. Note que tanto los hosts como los routers pueden generar direcciones link -local usando esta parte del proceso de autoconfiguración.

La próxima fase es ejecutada solo por los hosts; ésta envuelve escuchar los mensajes Router Advertisement que los routers transmiten periódicamente, o forzar un mensaje Router Advertisement inmediato mediante la transmisión de un mensaje Router Solicitation. Si ningún mensaje Router Advertisements es recibido, significando que no hay routers presentes, un método con estado, como DHCPv6, debe ser usado para completar el proceso de configuración.

Si los routers están presentes, los mensajes Router Advertisement serán periódicamente enviados. De acuerdo con RFC 2461, Router Advertisement incluye 2 flags claves, M y O, que son usadas en el proceso de autoconfiguración:

- El flag Managed Address Configuration (M) es indicado cuando M = 1. En este caso, los hosts deben usar el protocolo (con estado) administrado para autoconfiguración de direcciones, además de alguna otra dirección autoconfigurada usando autoconfiguración de dirección sin estado.
- El flag Other Stateful Configuration (O) es indicado cuando O = 1. Los hosts deben usar el protocolo (con estado) administrado para la autoconfiguración de otra información (no dirección).

Los mensajes Router Advertisement también pueden incluir una o más de las siguientes opciones: Source Link Layer Address, Maximum Transmission Unit (MTU), y Prefix Information. De acuerdo con RFC 2461, la opción Prefix Information incluye 2 flags clave, L y A, que pueden ser usadas con autoconfiguración de dirección:

- El flag On-Link (L) es indicado cuando L = 1, significando que este prefijo puede ser usado para determinación "on-link".
- El flag Autonomous Address Configuration (A) es indicado cuando A = 1, significando que este prefijo puede ser usado para configuración de direcciones autónomas.

Más especificaciones acerca de la autoconfiguración de direcciones sin estado es proveída en RFC 2462.

7.3. Dynamic Host Configuration Protocol v6 (DHCPv6)

En algunos casos, como cuando una dirección duplicada existe o routers que no están presentes, un proceso de autoconfiguración sin estado debe ser usado.

El protocolo Dynamic Host Configuration Protocol versión 6 (DHCPv6) provee estos parámetros de configuración a los nodos de internet. DHCPv6 consiste de 2 elementos: un protocolo que envía información de configuración específica al nodo desde un servidor DHCPv6 a un cliente y un mecanismo para asignar direcciones de red y otros parámetros a nodos IPv6.

DHCPv6 está construido en un modelo cliente-servidor, que confía en un total de 6 mensajes Request and Reply para la comunicación de estos detalles de parámetros. Algunos tipos de nodos DHCPv6 funcionales están definidos:

- Cliente DHCPv6: un nodo que inicia solicitudes en un link para obtener parámetros de configuración.
- Servidor DHCPv6: un nodo que responde a solicitudes de clientes para proveer parámetros de configuración. El servidor puede o no puede estar en el mismo link que el cliente.
- DHCPv6 Relay: un nodo que actúa como un intermediario para enviar mensajes DHCPv6 entre clientes y servidores, y está en el mismo link que el cliente.
- Agente DHCPv6: un servidor en el mismo link que el cliente o un relevo. La comunicación entre agentes DHCPv6 usa las siguientes bien conocidas direcciones multicast:

FF02:0:0:0:0:0:1:2 grupo multicast Link-Local All-DHCP-Agents
FF05:0:0:0:0:0:1:3 grupo multicast Site Local All-DHCP-Servers
FF05:0:0:0:0:0:1:4 grupo multicast Site Local All-DHCP-Relays

Todos los mensajes DHCPv6 tienen un formato similar, que comienza con un campo Message Type (Msg-type) indicando la función específica. Los parámetros de configuración, que son llamados extensiones, están incluidos en los mensajes DHCPv6. Las extensiones han sido definidas para especificar una dirección IP, husos horarios, DNS, Directory Agent, Network Time Protocol Server, Network Information Server, parámetros de TCP, Client-Server Authentification, y otros parámetros.

Un mensaje DHCPv6 Solicitado es enviado a un cliente (o relay, en el nombre de un cliente) para obtener una o más direcciones de servidor, y es identificado por Msg-type = 1. Este mensaje incluye un flag C, que solicita designación de los recursos del cliente en el servidor. También incluye las direcciones del cliente y posible relevo.

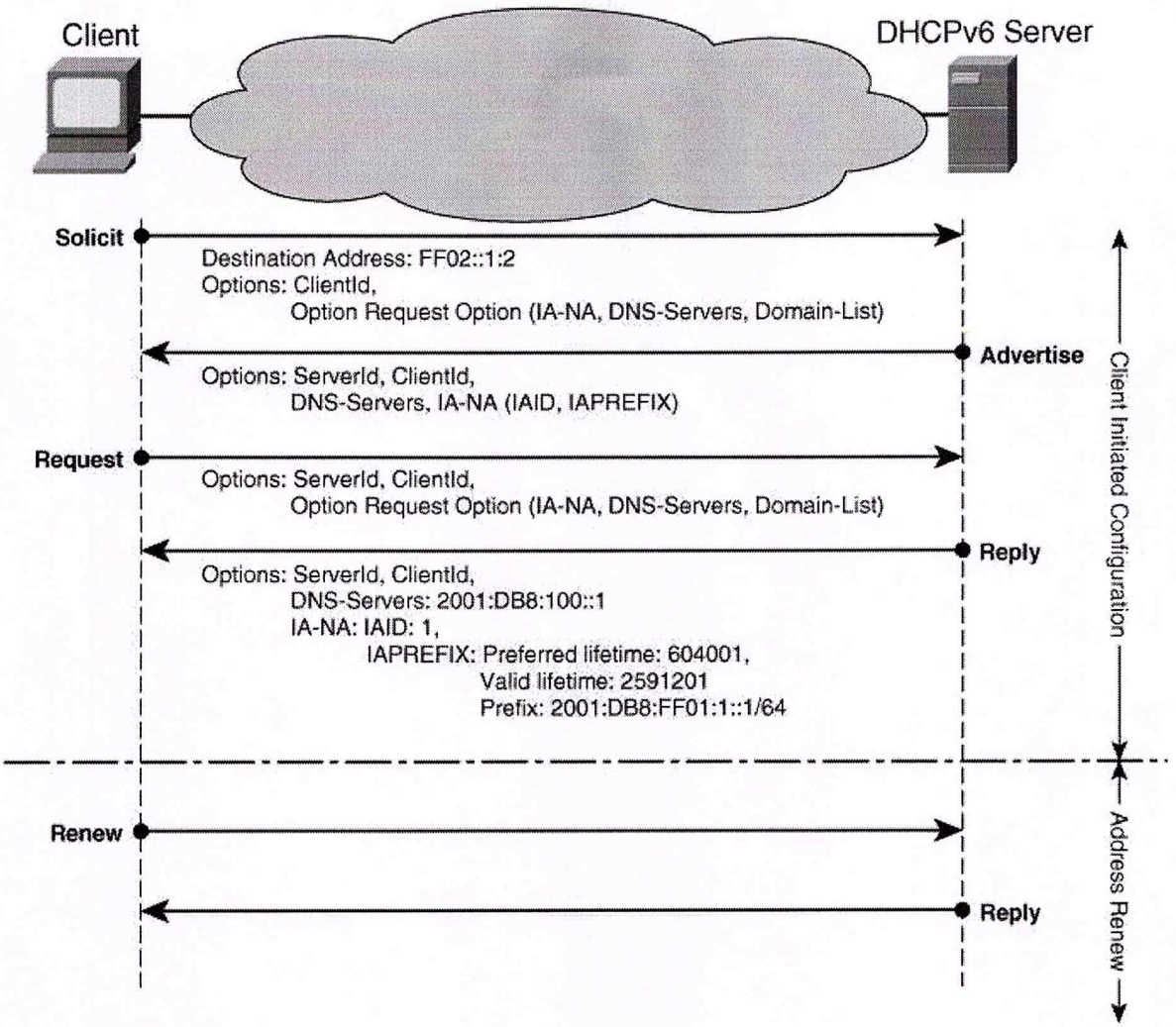
El mensaje **DHCPv6 Advertise** son enviado por un agente DHCPv6 para informar a un cliente prospecto acerca de la dirección IP donde los mensajes de la petición pueden ser enviados; es identificado por Msg-type=2. Este mensaje incluye un flag S, indicando que una dirección del servidor está presente también en el mensaje.

El mensaje **DHCPv6 Request** es enviado por un cliente para solicitar parámetros desde un servidor DHCPv6; es identificado por MSg-type=3. Este mensaje incluye un flag S, que indica que la dirección del servidor está presente; un flag C, que puede solicitar el servidor para limpiar todos los recursos y atascamientos asociados con el cliente, un Transaction identifier, y algunas direcciones y extensiones.

El mensaje **DHCPv6 Reply** es enviado por un servidor en respuesta a todos los mensajes **Request** o **Release** que son recibidos; es identificado por Msgtype = 4. Este mensaje incluye un flag L, que indica que una dirección Link-Local está presente; un Status, que indica el éxito o la razón del fallo de un intercambio de mensaje; un Transaction ID, y las posibles dirección y extensiones Link -Local del cliente.

El mensaje **DHCPv6 Release** es enviado desde un cliente al servidor (sin asistencia de un relevo) para solicitar el lanzamiento de las extensiones particulares; es identificado por Msg-type=5. Este mensaje incluye un flag D, que indica que el servidor debe enviar la respuesta directamente al cliente, un Transaction identifier y algunas direcciones y extensiones.

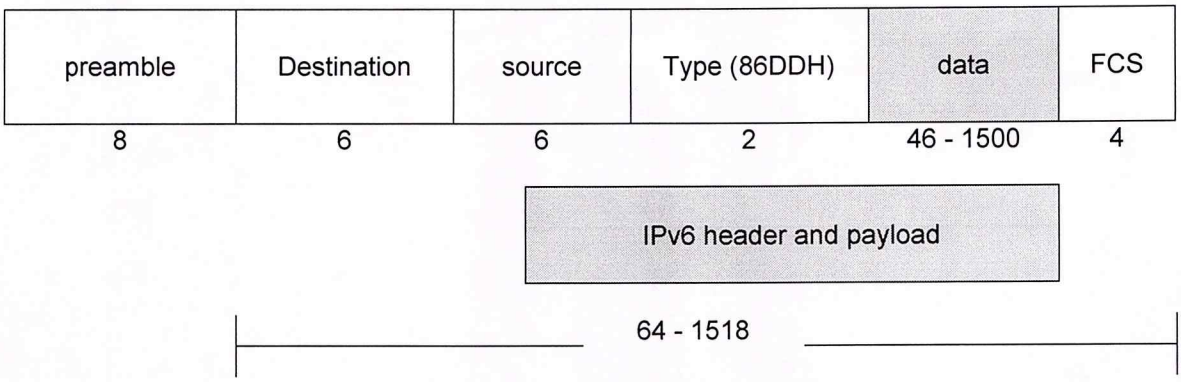
El mensaje **DHCPv6 Reconfigure** es enviado desde un servidor a un cliente (sin asistencia de un relevo) para indicar ciertos parámetros, que son especificados en las extensiones, necesarios a ser solicitados de nuevo por el cliente; es identificado por Msg-type=6. Este mensaje incluye un flag N, que indica que el cliente no debe esperar un **DHCP Reply** en respuesta de un **DHCP Request** que envié (al servidor) como resultado de un mensaje DHCP Reconfigure. También incluye un Transaction Identifier, un Server Address y extensiones.



7.4. IPv6 sobre Ethernet (RFC2464)

Ethernet, originalmente desarrollado por Digital Equipment Corporation (DEC) – ahora parte de Compaq Computer Corporation – Intel Corporation, y Xerox Corporation, ha sido tradicionalmente popular con los trabajos de red basados en TCP/IP. Soporte para IPv6 sobre redes Ethernet está documentado en RFC 2464.

El marco Ethernet puede cargar tanto como 1,500 octetos de datos en el campo de información; así, diríamos que la unidad máxima de transmisión (MTU) para Ethernet es 1,500 octetos. Este tamaño puede ser reducido por un paquete Router Advertisement especificando un MTU más pequeño, como se detalla en RFC 2461. El campo Ethernet Type (Ethertype) contiene el valor 86DDH para especificar IPv6.



La dirección Link-Local es formada preponiendo el prefijo de Link-Local (FE80::0) al identificador de interfase. Para redes Ethernet, el identificador de interfase (interface identifier) es la dirección de Ethernet de 48 bits, expandida en el centro con los caracteres hexadecimales FFFE para crear una dirección de 64 bits EUI-64 compatible.

Para las direcciones multicast, una dirección IPv6 con una dirección destino multicast es transmitida a la dirección multicast Ethernet que comienza con el valor 3333H y termina con los últimos 4 octetos de la dirección DST. (El valor 3333H ocupa los 2 primeros octetos de la dirección multicast Ethernet, y los últimos 4 octetos de la dirección IPv6 de 16 octetos (designadas DST13, DST14, DST15 y DST16) ocupan los últimos 4 octetos de la dirección Ethernet.)

Aunque ya han sido definidos protocolos para permitir el uso de IPv6 sobre cualquier tipo de red o topología (Token Ring, FDDI, ATM, PPP, ...), como ejemplo mucho más habitual y básico, centraremos este apartado en Ethernet (CSMA/CD y tecnologías full-duplex basadas en ISO/IEC8802-3).

Mas adelante, en este mismo documento, citaremos los protocolos adecuados para cada una de las otras tecnologías.
Los paquetes IPv6 se transmiten sobre tramas normalizadas Ethernet. La cabecera Ethernet contiene las direcciones fuente y destino Ethernet, y el código de tipo Ethernet con el valor hexadecimal 86DD.

El campo de datos contiene la cabecera IPv6 seguida por los propios datos, y probablemente algunos bytes para alineación/relleno, de forma que se alcance el tamaño mínimo de trama para el enlace Ethernet.

48 bits	48 bits	16 bits	
Dirección Ethernet Destino	Dirección Ethernet Fuente	1000011011011101 (86DD)	Cabecera y datos IPv6

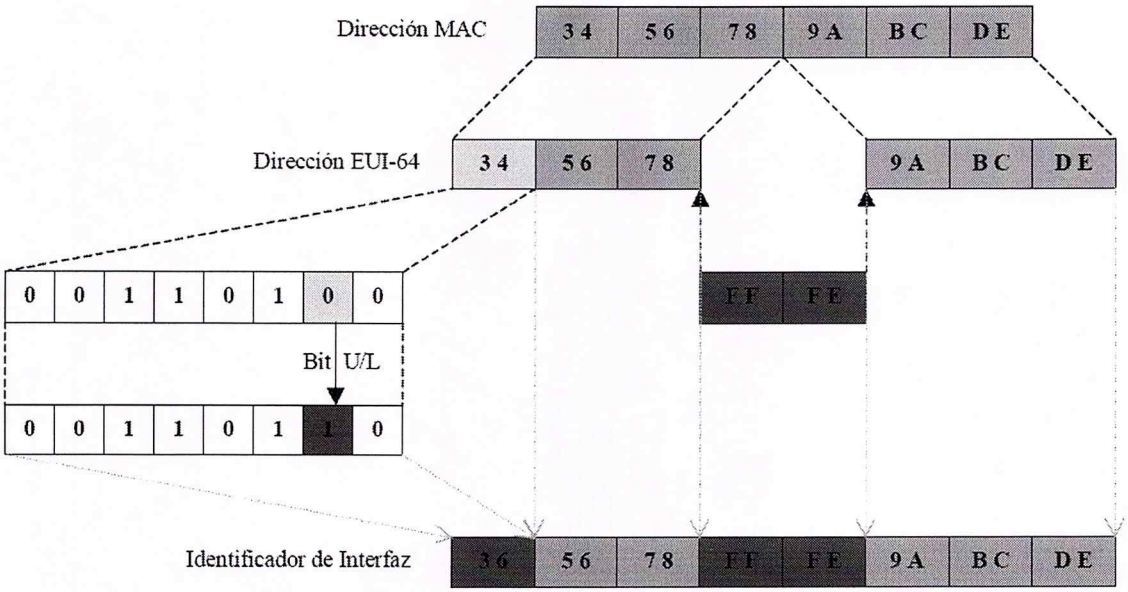
El tamaño máximo de la unidad de transmisión (MTU), para IPv6 sobre Ethernet, es de 1.500 bytes. Evidentemente, este puede ser reducido, manual o automáticamente (por los mensajes de anunciación de routers).

Para obtener el identificador de interfaz, de una interfaz Ethernet, para la autoconfiguración stateless, nos basamos en la dirección MAC de 48 bits (IEEE802). Tomamos los 3 primeros bytes (los de mayor orden), y les agregamos "FFFE" (hexadecimal), y a continuación, el resto de los bytes de la dirección MAC (3 bytes). El identificador así formado se denomina identificador EUI-64 (Identificador Global de 64 bits), según lo define IEEE.

El identificador de interfaz se obtiene, a continuación, partiendo del EUI-64, complementando el bit U/L (Universal/Local). El bit U/L es el siguiente al de menor valor del primer byte del EUI-64 (el 2º bit por la derecha, el 2º bit de menor peso). Al complementar este bit, por lo general cambiará su valor de 0 a 1; dado que se espera que la dirección MAC sea universalmente única, U/L tendrá un valor 0, y por tanto se convertirá en 1 en el identificador de interfaz IPv6.

Una dirección MAC configurada manualmente o por software, no debería ser usada para derivar de ella el identificador de interfaz, pero si no hubiera otra fórmula, su propiedad debe reflejarse en el valor del bit U/L.

Véase el esquema siguiente:



Para mapear direcciones unicast IPv6 sobre Ethernet, se utilizan los mecanismos ND para solicitud de vecinos.

Para mapear direcciones multicast IPv6 sobre Ethernet, se emplean los 4 últimos bytes de la dirección IPv6, a los que se antepone "3333".

7.5. Multi-homing

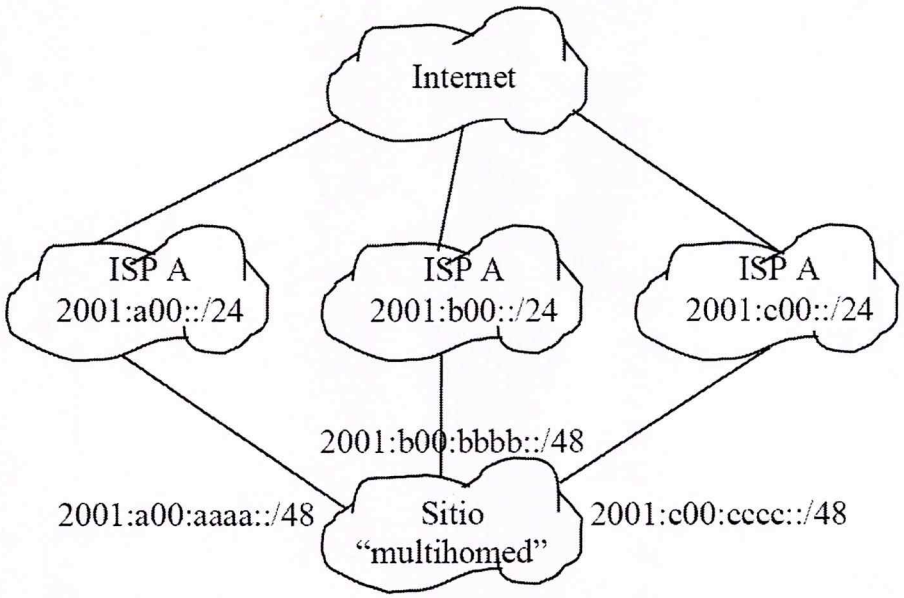
Como venimos viendo, el mecanismo de asignación de direcciones IPv6 es totalmente jerárquico.

El multi-homing ("múltiples hogares") es el mecanismo por el cual un determinado sitio o red puede estar conectado a otros por múltiples caminos, por razones de seguridad, redundancia, ancho de banda, balanceo de carga, etc.

Dado que un determinado sitio utiliza el prefijo de su ISP, o proveedor de nivel superior, un sitio puede ser "multi-homed" simplemente teniendo varios prefijos.

Frecuentemente, cada prefijo estará asociado a diferentes conexiones físicas, aunque no necesariamente, dado que se puede tratar de una sola conexión física y diversos túneles o conexiones virtuales.

La problemática se plantea por la dificultad de que un host decida, en una red "multi-homed", que dirección fuente utilizar.



Algunos de los documentos sobre los que se está trabajando en este campo son:

- Default Address Selections for IPv6 (draft-ietf-ipngwg-default-addr-select-00.txt).
- IPv6 Multi-homing with Route Aggregation (draft-ietf-ipngwg-ipv6multihomewith-aggr-00.txt).
- Multi-homed Routing Domain Issues for IPv6 (draft-ietf-ipngwg-multi-isp-00.txt).

7.6. IPv6 sobre PPP

El protocolo PPP es usado extensivamente para la transmisión del tráfico TCP/IP sobre links de WAN. El soporte de IPv6 sobre PPP está documentado en RFC 2472. PPP consiste de 3 elementos: un formato de encapsulamiento (o marco) para links en serie; un Link Control Protocol (LCP) para establecer, configurar, y probar la conexión del link; y una familia de Network Control Protocols (NCPs) para establecer y configurar diferentes capas de los protocolos de red. Por ejemplo, el NCP para establecer y configurar IPv6 sobre PPP es llamado el protocolo IPv6 Control Protocol o IPV6CP.

El marco PPP es mostrado en la figura siguiente. Note que un paquete IPv6 o un paquete IPV6CP cabría dentro del campo de información de ese marco PPP.

El campo Protocol define el tipo de paquete que es cargado: 0057H indica IPv6, mientras que 8057H indica IPV6CP.

flag	address	control	protocol	info (IPv6 - IPv6 packet)	flag
1	1	1	2	N	1

octetos

Para las LAN como Ethernet o token ring, el identificador de interfase usado con el proceso de Stateless Address Autoconfiguration es basado en la dirección del hardware, que es típicamente residente en el ROM o en la tarjeta de red. Para links PPP, el identificador de interfase puede ser seleccionado usando uno de los siguientes métodos (listados en el orden de preferencia):

1- Si un identificador global IEEE (EUI-48 o EUI-64) está disponible en cualquier parte del nodo, entonces esa dirección debe ser usada.
2- Si un identificador global IEEE no está disponible, entonces una fuente diferente de unicidad, como un número serial de la máquina, debe ser usado.
3- Si una buena fuente de unicidad no puede ser encontrada, un número aleatorio debe ser generado.

IPV6CP permite a los parámetros IPv6 ser negociados durante el inicio del link. Dos opciones, el Interface Identifier y el IPv6 Compression Protocol, han sido definidos. La opción Interface Identifier facilita la negociación de un identificador de interfase de 64 bits únicos para ese link, usando una de las 3 alternativas listadas arriba. La opción IPv6 - Compression-Protocol provee una manera de negociar el uso de un protocolo de compresión de paquetes IPv6.

Los valores corrientes para el campo Ipv6-Compression-Protocol son encontrados en el documento más reciente "Assigned Numbers" (actualmente RFC 1700).

Más detalles sobre soporte de PPP son encontrados en RFC 2472.

7.7. IPv6 sobre ATM

El soporte para IPv6 sobre redes ATM es definido en RFC 2492, que construye sobre las discusiones en redes NBMA desde RFC 2491 y provee detalles específicos sobre implementación de ATM.

ATM define 3 capas principales: una capa baja **Physical Layer** para conectividad de redes, una capa media **ATM Layer** donde las funciones de generación y encendido de células ATM son ejecutadas, y una capa alta **ATM Adaptation Layer (AAL)** que provee mecanismos para encapsular información desde las varias señales de las fuentes a ser transmitidas, Por ejemplo, **AAL Type 1 (AAL1)** es usado para una tasa de bits constante, servicio orientado a la conexión como emulación de circuito T1; **AAL Type 2 (AAL2)** es designado para tasa de bit variable , tráfico orientado a conexión, como video o voz comprimida; **AAL Type ¾ (AAL 3/4)** es designado para tasa de tráfico de bit variable, que puede ser orientado a conexión o sin conexión, como tráfico **Switched Multimegabit Data Service (SMDS)**; **AAL Type 5 (AAL5)** es designado para tasa de tráfico de bit variable, orientado a conexión, como FRAME RELAY. AAL5 es especificado en RFC 2492 para uso con IPv6.

En ambientes PVC, exactamente 2 nodos serán conectados, y así solo uso limitado de **Neighbor Discovery** y otras características IPv6 serán requerido. RFC 2492 define una encapsulación de paquete por defecto, que es usada con paquetes tanto unicast como multicast a través de links PVC de punto a punto. Este formato sigue el modelo definido en RFC 1483, "**Multiprotocol Encapsulation over AAL5**". El tamaño MTU por defecto es 9,180 octetos.

Para ambientes SVC, la encapsulación unicast es idéntica al caso PVC, y la encapsulación multicast incluye la encapsulación MARS con el campo **Cluster Member ID (pkt$cmi)** que es definido en RFC 2022.

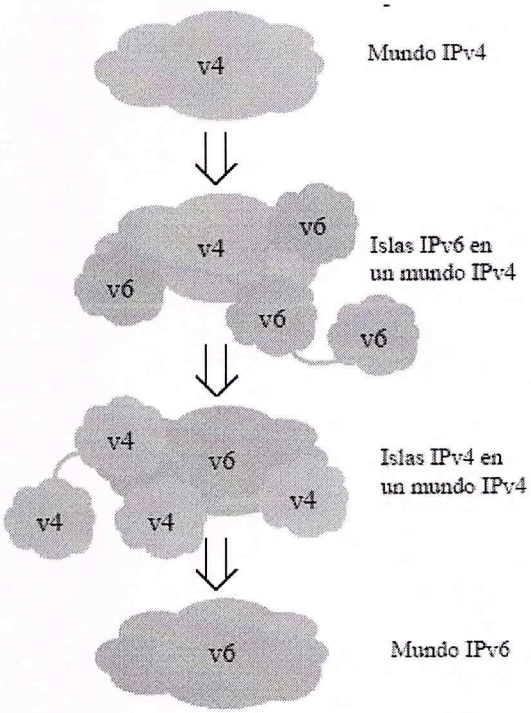
Los tokens de interfase (o identificadores de interfase) son también usados con ambientes IPv6 que emplean infraestructuras ATM. Hay muchas opciones descritas en RFC 2492 para generar el token de interfase, y el lector es referido a ese documento para más detalles.

8. ESTRATEGIA DE MIGRACION (DESARROLLO DEL SISTEMA)

Los desarrolladores de IPv6 reconocieron que no todos los sistemas se actualizarían desde IPv4 hacia IPv6 en el futuro inmediato, y algunos no se actualizarían por año. Para mayor complicación muchos de los sistemas de Internet son heterogéneos, con varios router, hosts, y son manufacturado por distintos vendedores. Si algo como un multivendedor de sistema fuera actualizado de una vez, la capacidad de IPv6 serian requerida en todos los elemento individuales ante de que el proyecto se realizada.

Asunciones de la transición

- Ningún "banderazo inicial": La última transición de Internet fue en 1983 (NCP --> TCP)
- La transición será incremental: Posiblemente tomara varios años
- Inexistencia de barreras IPv4/IPv6: Inexistencia de dependencias de transición (No hay requerimientos del nodo X antes del nodo Y)
- Debe ser fácil para el usuario final: La transición de IPv4 a dual stack no debe alterar los sistemas de información y comunicación



- La transición será desde en cliente final Determinada por la demanda de cliente: A excepción de nuevas redes IPv6 se diseña con la transición en mente
- Asunción de la coexistencia IPv4/IPv6 "Caja de herramientas de la transición" a aplicarse a las situaciones únicas innumerables

Se puede ver en la figura como se espera que sea la transición [50] [51] [52] [53] [54] [55] [56] [57] [58] [59] hacia IPv6 en el mundo. Partiendo de un mundo solo IPv4, van apareciendo algunas

[50] Javier Sedano, Mundo Linux (Revistas Profesionales)

redes IPv6, que poco a poco van interconectándose a veces de forma nativa, y a veces utilizando túneles sobre la red IPv4 para ello (esta es la situación actual).

El principal freno a la adopción del protocolo es la existencia de soluciones parciales a algunos de los problemas de IPv4: IpSec para la seguridad, NAT para el espacio de direcciones, IntServ y DiffServ para la calidad de servicio, etc. Esto puede hacer que la solución IPv6 pierda su oportunidad. Depende de la presión que se ejerza por parte de los involucrados (usuarios, proveedores de acceso, operadoras, fabricantes, compañías de software, etc.) y de los acontecimientos que sucedan en los mercados conectados a Internet.

Las ventajas de llevar a cabo un cambio del protocolo IPv4 a IPv6 se pueden considerar en gran medida como de interés general. Este hecho va a dificultar la adopción del protocolo IPv6, debido a que pocos organismos asumen como propio la obligación de promocionar el uso del nuevo protocolo, pues el hecho de ser pionero en un cambio siempre supone una serie de dificultades imprevistas, por lo que se ha de estar seguro del éxito de esta nueva iniciativa. Es por ello que las universidades y entidades de investigación juegan un papel preponderante en este liderazgo y, en la medida de lo posible, deben incorporar el protocolo a sus propias redes. El resto de la comunidad Internet, probablemente llevará a cabo el cambio cuando lo perciba como necesario.

Las estrategias de migración han de tener en cuenta la posibilidad de introducir las características avanzadas de IPv6, como autoconfiguración, movilidad y seguridad.

Los aspectos relacionados con la migración se encuentran situados en los diferentes niveles del modelo de referencia OSI, desde el nivel de enlace al de aplicación.

Los objetivos fundamentales de la etapa de transición son los siguientes:

---

[51] Estudio de la problemática de la implantación de IPv6 en la RECETGA (Andrés Gómez, José Carlos Pérez, Juan Villasuso, Natalia Costas) Enero 28 del 2005
[52] IPv6: Mecanismos de Transición IPv4 - IPv6
[53] Evolución de Internet desde IPv4 a IPv6: David Fernández Cambronero (Departamento de Ingeniería de Sistemas Telemáticas ETSIT-UPM)
[54] Sacando partido a IPv6, con redes IPv4 Jordi Palet, CTO Consulintel
[55] Comunicaciones de Telefónica I+D (Telefónica Investigación y Desarrollo) Marzo 2005
[56] IPv6 UJI - Luis Peralta, Febrero 19 del 2002
[57] Cisco IPv6 Implementations and Transitions, June 2006
[58] Designing Internetworks with IPv6, Henrik Lund Kramshoj, April 28, 2002
[59] http://www.microsoft.com

- Permitir a hosts IPv4 e IPv6 interoperar
- Permitir a hosts y routers IPv6 desplegarse en Internet de forma incremental
- La transición debe ser tan sencilla como sea posible para usuarios finales, administradores de sistemas y operadores de red. Tanto como para comprenderla como para llevarla a cabo.

