TITULO DEL PROYECTO: Elaboración de un estado del arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco.

AUTOR: **RAUL BAREÑO GUTIERREZ**

UNIVERSIDAD PONTIFICA BOLIVARIANA
FACULTAD DE INGENIERIA ELECTRONICA
ESPECIALIZACION EN TELECOMUNICACIONES
BUCARAMANGA
2010

➢ OBJETIVO GENERAL

Realizar una monografía sobre el protocolo IPV6 donde se condense su estado del arte, las tendencias de migración y el análisis para su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP, OSPF basados en dispositivos CISCO; aplicado sobre cualquier plataforma tecnológica de nueva generación.

➢ OBJETIVOS ESPECIFICOS

- Seleccionar las referencias bibliográficas más pertinentes que puedan existir con respecto al estado del arte del protocolo IPV6; su implementación y migración sobre los protocolos de enrutamiento RIPNG, EIGRP, OSPF.

- Realizar un informe con los resultados del análisis de las fuentes bibliográficas; donde además se expliquen los métodos actuales de migración hacia IPV6 en los dispositivos de enrutamiento, haciendo énfasis en los de estado doble y tunelización.

- Validar el funcionamiento de IPV6 sobre los protocolos de enrutamiento RIPNG, EIGRP, OSPF, mediante la selección e implementación de los sistemas operativos que los soporten, su configuración y prueba.

- Diseñar prácticas de laboratorio en entornos simulados; configurados e instalados en el laboratorio de CISCO® de las Unidades Tecnológicas de Santander donde se pueda verificar la implementación de IPv6 sobre dichos protocolos de enrutamiento y la factibilidad de la migración de IPv4 a IPv6 usando los métodos analizados.

- Elaborar la monografía y los manuales de laboratorio donde se condensen los resultados, el análisis, las evidencias de cada entorno configurado, los comandos usados; junto con las conclusiones de la indagación teórica y las pruebas realizadas.

TABLA DE CONTENIDO

RESUMEN:

Titulo: Elaboración de un estado del arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco.

AUTOR: Raúl Bareño Gutiérrez

FACULTAD: Esp. En telecomunicaciones

DIRECTOR: John Jairo Padilla Aguilar

El protocolo enrutado IPv6; es un nuevo protocolo que permitirá el crecimiento exponencial de internet de nueva generación; para la cantidad de usuarios que día a día solicitan más y más servicios en la mundialmente llamada internet.

Sera un protocolo que garantizara la masificación de nuevas plataformas tecnológicas; y además cambiara la manera de pensar, la manera de comunicarnos y hasta de jugar entre usuarios finales; debido a su facilidad de implementación y configuracion en dispositivos activos como routers y dispositivos de capa 3 como switches multicapa. Existen variaciones que deben efectuar los nuevos protocolos de enrutamiento dinámico que podrán ofrecer este protocolo IPv6 son: RIPNG protocolo de enrutamiento de nueva generación; OSPFv3 protocolo de enrutamiento de primero la ruta libre mas corta; y el protocolo EIGRP para IPv6 protocolo de enrutamiento de Gateway mejorado para IPv6 entre otros.

También comprenderá el alto espacio de direccionamiento ya que son direcciones de 128 bits expresados en notación hexadecimal de 8 campos cada campo será de 16 bits; que será el gran espacio de direcciones que se pueden entregar por persona en el mundo y empezara a suplir el agotamiento de direcciones IPv4 que existe en la actualidad.

Dentro de los mecanismos de transicion entre IPv4 e IPv6 se encuentran los de estado doble y tunelización que facilitaran la interactividad entre los dos protocolos enrutados

Otro aspecto a destacar es la manera como se diseñaron los diferentes laboratorios de práctica para que tanto los estudiantes como docentes lo entiendan de una manera muy practica ya que son ejercicios diseñados sobre entornos reales muy explicativos con comandos con las salidas respectivas para su fácil comprensión de cada laboratorio se dejan manuales de comandos y los montajes y imágenes respectiva todo basado montado e implementado sobre equipos de CISCO.

PALABRAS CLAVE: ripng, ospf; eigrp, estado dual, tunelización, cisco

SUMMARY:

Title: Development of a state of the art on the IPv6 protocol, and implementation of dynamic routing protocols such as RIPng, EIGRP and OSPF platform based on Cisco equipment.