Los mecanismos de transición son un conjunto de mecanismos de protocolo implementados en hosts y routers junto con algunas indicaciones operacionales para direccionamiento y despliegue, diseñados de forma que se realice la transición con la menor disrupción posible.

Estos mecanismos incluyen

- Actualización y despliegue incremental. Hosts y routers IPv4 individuales pueden actualizarse sin necesidad de hacerlo simultáneamente
- Dependencias de actualización mínimas. El único prerrequisito para actualizar hosts a IPv6 es que el servidor DNS se actualice en primer lugar para poder manejar entradas con direcciones IPv6. No hay prerrequisitos para actualizar routers
- Fácil direccionamiento. Cuando hosts o routers IPv4 existentes se actualicen a IPv6 pueden continuar utilizando su dirección existente. No necesitan que se les asigne nuevas direcciones. Los administradores no tienen que idear nuevos planes de direccionamiento
- Bajo coste inicial. Es necesaria poca preparación para actualizar sistemas IPv4 a IPv6, Los mecanismos empleados para la transición incluyen:
- Una estructura de direccionamiento IPv6 que incluye direcciones IPv4 embebidas en direcciones IPv6, y codifica otra información utilizada por los mecanismos de transición
- Un modelo de despliegue en el cual los hosts y routers actualizados a IPv6 en una etapa inicial tienen capacidad "dual" (implementan pilas IPv4 e IPv6 completas)
- La técnica de encapsulamiento de paquetes IPv6 con cabeceras IPv4 para transportarlos sobre segmentos del camino en los cuales los routers todavía no han sido actualizados con IPv6.
- Técnicas de traducción de cabecera para permitir la introducción eventual de topologías de encapsulamiento que encaminen solo el tráfico IPv6, y el despliegue

que hosts que soporten IPv6. La utilización de esta técnica es opcional y podría ser utilizada en las ultimas fases o no ser utilizada en absoluto

Los mecanismos de transición de IPv6 aseguran que los hosts de ambos protocolos pueden interoperar en cualquier punto de Internet hasta que se agoten las direcciones Ipv4, y permite a los hosts Ipv6 e IPv4 de un ámbito limitado a interoperar indefinidamente después de esto. Esta característica garantiza la enorme inversión realizada en IPv4 y asegura que IPv6 no convierte a IPv4 en un protocolo obsoleto

Descripción de los mecanismos de transición
Las posibles transiciones pueden clasificarse de la siguiente forma:

- doble capa IP (dual stack)
- mecanismos de control tipo túnel: se basan en encapsular un protocolo sobre otro. Están enfocados a unir dos islas IpvX a través de un océano IPvY
- túneles manuales
- túneles automáticos
  - tuneles 6to4
  - tuneles 6over4
- mecanismos de traducción: se basan en traducir, en un elemento de red, los paquetes de un formato a otro
  - NAT-PT
  - SOCKSv5
  - BIS (Bump in the stack)

8.1 Doble Pila IP (dual stack)

El camino más lógico y evidente de transición es el uso simultáneo de ambos protocolos, en pilas separadas. Los dispositivos con ambos protocolos también se denominan "nodos IPv6/IPv4"; Mediante esta técnica se proporciona soporte IP completo para ambos protocolos de Internet tanto en hosts como en routers.

De esta forma, un dispositivo con ambas pilas pueden recibir y enviar tráfico a nodos que sólo soportan uno de los dos protocolos (nodos sólo IPv4 o sólo IPv6).

El dispositivo tendrá una dirección en cada pila. Se pueden utilizar direcciones IPv4 e IPv6 relacionadas o no, y se pueden utilizar mecanismos manuales o automáticos para la asignación de las direcciones (cada una correspondiente al protocolo en cuestión).

Como ya hemos explicado en el apartado de direcciones especiales IPv6, se pueden emplear la dirección IPv4 (32 bits), anteponiéndole 80 bits con valor cero y 16 bits con valor 1, para crear una dirección IPv6 "mapeada desde IPv4".

Es la forma más sencilla de que los nodos IPv6 sean compatibles con los nodos que disponen únicamente de IPv4. Los nodos que poseen pila dual tienen la capacidad de enviar y recibir paquetes IPv6 e IPv4. Pueden interoperar con nodos IPv4 utilizando paquetes Ipv4 y con nodos IPv6 utilizando paquetes IPv6.

La técnica de pila dual puede utilizarse en conjunto con las técnicas de tunneling IPv6 sobre IPv4.

- Configuración de direcciones: Dado que se proporcionan ambos protocolos, debe asignarse a los nodos con pila dual ambos tipos de direcciones. Pueden utilizar para ello las técnicas típicas de uno u otro protocolo (Ejemplo: DHCP para IPv4 o autoconfiguración de direcciones sin estado para IPv6)
- DNS: Los nodos con capacidad dual deben de proporcionar librerías de resolución con capacidad para tratar con registros "A" IPv4 así como con registros "AAAA" y "A6"; Es decir el DNS podrá devolver la dirección IPv4, la dirección IPv6, o ambas.

8.2 Mecanismos de Tunneling

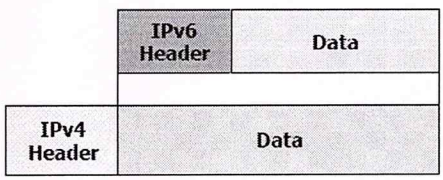
Proporcionan una forma de utilizar la estructura de routing IPv4 para transportar trafico IPv6.

Los túneles se clasifican según el mecanismo por el que el nodo que realiza el encapsulado determina la dirección del nodo extremo del túnel. En los dos primeros casos (router a router y host a router), el paquete IPv6 es tunelizado a un router.

El extremo final de este tipo de túnel, es un router intermedio que debe desencapsular el paquete IPv6 y reenviarlo a su destino final. En este caso, el extremo final del túnel es distinto del destino del destino final del paquete, por lo que la dirección en el paquete IPv6 no proporciona la dirección IPv4 del extremo final del túnel.

La RFC 2893 define la utilización básica de túneles La RFC 2893 define la utilización básica de túneles como mecanismo para transportar paquetes IPv6 como mecanismo para transportar paquetes IPv6 sobre redes IPv4 sobre redes IPv4.

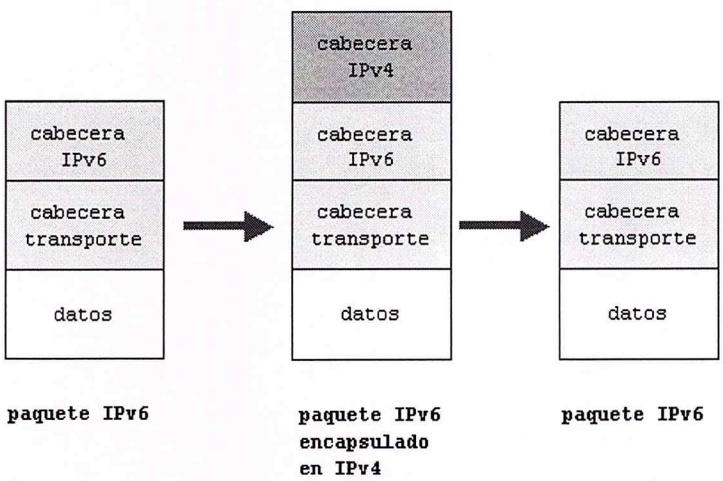
Los datagramas IPv6 se encapsulan sobre datagramas IPv4 para atravesar redes que aun no han sido migradas.



Los túneles se utilizan frecuentemente en las redes. Los túneles se utilizan frecuentemente en las redes actuales: actuales: Ej: MBONE, transporte multiprotocolo (IPX, : MBONE, transporte multiprotocolo (IPX, Appletalk Appletalk, etc etc) sobre redes IP, sobre redes IP, movilidad IP, IP, etc.

La dirección del extremo final del túnel ha de ser determinada a través de información de configuración en el nodo que realiza el túnel. Es lo que se denomina "túnel configurado", describiendo aquel tipo de túnel donde el extremo final del túnel es explícitamente configurado.

Los túneles proporcionan un mecanismo para utilizar las infraestructuras IPv4 mientras la red IPv6 esta siendo implantada. Este mecanismo consiste en enviar datagramas IPv6 encapsulados en paquetes IPv4.



Los extremos finales del túnel siempre son los responsables de realizar la operación de encapsulado del paquete/es IPv6 en IPv4.

Los hosts y routers pueden encapsular datagramas IPv6 en regiones con topología de routing IPv4. El tunneling puede utilizarse en diferentes escenarios:

- router a router
- host a router
- host a host
- router a host

En cualquiera de los casos se crea un túnel que comprende parte o la totalidad de la extensión del camino que toman los paquetes IPv6.

Las técnicas de encapsulamiento se clasifican generalmente en funciona del mecanismo de determinación de la dirección del nodo del final del túnel.

Los extremos finales del túnel siempre son los responsables de realizar la operación de encapsulado del paquete IPv6 en IPv4.

Estos túneles pueden ser utilizados de formas diferentes:

- **Router a router.** Routers con doble pila (IPv6/IPv4) se conectan mediante una infraestructura IPv4 y transmiten tráfico IPv6. El túnel comprende un segmento que incluye la ruta completa, extremo a extremo, que siguen los paquetes IPv6.
- **Host a router.** Hosts con doble pila se conectan a un router intermedio (también con doble pila), alcanzable mediante una infraestructura IPv4.

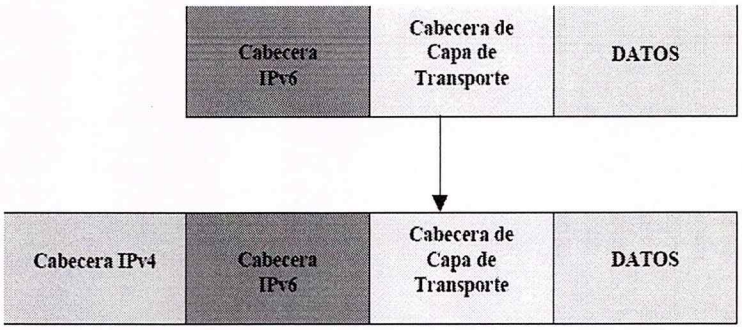
El túnel comprende el primer segmento de la ruta seguida por los paquetes.

En el caso del escenario router a router y host a router, el paquete IPv6 se envía mediante un túnel a un router. En este caso el fin del túnel es diferente del destinatario del paquete IPv6 que va por él, de forma que las direcciones del paquete transmitido mediante el túnel no proporcionan la dirección del destino del paquete, esta debe ser determinada mediante de configuración proporcionada en el modo que crea el túnel Se utiliza el termino "tunneling configurado o manual" para describir el tipo de tunneling en el cual el punto final se configura de forma explicita.

En los casos (host a host y router a host), el paquete IPv6 es tunelizado, durante todo el recorrido, a su nodo destino. El extremo final del túnel es el nodo destino del paquete, y

por tanto, la dirección IPv4 está contenida en la dirección IPv6. Este caso se denomina "túnel automático".

El "desencapsulado", en el extremo final del túnel, realiza la función opuesta, lógicamente.



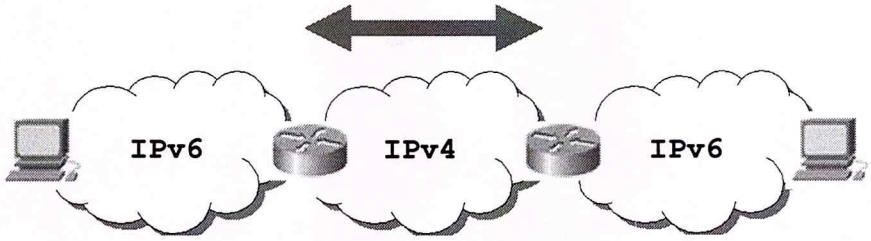
- **Host a host.** Hosts con doble pila interconectados por una infraestructura IPv4. El túnel comprende la ruta completa que siguen los paquetes.
- **Router a host**. Routers con doble pila que se conectan a hosts también con doble pila. El túnel comprende el último segmento de la ruta.

En los dos últimos casos de tunneling, host a host y router a host, el paquete IPv6 se transmite mediante un túnel toda la extensión hasta su destino final. En este caso, la dirección de destino tanto del paquete IPv6 como de la cabecera de encapsulación IPv4 identifica al mismo nodo. Este hecho permite que se pueda obtener la dirección IPv4 de destino de forma automática. En este hecho se basa la técnica de tunenling automático, la cual utiliza un formato de direcciones Ipv6 con direcciones Ipv4 embebidas que permiten a los nodos que se realizan el tunneling obtener automáticamente la dirección IPv4 de destino, eliminando la necesidad de configurar de forma explicita la dirección del punto final del túnel, simplificando así la configuración.

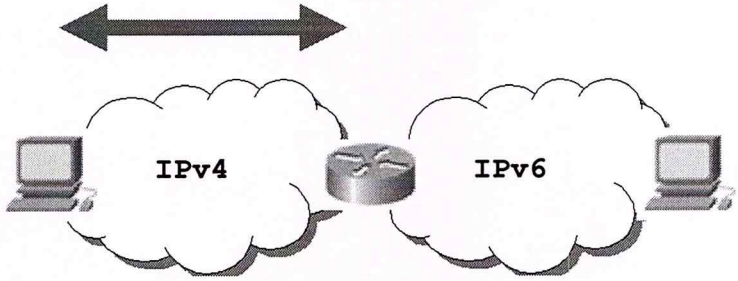
Nota: Cuando un host o router recibe un datagrama IPv4 con destino una de sus direcciones IP, y su valor del campo de protocolo es 41 (correspondiente a tipo de carga Ipv6), reensambla el paquete (en caso de que haya sido fragmentado), elimina la cabecera IPv4 y envía el datagrama al código de nivel IPv6.

Tipos de Túneles

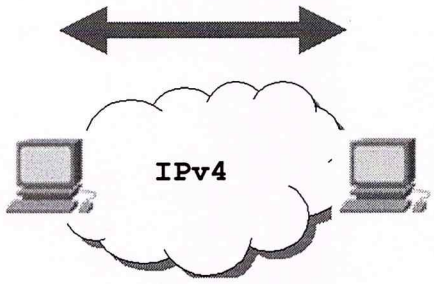
router to router, interconexión de islas Ipv6 a través de redes IPv4



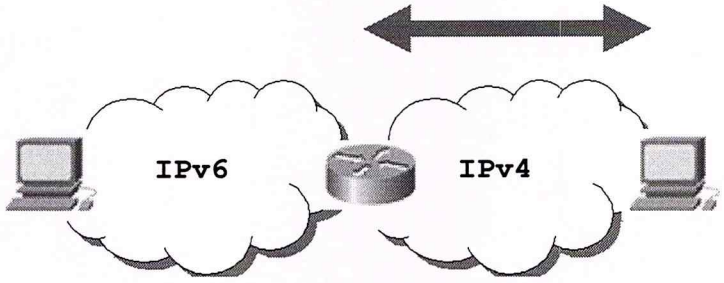
host-to-router, útil para conectar sistemas IPv6 aislados (ej. sin routers IPv6 locales)



host-to-host, sistemas IPv6 aislados



router-to-host, sistema destino sin router IPv6 local

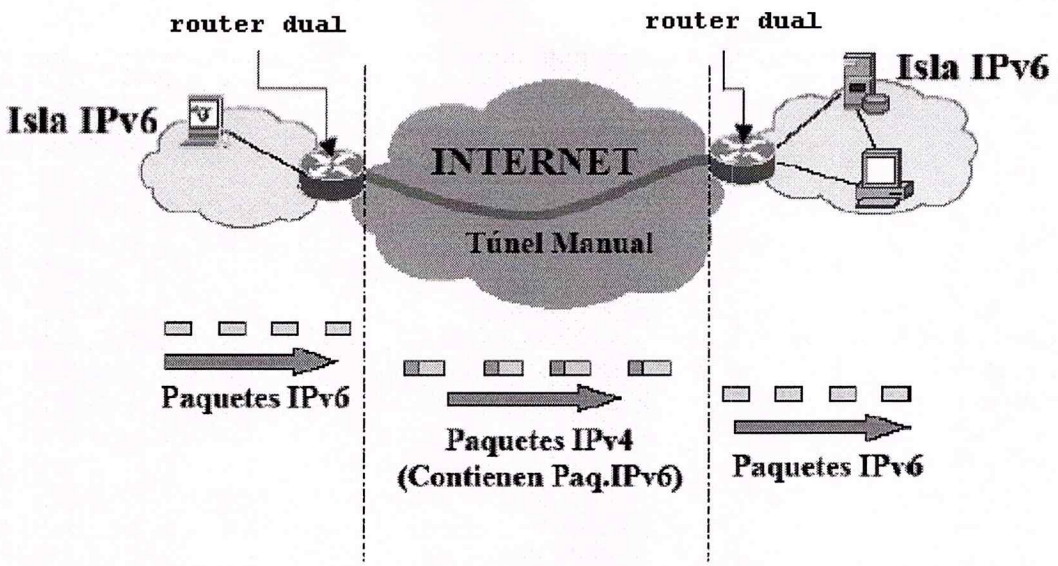


8.3 Configuración de encapsulamiento manual

Consiste en un túnel IPv6 en el cual la dirección del punto final Ipv4 esta determinada por información de configuración del nodo que realiza el encapsulamiento

Características:

- Su funcionalidad principal radica en interconectar islas IPv6 a través de un océano IPv4
- Cada extremo es un nodo dual y en ellos se configuran las direcciones IPv4 e IPv6 tanto local como remotas



En este caso la dirección del extremo del túnel viene determinada por la información de configuración del nodo que realiza la encapsulación, este debe almacenar la dirección extremo para cada túnel. Esto se realiza generalmente mediante la tabla de ruteo, la cual direcciona los paquetes basándose en su dirección de destino y utilizando la mascara de prefijo.

Hots IPv6/IPv4 conectados a enlaces que no disponen de un router IPv6 pueden utilizar un túnel manual para alcanzar a un router IPv6. Este túnel permite a los hosts comunicarse con el resto de Internet IPv6. (Nodos con direcciones nativas IPv6).Si se conoce la dirección IPv4 de un router de borde IPv6/IPv4 del backbone IPv6, puede utilizarse como dirección extremo del túnel

Como ventajas de este método se pueden citar las siguientes:

- se utiliza con frecuencia en el acceso al 6-bone y esta disponible en multitud de plataformas (Cisco, Linux, Solaris, Windows, etc.)
- es un método transparente al nivel IPv6 y superiores, con lo cual no afecta a las aplicaciones
- No consume execivo recursos (la MTU se reducen en 20 bytes de la cabecera IPv4 típica)
- Su aplicación principal es la conexión con ISP IPv6 remotos a través de Internet

Como desventajas de este método se pueden citar las siguientes

- No son dinámicos, deben establecerse manualmente o de forma semiautomática
- Si se unen N islas y no se considera un nodo central que realice el intercambio, el numero de túneles a establecer en cada sitio asciende a N-1, no siendo escalable

Existe una herramienta de gestión del establecimiento de túneles manuales: Túnel Broker

"Tunnel Server" y "Tunnel Broker": El documento draft-ietf-ngtrans-broker-02.txt sienta las bases para aplicaciones que permiten utilizar, de forma libre y gratuita, nuestras direcciones IPv4 actuales, sobre las infraestructuras IPv4, para acceder a redes y sitios IPv6.

Estos mecanismos se hacen indispensables para labores de investigación, dado que se requieren direcciones IPv6 y nombres DNS permanentes.

La diferencia con el mecanismo "6to4" es que el "Tunnel Broker" no requiere la configuración de un router.
Se trata de ISP's IPv6 "virtuales", proporcionando conectividad IPv6 a usuarios que ya tienen conectividad IPv4.

El "tunnel broker" es el lugar donde el usuario se conecta para registrar y activar "su túnel". El "broker" gestiona (crea, modifica, activa y desactiva) el túnel en nombre del usuario.

El "tunnel server" es un router con pila doble (IPv4 e IPv6), conectado a Internet, que siguiendo órdenes del "broker" crea, modifica o borra los servicios asociados a un determinado túnel/usuario.

El mecanismo para su configuración es tan sencillo como indicar, en un formulario Web, datos relativos al S.O., la dirección IPv4, un "apodo" para la máquina, y el país donde esta conectada. El servidor de túneles crea los registros DNS, el extremo final del túnel, y genera un script para la configuración del cliente.

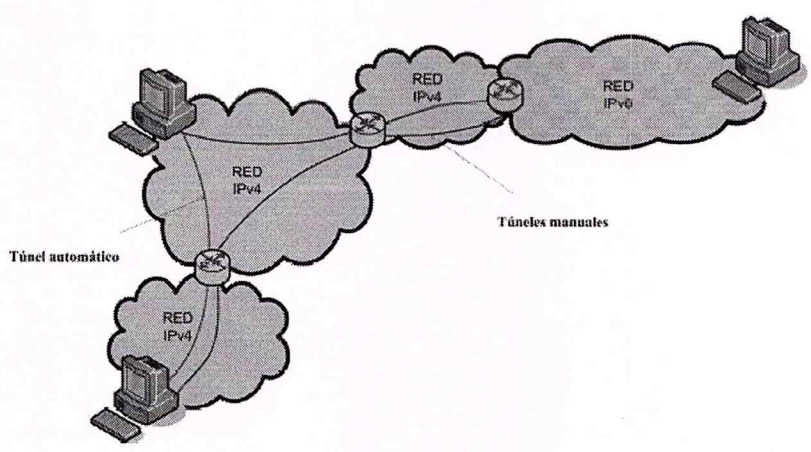
8.4. Configuración de Encapsulamiento Automático

Consiste en un túnel IPv6 sobre Ipv4 en el cual la dirección el punto final Ipv4 esta determinada por la dirección IPv4 embebida en la dirección de destino compatible IPv4 del paquete IP enviado al túnel.

Características principales de este método de encapsulación son:

- Permitir a nodos duales comunicarse a través de una infraestructura IPv4
- Hace uso de las direcciones IPv6 compatibles con IPv4
- Los paquetes destinados a direcciones compatibles IPv4 se envían por el túnel automático
- Se define una interfaz virtual para la dirección compatible IPv4
- Los paquetes destinados a direcciones compatibles IPv4 se envían por el túnel automático con las siguientes reglas
  - La dirección origen IPv6 es una dirección compatible IPv4 local
  - La dirección de destino IPv4 se obtiene de la dirección compatible IPv4

Pueden utilizarse tanto túneles automáticos como manuales en hosts aislados (sin routers IPv6 en el enlace).



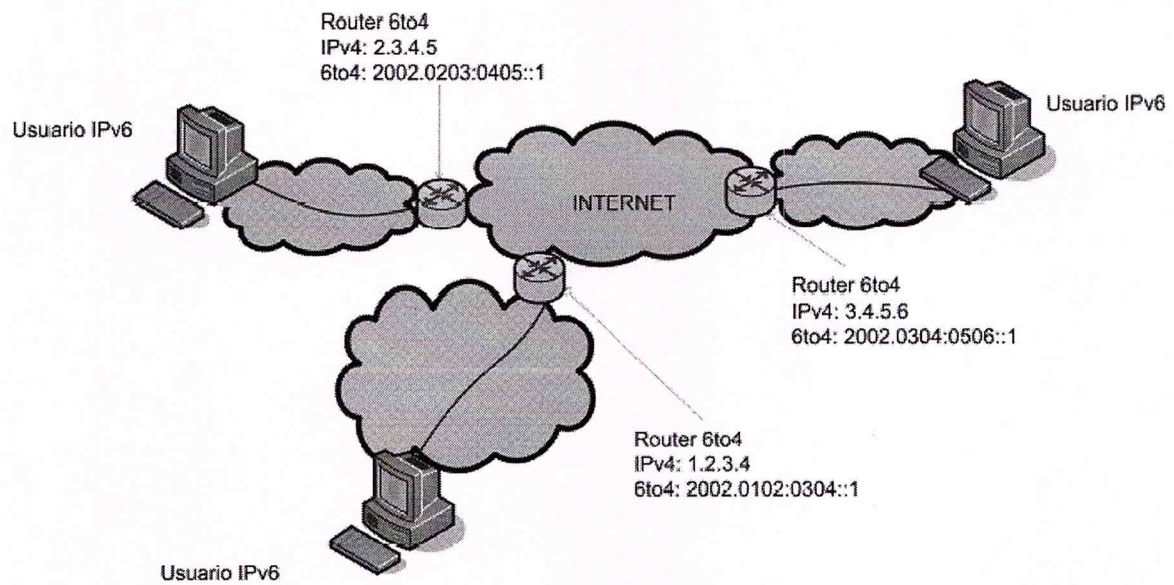
El tunneling automático, la dirección del extremo del túnel se determina del paquete a ser enviado. Si la dirección IPv6 es compatible IPv4, el paquete puede enviarse mediante tunnelin automático, si se trata de una dirección nativa IPv6, el paquete no puede enviarse mediante tunneling IPv6.

En lo túneles automáticos la dirección del extremo del túnel viene determinada por la dirección de destino compatible IPv4 del paquete a IPv6 a enviar por el túnel. Esta forma de encapsulamiento permite a los nodos IPv6/Ipv4 comunicarse sobre la infraestructuras de routing sin tuneles preconfigurados.

8.5. Configuración de encapsulamiento 6to4

Su aplicación principal es unir islas IPv6 dispersas en un océano IPv4.

A cada isla se le asigna un prefijo IPv6:2002::/16+Dir Ip del router frontera. El siguiente salto IPv4 esta contenido en la dirección IPv6. El routing entre las distintas islas se apoya en el routing Ipv4 subyacente.



Como ventajas pueden citarse:

- Al igual que los tuneles manuales son transparentes a nivel IPv6, no afectando a las aplicaciones:
- Se trata de tuneles establecidos dinámicamente y sin configuración previa
- Dadas N islas IPv6, solo se establecen los tuneles necesarios para las conexiones activas en cada momento.

El inconveniente principal radica en que las organizaciones que se conecten a un ISP IPv6 remoto no necesitan mas de un túnel (quizás dos por redundancia con otro ISP IPv6), por lo que se puede emplear un mecanismo de tuneles manuales, que se haya mas extendido.

8.6. Configuración de un encapsulamiento 6over4

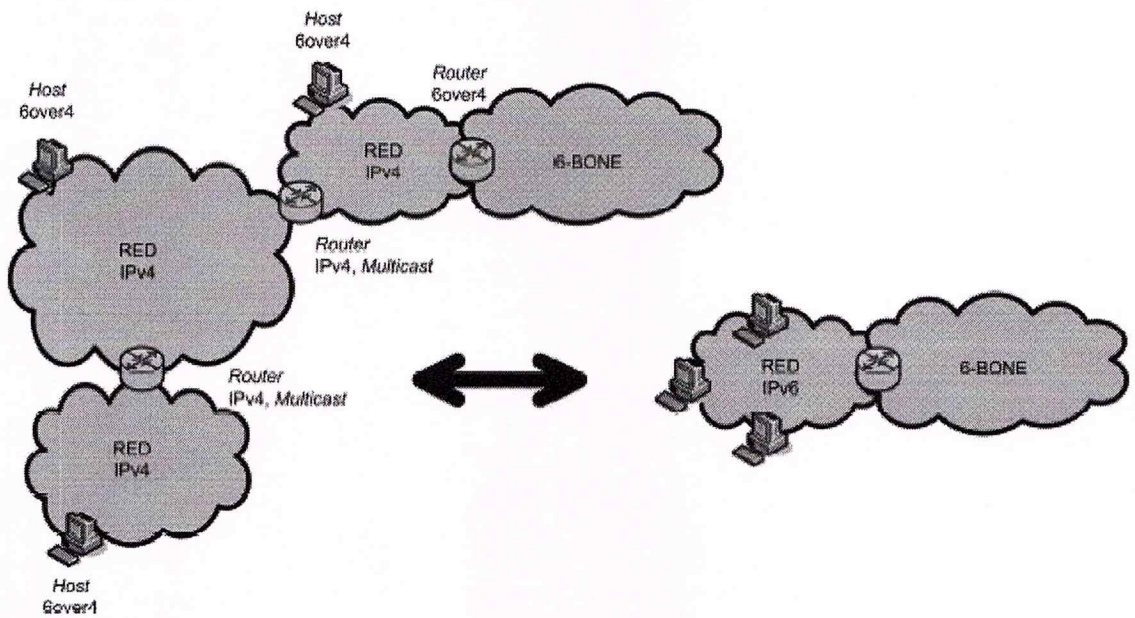
Consiste en encapsular paquetes IPv6 en cabeceras IPv4 de forma que se puedan enrutar a través de estructuras IPv4.

Se trata de un mecanismo utilizado por las direcciones compatibles IPv4 para encapsular automáticamente paquetes IPv6 sobre redes IPv4.

Se trata de tuneles punto a punto hechos encapsulando paquetes IPv6 con cabeceras IPv4, que les permitan ser enrutados sobre infraestructuras IPv4.

Sus características principales son las siguientes:

- Conectan nodos IPv6 dispersos en subredes IPv4, se forma una "LAN virtual" IPv6.
- El trafico IPv6 entre nodos es encapsulado en IPv4
- Los procesos de descubrimiento de vecinos (CDP) y router se realizan empleando multicast
- Si se dispone de un router 6over4 con acceso al 6-bone tendremos que todos los nodos pueden acceder al 6-bone.



Como ventajas destacan:

- Son transparentes al nivel IPv6, no afectando a las aplicaciones
- Son tuneles establecidos dinámicamente y sin configuración previa
- Permiten probar Ipv6 en nodos de una red corporativa IPv4 sin instalar Ipv6 en los routers internos
- Instalando en un único router la pila IPv6 y conectándolo al 6-bone se proporciona acceso a la red al resto de nodos IPv6.

Como inconveniente destacan:

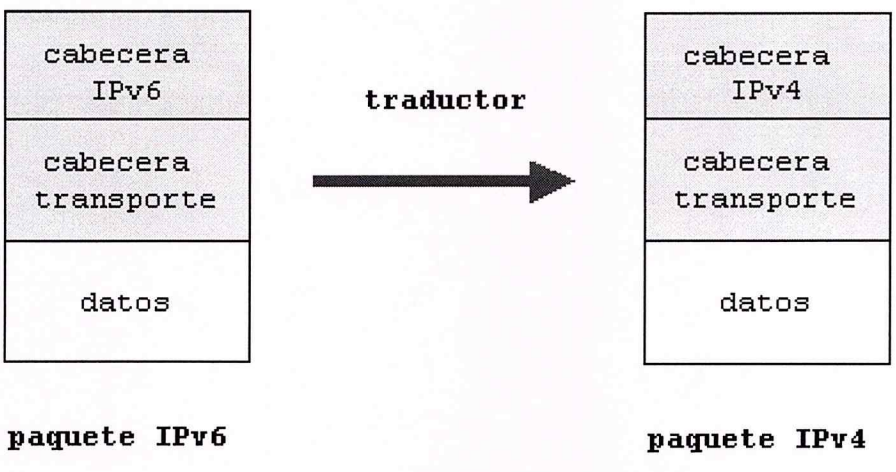
- Es un mecanismo adecuado para redes finales únicamente
- No esta ampliamente implementado

8.7. Tunneling multicast IPv4

Tunneling IPv6 sobre IPv4 en el cual la dirección del punto final IPv4 esta determinada mediante el procedimiento Descubriendo de Vecino (Neihbor Discovery). A diferencia del tunneling configurado no necesita configuración de direcciones y a diferencia del tunneling automático no requiere del uso de direcciones compatibles con IPv4. Sin embargo, el mecanismo asume que la infraestructura IPv4 soporta multicast IPv4.

8.8. Mecanismos de Traducción

Se basan en traducir en un elemento de red los paquetes de un formato a otro.

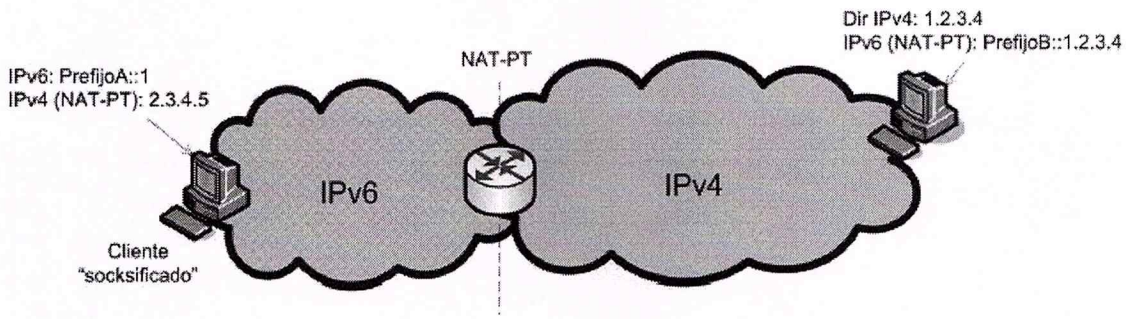


8.9. NAT-PT

Características principales: En los mecanismos de NAT tradicionales se realiza la traducción de direcciones (conexión de redes con direccionamiento IPv4 privado). En el caso de NAT-IP se realiza además la traducción de protocolo. Esta está basada en el algoritmo SIIT (RFC 2765).

Debe tenerse en cuenta que no es transparente al nivel de aplicación precisando de alunas extensiones

- DNS-ALG: transforma peticiones DNS "A" a peticiones "AAAA"
- FTP-ALG: las conexiones con FTP son problemáticas pues abren dos conexiones TCP intercambiando direcciones IP a nivel de aplicación.



Como ventajas cabe citar:

- Muchas redes corporativas poseen experiencia en la gestión/administración de NATs
- Implementando en la mayor parte de los router y en algunas plataformas habituales en nodos finales (Windows 2000)
- Si la comunicación extremo a extremo es hétero (IPvX-IPvY) NAT-PT resulta adecuado (teniendo en cuenta siempre la carga de trabajo prevista)

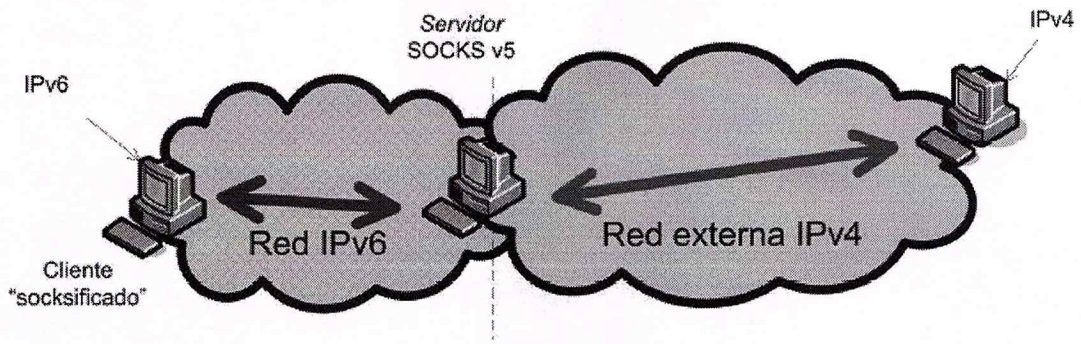
Como inconveniente resaltan:

- Los NATs poseen un alto coste de gestión/administración
- El proceso de traducción es mas costoso en recursos que el de encapsulamiento
- Si la comunicación extremo a extremo es homogénea (IPvX-IpcX) siempre es preferible emplear tuneles a dos sistemas de traducción consecutivos
- Si en un protocolo de aplicación se intercambian direcciones IP (DNS, FTP, etc.), es necesario una extensión o modulo que incluya un algoritmo para su tratamiento especifico (DNS-ALG, FTP-ALG)

8.10. SOCKSv5

El uso tradicional de SOCKSv5 es proporcionar conectividad IP directa a Internet en redes con firewall en determinados hosts. En este caso se hace uso de un servidor SOCKSv5 dual, que realiza además la función de traductor de protocolos (Algoritmos SIIT):

- Traducción IPv4-IPv6 y viceversa. Conexiones siempre iniciadas por el cliente
- Dos componentes: Servidor SOCKSv5+Librería SOCKSv5 (cliente)



Funcionamiento detallado: (Red IPv4 = Red interna)

- Una aplicación en el nodo cliente inicia una conexión TCP o UDP con un nodo externo empleando el nombre completo (FQDN)
- La librería SOCKSv5 en el cliente intercepta la resolución del nombre ("gethosname") e inicia una conexión TCP al puerto 1080 del servidor SOCKSv5.
- El servidor SOCKSv5 devuelve al cliente una dirección IPv4 falsa ("fake IPv4 address")
- El servidor SOCKSv5 inicia la conexión TCP o UDP con el nodo remoto y hace de proxy entre el cliente y el nodo externo. Si el nodo externo es IPv6, aplica además el algoritmo de traducción SIIT.
- En el cliente, los paquetes con la dirección IPV4 falsa como origen o destino son interceptados y tratados por la librería SOCKSv5 que los recibe o envía respectivamente al servidor SOCKSv5.

Como ventajas destacan:

- Se trata de un sistema apto para empresas que deseen dar acceso a determinados nodos internos a servicios IPv6 in probar exhaustivamente el protocolo
- Provee sistemas de autenticación adecuados para evitar usos indeseados

Presenta los siguientes inconvenientes:

- Necesidad de instalación de las librerías SOCKSv5 en todos los clientes a los que se desee dar acceso.
- El proceso de traducción es costoso en cuanto a consumo de recursos en el servidor, por lo que un factor limitante es la carga de tráfico prevista.
- Las conexiones solo pueden ser iniciadas por los nodos internos, con lo cual no es posible ofrecer servicios al exterior mediante este método
- Como todos los mecanismos de traducción debe incorporar algoritmos específicos para aquellos protocolos de aplicación que intercambien direcciones IP (FTP).

8.11. Estrategias de Migración

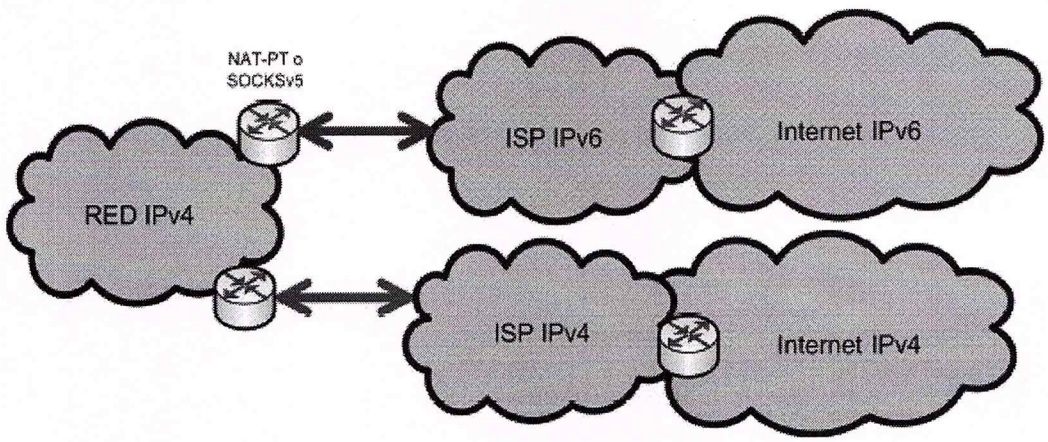
En general debe estudiarse la migración de las redes finales primero y, según aumente el trafico IPv6 realizar la migración de ISPs y backbones principales.

Para redes finales pueden seguirse las siguientes recomendaciones

- Servidores: "doble pila", para atender peticiones IPv4 e IPv6
- Clientes: "doble pila", conectividad con servidores IPv4 e IPv6

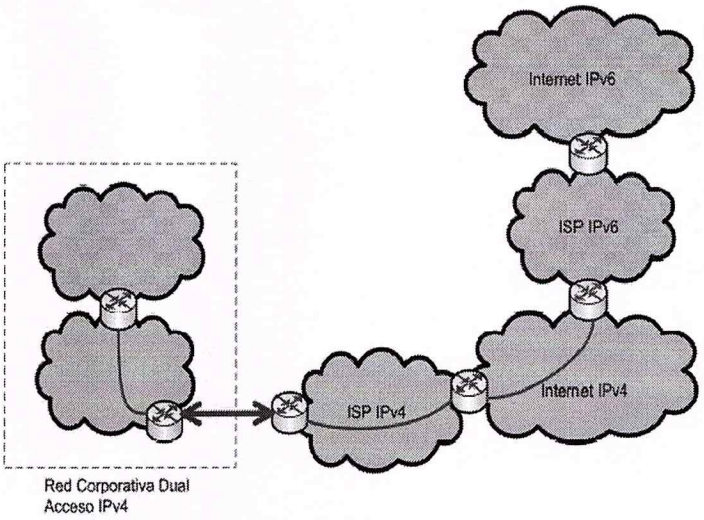
8.12. Mecanismos de migración de redes finales (clientes y servidores)

Migración mediante mecanismos de traducción



8.13. Migración mediante mecanismos de tunneling

- Primera fase: Conexión IPv4 al ISP y enviar el trafico IPv6 mediante un túnel sobre iPv4, hasta que el ISP ofrezca conexión con IPv6 nativo



- Segunda fase: Conexión IPv6 al ISP y túnel IPv4 sobre IPv6 para conectar IPv4 (caso complementario)

8.14. Estrategias de Transición (RFC1933)

La clave para la transición es la compatibilidad con la base instalada de dispositivos IPv4. Esta afirmación define un conjunto de mecanismos que los hosts y routers IPv6 pueden implementar para ser compatibles con host y routers IPv4.

Estos mecanismos permitirán usar infraestructuras IPv4 para IPv6 y viceversa, dado que se prevé que su uso será prolongado, e incluso indefinido en muchas ocasiones.

8.15. Estrategias de migración para ISPs

Estrategias de migración para ISPs:

- Conexión nativa a backbone IPv4 e IPv6, sin emplear tuneles
- Modos de acceso
  - ISP IPv4 tradicionales: Acceso IPv4 y tratar de ofrecer acceso a internet IPv6 mediante un traductor
  - Nuevos ISP IPv6: Acceso a IPv6 y mediante túnel a través de Internet. Ofrecer conectividad a Internet IPv4 mediante traductores

8.16. Estrategia de migración de backbones

- Mantener configuración actual y migrar cuando el trafico entunelado sea mayor que el trafico IPv4
- Debido a los problemas del numero de rutas existente, recomendar y colaborar con los ISP y otros backbone para evitar una migración forzosa

8.17. Conexión de dominios IPv6 sobre redes IPv4

El documento draft-ietf-ngtrans-6to4-04.txt nos indica un mecanismo comúnmente denominado "6 to 4", para asignar un prefijo de dirección IPv6 a cualquier sitio que tenga al menos una dirección IPv4 pública.

De esta forma, dominios o hosts IPv6 aislados, conectados a infraestructuras IPv4 (sin soporte de IPv6), pueden comunicar con otros dominios o hosts IPv6 con una configuración manual mínima.

Este mecanismo funciona aún cuando la dirección IPv4 global (pública) es única y se accede a la red mediante mecanismos NAT (Network Address Translation), que es el caso más común en las redes actuales para el acceso a Internet a través de ISP's.

8.17.1. Otros mecanismos de transición

Estas técnicas pueden ser utilizadas incluso de forma combinada. Se esta trabajando en varios mecanismos alternativos y modificaciones a los aquí expuestos, a través de los borradores draft-ietf-ngtrans-mech-06.txt

draftietf-ngtrans-translator-03.txt

draft-ietf-ngtrans-socks-gateway-04.txt

draft-ietfngtrans-dstm-01.txt

draft-ietf-ngtrans-tcpudp-relay-00.txt

draft-ietf-ngtranshometun-00.txt

draft-ietf-ngtrans-ipv4survey-00.txt

RFC 2893 "Transition Mechanism for IPv6 for Hosts and Routers", R. Gilligan, E. Nordmark, Agosto 2000

"IPv6; Mecanismos de Transición IPv4-IPv6", Carlos Ralli Ucendo. Telefonica I+D

9. SEGURIDAD EN EL PROTOCOLO IPv6

9.1. Estrategia de Seguridad

La integración de la seguridad en IP es uno de los trabajos más espinosos que ha tenido que afrontar el (IETF)[60]. La necesidad de autenticación, integridad de datos y confidencialidad es inmediata y de amplio uso. La estrategia de seguridad es:

- Promover la intercomunicación, empezar con mecanismos bien conocidos y ya implantados para la autenticación, integridad y confidencialidad.
- Diseñar un marco de seguridad que haga posible cambiar a otros mecanismos.

Los mecanismos iniciales seleccionados son:

- Clasificación de mensajes 5 (MD5 - Message Digest 5) para la autenticación e integridad de datos [61]
- Cifrado simétrico con el modo de Encadenamiento de bloques de cifrado del Estándar de cifrado de datos de Estados Unidos (**CBC-DES**)[62] para la confidencialidad.

Se puede usa clave pública para la distribución de claves.

9.2. Escenarios de Seguridad [63]

Existen muchas formas de usar las funciones de seguridad que se describirán mas adelante. Veamos algunos escenarios para entender, al menos, algunas de las posibilidades.

- **Escenario 1:** La compañía XYZ quiere salvaguardar sus comunicaciones internas cliente/servidor. Quieren eliminar la posibilidad de que alguien pueda comprometer sus datos falsificando las direcciones de origen o alterando los datos en tránsito.
- **Escenario 2:** Hay un administrador de la compañía XYZ quien copia archivos muy sensible entre distintos host. Sólo este administrador tiene permiso para realizar estas transferencias. También es importante evitar una escucha no autorizada de estos datos y un uso posterior de los mismos.
- **Escenario 3:** La compañía XYZ conecta su división de fabricación a su oficina remota mediante Internet. La compañía desea que todas las comunicaciones sean opacas respecto al mundo exterior.

---

[60] http://www.ietf.org Internet Engineering Task Force
[61] Actualmente, hay un problema cuando se usa MD5 con comunicaciones de muy alta velocidad, debido al tiempo necesario para realizar los cálculos.
[62] http://www.nsa.gov
[63] CISCO CCNA IPv6 IpSec transition

Por simplicidad, se puede pensar que los clientes y servidores tienen una única interfaz y una única dirección de IP. Sin embargo, todos los mecanismos de seguridad siguen funcionando cuando el sistema tiene múltiples interfaces y múltiples direcciones IP.

9.2.1. Escenario 1

La tecnología de clasificación de mensajes se usa para satisfacer los requisitos del escenario 1, es decir, autenticar a los emisores y detectar si se han modificado los datos. La clasificación de mensajes funciona de la siguiente manera:

- El origen y el destino conocen una clave secreta.
- El origen realiza un cálculo usando la clave secreta como entrada.
- El origen envía la respuesta con los datos
- El destino realiza el mismo cálculo y compara las respuestas.

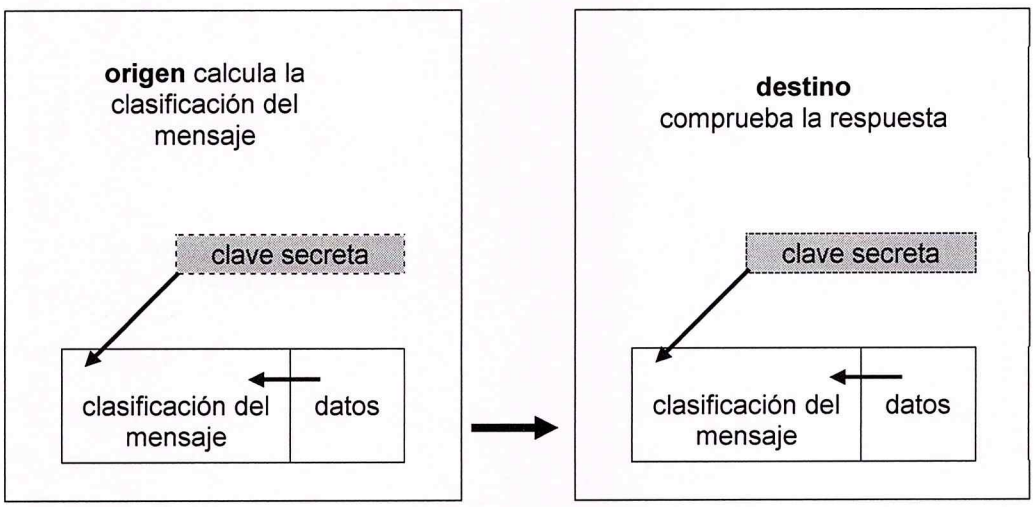


Figura: Uso de la clasificación de mensajes

Configuración de la información de autenticación en el escenario 1

Suponga que la compañía XYZ tiene un servidor importante en la dirección IP 130.15.20.2 El administrador de seguridad del servidor identifica los host clientes y asigna una clave secreta de autenticación a cada dirección IP del cliente.

El servidor necesita almacenar esta información de seguridad. Para almacenar estos parámetros de seguridad se puede emplear una tabla como la que se muestra en la Tabla La tabla tiene un índice que es el número asignado a cada host cliente, más

formalmente, el número se denomina el índice de parámetros de seguridad (Security Purameters index), o SPI[64]

Por supuesto, se necesita configurar cada cliente con el Índice de parámetros de seguridad y la clave secreta que debe usar cuando acceda al servidor. En la Tabla XX se muestran los datos de configuración del segundo cliente. Observándose que el cliente necesita entradas distintas para cada destino al que accede.

¿Qué ocurre cuando un host cliente quiere enviar un datagrama autenticado al servidor?

- El cliente busca la dirección IP destino en su tabla
- Se usa la clave de autenticación para calcular la clasificación
- Se pone el numero de SPI y la clasificación del mensaje en la cabecera de autentificación
- Se envía el datagrama

SPI (host client)	source IP address	client authentication key	client authentication method
301	130.15.24.4	X`2E-41-43-11-5A-5A-74-53-E3-01-88-55-10-15-CD-23	MD5
302	**130.15.60.10**	**X`35-14-4F-21-2B-2C-12-34-82-22-98-44-C0-1C-33-56**	**MD5**
...	...	...	...

Tabla: Información de seguridad en el destino 130.15.20.2

Cuando el servidor recibe el datagrama:

- El servidor usa el SPI de la cabecera de autenticación para buscar la entrada del cliente en la tabla.
- Se compara la dirección IP de origen del mensaje (source IP address) con la dirección de origen de la tabla.
- Se calcula la clasificación del mensaje usando la clave de autenticación de la entrada de la tabla (client authentication key)
- Se compara la respuesta con el valor de la cabecera de autenticación.

[64] Si el servidor tiene múltiples direcciones IP, la tabla tiene como índice la dirección IP destino

Asociación de seguridad en un sentido

Debe tenerse en cuenta que únicamente se ha realizado la mitad del trabajo. Se ha establecido la autenticación en sólo una dirección. Se autentican los datagramas que envía el cliente al servidor.

Se dice que la información que se ha descrito define una Asociación de seguridad en un sentido. En ambos extremos, el origen y el destino, la combinación de la dirección IP de destino de esta asociación y el SPI son suficientes para identificar la entrada a usar. Por tanto. Una Asociación de seguridad se corresponde con un destino y un SPI.

target IP address	SPI	client IP address	client authentication key	client authentication method
130.15.20.2	**302**	**130.15.60.10**	**X`35-14-4F-21-2B-2C-12-34-82-22-98-44-C0-1C-33-56**	**MD5**
130.15.65.4	...	...	...	...

Tabla: Información de seguridad en el origen 130.15.60.10.

Para autenticar los datos que van desde el servidor al cliente, se necesita un conjunto de distintas entradas en la tabla que definan las claves de autenticación de la Asociación de seguridad de la dirección inversa. Es decir, cada host necesita:

- Una tabla de seguridad cuando el host es el origen de los datagramas.
- Otra tabla de seguridad cuando el host es el destino de los datagramas.

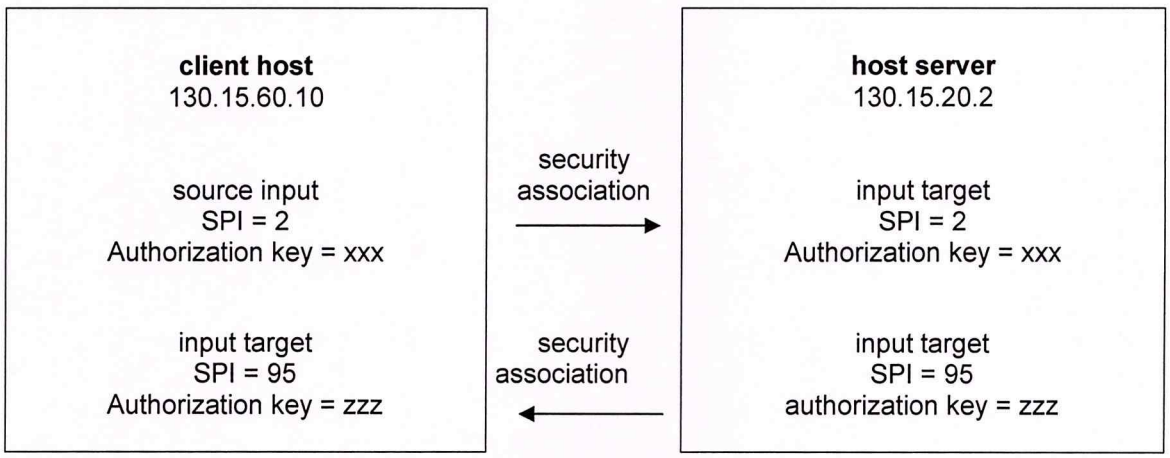


Figura: se muestra un par de Asociaciones de seguridad.

¿Cuántas claves de autenticación?

¿Cuántas claves de autenticación necesita usar un servidor cuando envía datagramas a sus clientes? Intuitivamente, parecería natural asignar a un servidor una única clave de autenticación MD5, que usaría para decir a sus clientes «Soy el servidor y ...».

Pero en ese caso, todos los clientes conocerían la clave. Un cliente podría usar una dirección IP falsa y sustituir al servidor para evitar que esto ocurra, se debería de asignar una clave de autenticación distinta para cada host cliente. El número total de claves se puede reducir usando la misma clave para la autenticación en el sentido cliente a servidor y para el sentido servidor a cliente.

9.2.2. Escenario 2

En el escenario 1, la seguridad se imponía en el nivel del host. Pero suponga que hay un usuario o un rol que requiere un nivel de seguridad diferente. El marco de seguridad se ofrece según la sensibilidad del usuario, el rol o la información.

Suponga que el host cliente que se ha tratado en el escenario 1 es un sistema multiusuario. Para el escenario 2, para los usuarios normales del host cliente 130.15.60.10 es suficiente una clave de autenticación por host. Sin embargo, la transferencia de archivos del administrador del sistema hacia el servidor necesita una autenticación especial y se necesita cifrar. En la Figura 24.3 se muestran las Asociaciones de seguridad creadas.

Viendo las tablas de las asociaciones de seguridad cuando se añaden entradas adicionales para el administrador con sus claves de cifrado. En la siguiente tabla (XX) se muestra la información de destino en el servidor y en la Tabla 24.4 la información de origen en el cliente.

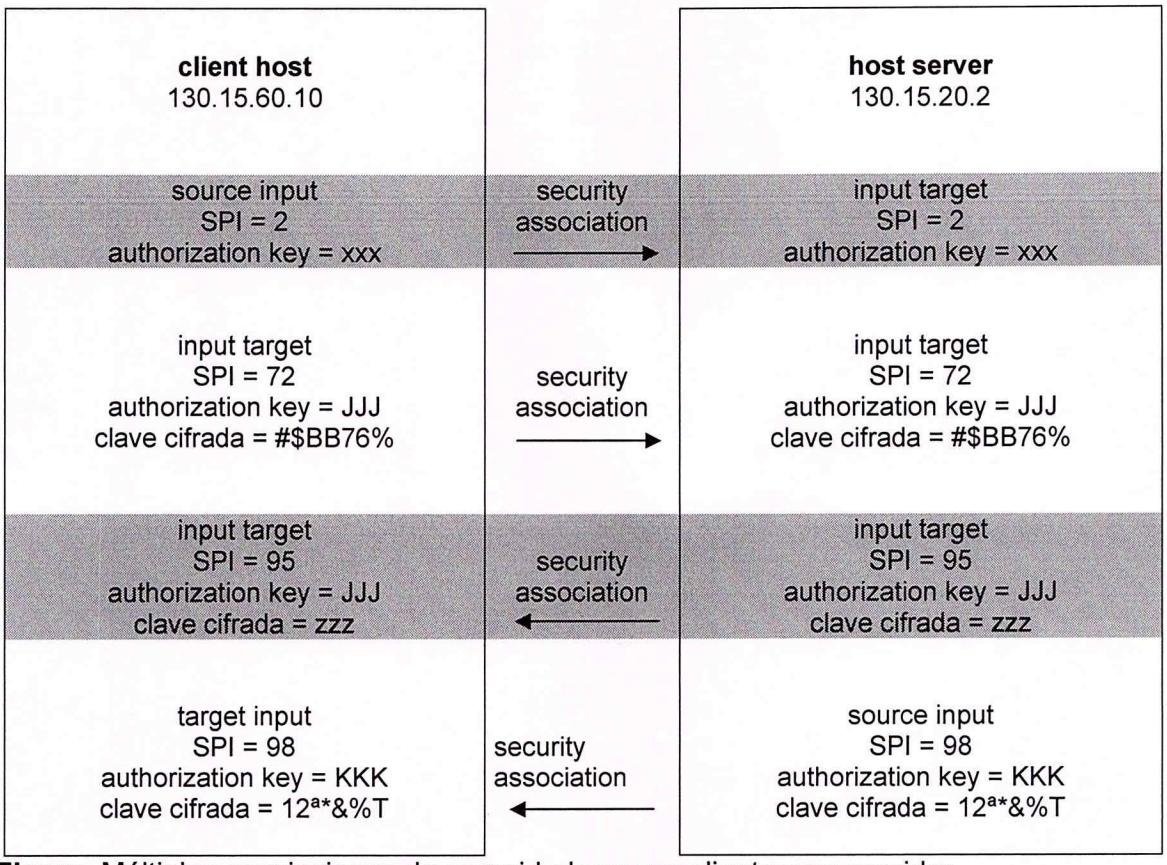


Figura Múltiples asociaciones de seguridad para un cliente y un servidor.

Ahora hay SPI distintas para los usuarios normales en 130.15.60.10 y para los administradores de la misma dirección.

SPI	source IP	client authentication key	client cifrado key	cifrado method
301	130.15.24.4	...	none	none
2	**130.15.60.10**	**...xxx..**	**none**	**none**
72	**130.15.60.10**	**...JJJ..**	**#$BB76%**	**CBC-DES**
...	**...**	**...**	**...**	**...**

Tabla: Información de seguridad de destino en 130.15.20.2 (con MD5 como método de autenticación del cliente)

Las Tablas siguientes (client autentication method = MD5) incluyen parámetros de seguridad para las asociaciones de seguridad en un sentido con el origen del cliente

130.15.6010 y el destino en el servidor 130.15.60.2. Se debería de definir un conjunto de parámetros para la dirección inversa. De nuevo, hay que planificar si se decide usarlas mismas claves en ambas direcciones o se asignan distintas claves para el tráfico cliente a servidor y pasa el trafico servidor a cliente.

source IP	**id user**	**SPI**	**target IP**	**client authentication key**	**client cifrado key**	**client cifrado method**
130.15.20.2	host	2	130.15.60.10	...xxx...	none	none
130.15.20.2	admin	72	130.15.60.10	...JJJ...	**#$BB76%**	**CBC-DES**
130.15.65.4	host	...	...	...	...	...
...	...	...	...	...	...	...

Tabla Información de seguridad de destino en 130.15.60.10

9.2.3. Escenario 3

El escenario 3 se muestra en la Figura 24.4. El objetivo es que todo el tráfico que la compañía XYZ envía por una red en la que no confía resulte opaco para el resto del mundo. Se usa en encapsulado en modo encapsulado. Es decir, los datagramas se cifran y se encapsulan dentro de otros datagramas.

Como se muestra en la figura, cuando un datagrama cuya dirección de destino está en la red 193.40.3 llega al encajuinador de frontera de la red 130.15, el router cifra el datagrama completo, incluso sus cabeceras. El router añade una cabecera de LP3 (en abierto) temporal y reenvía el datagrama por la red del proveedor de servicios hacia el router de frontera de la red 193.40.3. Entonces, se elimina la cabecera temporal, sc descifra el datagrama y se reenvía a su verdadero destino. En este caso, la asociación de seguridad se define entre dos routers de frontera.

Generalización

Se han visto algunos ejemplos concretos para familiarizarse con el marco básico de seguridad. Resulta fácil ver que! en general, se puede usar un conjunto común de mecanismos para asegurar el tráfico cuando se transmite:

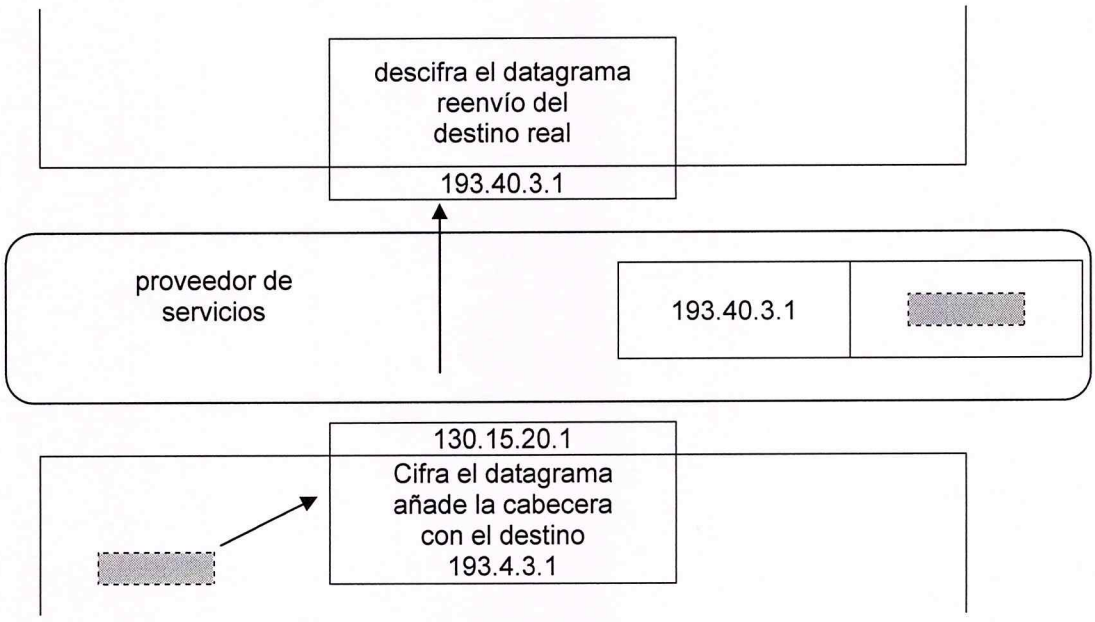


Figura: Encapsulamiento de tráfico entre dos redes

Además de la cabecera principal, también hay que añadir otras cabeceras, Por ejemplo, se podría añadir una cabecera distinta de autenticación para autenticar la transferencia entre routers.