Author: Raúl Gutiérrez Bareño

FACULTY: Esp in telecommunications

DIRECTOR: John Jairo Padilla Aguilar

IPv6 routing protocol, is a new protocol that will allow exponential growth of new generation Internet, for the number of daily users demanding more and more services in the world called internet.

A protocol that will ensure the mass of new technology platforms, and also changed the way we think, the way we communicate and even play among end users because of its ease of implementation and configuration in active devices such as routers and layer 3 devices and multilayer switches. There are variations to be made by the new dynamic routing protocols that can provide the IPv6 protocol are routing protocol RIPng new generation OSPFv3 Routing Protocol Path First Open Shortest, and EIGRP protocol to IPv6 Gateway Routing Protocol Enhanced IPv6 among others.

Also include the high address space because they are 128-bit address expressed in hexadecimal notation of 8 fields each field is 16 bits, which will address the large space that can be delivered per person in the world and begin to address depletion IPv4 address that exists today.

Among the mechanisms of transition between IPv4 and IPv6 are the dual state and tunneling to facilitate the interaction between the two routed protocols

Another aspect is how the different laboratories were designed practice for both students and teachers understand what a very practical way as they are exercises designed around real-world environments very explanatory with commands to respective outputs for easy understanding Each laboratory manuals stop commands and respective assemblies and pictures all assembled and implemented based on CISCO equipment.

KEY WORDS: RIPng, ospf, eigrp, dual status, tunneling, cisco

1.0 Explicando IPv6

1.1 Introducción a IPv6

IPv6 tiene la habilidad de escalar redes para futuras demandas requiere fuentes ilimitadas de direcciones IP y movilidad mejorada. IP versión 6 (IPv6) combina direccionamiento extendido con un encabezado más eficiente y de mejores características para satisfacer las demandas de redes escalables en el futuro.

IPv6 satisface las exigencias de complejos requerimientos de direccionamiento jerárquico que IP versión 4 (IPv4) no proporciona. Una de las principales ventajas de IPv6 es que puede permitir comunicaciones de extremo a extremo sin la necesidad de la traducción de direcciones de red (Network Address Translation -NAT) un requisito para una nueva generación de experiencias compartidas y aplicaciones en tiempo real.

Los routers Cisco Sytems actualmente soportan IPv6 en la versión Cisco IOS software 12.2 (2) T y posteriores. Para cualquier protocolo de enrutamiento dinámico como RIPNG[1], OSPF v3[2] y EIGRP.

Internet se transformará a IPv6 completamente reemplazando IPv4. Sin embargo, IPv4 no está en peligro de desaparecer de la noche a la mañana. Más bien, este coexistirá con IPv6 y gradualmente será reemplazado por este.

Este cambio ya ha iniciado, particularmente en Europa, Japón, y Asia pacífica. Estas áreas han agotado sus direcciones asignadas de IPv4, haciendo a IPv6 más atractivo. Además de su técnica y potencial de negocio, IPv6 ofrece una fuente virtual ilimitada de direcciones IP. IPv4 actualmente provee 2 mil millones de direcciones usables con sus 32 bits de espacio de dirección.

Como IPv6 tiene un espacio de 128 bits de dirección, puede generar un stock ilimitado virtual de direccionamiento suficiente para asignar a todas las personas del planeta.

Consecuentemente, algunos países, tales como Japón, están adoptando agresivamente IPv6. Otros, como en la Unión Europea, se están moviendo a IPv6, y China está considerando construir redes de IPv6 puras a partir de cero.

Incluso en Norteamérica, donde las direcciones de internet son abundantes, el departamento de defensa de Norteamérica (DoD) ordenó en Octubre 1, de 2006, que todos los nuevos equipos adquiridos deban tener capacidad para IPv6. El DoD piensa cambiar completamente a equipos IPv6 para el 2010.

---

[1] http://www.normes-internet.com/normes.php?rfc=rfc2080&lang=es
[2] http://tools.ietf.org/search/rfc5340

1.2 Características de IPv6

IPv6 es una mejora de gran alcance para IPv4, y varios rasgos de IPV6 ofrecen mejoras funcionales:

Mayor espacio de direccionamiento: ofrece mejoras en accesibilidad global y flexibilidad; la adición de prefijos que se anuncian en las tablas de enrutamiento; **multihoming** para varios proveedores de servicio de internet (ISPs); que pueden incluir la configuración automática de direcciones de la capa de enlace en el espacio de direcciones; opciones **plug and play**; redireccionamiento público a privado de extremo a extremo sin traducción de dirección; y mecanismos simples para la renumeración y modificación de direcciones.