- De un host a otro
- De un router a otro
- De un host a un router
- De un router a un host

Si un host de destino tiene más de una dirección de IP, se pueden definir conjuntos de parámetros de asociaciones de seguridad para cada dirección de destino. No existe ninguna barrera para proporcionar autenticación, integridad de datos y confidencialidad para las direcciones de destino de multienvío.

En el escenario 2, vimos que la seguridad se puede definir en el nivel de usuario o rol. Se puede hacer de grano tan fino como sea necesario. Más aún, los parámetros de seguridad se podrían configurar de acuerdo con la sensibilidad de la información, por ejemplo, sin clasificar o alto secreto. Por supuesto, el mantenimiento de los distintos conjuntos de parámetros dependerá de disponer de una buena aplicación de distribución de claves.

9.3. Donde Puede ser Implementado IpSec

Hay varias formas en las cuales se puede implementar IpSec, en un host o en conjunto con un router o un firewall (creando un security gateway). Algunos ejemplos frecuentes son:

a. Integrar IpSec en una implementación nativa IP. Requiere tener acceso al código fuente IP, y se puede aplicar tanto a host como a un security gateway.
b. "Puesto en la Pila" (BITS), IpSec se implementa "por debajo" de una implementación existente de una pila IP, entre el IP nativo y los drivers locales de la red. El acceso al código fuente para la pila IP no es requerido en este contexto, este contexto es apropiado para los sistemas antiguos. Este método, cuando se adopta, se emplea generalmente en hosts.
c. "Puesto en el cable" (BITW). El uso de un procesador criptográfico externo es una característica de diseño común de los sistemas de seguridad de red usados por los militares, y en algunos sistemas comerciales. Tales implementaciones se pueden diseñar para asistir a un host o un gateway (o a ambos). El dispositivo BITW generalmente tiene una IP direccionable. Cuando asiste a un único host, puede resultar análogo a una implementación BITS, pero en un router o en un firewall debe funcionar como un security gateway.

9.3.1. Observaciones y Advertencias

El grupo de protocolos IpSec y demás algoritmos asociados permiten proporcionar seguridad de alta calidad para el flujo de tráfico de Internet. Sin embargo, la seguridad ofrecida por estos protocolos depende en última instancia de la calidad de su implementación, que esta fuera del alcance de este libro. Además, la seguridad de un sistema informático o en una red es una función de muchos factores. IpSec solo es una parte de un sistema global de seguridad.

La seguridad proporcionada por el uso de IpSec dependerá bastante de diversos aspectos del ambiente operativo en el cual la implementación de IpSec se ejecuta. Por ejemplo, los defectos en la seguridad del sistema operativo, negligencia en la práctica de manejo de protocolos, etc., todo esto puede degradar la seguridad proporcionada por IpSec. Como se mencionó anteriormente, ninguna de estas características están dentro del alcance de este libro o de algún estándar de IpSec. Por ultimo, este documento no es una arquitectura global

10. TRANSICIÓN DE APLICACIONES

10.1. Introducción

La transición a la nueva versión del protocolo está siendo un proceso gradual en el que tienen que convivir ambos tipos de redes y aplicaciones. Actualmente, millones de aplicaciones IPv4 están repartidas por toda Internet y no pueden comunicarse directamente con aplicaciones desarrolladas para IPv6. En este artículo se presentarán los problemas de interoperabilidad de aplicaciones IPv4 e IPv6 y se estudiarán soluciones aplicables en los nodos extremos de la comunicación, donde normalmente tenemos acceso a la configuración de la máquina/nodo. Como caso de estudio se analizará la implantación de un mecanismo de transición que hemos desarrollado basándonos en una propuesta experimental de Internet Engineering Task Force (IETF).

Durante los primeros 1990 se hicieron obvios varios problemas de la implementación de IP desplegada, IPv4 -como el escaso espacio de direccionamiento y la gestión del routing. Con la intención de resolverlos se desarrollaron algunos mecanismos específicos, como por ejemplo Network Address Translation (NAT), que es en la actualidad uno de los más extendidos. Sin embargo, NAT elimina el servicio de comunicación entre entidades finales y rompe el modelo de comunicación extremo a extremo inicialmente planteado en IP. La demanda de comunicación entre sistemas finales de las nuevas aplicaciones Peer-To-Peer (P2P) y la necesidad de calidad de servicio en las comunicaciones, han impulsado el desarrollo de IPv6.

Actualmente millones de máquinas están conectadas a Internet usando IPv4 y es imposible realizar el cambio a IPv6 de forma inmediata. La transición se está realizando de forma gradual [3], primero portando la infraestructura de red, junto con sus servicios básicos y en segundo lugar, las aplicaciones.

Una de las principales preocupaciones durante el período de transición es la interoperabilidad entre las aplicaciones ya existentes y las nuevas desarrolladas para IPv6. En la mayoría de los casos la interoperabilidad de aplicaciones se consigue utilizando nodos que implementen ambos protocolos, es decir, nodos duales que puedan comunicarse utilizando tanto IPv4 como IPv6. Los nodos con pila dual proporcionan un mecanismo para permitir a las aplicaciones IPv4 comunicarse con aplicaciones IPv6 utilizando el protocolo IPv4 para el intercambio de paquetes entre los nodos finales. Sin embargo, en los escenarios en los que la conectividad entre los nodos origen y destino

sólo es posible utilizando IPv6, la pila dual no será suficiente para establecer la comunicación y se necesitará algún mecanismo de transición adicional.

El objetivo de este capitulo es proponer la interoperabilidad de aplicaciones IPv4 e IPv6 cuando sólo es posible utilizar una infraestructura de red IPv6, sin cambiar el código fuente de las mismas. En muchos casos no se dispone del código fuente, o existe un problema de licencias que impide modificarlo. Además, existen casos en los que, aunque se dispone del código, portarlo a la nueva interfaz de IPv6, distribuirlo e instalarlo puede resultar un trabajo costoso que requiera demasiado tiempo. Por estos motivos, el caso de estudio de este trabajo es de especial relevancia durante el período de transición, permitiendo convivencia de aplicaciones, o partes de una aplicación, ya portadas IPv6 con aplicaciones IPv4 existentes.

En el presente artículo se proporcionará una visión general de los mecanismos de transición a IPv6 en el ámbito de nodo (en términos de contexto y aplicación). En la sección 2 se analizarán los mecanismos experimentales propuestos por el IETF, Bump In the Stack (BIS) y Bump In the API (BIA). Y, finalmente, en la sección 6 se expondrán las conclusiones y los posibles trabajos futuros.

10.2. Implementación de BIA

El mecanismo BIA permite que las aplicaciones IPv4 sigan funcionando normalmente sobre una red IPv6, sin que haya que modificar el código fuente, ni recompilarlo. Dado que una aplicación IPv4 sólo es capaz de manejar direcciones IPv4, el mecanismo BIA proporcionará direcciones ficticias IPv4 a la aplicación para que sea transparente el hecho de que los nodos remotos son sólo direccionables mediante IPv6.

BIA se encarga de mantener la correspondencia entre las direcciones IPv4 ficticias y las direcciones IPv6 reales.

A continuación se describe la arquitectura e implementación que utilizado por el mecanismo BIA, así como su uso en aplicaciones cliente/servidor.

10.2.1. Interoperabilidad de aplicaciones IPv4 IPv6

La mayoría de los mecanismos de transición de IPv6 se han desarrollado para conectar redes IPv4 con redes IPv6 y basan su funcionamiento en entidades situadas en un punto intermedio de la red que realizan algún tipo de procesamiento, por ejemplo túneles o traducción de protocolos, para permitir su comunicación. El objetivo de este capitulo es estudiar la comunicación entre aplicaciones heterogéneas IPv4 e IPv6 sobre una red que permite únicamente conectividad IPv6, sin modificar ningún elemento intermedio de la red, donde muchas veces no hay la posibilidad de cambiar la configuración.

Partiendo del escenario en el que existen aplicaciones IPv4 que necesitan comunicarse con aplicaciones IPv6 sobre una red IPv6, lo lógico es introducir una traducción IPv4/IPv6 en el nodo donde se ejecuta la aplicación IPv4. Parece requisito indispensable que el nodo que realiza la traducción tenga instalada la doble pila, IPv4 para permitir que la aplicación se ejecute correctamente e IPv6 para establecer las comunicaciones.

Es posible utilizar un mecanismo basado en túneles para permitir la ejecución de aplicaciones IPv4 en redes IPv6. El túnel se establecería entre dos puntos, el nodo donde se ejecuta la aplicación IPv4 y otro nodo cualquiera de la red. Nótese que el hecho de utilizar túneles implica que las aplicaciones que están comunicándose deben haber sido desarrolladas para la misma versión del protocolo, ya que en el extremo final del túnel se proporciona el paquete tal y como fue emitido. Por tanto, si la aplicación remota es IPv6, sería necesario otro mecanismo de transición adicional antes de poder entregar el paquete original IPv4 en destino.

El IETF ha definido 2 métodos experimentales de transición para realizar la traducción IPv4/IPv6 en n nodo que ejecuta una aplicación IPv4, dependiendo del nivel en el se produzca la traducción: en la interfaz de programación de aplicaciones (Bump In the API, **BIA**) y en la pila IP (Bump In the Stack, **BIS**).

El mecanismo BIS intercepta los paquetes IP al salir del nivel IP de la máquina, antes de enviarlos a la tarjeta de red, y realiza la traducción entre IPv4 e IPv6 según los paquetes sean entrantes o salientes.

BIA sigue un funcionamiento análogo a BIS, salvo que la traducción de paquetes se realiza antes de construir el paquete, en la propia interfaz de programación de

aplicaciones. Por tanto, BIA es un mecanismo de transición más ligero ya que no necesita realizar una traducción del paquete, sino que construye el paquete IPv6 a partir de las funciones de la API IPv4.

Aunque BIA ha sido diseñado con el objetivo específico de permitir a las aplicaciones IPv4 funcionar sobre redes IPv6, este mecanismo no impone limitaciones para utilizarse conjuntamente con otros mecanismos de transición y así ofrecer la máxima interoperabilidad entre redes y aplicaciones heterogéneas.

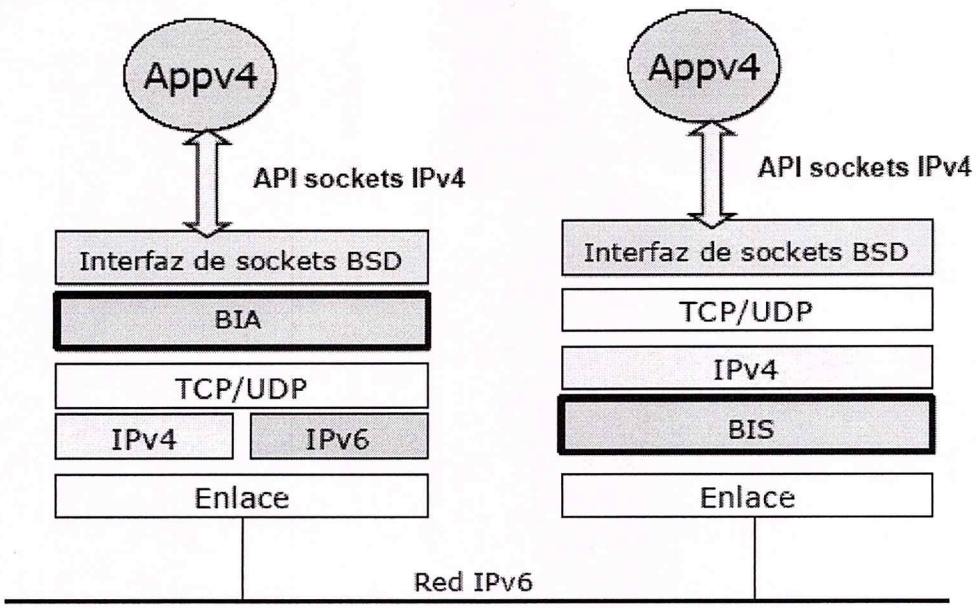


Figura: BIS y BIA, mecanismos de transición a IPv6 en el ámbito de un nodo.

10.2.2. Arquitectura de BIA

La arquitectura del mecanismo BIA que hemos desarrollado se divide en una serie de módulos encargados de realizar las siguientes funciones: extensión de la resolución de nombres, traducción de las funciones de la interfaz y traducción del mapa de direcciones.

El módulo de extensión de la resolución de nombres permite que una aplicación IPv4 reciba como respuesta a una consulta de resolución de un nombre de una máquina IPv6, una dirección ficticia IPv4.

El módulo traductor de funciones de la interfaz es el encargado de realizar la traducción entre la API de IPv4 e IPv6. Permite a la aplicación seguir usando la API de IPv4, aun cuando la aplicación acabe construyendo, enviando y recibiendo paquetes IPv6.

El módulo traductor del mapa de direcciones gestiona la asociación entre las direcciones IPv4 ficticias y las direcciones IPv6 reales.

10.3. Impacto de la transición en capas superiores [65]

- La arquitectura de red TCP/IP no está perfectamente dividida.
  Las aplicaciones identifican al nodo destino:
  - Usando la dirección IP.
  - Usando el nombre DNS.
- Las aplicaciones deben ser revisadas en ambos casos:
  - IPv6 maneja otro formato.
  - Cambia la interfaz de la capa de transporte.
- Durante la transición será necesario soportar tanto los nodos de IPv4 como los de IPv6.
- Se requieren traductores entre la interfaz de red IPv6 y la interfaz de programación IPv4.

Traductores
De capa de Red:
- SIIT (Stateless IP/ICMP Translator)
- NAT-PT (Network Address Translation - Protocol Translation
- BIS (Bump in the Stack)
- MBIS (Extensiones Multicast para BIS)

- De capa de Transporte: TRT (Transport Relay Translator).
- De capa de Aplicación: BIA (Bump in the API).

- **Usando una aplicación de IPv4**

  - Pueden conectarse nodos IPv4 o los duales.
  - Los nodos dual Stack pueden conectarse usando la red IPv6
  - Los nodos IPv6 no pueden usar aplicaciones IPv4 (si es posible con un traductor).

---

[65] Desarrollo de Aplicaciones con soporte IPv6 Ing. Azael Fernández Alcántara Universidad Nacional Autónoma de México, UNAM Grupo de Trabajo de IPv6 en Internet2 Capítulo Mexicano del Foro IPv6 NETLab Reunión de Otoño 2003 3 de octubre 2003 Cd. de Puebla, México

- **Usando aplicaciones IPv6 e IPv4**
  - Los nodos IPv6 y los duales pueden conectarse usando la red IPv6.
  - Una aplicación IPv6 puede usarse sobre la red IPv4: Si se usa una dirección compatible con IPv4 (::a.b.c.d)
  - Un nodo IPv4 puede conectarse con un nodo IPv6 si usa un traductor o por túnel.

10.4. Conversión de Aplicaciones para ipv6

- Escenarios
- Consideraciones y Cambios
- Herramientas
- Recomendaciones

ESCENARIOS

- Convirtiendo las redes existentes:
  - Aplicaciones solamente para IPv4.
  - Proveer dos aplicaciones diferentes.
  - Aplicaciones duales (IPv4 e IPv6).
- Dando de alta redes nuevas de IPv6:
  - Aplicaciones duales (IPv4 e IPv6).
  - Las aplicaciones pueden ser solo para IPv6 (Si son independientes del protocolo)
- Usando una aplicación existente de IPv4:
  - Mediante traductores (NAT-PT , SIIT , BIS)
  - Válido solamente con limitaciones.
- Convirtiendo una aplicación existente:
  - Aplicable sólo si el código fuente está disponible.
  - Convirtiendo las librerías de comunicaciones. (Ejemplo: Java net library)
- Desarrollando una nueva aplicación:
  - Independiente del protocolo.
  - Dependiente del protocolo.
    - No recomendado.
    - Desarrollar un código dual IPv4/IPv6.

10.5. Consideraciones y cambios

- Los códigos fuente y binario deben ser compatibles con los códigos existentes y las aplicaciones:
  - Los binarios existentes (IPv4) seguirán ejecutándose.
- Cambios mínimos en la API (<0,1%).
  - La conversión a IPv6 debe ser sencilla.
  - Mismas llamadas de sockets.
  - Pocas nuevas funciones.
  - Localizables en el código.
- **Del lado del servidor:**
  - Cambiar las funciones "socket"
  - Ajustar la función de registro para manejar direcciones IP más grandes.
  - Incrementar todos los datos de los miembros que guarden direcciones IP (BD).
- **Del lado del cliente:**
  - Cambiar las funciones "socket"
  - Ajustar las funciones de registro.
  - Ajustar la función interfaz del teclado y de despliegue para manejar direcciones IP más grandes.
- Algunas aplicaciones usan los dos puntos ":" para distinguir el puerto de la dirección.
  - Ejemplo: En los URLs.
  - En IPv6 las direcciones IPv6 se representan con paréntesis cuadrados: http://[3ffe:8070::1]/index.html
- Dependencias en la aplicación.
  - Porciones del código no afectadas
  - Porciones del código afectadas
- Naturaleza de la aplicación.
- Espacio de la aplicación.
- Arquitectura.
- No se ve afectada la secuencia de código típica.

Secuencia de Código Típica (IPv4 IPv6)

- ***Del lado del servidor:***
  - socket – se abre un socket
  - bind - de la dirección local al socket
  - listen – se escucha en un puerto

- accept – espera conexiones
- "read" y/o "write" si es TCP
- "recvfrom" y/o "sendto" si es UDP

- ***Del lado del cliente:***
  - socket - se abre un socket
  - connect – se conecta al servidor
  - "read" y/o "write" si es TCP
  - "recvfrom" y/o "sendto" si es UDP

Cambios requeridos en la API

- A través de los Sockets.
- En las partes de la API donde se muestre el tamaño de la dirección IP. (se requieren nuevas estructuras de datos).
- En las partes de aplicación que manipule la dirección IP.
- Funciones socket() del núcleo.
- Estructuras de datos para direcciones.
- Funciones de traducción de Nombre –Dirección.
- Funciones de conversión de direcciones.

Funciones socket() del núcleo.

- En IPv4 socket (PF_INET, SOCK_STREAM, 0);
- En IPv6 s = socket (PF_INET6, SOCK_STREAM, 0);

PF (Familia del Protocolo)

Funciones socket() del núcleo.

Longitud de dirección.

Espacio para nuevos campos en la cabecera.

Mecanismos para poner nuevos valores de campo:

Determinar la clase de trafico (QoS).

Poner opciones de seguridad (AH y ESP).

Requerimientos de espacio y memoria.

- Estructuras de datos para direcciones.
  1. Nueva Familia de Dirección AF_INET6.
  2. ssockaddr_in para IPv4
  3. sockaddr_in6 de 128 bits para IPv6
  4. sockaddr_storage independiente del protocolo

i. – sin_port sin6_port
ii. – sin_family sin6_family

- Funciones de traducción de Nombre –Dirección.
  - En IPv4 gethosbyname () y gethosbyaddr ()
  - En IPv6 getipnodebyname() y getipnodebyaddr()
- La norma POSIX 1003.g especifica funciones independientes del protocolo, (Nuevas funciones: getnameinfo() getaddrinfo())

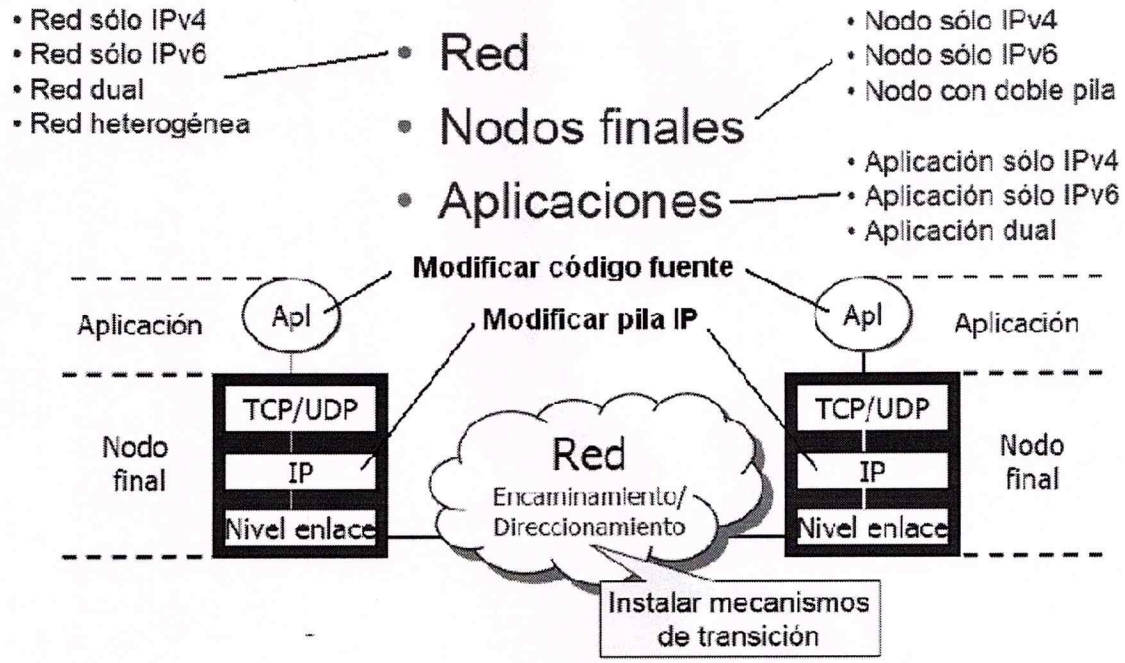
- Funciones de conversión de direcciones.
  - En IPv4:
    a. Cadena -> Binario inet_aton () y inet_addr ()
    b. Binario -> Cadena inet_ntoa ()
  - En IPv6 e IPv4:
    a. Cadena -> Binario inet_pton ()
    b. Binario -> Cadena inet_nton ()

	IPv4	IPv6
Estructuras de Datos	AF_INET	AF_INET6
	in_addr sockaddr_in	in6_addr sockaddr_in6
Funciones de Conversión de Direcciones	inet_aton() inet_addr()	inet_pton()
	inet_ntoa()	inet_ntop()
Funciones Nombre a Dirección	gethostbyname() gethostbyaddr() getnameinfo() getaddrinfo()	getipnodebyname() getipnodebyaddr() getnameinfo() getaddrinfo()

10.6. Herramientas

- Algunas disponibles:
  - Socket Scrubber de Sun
  - Socks v4 a v6
  - Checkv4 de Microsoft
- Ayudan a encontrar e identificar las líneas de código (fuente) que requieren cambiarse o actualizarse.

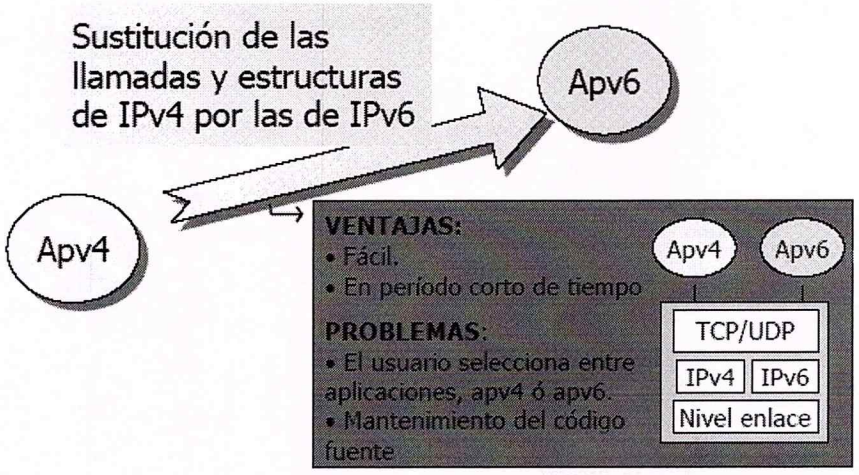
10.7. Arquitectura de Transición en las Aplicaciones



10.7.1 Evolución de aplicaciones [66]

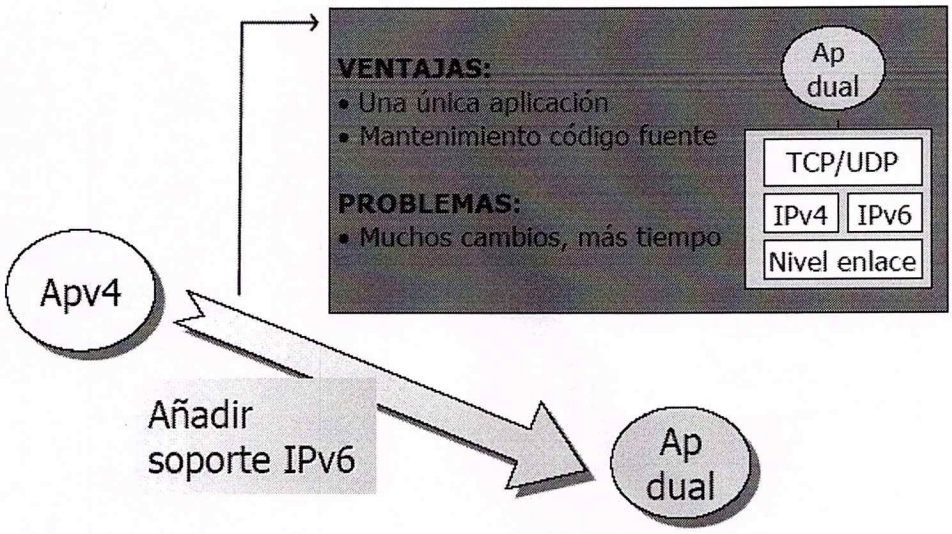
- De aplicaciones IPv4 a aplicaciones IPv6
- De aplicaciones IPv4 a aplicaciones duales
- Transición gradual

10.7.1.1. De aplicaciones IPv4 a aplicaciones IPv6

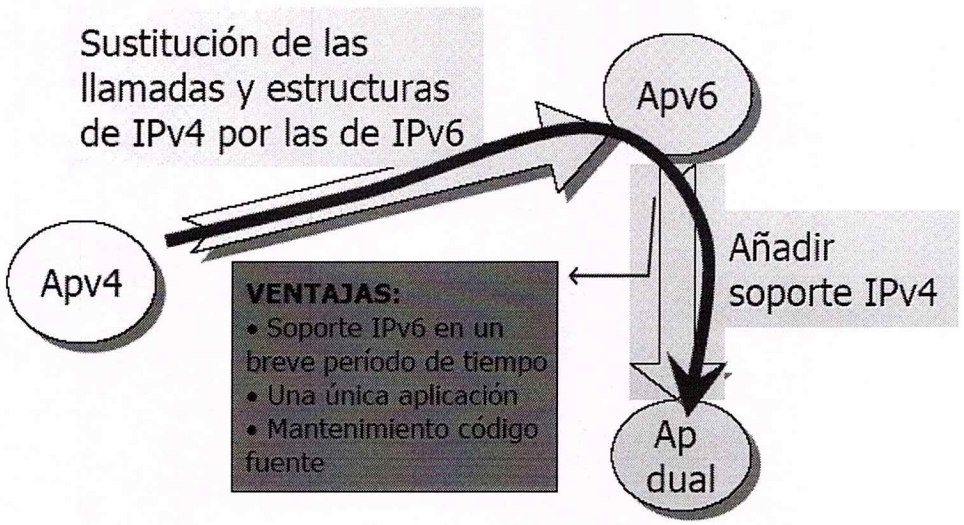


[66] Transición de aplicaciones y servicios a IPv6, Eva M. Castro, Grupo de Sistemas y Comunicaciones (GSyC), universidad Rey Juan Carlos (URJC)

10.7.1.2. De aplicaciones IPv4 a Aplicaciones Duales



10.7.1.3. Transición gradual

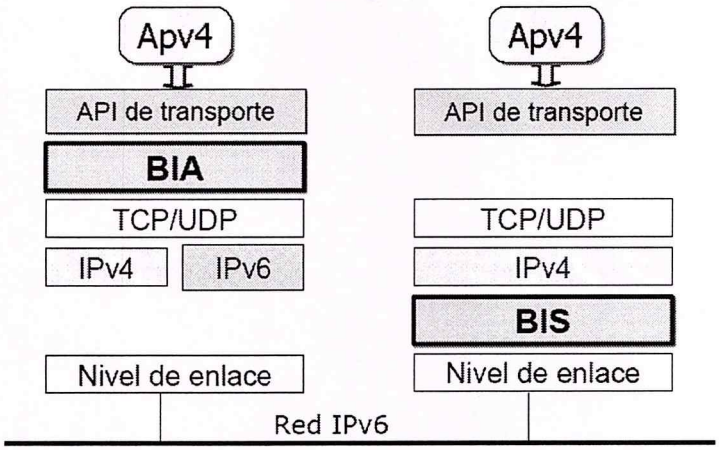


10.8. Escenarios de transición de aplicaciones

1. Aplicaciones IPv4 en nodos duales
2. Aplicaciones IPv6 en nodos duales
3. Aplicacion Servidor IPv6 en nodo dual
4. Aplicación Cliente IPv6 en nodo dual
5. Aplicaciones duales en nodos duales
6. Aplicaciones duales en nodos sólo IPv4

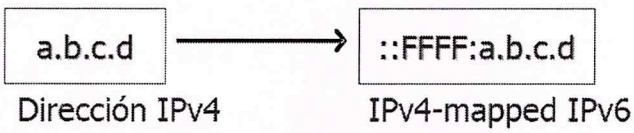
10.8.1. Aplicaciones IPv4 en Nodos Duales

- Dependencias en el código fuente con IPv4.
- Intercambian paquetes IPv4.
- Para su funcionamiento en redes IPv6:
  - Portar el código a IPv6
  - Si no es posible, utilizar mecanismos de transición. Las aplicaciones utilizan IPv4 pero se intercambian paquetes IPv6:
    - BIA (Bump In the API)
    - BIS (Bump In the Stack)

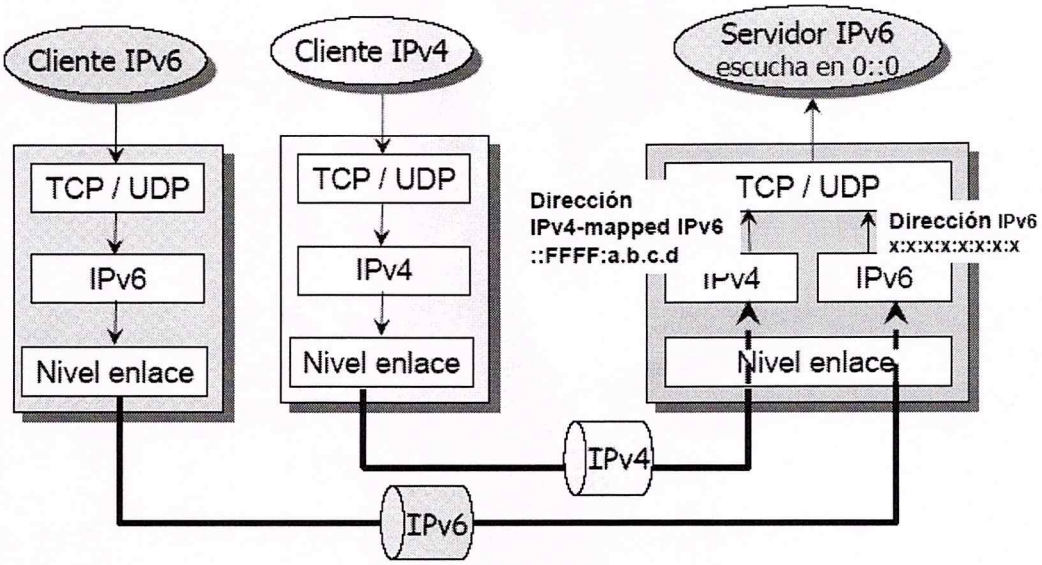


10.8.2. Aplicaciones IPv6 en Nodos Duales

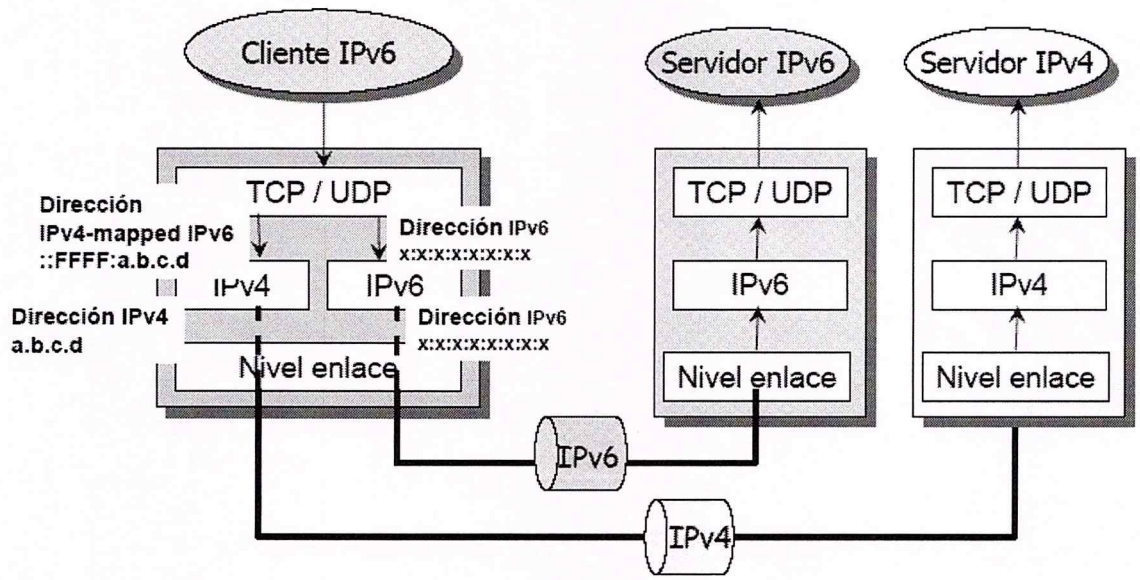
- Se han sustituido las estructuras y funciones de IPv4 por las de IPv6. Dependencias en el código fuente con IPv6
- Intercambian de paquetes IPv6.
- Para su funcionamiento en redes IPv4:
  - Portar a aplicaciones duales
  - Mantener 2 aplicaciones: ping4 y ping6 o
  - Utilizar direcciones IPv6 a partir de las direcciones IPv4, IPv4-mapped IPv6 addresses, no soportadas en todos las implementaciones.



10.8.3. Aplicación Servidor IPv6 en Nodo Dual



10.8.4. Aplicación Cliente IPv6 en Nodo Dual



10.8.5. Aplicaciones duales en nodos duales

- Aplicaciones válidas para redes IPv4 e IPv6:
- Implementación de **aplicaciones cliente:**
    - Resolver nombre de máquina del servidor a las posibles direcciones IP. Intentar conectar primero usando IPv6 y si falla probar con IPv4.
- Implementaciones de **aplicaciones servidor:**
    - Mantener conexiones diferentes de forma explícita para IPv4 e IPv6
    - Desarrollar una aplicación servidor IPv6 y confiar en las direcciones IPv4-mapped IPv6 para los clientes IPv4.

10.8.6. Aplicaciones duales en nodos sólo IPv4

- Las aplicaciones duales deberían funcionar en los nodos sólo IPv4 para evitar tener varias versiones de la misma aplicación.
  Requisito: Desarrollar el código fuente para que nodos que no tengan soporte del protocolo IPv6 puedan ejecutar dichas aplicaciones.

10.9. Dependencias en el Código Fuente

1. Formato de presentación de las direcciones IP
2. Resolución de nombres
3. API de la capa de transporte
4. Otras dependencias específicas

10.9.1. Formato de Presentación de Direcciones IP

- El formato de presentación es una cadena que contiene la dirección IP. Diferentes en IPv4 e IPv6:
    - IPv4: "a.b.c.d"
    - IPv6: "x:x:x:x:x:x:x:x"
- El formato de presentación en IPv6 necesita más memoria.
- Los analizadores sintácticos de direcciones deben ser revisados para adecuarse al nuevo formato.
- Ambigüedad con el carácter ":" en URLs (RFC 2732): http://[DirecciónIPv6]:puerto
- RECOMENDACIÓN: Utilizar FQDN (Fully Qualified Domain Name)

10.9.2. Resolución de Nombres

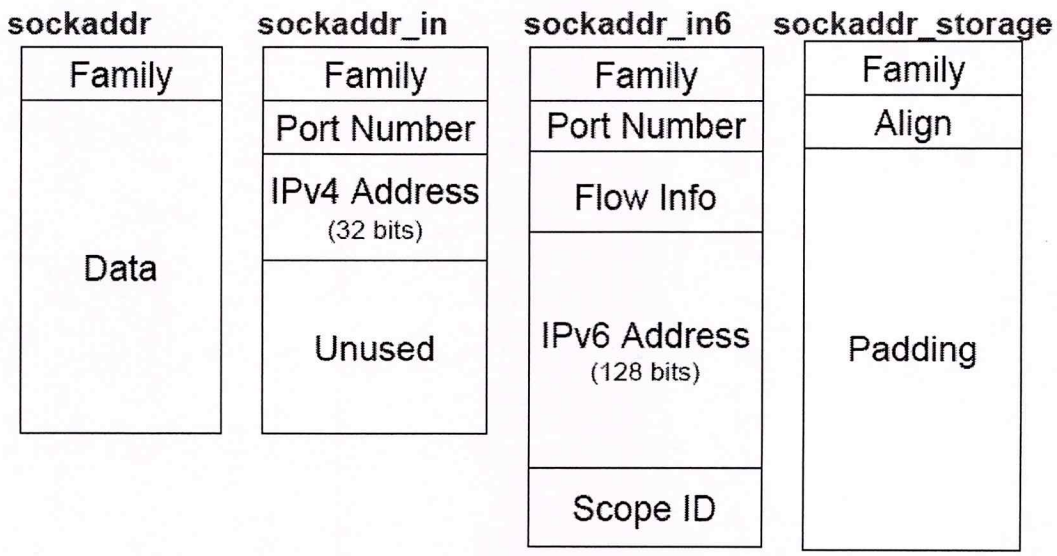
- Tipos de resolución:
  - Directa: a partir del nombre de la máquina obtener su dirección IP.
  - Inversa: a partir de la dirección IP obtener el nombre de máquina.
- Utilizar FQDN.
- Las consultas/respuestas de DNS se envían usando
- IPv4/IPv6 independientemente del tipo de registros que se soliciten.
- RECOMENDACIÓN: Usar las funciones de resolución independientes de protocolo.

10.9.3. API de la Capa de Transporte

En el caso concreto del API de sockets existen las siguientes dependencias:

- Estructuras de datos para las direcciones IP: sockaddr_in, sockaddr_in6, sockaddr_storage
- Funciones del API de comunicaciones: socket(), bind(), connect(), read()/write() ...
- Funciones de conversión de direcciones: entre el formato de presentación y las estructuras de datos de direcciones.
- Opciones de configuración de red.
- RECOMENDACIÓN: Desarrollar aplicaciones independientes de la versión IP

Estructuras de datos



10.9.4. Otras Dependencias Específicas

- Selección de la dirección IP: Los nodos automáticamente resuelven el problema de la selección de la dirección de origen, siguiendo una serie de reglas predefinidas (RFC 3484).
- Fragmentación a nivel de aplicación: Cálculo del tamaño del fragmento para que no haya degradación de prestaciones por fragmentación a nivel IP.
- Almacenamiento de direcciones IP: No almacenar direcciones IP, pueden cambiar. Si es necesario almacenar nombres y solicitar la resolución en el momento que se necesiten.
- RECOMENDACIÓN: Revisar el código exhaustivamente.

11. CONFIGURAR UN LABORATORIO DE PRUEBAS DE IPV6 [67] [68] [69]

IMPLEMENTACION

Esta sección proporciona información acerca de cómo puede utilizar cinco equipos para crear un laboratorio de pruebas con el propósito de configurar y probar el protocolo IPv6. Las instrucciones están diseñadas para guiarle a través de un conjunto de tareas que le mostrarán el protocolo IPv6 y las funciones asociadas. Además del conjunto de tareas, estas instrucciones le permiten crear una configuración funcional de IPv6. Puede utilizar esta configuración para aprender y experimentar acerca de las características y las funcionalidades de IPv6, de forma que le sirva de ayuda en el desarrollo de aplicaciones para IPv6 o la modificación de las aplicaciones existentes de IPv4.

11.1. Configurar la infraestructura

La infraestructura de la red del laboratorio de pruebas de IPv6 es una parte de la actual infraestrucutura de red que opera en una empresa de negocios (No vamos a decir el nombre por cuestiones de seguridad) la cual consta de cinco equipos que ejecutan los servicios siguientes:

- Un equipo con Windows Server 2003, Standard Edition que se utiliza como servidor de Sistema de nombres de dominio (DNS, Domain Name System). El nombre de este equipo es DNS1.
- Un equipo con Windows XP Professional que se utiliza como cliente. El nombre de este equipo es CLIENTE1.
- Un equipo con Windows Server 2003, Standard Edition que se utiliza como enrutador. El nombre de este equipo es ROUTER1.
- Un equipo con Windows Server 2003, Standard Edition que se utiliza como enrutador. El nombre de este equipo es ROUTER2.
- Un equipo con Windows XP Professional que se utiliza como cliente. El nombre de este equipo es CLIENTE2.
- Puede configurar los equipos ROUTER1 y ROUTER2 con Windows XP Professional. El equipo DNS1, sin embargo, debe configurarse con Windows Server 2003, Standard Edition.

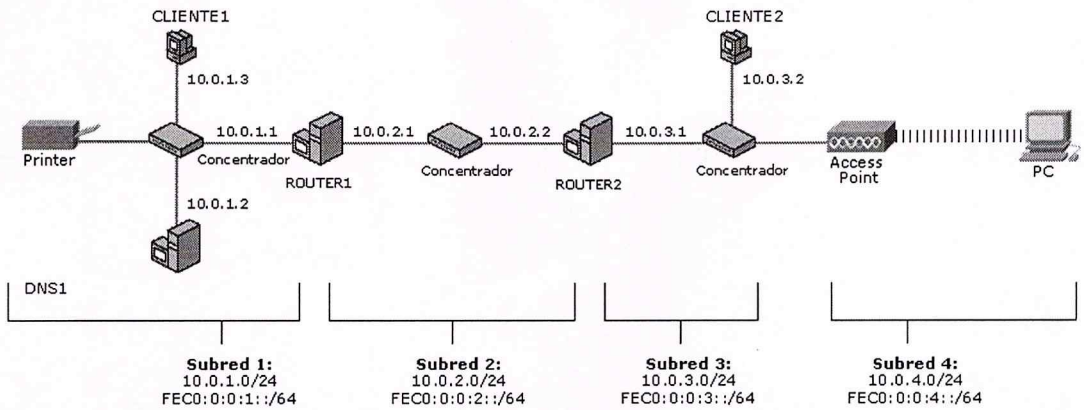
---

[67] Las instrucciones siguientes sirven para configurar un laboratorio de pruebas con un número mínimo de equipos. Son necesarios equipos individuales para separar los servicios suministrados en la red y para mostrar con claridad las funciones deseadas. Esta configuración no está diseñada para reflejar las prácticas recomendadas ni para reflejar una configuración deseada o recomendada para una red de producción. La configuración, incluidas las direcciones IP y los demás parámetros de configuración, está diseñada para funcionar sólo en una red de laboratorio de pruebas separada.

[68] http://www.microsoft.com/ipv6

[69] http://go.microsoft.com/fwlink/?LinkId=103

- En la ilustración siguiente se muestra la configuración del laboratorio de pruebas de IPv6.



Hay cuatro segmentos de red:

- Un segmento denominado Subred 1 que utiliza el Id. de red IP privada 10.0.1.0/24 y la Id. de subred local del sitio FEC0:0:0:1::/64
- Un segmento denominado Subred 2 que utiliza el Id. de red IP privada 10.0.2.0/24 y la Id. de subred local del sitio FEC0:0:0:2::/64
- Un segmento denominado Subred 3 que utiliza el Id. de red IP privada 10.0.3.0/24 y la Id. de subred local del sitio FEC0:0:0:3::/64
- Un segmento denominado Subred 4 que utiliza el Id. de red IP privada 10.0.3.0/24 y la Id. de subred local del sitio FEC0:0:0:4::/64

Todos los equipos de cada subred están conectados a un concentrador común o un conmutador de nivel 2 independiente. Los dos equipos enrutadores, ROUTER1 y ROUTER2, tienen adaptadores de red instalados.

Para la configuración de IPv4, cada equipo se configura manualmente con la dirección IP, máscara de subred, puerta de enlace predeterminada o gateway y dirección IP del servidor DNS adecuadas. No se utilizan servidores de Protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) o de Servicio de nombres Internet de Windows (WINS, Windows Internet Name Service). Para la configuración de IPv6, se utilizan inicialmente direcciones locales del vínculo.

En las secciones siguientes se describe cómo se configura cada uno de los equipos del laboratorio de pruebas. Para reconstruir el laboratorio de pruebas, configure los equipos en el orden indicado.

11.1.1. DNS1

DNS1 es un equipo en el que se ejecuta Windows Server 2003, Standard Edition. Proporciona servicios de servidor DNS para el dominio DNS testlab.microsoft.com. Para configurar este servicio en DNS1, lleve a cabo los pasos siguientes:

- Instale Windows Server 2003, Standard Edition como servidor independiente. Establezca la contraseña de administrador.
- Después de reiniciar, inicie sesión como administrador.
- Instale el protocolo IPv6.
- Instale el servicio de servidor del Sistema de nombres de dominio (DNS). Durante la instalación del DNS, defina una zona de búsqueda directa llamada testlab.microsoft.com y que permita actualizaciones dinámicas.
- Configure el protocolo TCP/IP con la dirección IP 10.0.1.2, la máscara de subred 255.255.255.0 y la puerta de enlace predeterminada 10.0.1.1.

Nota: Si utiliza Configurar el servidor para instalar el DNS, el Asistente para configurar un servidor DNS se ejecuta después de instalar el servicio DNS. El Asistente para configurar un servidor DNS le pedirá que defina una zona de búsqueda directa o inversa. Para completar las tareas del laboratorio de pruebas, debe definir una zona de búsqueda directa que permita actualizaciones dinámicas. La definición de una zona de búsqueda inversa es opcional.

11.1.2. CLIENTE1

CLIENTE1 es un equipo con Windows XP Professional y que se utiliza como cliente. Para configurar CLIENTE1 como equipo cliente, lleve a cabo los pasos siguientes:

1. En CLIENTE1, instale Windows XP como parte de un grupo de trabajo. Establezca la contraseña de administrador.
2. Después de reiniciar, inicie sesión como administrador.
3. Instale el protocolo IPv6.
4. Configure el protocolo TCP/IP con la dirección IP 10.0.1.3, la máscara de subred 255.255.255.0, la puerta de enlace predeterminada 10.0.1.1 y la dirección IP del servidor DNS 10.0.1.2.

11.1.3. ROUTER1

ROUTER1 es un equipo con Windows Server 2003, Standard Edition y que se utiliza como enrutador entre la Subred 1 y la Subred 2. Para configurar ROUTER1 como enrutador, lleve a cabo los pasos siguientes:

1. En ROUTER1, instale Windows Server 2003, Standard Edition como parte de un grupo de trabajo. Establezca la contraseña de administrador.
2. Después de reiniciar, inicie sesión como administrador.
3. Instale el protocolo IPv6.
4. Para la interfaz de la Subred 1, configure el protocolo TCP/IP con la dirección IP 10.0.1.1, la máscara de subred 255.255.255.0 y la dirección IP del servidor DNS 10.0.1.2
5. Para la interfaz de la Subred 2, configure el protocolo TCP/IP con la dirección IP 10.0.2.1, la máscara de subred 255.255.255.0 y la puerta de enlace predeterminada 10.0.2.2
6. Habilite el reenvío IP mediante el Servicio de enrutamiento y acceso remoto.

11.1.4. ROUTER2

ROUTER2 es un equipo con Windows Server 2003, Standard Edition y que se utiliza como enrutador entre la Subred 2 y la Subred 3. Para configurar ROUTER2 como enrutador, lleve a cabo los pasos siguientes:

1. En ROUTER2, instale Windows Server 2003, Standard Edition como parte de un grupo de trabajo. Establezca la contraseña de administrador.
2. Después de reiniciar, inicie sesión como administrador.
3. Instale el protocolo IPv6.
4. Para la interfaz de la Subred 2, configure el protocolo TCP/IP con la dirección IP 10.0.2.2, la máscara de subred 255.255.255.0 y la puerta de enlace predeterminada 10.0.2.1
5. Para la interfaz de la Subred 3, configure el protocolo TCP/IP con la dirección IP 10.0.3.1 y la máscara de subred 255.255.255.0.
6. Habilite el reenvío IP mediante el Servicio de enrutamiento y acceso remoto

11.1.5. CLIENTE2

CLIENTE2 es un equipo con Windows XP y que se utiliza como cliente. Para configurar CLIENTE2 como equipo cliente, lleve a cabo los pasos siguientes:

1. En CLIENTE2, instale Windows XP como parte de un grupo de trabajo. Establezca la contraseña de administrador.
2. Después de reiniciar, inicie sesión como administrador.
3. Instale el protocolo IPv6.
4. Configure el protocolo TCP/IP con la dirección IP 10.0.3.2, la máscara de subred 255.255.255.0 y la puerta de enlace predeterminada 10.0.3.1.
5. Haga ping a 10.0.1.3 desde el equipo CLIENTE2 para comprobar la integridad de la infraestructura de enrutamiento IPv4.

Para instalar IPv6

1. Abra Conexiones de red.
2. Haga clic con el botón secundario del mouse (ratón) en alguna conexión de área local y, a continuación, haga clic en **Propiedades**.
3. Haga clic en **Instalar**.
4. En el cuadro de diálogo **Seleccionar tipo de componente de red**, haga clic en Protocolo y, a continuación, en Agregar.
5. En el cuadro de diálogo **Seleccionar el protocolo de red**, haga clic en **Microsoft TCP/IP versión 6** y, a continuación, en **Aceptar**.
6. Haga clic en **Cerrar** para guardar los cambios en la conexión de red.

11.1.6. Instalar un servidor DNS

- Configurar un servidor DNS para utilizarlo con Active Directory
- Configurar un nuevo servidor DNS
- DNS Checklists
- Administración de servidores mediante Dnscmd
- Abrir la consola DNS

Para instalar un servidor DNS

1. Abra el Asistente para componentes de Windows.
2. En **Componentes**, active la casilla de verificación **Servicios de red** y después haga clic en Detalles.

3. En **Subcomponentes de Servicios de red**, active la casilla de verificación **Sistema de nombres de dominio (DNS)**, haga clic en **Aceptar** y, a continuación, en **Siguiente**.
4. Si se le pide, en **Copiar archivos de**, escriba la ruta de acceso completa de los archivos de distribución y, a continuación, haga clic en **Aceptar**.(Se copiarán los archivos necesarios en el disco duro)

Notas

- Para llevar a cabo este procedimiento, debe ser miembro del grupo Administradores en el equipo local o tener delegada la autoridad correspondiente. Si el equipo está conectado a un dominio, los miembros del grupo Administradores de dominio podrían llevar a cabo este procedimiento. Como práctica recomendada de seguridad, considere la posibilidad de utilizar la opción Ejecutar como para realizar este procedimiento.
- Para abrir el Asistente para componentes de Windows, haga clic en **Inicio**, **Panel de control**, haga doble clic en **Agregar o quitar programas** y, a continuación, haga clic en **Agregar o quitar componentes de Windows**.
- Es posible que se deba configurar algunos componentes de Windows para poder utilizarlos. Si ha instalado uno o varios componentes de ese tipo y no los ha configurado, cuando haga clic en **Agregar o quitar componentes de Windows** se mostrará una lista con los componentes que es necesario configurar. Para iniciar el Asistente para componentes de Windows, haga clic en **Componentes**.
- Se recomienda configurar manualmente el equipo para utilizar una dirección IP estática. Si el servidor DNS está configurado para utilizar direcciones dinámicas asignadas mediante DHCP, cuando el servidor DHCP asigne una nueva dirección IP al servidor DNS, los clientes DNS configurados para utilizar la dirección IP anterior de dicho servidor DNS no podrán resolver la dirección IP anterior y localizar el servidor DNS.
- Después de instalar un servidor DNS, puede decidir cómo administrar el servidor y sus zonas. Aunque puede utilizar un procesador de texto para hacer los cambios en los archivos de inicio de servidor y de zona, este método no es aconsejable. La consola DNS y la herramienta de línea de comandos DNS, dnscmd, simplifican el mantenimiento de estos archivos y se deben utilizar

siempre que sea posible. Una vez empiece a utilizar la consola o la línea de comandos para administrar estos archivos, se recomienda no modificarlos manualmente.

- Las zonas DNS almacenadas en Active Directory sólo pueden administrarse utilizando la consola DNS o la herramienta de línea de comandos dnscmd. Estas zonas no pueden administrarse con un editor de texto.
- Si desinstala un servidor DNS que aloja zonas integradas en Active Directory, estas zonas se guardarán o eliminarán según su tipo de almacenamiento. Para todos los tipos de almacenamiento, los datos de zona se almacenan en otros controladores de dominio o servidores DNS y no se eliminarán a menos que el servidor DNS que haya desinstalado en el último servidor DNS aloje dicha zona.
- Si desinstala un servidor DNS que aloja zonas DNS estándar, los archivos de zona permanecerán en el directorio raízDelSistema\system32\Dns, pero no volverán a cargarse si el servidor DNS vuelve a instalarse. Si crea una zona nueva con el mismo nombre que una zona antigua, se reemplazará el archivo de la antigua por el de la nueva.
- Cuando se escriben los datos de inicio de servidor DNS y de zona en archivos de texto, los servidores DNS utilizan el formato de archivo Dominio de nombres Internet de Berkeley (BIND, Berkeley Internet Name Domain) reconocido por los servidores BIND 4 heredados, en lugar del formato BIND 8 más reciente.

11.1.7. Configurar TCP/IP para direccionamiento estático

1. Abra Conexiones de red.
2. Haga clic con el botón secundario del mouse (ratón) en la conexión de red que desea configurar y, a continuación, haga clic en **Propiedades**.
3. En las fichas **General** (para una conexión de área local) o **Red** (para el resto de las conexiones), haga clic en **Protocolo Internet (TCP/IP)** y, a continuación, en **Propiedades**.
4. Haga clic en **Utilizar la siguiente dirección IP** y elija una de las opciones siguientes:
   - Para una conexión de área local, en **Dirección IP, Máscara de subred y Puerta de enlace predeterminada**, escriba la dirección IP,

la máscara de subred y las direcciones de puerta de enlace predeterminadas.

- Para las demás conexiones, escriba la dirección IP en **Dirección IP.**

5. **Haga** clic en **Usar las siguientes direcciones de servidor DNS**.
6. En **Servidor DNS preferido** y en **Servidor DNS alternativo**, escriba las direcciones de los servidores DNS principal y secundario.

Para configurar las opciones avanzadas de direcciones estáticas de una conexión de área local, haga clic en **Configuración avanzada** y siga uno o varios de los pasos siguientes:

Para configurar direcciones IP:

1. En la ficha **Configuración de IP**, en **Direcciones IP**, haga clic en **Agregar**.
2. En **Dirección TCP/IP**, escriba una dirección IP en **Dirección IP** y una máscara de subred en **Máscara de subred** y, a continuación, haga clic en **Agregar**.
3. Repita los pasos 1 y 2 para cada dirección IP que desee agregar y, a continuación, haga clic en **Aceptar**.

Para configurar puertas de enlace predeterminadas adicionales: En la ficha **Configuración de IP**, en **Puertas de enlace** predeterminadas, haga clic en **Agregar**.

1. En **Dirección TCP/IP de puerta de enlace**, escriba la dirección IP de la puerta de enlace predeterminada en **Puerta de enlace**. Para configurar manualmente una métrica de ruta predeterminada, desactive la casilla de verificación **Métrica automática** y escriba una métrica en **Métrica**.
2. Haga clic en **Agregar**.
3. Repita los pasos del 1 al 3 para cada puerta de enlace predeterminada que desee agregar y, a continuación, haga clic en **Aceptar**.

Para configurar una métrica personalizada para esta conexión, desactive la casilla de verificación **Métrica automática** y, a continuación, escriba un valor de métrica en **Métrica de la interfaz.**

Notas

- Para realizar este procedimiento, debe ser miembro del grupo Administradores u Operadores de configuración de red en el equipo local.
- Para abrir Conexiones de red, haga clic en Inicio, Panel de control y, a continuación, haga doble clic en Conexiones de red.

11.2. Tareas del laboratorio de pruebas de IPv6

Las tareas siguientes están diseñadas para guiarle en los pasos habituales para configurar IPv6, gracias al uso de la infraestructura del laboratorio de pruebas que se preparó en Configurar la infraestructura IPv6.

- Ping local del vínculo
- Creación de una infraestructura de enrutamiento estática
- Uso de la resolución de nombres
- Utilizar direcciones temporales

Para completar estas tareas debe utilizar los comandos Netsh para la interfaz IPv6 en el símbolo del sistema.

Para hacer ping a un host mediante direcciones locales del vínculo y ver las entradas creadas en la caché de vecinos y de enrutamiento, lleve a cabo los pasos siguientes:

1. En DNS1, escriba el comando **netsh interface ipv6 show interface "Conexión de área local"** para obtener la dirección local del vínculo de la interfaz llamada **Conexión de área local.**
2. En CLIENTE1, escriba el comando **netsh interface ipv6 show interface "Conexión de área local"** para obtener la dirección local del vínculo y el índice de interfaz de la interfaz llamada **Conexión de área local**.
3. En CLIENTE1, escriba el siguiente comando para hacer ping a la dirección local del vínculo de DNS1:

   ping direcciónLocalDelVínculoDeDNS1%identificadorDeInterfaz

   Por ejemplo, si la dirección local del vínculo de DNS1 es FE80::2AA:FF:FE9D:10C5 y el índice de la interfaz **Conexión de área local** de CLIENTE1 es 3, el comando será:

   ping FE80::2AA:FF:FE9D:10C5%3
4. En CLIENTE1, escriba el comando siguiente:

   netsh interface ipv6 show neighbors

   para ver la entrada de la caché de vecinos de CLIENTE1 para DNS1.
5. En CLIENTE1, escriba el comando siguiente:

   netsh interface ipv6 show destinationcache

   para ver la entrada correspondiente a DNS1 en la caché de destino de CLIENTE1.
6. En CLIENTE1, escriba el comando siguiente:

   netsh interface ipv6 show routes

   para ver las entradas de la tabla de enrutamiento de CLIENTE1.

11.2.1. Creación de una infraestructura de enrutamiento estática

Para configurar una infraestructura de enrutamiento IPv6 estática de forma que se tenga acceso a todos los nodos del laboratorio de pruebas mediante tráfico IPv6, lleve a cabo los pasos siguientes:

1. En ROUTER1, escriba el comando **netsh interface ipv6 show address** para obtener el índice de las interfaces conectadas a la conexión Subred 1, la conexión Subred 2 y sus direcciones locales del vínculo.
2. En ROUTER2, escriba el comando **netsh interface ipv6 show address** para obtener el índice de las interfaces conectadas a la conexión Subred 2, la conexión Subred 3 y sus direcciones locales del vínculo.
3. Escriba los siguientes comandos en ROUTER1:

   netsh interface ipv6 set interface [interface=]"conexión Subred 1"[forwarding=]enabled [advertise=]enabled

   netsh interface ipv6 set interface [interface=]"conexión Subred 1"[forwarding=]enabled [advertise=]enabled

   netsh interface ipv6 add route [prefix=]FEC0:0:0:1::/64 [interface=]"conexión Subred 1"[publish=]yes

   netsh interface ipv6 add route [prefix=]FEC0:0:0:2::/64 [interface=]"conexión Subred 2"[publish=]yes

   netsh interface ipv6 add route [prefix=]::/0 [interface=]"conexión Subred 2"[nexthop=]direcciónDeENRUTADOR2EnSubred2 **[publish=]yes**

   En el comando anterior, direcciónDeENRUTADOR2EnSubred2 representa la dirección local del vínculo asignada a la interfaz de conexión Subred 2 del ROUTER2.