Encabezamiento simple: provee mejor eficiencia de enrutamiento; no hace broadcast y así no hay amenaza potencial de tormentas de broadcast; no hay requerimiento de proceso de cheksum; mecanismos de encabezado más simple y eficiente; y etiquetas de flujo para cada procesamiento por flujo con la no necesidad de abrir la capa de transporte interno de paquetes para identificar los diferentes flujos de tráfico.

Movilidad y seguridad: asegura el cumplimiento de los estándares de funcionamiento IPsec y móviles IP; la movilidad se basa en estos, así cualquier nodo IPv6 se puede usar cuando sea necesario; y permite a las personas moverse en las redes con dispositivos móviles de red con muchas conectividades inalámbricas.

IP móvil es un estándar de Grupo de Trabajo en Ingeniería de internet (Internet Engineering Task Force -IETF) disponible tanto para IPv4 e IPv6. El estándar activa los dispositivos móviles para moverse sin interrupción en las conexiones de red establecidas. Como IPv4 no provee automáticamente la clase de movilidad, se debe agregar esta a las configuraciones adicionales.

IPsec es el estándar IETF para seguridad de red IP, disponible tanto para IPv4 e IPv6. Aunque las funciones son esencialmente idénticas en ambos entornos, IPsec es obligatorio en IPv6. IPsec está activo en todos los nodos IPv6 y están disponibles para su uso. La disponibilidad de IPsec en todos los nodos hace que el Internet IPv6 sea más seguro. IPsec también requiere claves para cada parte, lo que implica el empleo y distribución de una clave global.

Riqueza de transición: Se pueden incorporar capacidades de IPv4 existente en IPv6 de la siguiente manera:

- Configurando un router de estado doble con IPv4 e IPv6 en la interfaz de un dispositivo de red.

- Usando la técnica IPv6 sobre IPv4 (también llamado túnel 6 a 4) el cual usa un túnel IPv4 para transportar el tráfico IPv6. Ese método (RFC 3056) reemplaza el túnel compatible IPv4 (RFC 2893). La

versión del software Cisco IOS versión 12.3 (2) T (y posteriores) solo permiten el protocolo de traducción (NAT-PAT) entre IPv6 e IPv4. Esta traducción permite la comunicación directa entre hosts que hablan en diferentes protocolos.

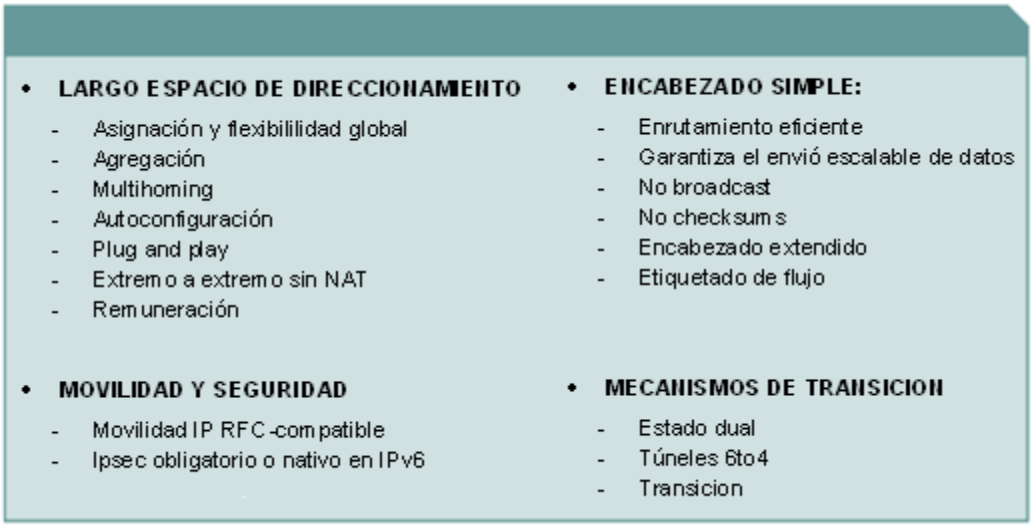


Fig.1 Características Avanzadas de IPv6[3]

1.3 Mayor Espacio de Direccionamiento

IPv6 incrementa el número bits de dirección por un factor de 4, de 32 a 128, permitiendo un gran número de nodos direccionales. Sin embargo, como en cualquier esquema de direccionamiento, no todas las direcciones están utilizadas o disponibles.