   Por ejemplo, si la interfaz de conexión Subred 2 del ROUTER2 es FE80::2AA:FF:FE87:4D5C, el último comando se escribirá del modo siguiente:

   netsh interface ipv6 add route [prefix=]::/0 [interface=]"conexión Subred 2"[nexthop=]=fe80::2aa:ff:fe87:4d5c [publish=]yes
4. Escriba los siguientes comandos en ROUTER2:

   netsh interface ipv6 set interface [interface=]"conexión Subred 2"[forwarding=]enabled [advertise=]enabled

   netsh interface ipv6 set interface [interface=]=]"conexión Subred 3" [forwarding=]enabled [advertise=]enabled

   netsh interface ipv6 add route [prefix=]FEC0:0:0:2::/64 [interface=]=]"conexión Subred 2"[publish=]yes

netsh interface ipv6 add route [prefix=]FEC0:0:0:3::/64
[interface=]=]"conexión Subred 3"[publish=]yes
netsh interface ipv6 add route [prefix=]::/0 [interface=]=]"conexión Subred
2"[nexthop=]direcciónDeENRUTADOR1EnSubred2 **[publish=]yes**

En el comando anterior, direcciónDeENRUTADOR1EnSubred2 representa la dirección local del vínculo asignada a la interfaz de conexión Subred 2 del ROUTER1.
Por ejemplo, si la dirección local del vínculo de la interfaz de conexión Subred 2 del ROUTER1 es FE80::2AA:FF:FE9A:203F, el último comando se escribirá del modo siguiente:
netsh interface ipv6 add route ::/0 "conexión Subred 2"
nexthop=fe80::2aa:ff:fe9a:203f publish=yes
Si el ROUTER2 ejecuta Windows Server 2003, escriba los comandos adicionales siguientes:
netsh interface ipv6 set interface "conexión Subred 2" siteid=1
netsh interface ipv6 set interface "conexión Subred 3" siteid=1

Compruebe la integridad de la infraestructura de enrutamiento IPv6.

En CLIENTE2, escriba los comandos siguientes:
ping direcciónLocalDelSitioDelCLIENTE1
tracert -d direcciónLocalDelSitioDelCLIENTE1

11.2.2. Uso de la resolución de nombres

Para ver registros AAAA (cuádruple A) de DNS y probar el uso de DNS con IPv6, realice las siguientes acciones:

1. En DNS1, abra la consola DNS. En el servidor DNS1, haga clic en Zonas de búsqueda directa. En el panel derecho, haga doble clic en microsoft.com. En dicho panel aparecerán los registros A de IPv4 y los registros AAAA de IPv6. Para ver las propiedades del registro cuádruple A de uno de los clientes de la red, haga clic en él.
   Por ejemplo, para la dirección local del sitio de CLIENTE2 de FEC0::3:260:8FF:FE52:F9D8, el contenido del registro de recursos AAAA es:
   Nombre: cliente2.testlab.microsoft.com
   Dirección: FEC0::3:260:8FF:FE52:F9D8

2. En CLIENTE1, escriba el comando siguiente:
   ping -6 cliente2.testlab.microsoft.com
   El nombre cliente2.testlab.microsoft.com se resuelve en su dirección local del sitio mediante el envío de una consulta DNS a DNS1.
3. En CLIENTE2, cree la entrada siguiente en el archivo Hosts (que se encuentra en la carpeta raízDelSistema\System32\Drivers\Etc):
   cliente1 direcciónLocalDelSitioDeCliente1
4. En CLIENTE2, escriba el comando siguiente:
   ping -6 cliente1
   El nombre cliente1.testlab.microsoft.com se resuelve en su dirección local del sitio mediante el archivo Hosts local.

11.2.3. Utilizar direcciones temporales

Para utilizar direcciones temporales en los prefijos de direcciones globales, lleve a cabo los pasos siguientes:

1. Escriba el comando siguiente en ROUTER1:
   netsh interface ipv6 add route 3FFE:FFFF:0:1::/64 índiceDeInterfazDeSubred1 **publish=yes**
   donde índiceDeInterfazDeSubred1 es el índice de interfaz de ROUTER1 en la Subred 1.
   Por ejemplo, si el índice de interfaz de la Subred 1 es 4, el comando será:
   netsh interface ipv6 add route 3FFE:FFFF:0:1::/64 4 publish=yes
2. En CLIENTE1, escriba el comando **netsh interface ipv6 show interface** para ver la nueva dirección en la interfaz de LAN basada en el prefijo global de 3FFE:FFFF:0:1::/64.
   Debería haber dos direcciones basadas en el prefijo 3FFE:FFFF:0:1::/64. Una dirección utiliza un identificador de interfaz basado en la dirección EUI-64 de la interfaz. La otra dirección es una dirección temporal de la que se deriva aleatoriamente el identificador de interfaz..
3. Escriba el comando siguiente en ROUTER1:
   netsh interface ipv6 delete route 3FFE:FFFF:0:1::/64 índiceDeInterfazDeSubred1**store=persistent**
   donde índiceDeInterfazDeSubred1 es el índice de interfaz de ROUTER1 en la Subred 1.

Por ejemplo, si el índice de interfaz de la Subred 1 es 4, el comando será:

netsh interface ipv6 delete route 3FFE:FFFF:0:1::/64 4 store=persistent

Este comando quita el prefijo global de la tabla de enrutamiento de ROUTER1 e impide que éste lo anuncie en sus interfaces.

11.2.4. Conexión de Access Point en Red IPv6

Al agregar un Access Point, como equipo complementario para brindar el servicio de conectividad, podrían ocurrir dos escenarios:

1.- Que el Access Point (AP) solo brinde servicios de conectividad inalámbrica.

2.- Que el Access Point trabaje como Internet Router y ofrezca servicios adicionales, tales como DHCP Server, NAT, etc.

En el primer caso el AP se comportaría como un "switch" con dos puertos, un puerto conectado a la red cableada y otro puerto conectado a una especie "hub inalámbrico", es decir que este "swicth" no solo se ocuparía de conmutar tramas entre los dos puertos, sino que también haría una labor de conversión de tramas, ya que las tramas del medio inalámbrico son diferentes a las tramas del medio cableado.

Pero independientemente de esta conversión, el paquete encapsulado de IPV6 se transmitiría tal cual, lo que permitiría decir que para la capa de red (en la que están los paquetes IPV6) esto sería transparente.

En el segundo caso el AP se comportaría como un router con funciones adicionales, por lo que si no es un AP que soporta IPV6, la única opción, manteniendo los servicios del switch, sería la de construir una "isla" IPV4, conectada a un punto de conexión y conversión a la red IPV6, o la de construir un túnel IPV4 si se quiere conectar con otra red que también sea IPV4.

11.2.5. PC con acceso a WLAN via Wireless

En este caso basta con que el sistema operativo cargado en la PC soporte IPV6, ya que la forma de conexión en la capa de enlace de datos sería transparente para la capa de red. Otra opción sería la de construir una "isla" IPV4 o un túnel a través de los cuales se podría conectar el PC.

11.2.6. Impresora de Red

En este caso basta con que el sistema operativo cargado en la PC soporte IPV6, ya que la forma de conexión en la capa de enlace de datos sería transparente para la capa de red. Otra opción sería la de construir una "isla" IPV4 o un túnel a través de los cuales se podría conectar la impresora

11.3 Instalación de IPv6 en Plataformas Windows [70] [71]

- Introducción
- Windows 2003 Server
- Windows XP
- Windows 2000
- Windows 2000 SP1
- Windows 2000 con SP2, SP3 o SP4
- Windows 95, 98 y NT4.0
- Windows CE.NET, Pocket PC, Mobile 2003 y Smartphone

Introducción

En general, las plataformas de Microsoft disponen de un buen soporte para IPv6. A partir de su versión de sistema operativo "Windows XP", el protocolo viene preinstalado y su configuración es muy sencilla. En la página **http://www.microsoft.com/ipv6** de Microsoft, aparece todo el soporte de la empresa al protocolo IPv6 en sus Sistemas Operativos.

11.3.1. Windows 2003 Server

En Windows 2003, IPv6 ya esta instalado, pero es preciso habilitarlo. Para ello es necesario ejecutar, con privilegios de administrador, el siguiente comando (Menú de Inicio – Ejecutar – CMD – Enter): **prompt> netsh interface ipv6 install**

Aparecerá un mensaje indicando que se ha configurado correctamente.

---

[70] Documento original suministrado por Jordi Palet Martínez, Adaptación por: René Serral i Gracià, editado para los objetivos de la presente tesis

[71] http://www.microsoft.com/ipv6

También se puede utilizar la interfaz gráfica, seleccionando **propiedades** sobre la interfaz LAN en la que se desea habilitar IPv6. A continuación, **instalar, protocolo, IPv6**; Para comprobar que ha sido correctamente instalado, usar:

```
prompt>netsh interface ipv6 show address
Consultando el estado activo...
Interfaz 4: Ethernet
Tipo Dir. Estado DAD Vida válida Vida Pref. Dirección
--------- ---------- ----------- ---------- --------------------
Público         Preferido       infinite infinite 2001:7A0:712:13e0:204:bfc:f6bf:b008
Vínculo Preferido infinite infinite fe80::5202:b4ff:fcb1:5005


Interfaz 2: Automatic Tunneling Pseudo-Interface
Tipo Dir. Estado DAD Vida válida Vida Pref. Dirección
--------- ---------- ----------- ---------- --------------------
Vínculo Preferido infinite infinite fe80::5202:192.168.1.6


Interfaz 1: Loopback Pseudo-Interface
Tipo Dir. Estado DAD Vida válida Vida Pref. Dirección
--------- ---------- ----------- ---------- --------------------
Bucle invertido Preferido infinite infinite ::1
Vínculo Preferido infinite infinite fe80::1
prompt>
```

Se mostrará la configuración y las direcciones IPv6 adquiridas (auto-configuradas) para cada interfaz de red existente.

"netsh interface ipv6" se puede utilizar para comprobar y configurar manualmente interfaces, direcciones y rutas (usuarios avanzados).

```
prompt>netsh interface ipv6
Los siguientes comandos están disponibles:
Comandos en este contexto:
6to4        - Cambia al contexto 'netsh interface ipv6 6to4'.
?           - Muestra una lista de comandos.
add         - Agrega una entrada de configuración en la tabla.
delete  - Elimina una entrada de configuración en la tabla.
dump        - Muestra una secuencia de comandos de configuración.
help        - Muestra una lista de comandos.
install  - Instala IPv6.
isatap  - Cambia al contexto `netsh interface ipv6 isatap'.
renew  - Reinicia las interfaces IPv6.
reset   - Restablece el estado de configuración de IPv6.
set         - Establece la configuración de la información.
show        - Muestra información.
uninstall   - Desinstala IPv6.
```

Los siguientes subcontextos están disponibles: **6to4 isatap**

Para ver más ayuda acerca de un comando, escríbalo seguido de un espacio y después escriba ?. **prompt> ?**

Algunos subcomandos requieren privilegios de administrador local:

Se puede comprobar el correcto funcionamiento de la pila ipv6 con:

```
prompt>ping ::1
Haciendo ping a ::1 desde ::1 con 32 bytes de datos:
Respuesta desde ::1: tiempo<1m
Respuesta desde ::1: tiempo<1m
Respuesta desde ::1: tiempo<1m
Respuesta desde ::1: tiempo<1m
Estadísticas de ping para ::1:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 0ms, Media = 0ms
prompt>
```

::1 es la dirección de loopback en IPv6, al igual que 127.0.0.1 en IPv4. Windows 2003 incorpora la versión 6 del Internet Explorer, adaptada para navegar en webs IPv6 (e IPv4). Algunos comandos, como "tracert", "telnet", y "ftp", han sido adaptados para utilizar IPv6 por defecto, salvo que se indique "-4" (para IPv4) o si no existe dirección IPv6 de destino (caso en el que se usa por defecto la IPv4 correspondiente). Existen también algunos comandos nuevos como "ipsec6".

11.3.2. Windows XP

Si posees XP con Service Pack 1 o posterior (que es el caso más probable si tu sistema se actualiza con cierta frecuencia), sigue las instrucciones indicadas para el caso anterior (Windows 2003). Para comprobar tu versión de XP, puedes usar la interfaz gráfica, seleccionando propiedades en "Mi PC". Debajo de la opción "Sistema", en la pestaña que aparece por defecto (General), te indicará que sistema operativo tienes instalado, la versión, así como el nivel de Service Pack (en caso de tener alguno).

En cualquier caso, todas las versiones de XP, incluyen IPv6 preinstalado, pero es preciso habilitarlo. Para ello es necesario ejecutar, con privilegios de administrador, el siguiente comando (Menú de Inicio – Ejecutar – CMD – Enter): **prompt>ipv6 install**
Aparecerá un mensaje indicando que se ha configurado correctamente. Para comprobar que ha sido correctamente instalado, usar:

```
prompt>ipv6 if
Interfaz 4: Ethernet: Conexión de área local
usa unidad de detección de equipos cercanos (Neighbor Discovery)
utiliza descubrimiento de enrutador
dirección de capa de vínculo: 00-03-47-cc-30-6d
preferred link-local fe80::203:47ff:fecc:306d, duración infinite
multidifusión interface-local ff01::1, 1 referencias, no se puede informar
multidifusión link-local ff02::1, 1 referencias, no se puede informar
multidifusión link-local ff02::1:ffcc:306d, 1 referencias, último informe
vínculo MTU 1500 (vínculo MTU verdadero 1500)
limite de saltos actual 128
tiempo accesible 41000ms (base 30000ms)
intervalo de retransmisión 1000ms
transmisiones DAD 1
(...)
```

Se mostrará la configuración y las direcciones IPv6 adquiridas (auto-configuradas) para cada interfaz de red existente.

"ipv6" se puede utilizar para comprobar y configurar manualmente interfaces, direcciones y rutas (usuarios avanzados).

```
prompt>ipv6 help
Uso: ipv6 [-v] if [ifindex]
ipv6 [-p] ifcr v6v4 v4src v4dst [nd] [pmld]
ipv6 [-p] ifcr 6over4 v4src
ipv6 [-p] ifc ifindex [forwards] [-forwards] [advertises] [-advertises] [
mtu #bytes] [identificador-sitio] [preference P]
ipv6 rlu ifindex v4dst
ipv6 [-p] ifd ifindex
ipv6 [-p] adu ifindex/address [life validlifetime[/preflifetime]] [anycast] [unicast]
ipv6 nc [ifindex [address]]
ipv6 ncf [ifindex [address]]
ipv6 rc [ifindex address]
ipv6 rcf [ifindex [address]]
ipv6 bc
ipv6 [-v] rt
ipv6 [-p] rtu prefix ifindex[/address] [life valid[/pref]] [preference P]
[publish] [age] [spl SitePrefixLength]
ipv6 spt
ipv6 spu prefix ifindex [life L]
ipv6 gp
ipv6 [-p] gpu [valor de parámetro] ... (vea -?)
ipv6 renew [ifindex]
ipv6 ppt
ipv6 [-p] ppu prefix precedence P srclabel SL [dstlabel DL]
ipv6 [-p] ppd prefix
ipv6 [-p] reset
ipv6 install
ipv6 uninstall
```

Algunos subcomandos requieren privilegios de **administrador local**.
Se puede comprobar el correcto funcionamiento de la pila ipv6 con:

```
prompt>ping6 ::1
Haciendo ping ::1
de ::1 con 32 bytes de datos:
Respuesta desde ::1: bytes=32 tiempo<1m
Respuesta desde ::1: bytes=32 tiempo<1m
Respuesta desde ::1: bytes=32 tiempo<1m
Respuesta desde ::1: bytes=32 tiempo<1m
Estadísticas de ping para ::1:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 0ms, Media = 0ms
prompt>
```

::1 es la dirección de loopback en IPv6, al igual que 127.0.0.1 en IPv4. XP incorpora la versión 6 del Internet Explorer, adaptada para navegar en webs IPv6 (e IPv4). Existen otros comandos como "tracert6", "telnet6", "ftp", "ipsec6", "tlntserver", "ttcp", y "6to4-cfg".

Más información disponible en la ayuda del propio Sistema Operativo y en la web:
http://www.microsoft.com/WINDOWSXP/pro/techinfo/administration/ipv6/default.asp.

11.3.3. Windows 2000

Puede usarse la interfaz gráfica para verificar tu Sistema Operativo y versión. Para ello, selecciona **propiedades** en "**Mi PC**". Debajo de la opción **Sistema**, en la pestaña que aparece por defecto (General), indicará que sistema operativo tienes instalado, la versión, así como el nivel de Service Pack (en caso de tener alguno).

Según el nivel de SP (Service Pack) que tengas instalado, sigue las instrucciones del apartado correspondiente en las siguientes paginas.

11.3.3.1. Windows 2000 SP1

En el caso de que se desee utilizar este sistema para navegar por sitios web IPv6, es preciso utilizar el Internet Explorer **versión 5** o posterior (u otros navegadores que soporten IPv6).

Esta instalación es válida en cualquier versión comercial de Windows 2000, siempre que tenga instalado **Service Pack 1**.
Ejecute el archivo tpipv6-001205.exe desde:
http://msdn.microsoft.com/downloads/sdks/platform/tpipv6/download.asp

Descomprimirlo en una carpeta local, como por ejemplo C:\IPv6TP, ejecute, desde dicha carpeta, **setup.exe**. Probablemente sea preciso reiniciar el pc si así lo indica.

Desde el escritorio, pulsar el **botón derecho de Entorno de Red**, pulsar **propiedades**, y de nuevo, con el **botón derecho sobre la tarjeta de red** en la que se quiere instalar IPv6 (generalmente la tarjeta de red local), haciendo clic en propiedades.

Hacer clic sobre **Instalar**, y seleccionar **protocolo y añadir**. Escoja **Microsoft IPv6** y pulsar sobre **OK**. Pulsar sobre **cerrar**. Para comprobar que ha sido correctamente instalado, usar:

```
prompt>ipv6 if
Interfaz 4: Ethernet: Conexión de área local
usa unidad de detección de equipos cercanos (Neighbor Discovery)
utiliza descubrimiento de enrutador
dirección de capa de vínculo: 00-03-47-cc-30-6d
preferred link-local fe80::203:47ff:fecc:306d, duración infinite
multidifusión interface-local ff01::1, 1 referencias, no se puede informar
multidifusión link-local ff02::1, 1 referencias, no se puede informar
multidifusión link-local ff02::1:ffcc:306d, 1 referencias, último informe
vínculo MTU 1500 (vínculo MTU verdadero 1500)
limite de saltos actual 128
tiempo accesible 41000ms (base 30000ms)
intervalo de retransmisión 1000ms
transmisiones DAD 1
(...)
```

Se mostrará la configuración y las direcciones IPv6 adquiridas (auto-configuradas) para cada interfaz de red existente.

"ipv6" se puede utilizar para comprobar y configurar manualmente **interfaces**, **direcciones** y **rutas** (usuarios avanzados).

```
prompt>ipv6 help
Uso: ipv6 [-v] if [ifindex]
ipv6 [-p] ifcr v6v4 v4src v4dst [nd] [pmld]
ipv6 [-p] ifcr 6over4 v4src
ipv6 [-p] ifc ifindex [forwards] [-forwards] [advertises] [-advertises] [
mtu #bytes] [identificador-sitio] [preference P]
ipv6 rlu ifindex v4dst
ipv6 [-p] ifd ifindex
ipv6 [-p] adu ifindex/address [life validlifetime[/preflifetime]] [anycast] [unicast]
ipv6 nc [ifindex [address]]
ipv6 ncf [ifindex [address]]
ipv6 rc [ifindex address]
ipv6 rcf [ifindex [address]]
ipv6 bc
ipv6 [-v] rt
ipv6 [-p] rtu prefix ifindex[/address] [life valid[/pref]] [preference P]
[publish] [age] [spl SitePrefixLength]
ipv6 spt
ipv6 spu prefix ifindex [life L]
ipv6 gp
ipv6 [-p] gpu [valor de parámetro] ... (vea -?)
ipv6 renew [ifindex]
ipv6 ppt
ipv6 [-p] ppu prefix precedence P srclabel SL [dstlabel DL]
ipv6 [-p] ppd prefix
ipv6 [-p] reset
ipv6 install
ipv6 uninstall
```

Se puede comprobar el correcto funcionamiento de la pila ipv6 con:

```
prompt>ping6 ::1
Haciendo ping ::1
de ::1 con 32 bytes de datos:
Respuesta desde ::1: bytes=32 tiempo<1m
Respuesta desde ::1: bytes=32 tiempo<1m
Respuesta desde ::1: bytes=32 tiempo<1m
Respuesta desde ::1: bytes=32 tiempo<1m
Estadísticas de ping para ::1:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 0ms, Media = 0ms
prompt>
```

::1 es la dirección de loopback en IPv6, al igual que 127.0.0.1 en IPv4

Existen otros comandos y utilidades (subdirectorio files de la instalación), como: "tracert6", "telnet6", "ftp6", "ipsec6", "ttcp", y "6to4-cfg".

Más información disponible en:

- http://msdn.microsoft.com/downloads/sdks/platform/tpipv6.asp
- http://msdn.microsoft.com/downloads/sdks/platform/tpipv6/faq.asp

11.3.3.2. Windows 2000 con SP2, SP3 o SP4

En el caso de que se desee utilizar este sistema para navegar por sitios web IPv6, es preciso utilizar el Internet Explorer **versión 5 o posterior** (u otros navegadores que soporten IPv6).

Esta instalación es válida en cualquier versión comercial de Windows 2000, siempre que tenga instalado Service Pack 2, 3 o 4.

Para SP2, descargue el archivo tpipv6-001205-SP2-IE6.zip desde:

- http://www.ipng.nl/tpipv6-001205-SP2-IE6.zip

Para SP3 o 4, descargue el archivo tpipv6-001205-SP3-IE6.zip desde:

- http://www.ipng.nl/tpipv6-001205-SP3-IE6.zip

Descomprimirlo en una carpeta local, como por ejemplo C:\IPv6TP. Ejecute, desde dicha carpeta, **setup.exe**. Probablemente sea preciso **reiniciar** el pc si así lo indica.

Desde el **escritorio**, pulsar el botón **derecho de Entorno de Red**, pulsar **propiedades**, y de nuevo, con el **botón derecho sobre la tarjeta de red** en la que se quiere instalar IPv6 (generalmente la tarjeta de red local), haciendo clic en propiedades.

Hacer clic sobre **Instalar**, y seleccionar **protocolo y añadir**. Escoja **Microsoft IPv6** y pulsar sobre **OK.** Pulsar sobre **cerrar**. Para comprobar que ha sido correctamente instalado, usar:

```
Interfaz 4: Ethernet: Conexión de área local
usa unidad de detección de equipos cercanos (Neighbor Discovery)
utiliza descubrimiento de enrutador
dirección de capa de vínculo: 00-03-47-cc-30-6d
preferred link-local fe80::203:47ff:fecc:306d, duración infinite
multidifusión interface-local ff01::1, 1 referencias, no se puede informar
multidifusión link-local ff02::1, 1 referencias, no se puede informar
multidifusión link-local ff02::1:ffcc:306d, 1 referencias, último informe
vínculo MTU 1500 (vínculo MTU verdadero 1500)
limite de saltos actual 128
tiempo accesible 41000ms (base 30000ms)
intervalo de retransmisión 1000ms
transmisiones DAD 1
```

Se mostrará la configuración y las direcciones IPv6 adquiridas (auto-configuradas) para cada interfaz de red existente.

"ipv6" se puede utilizar para comprobar y configurar manualmente interfaces, direcciones y rutas (usuarios avanzados).

```
Uso: ipv6 [-v] if [ifindex]
ipv6 [-p] ifcr v6v4 v4src v4dst [nd] [pmld]
ipv6 [-p] ifcr 6over4 v4src
ipv6 [-p] ifc ifindex [forwards] [-forwards] [advertises] [-advertises] [
mtu #bytes] [identificador-sitio] [preference P]
ipv6 rlu ifindex v4dst
ipv6 [-p] ifd ifindex
ipv6 [-p] adu ifindex/address [life validlifetime[/preflifetime]] [anycast] [unicast]
ipv6 nc [ifindex [address]]
ipv6 ncf [ifindex [address]]
ipv6 rc [ifindex address]
ipv6 rcf [ifindex [address]]
ipv6 bc
ipv6 [-v] rt
ipv6 [-p] rtu prefix ifindex[/address] [life valid[/pref]] [preference P]
[publish] [age] [spl SitePrefixLength]
ipv6 spt
ipv6 spu prefix ifindex [life L]
ipv6 gp
ipv6 [-p] gpu [valor de parámetro] ... (vea -?)
ipv6 renew [ifindex]
ipv6 ppt
ipv6 [-p] ppu prefix precedence P srclabel SL [dstlabel DL]
ipv6 [-p] ppd prefix
ipv6 [-p] reset
ipv6 install
ipv6 uninstall
```

Se puede comprobar el correcto funcionamiento de la pila ipv6 con:

```
prompt>ping6 ::1
Haciendo ping ::1
de ::1 con 32 bytes de datos:
Respuesta desde ::1: bytes=32 tiempo<1m
Respuesta desde ::1: bytes=32 tiempo<1m
Respuesta desde ::1: bytes=32 tiempo<1m
Respuesta desde ::1: bytes=32 tiempo<1m
Estadísticas de ping para ::1:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 0ms, Media = 0ms
prompt>
```

::1 es la dirección de loopback en IPv6, al igual que 127.0.0.1 en IPv4.

Existen otros comandos y utilidades (subdirectorio files de la instalación), como: "tracert6", "telnet6", "ftp6", "ipsec6", "ttcp", y "6to4-cfg".

Más información disponible en:

- http://msdn.microsoft.com/downloads/sdks/platform/tpipv6.asp
- http://msdn.microsoft.com/downloads/sdks/platform/tpipv6/faq.asp

11.3.4. Windows 95, 98 y NT4.0

Microsoft no soporta IPv6 en estas plataformas, sin embargo existen diferentes alternativas para su uso.

Trumpet Software suministra una pila IPv6, con prueba para 30 días. Para descargarla, dirigirse a: http://www.trumpet.com.au/downloads.html (Winsock 5.0).

Alternativamente, existe una implementación de un protocolo denominado Toolnet6, de Hitachi, válida solo para algunas tarjetas de red. La información esta disponible en: http://www.hitachi.co.jp/Prod/comp/network/pexv6-e.htm.

11.3.5. Windows CE.NET, Pocket PC, Mobile 2003 y Smartphone

Las últimas generaciones de Microsoft para PDAs, teléfonos móviles, dispositivos embebidos y similares, ofrecen soporte de IPv6 de forma automática.

Para más información, diríjase a sus respectivas webs:

- http://www.microsoft.com/ipv6
- http://www.microsoft.com/windowsmobile/default.mspx

11.4. Instalación de IPv6 en plataformas Linux [72] [73]

- Introducción
- Distribuciones
- Aplicaciones
- Soporte IPv6
- Scripts de configuración IPv6
- Configuración de red
- Mostrar direcciones IPv6
- Añadir una dirección IPv6
- Eliminar una dirección IPv6
- Mostrar rutas IPv6
- Añadir una ruta IPv6 a través de un gateway
- Eliminar una ruta IPv6 a través de un gateway
- Añadir una ruta IPv6 a través de una interfaz
- Eliminar una ruta IPv6 a través de una interfaz
- ping6
- traceroute6 y tracepath6
- tpcdump

Introducción

El presente documento en ningún momento pretende hacer un análisis exhaustivo de ningún aspecto concreto de IPv6 ni de Linux, sino que el objetivo es dar una visión global y eminentemente práctica.

Se presupone del lector unos conocimientos básicos de redes TCP/IP, servicios (DNS, web, etc.) y de Linux.

---

[72] Documento original suministrado por Jordi Palet Martínez, Adaptación por: René Serral i Gracià, editado para los objetivos de la presente tesis

[73] http://www.bieringer.de/linux/IPv6/status/IPv6+Linux-status-distributions.html

11.4.1. Distribuciones

En linux IPv6 se implementa como un módulo del kernel. Así, las distribuciones con **kernel 2.2.x y 2.4.x ya vienen con este soporte y normalmente el módulo IPv6 ya está instalado**. De todas formas, habrá que asegurarse que el módulo se carga al arrancar.

Este documento se basa en la distribución Red Hat. Una información detallada sobre el soporte IPv6 en las distribuciones más comunes puede encontrarse en:

http://www.bieringer.de/linux/IPv6/status/IPv6+Linux-status-distributions.html (Se añadirán instrucciones sobre otras distribuciones: Debian, SUSE, Mandrake, etc., siempre que ésta incorpore cambios significativos)

11.4.2. Aplicaciones

Ya existen muchas aplicaciones que funcionan con IPv6. Las últimas versiones de los servidores más usados para los servicios básicos ya soportan IPv6:

- WEB (Apache: http://www.apache.org).
- DNS (BIND: http://www.isc.org).
- FTP
- TELNET
- SSH (OpenSSH: http://www.openssh.com).
- E-MAIL (Sendmail: http://www.sendmail.org).

También existen clientes de estos servicios con soporte IPv6. Incluso se pueden encontrar escritorios completos que ofrecen la mayoría de sus aplicaciones en IPv6, un ejemplo de esto es KDE.

Para una información más detallada ver:

http://www.bieringer.de/linux/IPv6/status/IPv6+Linux-status-apps.html

11.4.2.1. Soporte IPv6

Para comprobar que el kernel soporta IPv6, habrá que comprobar que existe la siguiente entrada: **/proc/net/if_inet6**

Si no existe, se puede intentar cargar el módulo ipv6 con:
#> modprobe ipv6

Si se ha cargado correctamente debe existir la entrada mencionada arriba.

Nota: Descargar el módulo puede, a veces, provocar la caída del sistema. Aunque en versiones actuales de los módulos (**kernel 2.4.19** adelante) el soporte es muy estable.

Para que cargue de forma automática el módulo IPv6 cuando se demande, se añade al archivo /etc/modules.conf la siguiente línea:

```
alias net-pf-10 ipv6
alias sit0 ipv6
alias sit1 ipv6
alias tun6to4 ipv6
```

Para deshabilitar la carga automática usar alias net-pf-10 off
Se necesitan herramientas para configurar IPv6:

- Paquete net-tools: Usando ifconfig, route. Todas las versiones actuales soportan las extensiones IPv6.
- Paquete iproute: Debe existir el programa /sbin/ip, dado que este programa es una extensión del paquete anterior, todas las versiones tienen incorporado el soporte IPv6.

11.4.2.2. Scripts de configuración IPv6

Se utilizan scripts para inicializar todo lo relacionado con IPv6 y para configurar la direcciones v4/v6 de las interfaces. Conviene actualizar a la última versión de los mismos. Estos scripts pueden obtenerse en:
http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/scripts/current/index.html

Aun qué la mayoría de distribuciones actuales configuran estos script en la instalación del sistema.

Se descarga la última versión (IPv6-initscripts-20020125.tar.gz) y se descomprime.

NOTA: existen paquetes rpm (o deb), de más fácil instalación, pero por motivos didácticos aquí se hace todo paso a paso.

Se copian los archivos de script a los directorios correspondientes:

```
/etc/sysconfig/network-scripts/network-functions-ipv6
/etc/sysconfig/network-scripts/init.ipv6-global
/etc/sysconfig/network-scripts/ifup-ipv6
/etc/sysconfig/network-scripts/ifdown-ipv6
/etc/sysconfig/network-scripts/ifup-sit
/etc/sysconfig/network-scripts/ifdown-sit
/etc/ppp/ip-up.ipv6to4
/etc/ppp/ip-down.ipv6to4
/etc/ppp/ipv6-up
/etc/ppp/ipv6-down
/usr/sbin/test-ipv6-installation
/etc/sysconfig/static-routes-ipv6
```

Aplicar "parches":

- NOTA: Algunos parches solo se aplican a determinadas versiones de Red Hat, como se indica. Por ejemplo con ifup.diff que solo se usa para RH 7.1.
- Copiar archivo .diff al mismo directorio donde está el archivo a parchear

```
#>cat network.diff | patch (/etc/sysconfig/)
#>cat ifup.diff | patch (/etc/sysconfig/network-scripts/ [link -> /sbin/)(RH 7.1)]
#>cat network.diff | patch (/etc/rc.d/init.d/) (RH 7.1)
```

Se recomienda instalar ipv6calc para habilitar la detección de direcciones extendidas. Puede obtenerse de:
http://www.bieringer.de/linux/IPv6/ipv6calc/index.html

El tar.gz (ipv6calc-0.39.tar.gz) incluye el archivo spec-file, de forma que se puede crear el RPM mediante:

```
root# rpm –ta ipv6calc-version.tar.gz
```

Para instalar:

```
root# cd /usr/src/redhat/RPMS/i386
root# rpm –i ipv6calc-version.i386.rpm
```

Debe existir, ahora, /bin/ipv6calc

En el archivo sysconfig-ipv6.txt que viene con el paquete de scripts, se da información detallada de los parámetros que se pueden configurar en cada script.

Para comprobar que la configuración es correcta, se puede ejecutar el script: **/usr/sbin/test-ipv6-installation**
Que viene con el paquete.

11.4.2.3. Configuración de red

Para cambiar el nombre del host se pone en /etc/sysconfig/network, la línea: **HOSTNAME=nombre_host**

Conviene, después de esto, añadirlo en el archivo /etc/hosts:
::1 nombre_host

El nombre de host puede verse en **/proc/sys/kernel/hostname**, o simplemente ejecutando **/bin/hostname** sin ningún parámetro.

Se deben añadir entradas en **/etc/hosts** para IPv6:

```
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

Comprobar que en **/etc/protocols/** aparecen:

```
ipv6 41 IPv6
ipv6-route 43 IPv6-Route
ipv6-frag 44 IPv6-Frag
ipv6-crypt 50 IPv6-Crypt
ipv6-auth 51 IPv6-Auth
ipv6-icmp 58 IPv6-ICMP
ipv6-nonxt 59 IPv6-NoNxt
ipv6-opts 60 IPv6-Opts
```

Comprobar que el archivo /etc/nsswitch.conf es correcto. Si no se pretende utilizar NIS (ni NIS+), habrá que comentar/eliminar las entradas con nisplus.

```
hosts: files dns
networks: files dns
```

Configurar **/etc/host.conf**

```
order hosts,bind
multi on
```

De forma que el resolver primero consulte el archivo **/etc/hosts** y luego al servidor de nombres.

La segunda línea hace que el resolver devuelva todas las direcciones válidas para un host encontrado en /etc/hosts/, en vez de sólo la primera.

Configurar **/etc/resolv.conf**

- domain: especifica el nombre del dominio local
- search: lista de nombres de dominio alternativo para búsqueda del nombre de un host
- nameserver: dirección IP de servidores de nombre a los que consultar (pueden ser varios, varias líneas "nameserver").

Para cada interfaz existirá un archivo con la configuración que se le asignará al arrancar. Supongamos que se tiene una interfaz hacia la red local (10.0.0.x/24). En /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
IPADDR=10.0.0.3
NETMASK=255.255.255.0
NETWORK=10.0.0.0
BROADCAST=10.0.0.255
GATEWAY=10.0.0.1
ONBOOT=yes
```

El archivo **/etc/sysconfig/network** tiene, respecto a IPv4:

```
GATEWAYDEV=eth0
GATEWAY=10.0.0.1
```

Que añade la ruta por defecto a través de eth1 y la IP del switch de salida hacia el ISP.

- NOTA: Es equivalente al comando route add -net 0.0.0.0/0 gw 10.0.0.1
- CONSEJO: Para establecer rutas de manera estática al arrancar el equipo (o la configuración de red) se puede utilizar el archivo **/etc/sysconfig/static-routes** (para IPv4) o **/etc/sysconfig/static-routes-ipv6** (para IPv6).

En el script **/etc/init.d/network** se encuentra:

```
# Add non interface-specific static-routes
if [-f /etc/sysconfig/static-routes]; then
grep "^any" /etc/sysconfig/static-routes | \
while read ignore args; do
/sbin/route add -$args
done
fi
```

Un ejemplo de archivo **/etc/sysconfig/static-routes**

any net 10.0.0.0/24 gw 192.168.11.1

Que añade la ruta para la red 10.0.0.0/24 a través de la puerta de enlace 192.168.11.1.

Para asignar a eth0 direcciones IPv6 se realiza lo siguiente:

En el directorio **/etc/sysconfig/network-scripts/** habrá un archivo para cada interfaz (eth0).Se añade: **A ifcfg-eth0** (CASO DE AUTOCONFIGURACIÓN):

```
IPV6INIT=yes # Habilita IPv6 en este interfaz
IPV6AUTOCONF=yes # habilita autoconfiguración
```

Es esta red se encuentra un router con el RA activado, de forma que la dirección IPv6 se configura automáticamente.

A **ifcfg-eth0** (CASO ASIGNACIÓN IPv6 ESTÁTICA):

```
IPV6INIT=yes # Habilita IPv6 en este interfaz
IPV6AUTOCONF=no # No habilita autoconfiguración
IPV6ADDR=3ffe:3328:6:2a03::3 # asigna dirección IPv6 fija
```

A esta interfaz se le asigna una dirección IPv6 fija.

```
El archivo /etc/sysconfig/network tiene, respecto a IPv6:
NETWORKING_IPV6=yes
IPV6FORWARDING=no
IPV6_AUTOCONF=yes
IPV6_AUTOTUNEL=no
IPV6_DEFAULTGW="3ffe:3328:6:2a03::1%eth0"
```

Que establece como gateway para IPv6 el router que se conecta por la interfaz eth0.

Mediante ifconfig, comprobar la configuración IPv6.

- NOTA: Cuando se haga un cambio en la configuración de red, se puede reiniciar todo el sistema de red ejecutando el script: /etc/rc.d/init.d/network restart.

También acepta otros parámetros (stop, start, status, etc).

11.4.3. Comandos útiles

11.4.3.1. Mostrar direcciones IPv6

Se puede hacer mediante el uso de ip o ifconfig:

```
#> /sbin/ip -6 addr show dev <interface>
#> /sbin/ifconfig <interface>
```

Donde <interface> puede ser lo, eth0, etc. Por ejemplo:

```
#> /sbin/ip -6 addr show dev eth0
#> /sbin/ifconfig eth0 5.2.
```

11.4.3.2. Añadir una dirección IPv6

Se puede hacer mediante el uso de ip o ifconfig:

```
#> /sbin/ip -6 addr add <ipv6address>/<prefixlength> dev <interface>
#> /sbin/ifconfig <interface> inet6 add <ipv6address>/<prefixlength>
```

Donde <interface> puede ser lo, eth0, etc. Por ejemplo:

```
#> /sbin/ip -6 addr add 3ffe:ffff:0:10:2a01::2/64 dev eth0
#> /sbin/ifconfig eth0 inet6 add 3ffe:ffff:0:10:2a01::2/64 5.3.
```

11.4.3.3. Eliminar una dirección IPv6

Se puede hacer mediante el uso de ip o ifconfig:

```
#> /sbin/ip -6 addr del <ipv6address>/<prefixlength> dev <interface>
#> /sbin/ifconfig <interface> inet6 del <ipv6address>/<prefixlength>
```

Donde <interface> puede ser lo, eth0, etc. Por ejemplo:

```
#> /sbin/ip -6 addr del 3ffe:ffff:0:10:2a01::2/64 dev eth0
#> /sbin/ifconfig eth0 inet6 del 3ffe:ffff:0:10:2a01::2/64
```

11.4.3.4. Mostrar rutas IPv6

Se puede hacer mediante el uso de ip o route:

```
#> /sbin/ip -6 route show [dev <device>]
#> /sbin/route -A inet6
```

Donde <device> puede ser lo, eth0, etc. Por ejemplo:

```
#> /sbin/route -A inet6 |grep -w "eth0" 5.5
```

11.4.3.5. Añadir una ruta IPv6 a través de un gateway

Se puede hacer mediante el uso de ip o route:

```
#> /sbin/ip -6 route add <ipv6network>/<prefixlength> via <ipv6address> [dev <device>]
#> /sbin/route -A inet6 add <ipv6network>/<prefixlength> gw <ipv6address> [dev <device>]
```

Donde <device> puede ser lo, eth0, etc. Por ejemplo:

```
#> /sbin/ip -6 route add 2000::/3 via 3ffe:ffff:0:f101::1 dev eth0
#> /sbin/route -A inet6 add 2000::/3 gw 3ffe:ffff:0:f101::1 dev eth0
```

11.4.3.6. Eliminar una ruta IPv6 a través de un gateway

Se puede hacer mediante el uso de ip o route:

```
#> /sbin/ip -6 route del <ipv6network>/<prefixlength> via <ipv6address> [dev <device>]
#> /sbin/route -A inet6 del <ipv6network>/<prefixlength> gw <ipv6address> [dev <device>]
```

Donde <device> puede ser lo, eth0, etc. Por ejemplo:

```
#> /sbin/ip -6 route del 2000::/3 via 3ffe:ffff:0:f101::1 dev eth0
#> /sbin/route -A inet6 del 2000::/3 gw 3ffe:ffff:0:f101::1 dev eth0
```

11.4.3.7. Añadir una ruta IPv6 a través de una interfaz

Se puede hacer mediante el uso de ip o route:

```
#> /sbin/ip -6 route add <ipv6network>/<prefixlength> dev <device> metric 1
#> /sbin/route -A inet6 add <network>/<prefixlength> dev <device>
```

Donde <device> puede ser lo, eth0, etc. Por ejemplo:

```
#> /sbin/ip -6 route add 2000::/3 dev eth0 metric 1
#> /sbin/route -A inet6 add 2000::/3 dev eth0
```

11.4.3.8. Eliminar una ruta IPv6 a través de una interfaz

Se puede hacer mediante el uso de ip o route:

```
#> /sbin/ip -6 route del <ipv6network>/<prefixlength> dev <device> metric 1
#> /sbin/route -A inet6 del <network>/<prefixlength> dev <device>
```

Donde <device> puede ser lo, eth0, etc. Por ejemplo:

```
#> /sbin/ip -6 route del 2000::/3 dev eth0 metric 1
#> /sbin/route -A inet6 del 2000::/3 dev eth0
```

11.4.3.9. ping6

Normalmente incluido en el paquete iputils. Uso:

```
#> ping6 <hostwithipv6address>
#> ping6 <ipv6address>
#> ping6 [-I <device>] <link-local-ipv6address>
```

11.4.3.10 traceroute6 y tracepath6

incluido en el paquete iputils. Uso: **#>traceroute6 www.kame.net**

11.4.3.11. tpcdump

Herramienta muy útil para capturar paquetes en la red. Ver (tcpdump(8)).

11.5. Compatibilidad, direcciones de compatibilidad

Para facilitar la migración de IPv4 a IPv6 y la coexistencia de ambos tipos de hosts, se han definido las direcciones siguientes:

11.5.1. Dirección compatible con IPv4

La dirección compatible con IPv4, 0:0:0:0:0:0:w.x.y.z o ::w.x.y.z (donde w.x.y.z es la representación decimal con puntos de una dirección IPv4 pública), la utilizan los nodos de pila dual que se comunican con IPv6 a través de una infraestructura IPv4. Los nodos de pila dual son nodos con protocolos IPv4 e IPv6. Cuando la dirección compatible con IPv4 se utiliza como destino IPv6, el tráfico IPv6 se encapsula de forma automática con un encabezado IPv4 y se envía al destino mediante la infraestructura IPv4.

11.5.2. Dirección asignada a IPv4

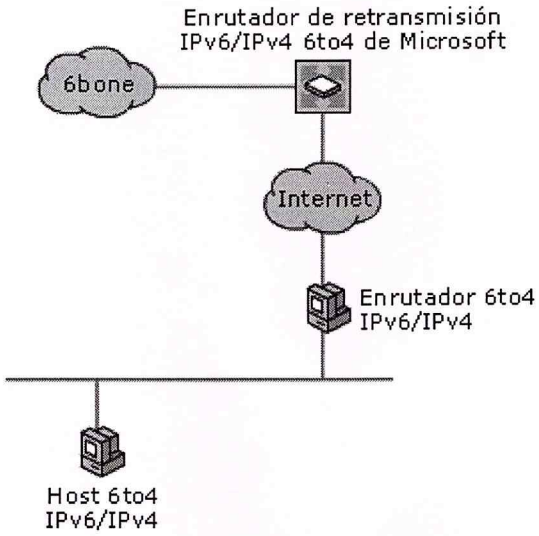
La dirección asignada a IPv4, 0:0:0:0:0:FFFF:w.x.y.z o ::FFFF:w.x.y.z se utiliza para representar un nodo exclusivo de IPv4 ante un nodo IPv6. Sólo sirve para la representación interna. La dirección asignada a IPv4 nunca se utiliza como dirección de origen o destino de un paquete IPv6. El protocolo IPv6 no admite el uso de direcciones asignadas a IPv4.

11.5.3. Dirección 6to4

La dirección 6to4 se utiliza para la comunicación entre dos nodos que ejecutan IPv4 e IPv6 sobre Internet. La dirección 6to4 se crea mediante la combinación del prefijo 2002::/16 con los 32 bits de la dirección IPv4 pública del nodo, con lo que se forma un prefijo de 48 bits. Por ejemplo, para la dirección IPv4 de 131.107.0.1, el prefijo de dirección 6to4 es 2002:836B:1::/48.

11.5.4. Conectar a la red Internet IPv6

La manera más sencilla de conectarse a la red Internet IPv6 es utilizar 6to4, que se incluye con el protocolo IPv6 en la familia de Windows Server 2003. Puede utilizar 6to4 como host 6to4 o como enrutador 6to4 si habilita Conexión compartida a Internet (ICS, Internet Connection Sharing) en un equipo que esté conectado a Internet. El Servicio de ayuda de IPv6 se configura automáticamente con las direcciones 6to4 adecuadas y utiliza un enrutador de retransmisión 6to4 específico en Internet. En la ilustración siguiente se muestra la configuración de un host que utiliza 6to4 para comunicarse en la red Internet IPv6 mediante un enrutador de retransmisión 6to4.



Con 6to4 puede hacer ping a otros equipos de la red Internet IPv6, por ejemplo, **ping -6 ipv6.research.microsoft.com**

Es posible que no se pueda tener acceso a algunos sitios de Internet IPv6. También es posible que surjan problemas de conectividad. En ambos casos, el comando **tracert -d***dirección* puede resultar útil. El parámetro **-d** impide la búsqueda DNS inversa en direcciones de enrutadores intermedios.

12 .IPV6 EN EL ENTORNO NACIONAL

IPv6 en la Escuela Politecnica Nacional [74]

Actualmente, uno de los proyectos en los que se trabaja sobre IPv6 es el uso de las redes académicas avanzadas impulsando la colaboración entre investigadores y docentes con herramientas como Video Conferencia.

El sistema de Video Conferencia que estamos utilizando es un software desarrollado por la Universidad Politécnica de Madrid (UPM), el mismo que tiene varias características como el de compartir recursos e interacción en tiempo real de varios participantes conectados a un server por IPv4 o por IPv6.

Algunos de los proyectos propuestos para IPv6 son:

- Video Conferencia IPv6
- Grid de IPv6
- DNS IPv6
- Web Page EPN en IPv6

El uso de Isabel potencializa las comunicaciones con paises y contactos que utilicen éste software mientras se use a nivel de escritorio y no para video conferencias profesionales, por lo que es necesario para video conferencia profesional el uso de equipos de Video Conferencia profesionales como SONY, TAGBERG, POLICOM, entre otros.

Estos equipos de Video Conferencia son parte de uno de los proyectos futuros de la Escuela como parte del desarrollo tecnológico en el que se encuentra inmersa actualmente.

[74] http://www.epn.edu.ec/index.php?option=com_content&task=view&id=334&Itemid=1

Asociacion de empresas Proveedoras de internet, valor agregado, portadores y tecnologías de la información [75]

Como inicio de su programa para impulsar la adopción de IPv6 entre sus asociados y del Ecuador en general, el pasado viernes 6 de julio de 2007, AEPROVI organizó un evento denominado "Introducción al IPv6".

Dentro del evento, Fabián Mejía, administrador de NAP.EC, realizó una evaluación del consumo actual de IPv4, difundió el inicio de la campaña 1/1/11 de LACNIC y realizó una capacitación teórica sobre las características de IPv6 y mecanismos de transición IPv4-IPv6.
La práctica de estos últimos temas se profundizará en el denominado "IPv6 Tour" que se encuentra coordinando AEPROVI y que se realizará dentro del segundo semestre de 2007. Este evento se realizará en parte gracias al auspicio de LACNIC.

[75] http://www.aeprovi.org.ec/content/view/136/1/

13. CONCLUSIONES, RECOMENDACIONES Y FUTURO

13.1. Conclusiones

Conforme fue avanzando el proyecto los objetivos tuvieron que ser ampliados, ya que debido a la gran complejidad y amplitud de aspectos cubiertos por estas especificaciones, resultaban imposibles de estudiar de forma aislada.

La adopción tanto de una cabecera como de unos campos de longitud fija, permiten un procesamiento más rápido y eficiente de los routers, acelerando el proceso de enrutaminamiento por INTERNET. Además el esquema de cabeceras de extensión también ayuda a la flexibilidad del protocolo, permitiendo especificar opciones tanto al destino como a los routers intermedios.

- IPv6 sigue necesitando de una aplicación "estrella" que convierta al protocolo en indispensable. Para ello esta aplicación estrella deberá ir unida a un consumo "desorbitado" de direcciones IP. Se perfilan por lo tanto algunas candidatas:
- La favorita puede ser la telefonía móvil. Con el rápido despliegue que han sufrido los teléfonos móviles, imaginando cada uno de estos aparatos dotado de una dirección IP, se vislumbra como posible la adopción de IPv6 en este tipo de terminales. Esto sería seguramente en el marco del nuevo estándar UMTS para los móviles de tercera generación.
- Otra aplicación que puede acelerar la adopción de IPv6 es la VoIP. De la misma forma que en el caso de la telefonía móvil, si se pretende dotar a todo teléfono de una dirección IP, siguiendo con la tendencia prevista de que las redes de datos suplan a las telefónicas, la escasez de direcciones se verá agudizada.
- Por último, existe una categoría de aplicaciones relacionadas con las denominadas Internet appliances que abarcan equipos como el WebTV, los juegos en red, la domótica o el home networking, aplicaciones todas ellas que serán más fácilmente desplegadas asignando una dirección IP a cada dispositivo, con lo que de nuevo el protocolo IPv6 puede jugar un papel importante.
- Hay que destacar que IPv6 además de proporcionar un mayor espacio de direcciones, cuenta con características muy adecuadas para estas aplicaciones. Entre estas características destacan la autoconfiguración, un entorno plug&play, la renumeración automática de redes, etc. Estas características se perfilan como diferenciadoras frente a otras, como QoS o seguridad, que se están incorporando a IPv4.

- BIA permite a las aplicaciones IPv4 sencillas que siguen el clásico modelo cliente/servidor, operar con aplicaciones IPv6, sin necesidad de cambiarlas, ni siquiera recompilarlas. Para ello utiliza la traducción de protocolos en la API de comunicaciones, antes de construir el paquete IP. BIA es un mecanismo más sencillo ya que no se requiere la traducción de cabeceras que realizan otros mecanismos en el nivel IP.
- BIA es un mecanismo muy ligero que puede convertirse en uno de los procesos clave para la interoperabilidad de aplicaciones IPv4 e IPv6. Sin embargo, ciertos detalles de implementación de las aplicaciones IPv4 pueden provocar fallos en BIA.
- Por este motivo, se requiere un pan de pruebas lo más exhaustivo posible para detectar incompatibilidades y realizar una clasificación aún más detallada de las posibles fuentes de error en el código de las aplicaciones IPv4.
- La portabilidad será a través de aplicaciones independientes del protocolo a través del uso de librerías para el manejo de sockets, ocultando la dependencia del protocolo y simplificando el código de la aplicación; utilización de las funciones getaddrinfo, getnameinfo en vez de gethostbyname y gethostbyaddr
- El objetivo final debe ser portar el código de las aplicaciones a IPv6 para su funcionamiento de forma nativa.
- Aunque puede parecer un esquema muy complejo, en realidad es muy simple y sobre todo, muy eficiente. Los resultados de este esquema son:
    - Las direcciones siguen siendo asignadas por el proveedor, pero al cambiar de proveedor, sólo cambia el prefijo, y la red se "renumera" automáticamente (routers, sitios y nodos finales – dispositivos – servidores).
    - Las direcciones tienen ámbito (Global, Sitio, Enlace).
    - Las direcciones, al estar compuestas por un prefijo y un identificador de interfaz, permiten separar "quién es" de "donde esta conectado":
    - Las direcciones tienen un período de vida (de validez).
- Las soluciones adoptadas en las capas superiores (SSL, SET...) tienen el gran inconveniente de que al no pertenecer a la definición del protocolo, son implementadas en el nivel de aplicación, dependiendo totalmente de la implementación de software que realice el proveedor del servicio. Además como no son universales, no todos los usuarios las contemplan e incluso pueden proporcionar la suya propia.
- IPv6 no requiere administración especial
- Las herramientas de interoperabilidad con que cuenta IPv6 facilitarán la integración

- La implementación en doble pila es una opción de rápida configuración. Se debe tener en cuenta si el hardware de comunicaciones y el hardware de usuarios finales soportan la característica de Ipv6.
- Los navegadores no soportan como recurso URL una dirección en IPv6. Por lo que es necesario configurar un servidor DNS para los recursos publicados con IPv6.
- La transición/coexistencia IPv4/IPv6 es un proceso lento e incremental que ha comenzado ya
    - Las redes académicas y de I+D ya han comenzado la introducción acelerada de IPv6 en sus infraestructuras
    - Varios países, tales como Japón, Corea, China, ... donde existe escasez de direcciones IPv4, han comenzado la transición y disponen ya de diversos servicios comerciales
    - No parece haber un modelo de negocio claro en los ISPs en Europa y EEUU, aunque IPv6 ya se empieza a ofertar de forma precomercial

13.2. Recomendaciones

- Desarrollar aplicaciones duales válidas para cualquier tipo de nodo y para comunicarse con cualquier aplicación utilizando IPv4 o IPv6.
- Conforme se mueven las actividades de implementación de IPv6, se propone una evaluación que sirva para identificar los servicios básicos para el funcionamiento de ambientes operativos en redes IPv6. Aplicaciones de correo, servicio web y servidores de nombres por ejemplo, pueden estar incluidos en estas actividades. Este último, el servicio de nombres de dominio (DNS), es considerado por muchos, una tarea de coexistencia primaria.
- Desarrollar aplicaciones independientes de la familia de direcciones:
- La mejor manera de conversión para tener la mayor portabilidad posible.
- Esconder el código dependiente del protocolo mediante el uso de las funciones: getnameinfo() y getaddrinfo()
- Habilitar la aplicación para usar las características de IPv6.

13.3. Futuro

- Se cree que más adelante el aspecto de las Redes (en la generalidad de organizaciones de carácter empresarial), que pueda soportar ambas versiones del protocolo IP. Por esto, esfuerzos futuros pudiesen ir guiados hacia la implementación de aplicaciones novedosas atadas a IPv6 que no interfieran en los servicios IPv4, los que se esperan permanecerán por muchos años.
- En base a lo dicho, IPv6 puede ser definido como uno de los trabajos más ambiciosos en el ámbito de redes y de la Internet en particular. Con cientos de miles de cooperadores a lo largo del planeta, la nueva versión del protocolo de red se ha nutrido con la máxima capacidad tecnológica, un elevado conocimiento, y una fuerte convicción por encausar y mejorar el desempeño de las redes.
- Los cambios para lograr esta transición son: actualizar a los dispositivos físicos como el DNS, el software de aplicación seguirá regido por APIs, los host y ruteadores deberán saber con que protocolo están trabajando. Además de contar con los diferentes tipos de nodos para el apoyo a ambos protocolos.

14. GLOSARIO DE TÉMINOS

Glosario de términos empleados en IPv6. Hay que tener en cuenta que a veces las traducciones son difíciles, por ejemplo: "colon notation" por "notación con dos puntos", y que muchos de los términos no aparecen en el diccionario de la RAE.

6over4

Una tecnología IPv6 diseñada para favorecer la coexistencia con IPv4, que proporciona conectividad unicast y multicast a través de una infraestructura IPv4 con soporte para multicast, empleando la red IPv4 como un enlace lógico multicast.

6to4

Una tecnología IPv6 diseñada para favorecer la coexistencia con IPv4, que proporciona conectividad unicast entre redes y máquinas IPv6 a través de una infraestructura IPv4. 6to4 utiliza una dirección pública IPv4 para construir un prefijo global IPv6.

A

agente propio

Un router situado en el enlace propio que mantiene información sobre la localización de los nodos móviles que están fuera de la red propia y de la dirección "care-of" que están empleando. Si el nodo móvil está en la red propia, el agente propio opera como un router tradicional. Si el nodo móvil está fuera de la misma el agente propio envía los datos al nodo a través de un túnel que establece hasta la dirección "care-off" del mismo.

AH

(Authentication Header) Ver cabecera de autenticación.

ámbito (scope)

Para las direcciones IPv6, el ámbito es la porción de la red a la que se supone que se va a propagar el
tráfico.

anuncio de routers

Mensaje de descubrimiento de vecinos enviado por un router bien de forma pseudo-periódica o como respuesta a un mensaje de solicitud de router. El anuncio incluye al menos información acerca de un prefijo que será el que luego utilice el host para calcular su dirección IPv6 unicast según el mecanismo "stateless".

arquitectura de pila dual

Una arquitectura para nodos IPv6/IPv4 en la que existen dos implementaciones completas de la pila de protocolos, una para IPv4 y otra para IPv6, cada una de ellas con su propia implementación de la capa de transporte (TCP y UDP).

autoconfiguración de direcciones

Proceso de configuración automática de direcciones IPv6 en un interfaz. Ver autoconfiguración de
direcciones "stateful" y autoconfiguración de direcciones "stateless".

autoconfiguración de direcciones "stateful"

Utilización de un protocolo de autoconfiguración de direcciones "stateful", por ejemplo DHCPv6, para obtener direcciones IPv6 y parámetros de configuración asociados.

autoconfiguración de direcciones "stateless"

Uso de procedimientos de descubrimiento de vecinos (y anuncios de routers) para obtener las direcciones IPv6 y los parámetros de configuración asociados.

B

bucle de rutado

Situación indeseable en una red, que provoca que el tráfico se retransmita siguiendo un bucle cerrado, con lo cual nunca llega a su destino.

C

cabecera de autenticación

Una cabecera de extensión IPv6 que proporciona autenticación del origen de datos, integridad de datos y servicio anti-repetición para la carga del datagrama y la cabecera IPv6 a excepción de los campos variables.

cabeceras de extensión

cabeceras que se sitúan entre la cabecera IPv6 y las cabeceras de los protocolos de nivel superior que son empleadas para dotar de funcionalidades adicionales a IPv6.

cabecera de fragmentación

Una cabecera de extensión IPv6 que contiene información para reensamblado para ser utilizada en el nodo receptor.

cabecera de opción de salto-a-salto

Una cabecera de extensión de IPv6 que contiene opciones que deben ser procesadas por todos los routers intermedios y el final.

caché de routers

Ver caché de destinos.

caché de destinos

Tabla mantenida por cada nodo IPv6 que mapea cada dirección (o rango de direcciones) destino con la dirección del siguiente router al que hay que enviar el datagrama. Además almacena la MTU de la ruta asociada.

caché de vecinos

Es una caché mantenida por cada nodo IPv6 que almacena la dirección IP de sus vecinos en el enlace, sus correspondientes direcciones de nivel de enlace, y una indicación de su estado de accesibilidad. Las caché de vecinos es equivalente a la caché ARP en IPv4.

capa IP dual

Una arquitectura para nodos IPv6/IPv4 en la que existe una única implementación de la capa de transporte como TCP o UDP que opera sobre implementaciones distintas de la capa de red IPv6/IPv4.

care-of address

Ver dirección "care-of".

checksum de la capa superior

Cálculo del checksum realizado en ICMPv6, TCP y UDP que utiliza la pseudo-cabecera IPv6.

CNA

Ver dirección del nodo corresponsal.

CoA

Care-of Address, ver dirección "care-of".

control de acceso al medio

Es un subnivel del nivel de enlace de datos ISO definido por el IEEE. Sus funciones son la creación de
tramas y la gestión del acceso al medio.