El protocolo de direccionamiento actual IPv4 es ampliado aplicando técnicas como NAT y asignación de direccionamiento temporal. Pero la manipulación de carga útil de datos para dispositivos intermedios desafía (o complican) las ventajas de la comunicación punto a punto y la calidad de servicio (QoS).

IPv6 ofrece a todos los usuarios múltiples direcciones globales que pueden ser usados por una amplia variedad de dispositivos, incluyendo teléfonos celulares, asistentes digitales personales (PDAs), y vehículos con IP activo. Estas direcciones son accesibles sin necesidad de utilizar la traducción de direcciones IP, agrupación y técnicas temporales de distribución.

El incremento del número de bits para el direccionamiento también incrementa el tamaño del encabezado IPv6. Porque cada encabezado IP contiene una dirección de origen y destino, el tamaño del campo de encabezamiento es de 256 bits para IPv6, comparado con 64 bits para IPv4.

[3] Tomada del material virtual del curriculum CCNP versión 5.

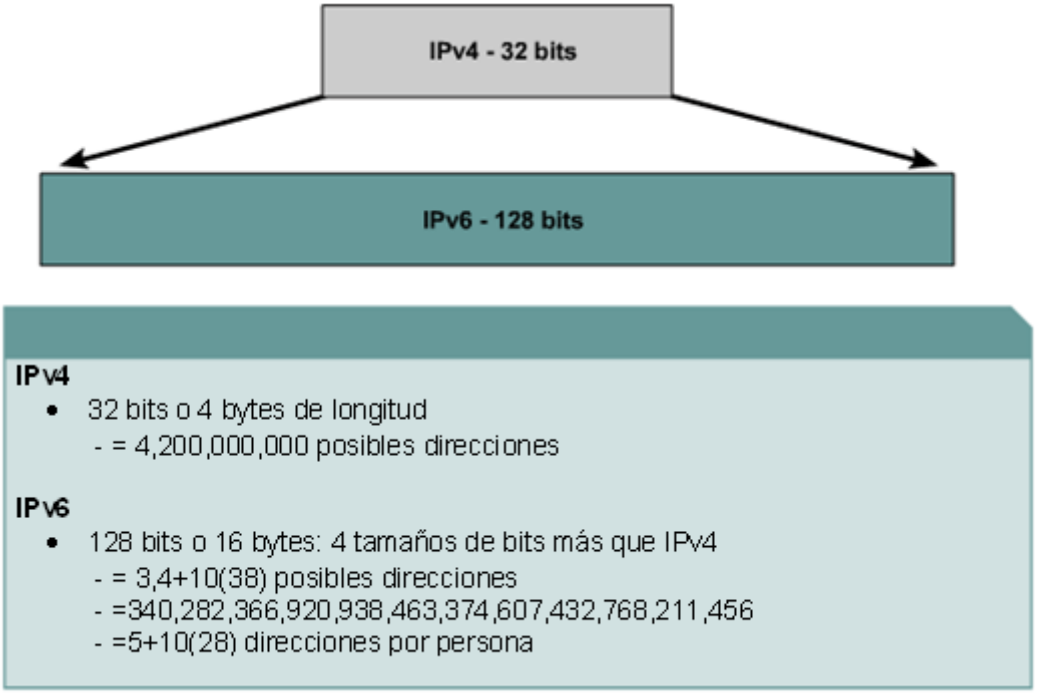


Fig. 2 Gran Espacio de Direcciones[4]

El mayor espacio de direccionamiento hace el espacio de asignaciones de direcciones más grande para los ISPs y organizaciones. Un ISP agrega todos los prefijos de sus clientes en un prefijo único y anuncia el prefijo único a la Internet IPV6. El incremento del espacio de direcciones es suficiente para permitir a las organizaciones definir un prefijo único para toda la red.

La agregación de prefijos de cliente resulta en una tabla de enrutamiento eficiente y escalable. El enrutamiento escalable es necesario para expandir la adopción amplia de funciones de red, permitiendo al Internet ajustar lo siguiente:

- Incremento del número de consumidores de banda ancha de alta velocidad, con conexión siempre activa.
- Los usuarios que dedican más tiempo en línea comprando servicios de comunicación (como música) y participación en valores altos de búsquedas de ofertas.
- Redes de hogar con aplicaciones de redes grandes como voz IP inalámbrica (VoIP), vigilancia de hogar, y servicios avanzados como la demanda de video en tiempo real (VoD).
- Juegos masivamente escalables con participantes globales.
- Medios ricos de aprendizaje en línea, proporcionando a alumnos demanda de laboratorios a distancia y simulación de laboratorios.

[4] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 699.

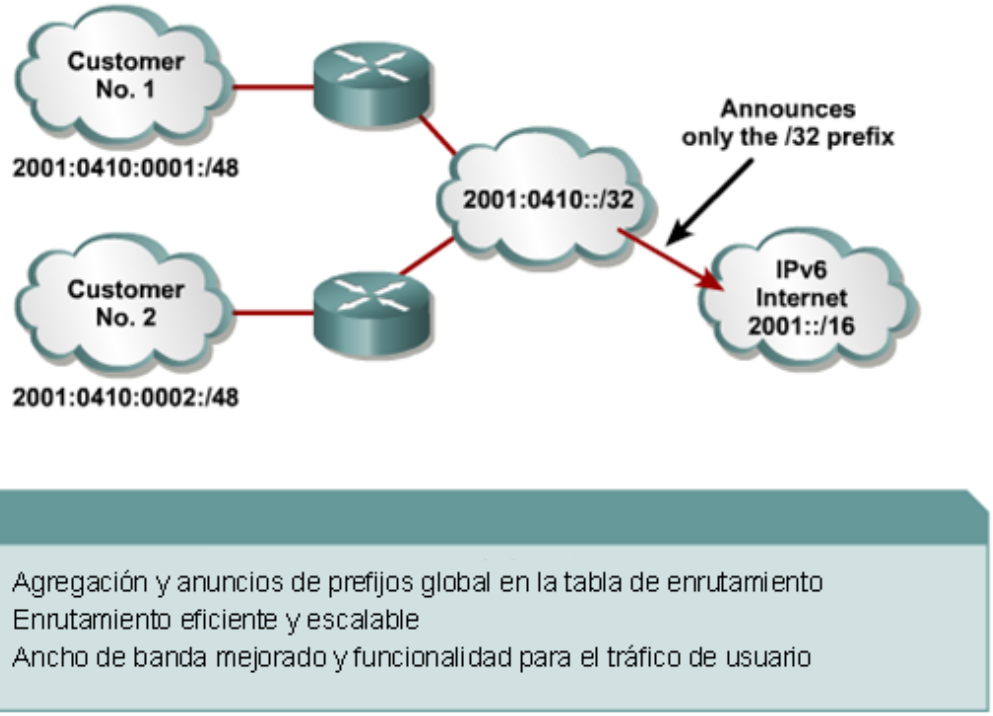


Fig. 3 Mayor Espacio de Direcciones Permite la Agregación de Direcciones[5]

2.0 Direccionamiento IPv6

2.1 Arquitectura de Direccionamiento IPv6

El encabezado IPv4 contiene 12 campos básicos de encabezamiento, seguido por un campo de opciones y una parte de datos (usualmente el segmento de capa de transporte). El encabezamiento IPv4 básico tiene un tamaño fijo de 20 octetos. La variable de opciones de longitud de campo incrementa el tamaño de todo el encabezado IP. IPv6 contiene 5 de los 12 campos de encabezamiento básico de IPv4. El encabezado IPv6 no requiere los otros 7 campos.

Los Routers manejan la fragmentación en IPv4, lo que causa una gran variedad de problemas de procesamiento. Los Routers IPv6 no desarrollan fragmentación. A cambio un proceso de descubrimiento determina la máxima unidad óptima de trasmisión (MTU) a usarse durante las sesiones dadas.

En el proceso de descubrimiento, el dispositivo origen IPv6 procura enviar un paquete en el tamaño especificado por las capas superiores, como la capa de transporte o aplicación. Si el dispositivo recibe un paquete ICMP[6] con un mensaje muy grande, este retransmite el paquete MTU de descubrimiento con un MTU más pequeño y repite el proceso hasta obtener una respuesta

[5] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 706.
[6] http://www.faqs.org/rfcs/rfc2463.html

de que el paquete de descubrimiento llegó intacto. Entonces se fija el MTU para la sesión.