D

descubrimiento de prefijo

Procedimiento de descubrimiento de vecinos que permite a un determinado host o equipo final descubrir los prefijos de red para destinos de enlace local o de cara a los procedimientos de configuración de direcciones "stateless".

descubrimiento de receptores Multicast

Conjunto de mensajes ICMPv6 empleados por equipos y routers para gestionar los miembros de un grupo multicast en una subred.

descubrimiento de MTU de la ruta

Consiste en el empleo del mensaje Too Big mediante ICMPv6 para descubrir el valor máximo de MTU IPv6 en todos los enlaces entre dos equipos.

descubrimiento de parámetros

Proceso de descubrimiento de vecinos que permite a los equipos conocer los parámetros de configuración, incluyendo la MTU del enlace y el límite de saltos por defecto para los paquetes salientes.

descubrimiento de routers

Procedimiento de descubrimiento de vecinos que permite descubrir los routers conectados en un
determinado enlace.

descubrimiento de vecinos

Es un conjunto de mensajes y procesos ICMPv6 que determinan las relaciones entre nodos vecinos. El descubrimiento de vecinos reemplaza a ARP, el descubrimiento de rutas ICMP y el mensaje de redirección ICMP empleados en IPv4. También proporciona detección de vecino inaccesible.

detección de accesibilidad de vecinos

Es el proceso de descubrimiento de vecinos que determina si el nivel IPv6 de un vecino puede o no recibir paquetes. El estado de accesibilidad de cada vecino con el que se comunica un nodo se almacena en la caché de vecinos del mismo.

descubrimiento de dirección del agente propio

Un proceso en movilidad IPv6 por el que un nodo móvil que está fuera de su red descubre la lista de
agentes propios que están en su enlace propio.

dirección

Identificador asignado a nivel de la capa de red a un interfaz o conjunto de interfaces que puede ser
empleado como campo de origen o destino en datagramas IPv6.

dirección 6over4

Una dirección del tipo [prefijo 64-bit]:0:0:WWXX:YYZZ, en la que WWXX:YYZZ es la representación
hexadecimal de w.x.y.z (una dirección publica o privada IPv4), empleada para representar una máquina en la tecnología 6over4.

dirección 6to4

Una dirección del tipo 2002:WWXX:YYZZ:[SLA ID]:[Interfaz ID], en la que WWXX:YYZZ es la representación hexadecimal de w.x.y.z (una dirección publica IPv4), empleada para representar un nodo en la tecnología 6to4.

dirección anónima

Ver dirección temporal.

dirección anycast

Es una dirección del rango reservado para las direcciones unicast que identifica múltiples interfaces y es empleada para la entrega de uno a uno-entre-varios. Con un rutado apropiado, los datagramas dirigidos a una dirección de tipo anycast serán entregados en un único interfaz, el más cercano.

dirección anycast de router de subred

Dirección anycast (prefijo de 64 bits::) que se asigna a las interfaces de los routers.

dirección "care-of"

Una dirección global IPv6 utilizada por un nodo móvil cuando está conectado a un enlace ajeno. Se usa más el término inglés "care-of address" o CoA.

dirección compatible con IPv4

Es una dirección de la forma 0:0:0:0:0:0:w.x.y.z o ::w.x.y.z, donde w.x.y.z es la representación decimal de una dirección pública IPv4. Por ejemplo, ::131.107.89.42 es una dirección compatible con IPv4. Estas direcciones se emplean en túneles IPv6 Automáticos.

direcciones de compatibilidad

Direcciones IPv6 que son empleadas al enviar tráfico IPv6 sobre una infraestructura IPv4. Ejemplos de direcciones de compatibilidad son: las direcciones compatibles-IPv4, las direcciones 6to4 y las direcciones ISATAP.

dirección de lazo local

Es la dirección IPv6 ::1, que se asigna a la interfaz local.

dirección de uso local

Dirección unicast IPv6 que no es alcanzable en la Internet IPv6. Las direcciones de uso local incluyen
direcciones locales del enlace y direcciones locales del sitio.

dirección del agente propio

La dirección global IPv6 del interfaz del agente propio situado en el enlace propio.

dirección del nodo corresponsal

La dirección global asignada a un nodo corresponsal cuando se comunica con un nodo móvil que se encuentra fuera de su red propia.

dirección EUI-64

Una dirección del nivel de enlace de 64 bits que se usa como base para la generación de identificadores de interfaz en IPv6.

dirección global

Ver dirección global agregable unicast.

dirección global agregable unicast

También conocidas como direcciones globales, las "direcciones globales agregables unicast" se identifican por el formato del prefijo 001 (2000::/3). Las direcciones globales IPv6 son equivalentes a las direcciones públicas IPv4 y son globalmente rutables y alcanzables en el fragmento IPv6 de Internet.

dirección IPv4 mapeada

Es una dirección de la forma 0:0:0:0:0:FFFF:w.x.y.z o ::FFFF:w.x.y.z, donde w.x.y.z es una dirección IPv4. Las direcciones IPv4 mapeadas se emplean para representar un nodo con soporte sólo IPv4 ante un nodo IPv6.

dirección ISATAP

Es una dirección del tipo [prefijo de 64-bit]:0:5EFE:w.x.y.z, siendo w.x.y.z una dirección IPv4, pública o privada, que se asigna a un equipo ISATAP.

dirección local de sitio

Dirección de uso local identificada por el prefijo 1111 1110 11 (FEC0::/10). El ámbito de utilización de ese tipo de direcciones es el "sitio" local (de una organización), sin la necesidad de un prefijo global. Las direcciones locales de sitio no son accesibles desde otros sitios y los routers no deberían encaminar tráfico correspondiente al sitio local fuera del propio sitio. En la actualidad, se debate la necesidad de las mismas, y muy probablemente desaparezcan de la especificación de IPv6.

dirección local del enlace

Es una dirección de uso local identificada por el prefijo 1111 1110 10 (FE80::/10), cuyo ámbito es el del enlace local. Los nodos utilizan estas direcciones para comunicarse con nodos vecinos en el mismo enlace.

Son equivalentes a direcciones privadas IPv4 APIPA (Automatic Private IP Addressing).

dirección MAC

Dirección de nivel de enlace de tecnologías típicas de redes locales como Ethernet, Token Ring y FDDI. También se la conoce como dirección física, dirección del hardware o dirección del adaptador de red.

dirección multicast

Es una dirección que identifica múltiples interfaces y que se emplea en entregas de datos uno-a-muchos. Mediante la topología de rutado multicast apropiada, los paquetes dirigidos a una dirección multicast se entregarán a todas las interfaces identificadas por ella.

dirección no especificada

La dirección 0:0:0:0:0:0:0:0 (::) se emplea para reflejar la ausencia de una dirección, de forma equivalente a la dirección 0.0.0.0 de IPv4. En IPv6 se utiliza, por ejemplo, como dirección origen en los datagramas utilizados en el procedimiento para verificar la

dirección propia

Una dirección global IPv6 asignada al nodo móvil cuando está unido al enlace local y a través del cual el nodo es alcanzable independientemente de su localización en la internet IPv6.

dirección temporal

Dirección que utiliza un identificador de interfaz obtenido aleatoriamente. Este tipo de direcciones cambia con el tiempo, dificultando el seguimiento de las actividades de un host IPv6.

dirección tentativa

Dirección unicast cuya unicidad no se ha comprobado todavía.

dirección unicast

Dirección que identifica a una única interfaz y que permite comunicaciones punto a punto a nivel de red. El alcance o ámbito de utilización de esa dirección es precisamente aquél en el que esa dirección es única.

DNS

(Domain Name System.) Ver sistema de nombres de dominio

dos puntos dobles (double colon)

Práctica de comprimir series continuas de bloques de 0, en direcciones IPv6 como "::". Por ejemplo, la dirección de multicast FF02:0:0:0:0:0:0:2 se expresa como FF02::2. Si hay dos series de bloques de 0, de longitud máxima, sólo se codifica de esta manera el bloque que figura más a la izquierda de la dirección.

DHCP (Dynamic Host Configuration Protocol)

Un protocolo de configuración con estado ("stateful") que proporciona direcciones IP y otros parámetros de configuración para conexión a una red IP.

E

encapsulado de seguridad ESP (Encapsulating Security Payload)

Una cabecera y cola de extensión IPv6 que proporciona autenticación del origen de datos, integridad y confidencialidad de datos y servicio anti-repetición para la carga del datagrama encapsulado por la
cabecera y cola.

enlace

Uno o más segmentos de una red de área local limitados por routers.

enlace de acceso múltiple no-broadcast

Es una tecnología de nivel de enlace que soporta enlaces con más de dos nodos, pero sin permitir el envío de un paquete a múltiples destinos (broadcast). Por ejempo, X.25, Frame Relay y ATM.

enlace propio

Home link. En IP móvil, el enlace en el que el nodo móvil reside en su red. El nodo móvil, emplea el prefijo del enlace propio para crear su dirección propia..

estado del enlace

Tecnología de protocolo de rutado que intercambia información de rutas que consta de los prefijos de las redes conectadas a un router y su coste asociado. La información del estado del enlace se anuncia en el arranque, así como cuando se detectan cambios en la topología de la red.

EUI (Extended Unique Identifier)

Dirección del nivel de enlace definida por el IEEE (Institute of Electrical and Electronic Engineers).

F

fichero hosts

Un fichero de texto empleado para contener correspondencias nombre-dirección IP. En windows XP o .NET server está en el directorio \SystemRoot\System32\Drivers\Etc. En máquinas Unix está en el directorio /etc.

flujo

Una serie de datagramas intercambiados entre una fuente y un destino que requieren un tratamiento especial en los routers intermedios, y definidos por una dirección IP origen y destino específico, así como por una etiqueta de flujo con un valor distinto de 0.

fragmentación

Proceso por el que se divide la carga de un datagrama IPv6 en fragmentos por la máquina emisora de modo
que todos los fragmentos tienen una MTU apropiada al camino a seguir hasta el destino.

fragmento

Una porción de una carga enviada en un datagrama IPv6 enviada por un host. Los fragmentos contienen una cabecera de fragmentación.

G

grupo de máquinas (host group)

Conjunto de máquinas que en tráfico multicast escuchan una determinada dirección multicast.

grupo multicast

Conjunto de equipos escuchando una dirección multicast específica.

GSM

Global System for Mobile communications (Sistema Global para las Comunicaciones Móviles), anteriormente conocida como "Group Special Mobile" (GSM, Grupo Especial Móvil) es un estándar mundial para teléfonos móviles digitales

H

HA

Home Address, ver dirección propia.

HAA

Home Agent Address, ver dirección del agente propio.

home agent

Ver agente propio.

Home Agent Address Discovery

Ver descubrimiento de dirección del agente propio.

home link

Ver enlace propio.

host

Ver máquina (host).

I

ICMPv6 (Internet Control Message Protocol for IPv6)

Protocolo para los mensajes de control de Internet para IPv6) Un protocolo que proporciona mensajes de error para el rutado y entrega de datagramas IPv6 y mensajes de información para diagnóstico, descubrimiento de vecinos, descubrimiento de receptores multicast y movilidad IPv6.

identificador de agregación de sitio

SLA ID (Site-Level Aggregation Identifier). Campo de 16 bits dentro de la dirección global unicast que utiliza una organización para identificar subredes dentro de su red.

identificador de agregación de máximo nivel

TLA ID (Top-Level Aggregation Identifier). Campo de 13 bits dentro de la dirección unicast global reservada para grandes organizaciones o ISP por el IANA, y que por tanto identifica el rango de direcciones que tienen delegado.

identificador de agregación de siguiente nivel

NLA ID (Next-Level Aggregation Identifier). Es un campo de 24 bits en la dirección unicast global agregable que permite a los ISPs crear varios niveles jerárquicos de direccionamiento en sus redes para organizar las direcciones y el rutado hacia otros ISPs, así como para identificar los sitios de la organización.

identificador de grupo

Los últimos 112 bits o los últimos 32 bits (de acuerdo a la recomendación de la RFC 2373) de una dirección IPv6 multicast, que identifica un grupo de multicast.

identificador de interfaz

Los 64 últimos bits de una dirección IPv6 unicast o anycast.

interfaz

Una representación de un nexo físico o lógico de un nodo a un enlace. Un ejemplo de un interfaz físico es un interfaz de red. Un ejemplo de un interfaz lógico es un interfaz de túnel.

interfaz local

Interfaz interna que permite que un nodo se envíe paquetes a sí mismo.

IPv6 en IPv4

Ver túneles IPv6 sobre IPv4.

IP6.INT

El dominio DNS creado para la resolución inversa en IPv6. La resolución inversa tiene por objeto determinar el nombre de una máquina a partir de su dirección.

IPsec (Internet Protocol SECurity)

Seguridad del protocolo de Internet. Un marco de estándares abiertos que proporciona comunicaciones privadas y autenticadas a nivel de red, por medio de servicios criptográficos. IPsec soporta autenticación a nivel de entidades de red, autenticación del origen de datos, integridad y cifrado de datos y protección ante repeticiones.

ISATAP (Intra-site Automatic Tunneling Addressing Protocol)

Ver protocolo de Direccionamiento de Túneles Internos Automáticos.

J

jumbograma

Paquete IPv6 que tiene una carga útil mayor de 65.535 bytes. Los jumbogramas se indican con un valor 0 en el campo de longitud de carga útil de la cabecera IPv6, e incluyendo una opción de carga útil del Jumbo en la cabecera de opciones Salto-a-Salto.

L

lista de agentes propios

Una tabla mantenida por los agentes propios en la que se almacena la lista de routers en el enlace propio que pueden actuar como agentes propios.

lista de prefijos

Lista de prefijos de enlace mantenida por cada host. Cada entrada define directamente el rango de

direcciones IP que son alcanzables directamente, esto es, vecinos.

lista de routers de defecto

Una lista mantenida por cada máquina, en la que aparecen todos los routers de los que se ha recibido un anuncio de router con un valor de "Tiempo de vida de router" no nulo.

LL

llamada a procedimientos remotos (RPC)

Interfaz utilizada para crear programas cliente/servidor distribuidos. Las librerías que implementan el sistema de llamadas a procedimientos remotos o RPCs se encargan de gestionar los detalles relacionados con los protocolos de red y las comunicaciones.

M

MAC

Ver control de acceso al medio, dirección MAC.

máquina (host)

Un nodo que no puede reenviar datagramas no originados por sí mismo. Una máquina es típicamente el origen y destino del tráfico IPv6 y va a descartar discretamente tráfico que no esté dirigido específicamente a él mismo.

máquina 6to4

Una máquina IPv6 que está configurada con al menos una dirección 6to4 (una dirección global con el prefijo 2002::/16). Las máquinas 6to4 no requieren configuración manual y crean las direcciones 6to4 empleando mecanismos clásicos de autoconfiguración.

máquina ISATAP

Es un equipo al que se le asigna una dirección ISATAP.

MLD

Ver descubrimiento de receptores Multicast.

mobile IP

Ver movilidad IPv6.

movilidad IPv6

Un conjunto de mensajes y procesos que permiten a un nodo IPv6 cambiar arbitrariamente su posición (subred de acceso a Internet IPv6) y mantener activas las conexiones establecidas previamente.

MTU

Ver unidad máxima de transmisión.

MTU del enlace

La unidad de transmisión máxima (MTU) -número de bytes en el paquete IPv6 más grande- que puede enviarse sobre el enlace. Dado que el tamaño máximo de trama incluye las cabeceras y colas de nivel de enlace, la MTU del enlace no coincide con el tamaño máximo de trama del enlace. La MTU del enlace coincide con el máximo tamaño de carga útil de la tecnología de nivel de enlace.

MTU de la ruta

Tamaño máximo de un paquete IPv6 que puede enviarse sin emplear fragmentación entre una fuente y un destino sobre una ruta en una red IPv6. La MTU de la ruta coincide con la menor MTU de enlace para todos los enlaces de dicha ruta.

MTU IPv6

El tamaño máximo de un paquete IP que se puede enviar sobre un enlace.

N

NAT

Ver traductor de direcciones de red.

ND

Ver descubrimiento de vecinos.

NLA ID

Ver identificador de agregación de siguiente nivel.

nodo corresponsal

Un nodo que se comunica con un nodo móvil que se encuentra fuera de su red propia..

nodo IPv4

Un nodo que implementa IPv4; puede enviar y recibir paquetes IPv4. Puede ser un nodo con soporte sólo IPv4 o un nodo dual IPv4/IPv6.

nodo IPv6

Nodo que implementa IPv6 (Puede enviar y recibir paquetes IPv6). Un nodo IPv6 puede ser bien un nodo con soporte IPv6 o un nodo dual IPv6/IPv4.

nodo IPv6/IPv4

Es un nodo que dispone de implementaciones de IPv4 e IPv6.

nodo móvil

Un nodo IPv6 que puede cambiar el punto de acceso a Internet IPv6 y por tanto su dirección, y mantener también su alcanzabilidad a través de su dirección propia. Un nodo móvil conoce tanto su dirección propia como su dirección "care-of" y comunica este mapeado tanto a agente propio como a las nodos corresponsales con los que tiene una comunicación establecida.

nombre ISATAP

El nombre resuelto por ordenadores con sistema operativo Windows XP Service Pack 1 o bien de la familia de Windows .NET Server 2003 para descubrir automáticamente la dirección del router ISATAP. Los equipos con Windows XP tratan de resolver el nombre "_ISATAP."

notación hexadecimal separada con dos puntos (colon hexadecimal notation)

La notación empleada para expresar direcciones IPv6. La dirección de 128 bits es dividida en 8 bloques de 16 bits. Cada bloque se expresa como un número hexadecimal y éstos se separan del siguiente por medio del signo ortográfico dos puntos (:). Dentro de cada bloque, los ceros situados a la izquierda son eliminados.

Un ejemplo de una dirección IPv6 unicast representada en notación hexadecimal separada por dos puntos es 3FFE:FFFF:2A1D:48C:2AA:3CFF:FE21:81F9.

notación prefijo-longitud

Notación mediante la cual se expresan los prefijos de red. Tiene la forma dirección/longitud del prefijo, siendo dicha longitud el número de bits iniciales de la dirección que se fijan para definir el prefijo.

NUD

Ver detección de accesibilidad de vecinos.

O

obtención del salto siguiente

Es el proceso de obtención de la dirección o interfaz del siguiente salto para enviar o reenviar un paquete basándose en el contenido de la tabla de rutado.

opción de carga útil del Jumbo

Una opción en la cabecera de opciones Salto-a-Salto que indica el tamaño del jumbograma.

opciones de descubrimiento de vecinos

Son las opciones de los mensajes de descubrimiento de vecinos que indican las direcciones de nivel de enlace, información sobre los prefijos, MTU, redirecciones, rutas e información de configuración para movilidad IPv6.

P

paquete

La unidad de datos del protocolo (PDU) existente a nivel Internet. En el caso de IPv6, un paquete consta de una cabecera y la carga útil IPv6.

PDU

Ver unidad de datos del protocolo (PDU).

prefijo de formato

Los bits de orden alto con un valor fijo que definen un tipo de dirección IPv6.

prefijo de red

Es la parte fija de la dirección que se utiliza para determinar el identificador de la subred, la ruta o el rango de direcciones.

prefijo de sitio

Típicamente un prefijo de 48 bits que se utiliza para referirse a todas las direcciones del sitio. Los prefijos de sitio se almacenan en una tabla de prefijos que se emplea para confinar todo el tráfico asociado a esos prefijos dentro del sitio.

protocolo de Direccionamiento de Túneles Internos Automáticos

Una tecnología de coexistencia que proporciona conectividad IPv6 unicast entre máquinas IPv6 situadas en una intranet IPv4. ISATAP, obtiene un identificador de interfaz a partir de la dirección IPv4 (pública o privada) asignada a la máquina. Este identificador se utiliza para el establecimiento de túneles automáticos a través de la infraestructura IPv4.

protocolo del nivel superior

Protocolo que utiliza IPv6 como transporte y se sitúa en la capa inmediatamente superior a IPv6, como ICMPv6, TCP y UDP.

protocolo Punto-a-Punto

Método de encapsulación de red punto-a-punto que proporciona delimitadores de tramas, identificación del protocolo y servicios de integridad a nivel de bit.

protocolos de rutado

Procedimientos y conjuntos de mensajes relativos a rutas que se intercambian entre routers para construir las tablas de rutado dinámicamente.

pseudo-cabecera

Cabecera temporal que se construye para calcular el checksum necesario para asociar la cabecera IPv6 con la carga. En IPv6 se utiliza un nuevo formato de pseudo-cabecera al calcular el checksum de UPD, TCP y ICMPv6.

pseudo-periódico

Suceso que se repite en intervalos no constantes. Por ejemplo, el anuncio de rutas enviado por un router IPv6 se produce en intervalos que se calculan aleatoriamente entre un mínimo y un máximo.

R

red

Dos o más subredes conectadas por routers. Otro término empleado es interred.

redireccionar

Procedimiento englobado dentro de los mecanismos de descubrimiento de vecinos por el cual se informa a un host de la dirección IPv6 de otro que resulta más adecuado como siguiente salto hacia un determinado destino.

reensamblado

Proceso mediante el cual se reconstruye la carga original de un datagrama a partir de varios fragmentos.

registro de direcciones de equipos IPv6

Ver registro AAAA.

registro AAAA

El tipo de registro en el DNS (Sistema de Nombres de Dominio) que se emplea para resolver un nombre FDQN (Fully Qualified Domain Name) a una dirección IPv6.

registro PTR

Registro de DNS que permite resolver una dirección IP a un nombre.

resolución de nombres

Es el proceso de obtención de una dirección a partir de un nombre. En IPv6, la resolución de nombres permite obtener direcciones a partir de nombres de equipos o nombres de dominio totalmente cualificado (FQDN).

relay router 6to4

Un router IPv6/IPv4 que redirige tráfico dirigido a direcciones 6to4 entre routers 6to4 en Internet y máquinas de la Internet IPv6

retardo de unión

Tiempo transcurrido entre el envío de un mensaje de Informe de Escucha de Multicast (Multicast Listener Report) por parte de un nuevo miembro de un grupo multicast en una subred que no dispone de miembros de grupo, y el envío de los paquetes multicast de ese grupo sobre la subred.

resolución de direcciones

Proceso de resolución de direcciones del nivel de enlace para la dirección de next-hop (siguiente salto, gateway) en un enlace.

router

Nodo que puede retransmitir datagramas que no van específicamente destinados a él. En una red IPv6 un router suele enviar además anuncios relativos a su presencia y su información de configuración. A veces denominado enrutador o encaminador.

router advertisment

Ver anuncio de routers.

router 6to4

Un router IPv6/IPv4 que soporta el empleo de un interfaz de túnel 6to4 empleado para reenviar tráfico dirigido a direcciones 6to4 entre máquinas 6to4 de una red y otros routers 6to4 o routers relay 6to4 en la Internet IPv4.

router ISATAP

Un router IPv6/IPv4 que responde a las solicitudes de equipos ISATAP a través de túneles y encamina el tráfico entre equipos y nodos ISATAP de otra red o subred ISATAP.

RPC

Ver llamada a procedimientos remotos (RPC).

ruta asociada a una subred

Ruta cuyo prefijo de 64 bits corresponde al de una subred en concreto.

rutado estático

Utilización de rutas introducidas manualmente en las tablas de rutado de los routers.

ruta por defecto

La ruta con prefijo ::/0. La ruta de defecto, recoge todos los destinos y es la ruta empleada para obtener la siguiente dirección de destino cuando no hay otras rutas coincidentes.

S

segmento de una red de área local

Porción de un enlace que consta de un único medio limitado por puentes o conmutadores de nivel 2.

segmento de red

Ver subred.

selección de ruta adecuada

Es el algoritmo empleado por el proceso de selección de rutas para escoger las rutas de la tabla de rutado que más se acercan a la dirección de destino a la que se debe enviar o encaminar el paquete.

sistema de determinación de ruta

Proceso por el cuál se selecciona cuál es la ruta concreta de la tabla de rutado por la que se va a encaminar el datagrama. Esto es, se selecciona el siguiente router al que se va a mandar el datagrama.

sistema de nombres de dominio

Un sistema jerárquico de almacenamiento y su protocolo asociado para almacenar y recuperar información sobre nombres y direcciones IP.

SLA ID

Ver identificador de agregación de sitio.

dirección de nodo solicitada (solicited-node address)

Dirección muticast utilizada por los nodos durante el proceso de resolución de direcciones. La dirección de nodo solicitada se construye con el prefijo FF02::1:FF00:0/104 y los últimos 24 bits de la dirección IPv6 unicast. Esa dirección se emplea a modo de pseudo dirección unicast para llevar a cabo una resolución de direcciones más eficiente en los enlaces IPv6.

subred

En IPv6 uno o más enlaces que utilizan el mismo prefijo de 64 bits.

T

tabla de rutado IPv6

Conjunto de rutas empleadas para determinar la dirección e interfaz del siguiente nodo en el tráfico IPv6 enviado por un equipo o reencaminado por un router.

tiempo de vida en estado "preferred" preferida

Tiempo durante el que una dirección unicast obtenida mediante el mecanismo de autoconfiguración stateless permanece en estado "preferred" o de preferida. Este tiempo viene indicado por el campo "Preferred Lifetime" de la opción "Prefix Information" (información de prefijo) de los mensajes de anuncio de routers.

tiempo máximo de validez de una dirección

Tiempo en el que una dirección unicast conseguida mediante el proceso de autoconfiguración stateless permanece en estado válido (tanto preferido como desaprobado o deprecated).

TLA ID (Top-Level Aggregation Identifier)

Ver identificador de agregación de máximo nivel.

traductor de direcciones de red

Es un router IPv4 que traduce direcciones y puertos al reenviar paquetes entre una red con direcciones privadas e Internet.

transición

Hablando de IPv6, consiste en la conversión de nodos sólo IPv4 a nodos con doble pila, o sólo IPv6.

túnel

Un túnel IPv6 sobre IPv4, en los que los puntos finales sin determinados por configuración manual.

túnel automático

Un túnel IPv6 sobre IPv4 en el que los puntos finales son determinados por el empleo de interfaces lógicos de túneles, rutas y direcciones orígenes y destino IPv6.

túneles IPv6 automáticos

Creación automática de túneles que se emplea con direcciones compatibles con IPv4.

túneles IPv6 sobre IPv4

Consiste en enviar paquetes IPv6 con una cabecera IPv4, de forma que el tráfico IPv6 pueda enviarse sobre una infraestructura IPv4. En la cabecera IPv4, el campo de Protocolo toma el valor 41.

túnel IPv4 multicast

Ver 6over4.

túnel máquina-a-máquina

Un tunelado IPv6 sobre IPv4 en el que los dos extremos son máquinas.

túnel máquina-a-router

Un tunelado IPv6 sobre IPv4 en el que el túnel empieza en un host y acaba en un router IPv6/IPv4.

U

unidad de datos del protocolo (PDU)

Conjunto de datos correspondiente a una capa concreta en una arquitectura de red en capas. La unidad de datos de la unidad n se convierte en la carga útil de la capa n-1 (la capa inferior).

unidad máxima de transmisión (MTU)

Es la unidad de datos del protocolo más grande que se puede enviar. Las unidades máximas de
transmission se definen a nivel de enlace (tamaño máximo de trama) y a nivel de red o de Internet (tamaño máximo de los paquetes IPv6).

Sistema universal de telecomunicaciones mobiles (UMTS)

Universal Mobile Telecommunications System (UMTS) es una de las tecnologías usadas por los móviles de tercera generación (3G). Sucesor de GSM, también llamado W-CDMA.

V

vecino

Nodo conectado al mismo enlace.

vector de distancia

Una tecnología para protocolos de rutado que propaga información de rutado en la forma de un identificador de red y su distancia en número de saltos.

vector de ruta

Se trata de una tecnología de protocolo de rutado que intercambia secuencias de información de saltos indicando el camino a seguir en una ruta. Por ejemplo, BGP-4 intercambia secuencias de números de sistemas autónomos. Un sistema autónomo es una porción de la red perteneciente a la misma autoridad administrativa.

W

Acceso múltiple de banda ancha por división de código (W-CDMA)

Acronimo de Wideband-Code Division Multiple Access. Constituye una tecnología móvil inalámbrica de tercera generación que aumenta las tasas de transmisión de datos de los sistemas GSM utilizando la interfaz aérea CDMA en lugar de TDMA (Acceso Múltiple por División de Tiempo) y por ello ofrece velocidades de datos mucho más altas en dispositivos inalámbricos móviles y portátiles que las ofrecidas hasta el momento.
W-CDMA es la conexión 3G para GSM

15. BIBLIOGRAFIA

- http://www.microsoft.com/ipv6
- IPv6 UJI - Luís Peralta, Febrero 19 del 2002
- Cisco IPv6 Implementations and Transitions, June 2006
- Estudio de la problemática de la implantación de IPv6 en la RECETGA (Andrés Gómez, José Carlos Pérez, Juan Villasuso, Natalia Costas) Enero 28 del 2005
- Deploying IPv6 Networks (By Ciprian Popoviciu, Eric Levy-Abegnoli, Patrick Grossetete)
- Understanding IPv6 - Joseph Davies, Microsoft 2004
- Una breve historia de Internet (Primera Parte) Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E.
- Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Lawrence G. Roberts, Stephen Wolff
- Cisco Networking Academy Program
- Internet Architecture Board
- Designing Internetworks with IPv6, Henrik Lund Kramshøj, April 28, 2002
- RFC 2460
- Internet Engineering Task Force http://www.ietf.org
- RFC 2401: Security Architecture for the Internet Protocol
- OReilly.IPv6.Essentials.2nd.Edition.May.2006
- Una breve historia de Internet (Primera Parte) Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Lawrence G. Roberts, Stephen Wolff
- Sacando partido a IPv6 con redes IPv4, Palet Jordi, CTO Consulitel
- Internet Architecture Board
- Internet Corporation for Assigned Names and Numbers (ICANN) http://www.icann.org/announcements/IPv6-report-06sep05.htm
- IPv6 - La Internet de nueva generación (2005) Latif Laid
- J. Postel (Editor): "Internet Protocol," IETF Standard RFC 791/STD 5, septiembre 1981 (ftp://ftp.rfceditor.org/innotes/rfc791.txt).
- V. Fuller y otros: "Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy," IETF Proposed Standard RFC 1519, septiembre 1993

- Durand y otros: "The H-Density Ratio for Address Assignment Efficiency An Update on the H ratio", IETF Informational RFC, RFC 3194, noviembre de 2000
- P. Srisuresh y otros: "IP Network Address Translator (NAT) Terminology and Considerations," IETF Informational RFC, RFC 2663, agosto de 1999
- B. Dutcher: "The NAT Handbook: Implementing and Managing Network Address Translation," John Wiley & Sons,352 páginas, ISBN 0471390895, noviembre de 2000.
- S. Bradner y otros: "The Recommendation for the IP Next Generation Protocol," IETF Proposed Standard RFC 1752, enero de 1995
- R. Droms: "Dynamic Host Configuration Protocol," IETF Draft Standard RFC 2131, March 1997
- National Security Agency (NSA) http://www.nsa.org
- Driscol &Associates 1995, 2002, 2003
- http://www.telefonica.com/sociedad_de_informacion/
- http://www.ipv6.org
- Internet Architecture Board
- Foro UMTS/GSM
- Palet Jordi, CTO Consulitel
- CISCO Systems CCNA Curriculum V 3.1
- IPv6 Essentials, 2nd Edition (2006)
- Javier Sedano, Mundo Linux (Revistas Profesionales)
- Estudio de la problemática de la implantación de IPv6 en la RECETGA (Andrés Gómez, José Carlos Pérez, Juan Villasuso, Natalia Costas) Enero 28 del 2005
- IPv6: Mecanismos de Transición IPv4 - IPv6
- Evolución de Internet desde IPv4 a IPv6: David Fernández Cambronero (Departamento de Ingeniería de Sistemas Telemáticas ETSIT-UPM)
- Comunicaciones de Telefónica I+D (Telefónica Investigación y Desarrollo) Marzo 2005
- IPv6 UJI - Luis Peralta, Febrero 19 del 2002
- Designing Internetworks with IPv6, Henrik Lund Kramshoj, April 28, 2002
- CISCO CCNA IPv6 IpSec transition

- Desarrollo de Aplicaciones con soporte IPv6 Ing. Azael Fernández Alcántara Universidad Nacional Autónoma de México, UNAM Grupo de Trabajo de IPv6 en Internet2 Capítulo Mexicano del Foro IPv6 NETLab Reunión de Otoño 2003 3 de octubre 2003 Cd. de Puebla, México

- Transición de aplicaciones y servicios a IPv6, Eva M. Castro, Grupo de Sistemas y Comunicaciones (GSyC), universidad Rey Juan Carlos (URJC)

- http://go.microsoft.com/fwlink/?LinkId=103

- http://www.bieringer.de/linux/IPv6/status/IPv6+Linux-status-distributions.html

- http://www.epn.edu.ec/index.php?option=com_content&task=view&id=334&Itemid=1

- http://www.aeprovi.org.ec/content/view/136/1/