El paquete ICMP con un mensaje muy grande contiene el tamaño apropiado de la MTU para la ruta. Cada dispositivo origen necesita rastrear el tamaño de la MTU para cada sesión. Generalmente, el rastreo se hace mediante la creación de un cache que se basa en la dirección de destino. Sin embargo, esto solo puede hacerse usando la etiqueta de flujo. Si el enrutamiento (envío) basado en el origen se desarrolla, el rastreo del tamaño de la MTU puede utilizar las direcciones de origen.

El proceso de descubrimiento es benéfico ya que, como las rutas de enrutamiento varían, un nuevo MTU puede ser más apropiado. Cuando un dispositivo recibe un paquete ICMP muy grande, este disminuye el tamaño de su MTU si el protocolo de Internet de control de mensaje (Internet Control Message Protocol - ICMP) contiene un MTU recomendado menor al actual MTU del dispositivo.

Un dispositivo realiza el descubrimiento de MTU cada 5 minutos para ver si la MTU se ha incrementado a lo largo de la ruta. Las capas de aplicación y transporte para IPV6 aceptan las notificaciones de reducción de la MTU de la capa IPv6.

Si ellos no aceptan las notificaciones, IPv6 tiene un mecanismo para fragmentar los paquetes que son muy grandes. Sin embargo, las capas superiores son animadas a evitar el envió de mensajes que requieran la fragmentación.

Las tecnologías de capa de enlace ya desarrollan la suma de comprobación y control de errores. Como las tecnologías de capa de enlace son relativamente confiables, el encabezado IP de suma de comprobación se considera redundante. Sin la suma de comprobación de encabezado IP, la capa superior de comprobación opcional, como el protocolo de datagrama de usuario (UDP), son ahora obligatorios.

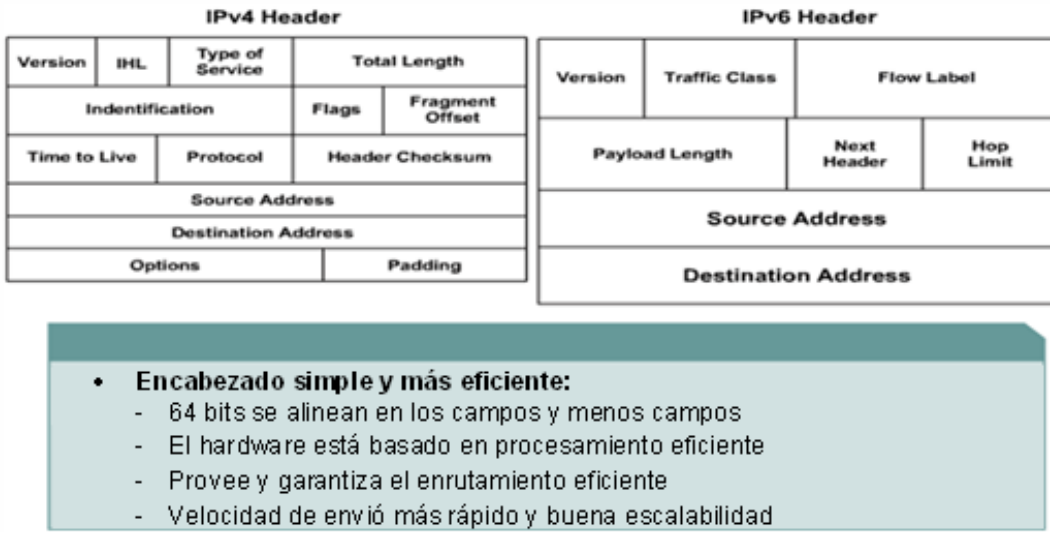


Fig.4 Encabezado Simple y Eficiente[7]

2.2 Comparación del Encabezado IPv4 e IPv6

El encabezado de **IPv6 tiene 40 octetos**, en contraste con el de **IPv4 que es de 20 octetos.** IPv6 tiene un menor número de campos, y el encabezado es de 64 bit alineados para permitir el procesamiento rápido de los procesos actuales. Los campos de dirección son 4 veces más grandes que en IPv4.

El encabezado IPv6 contiene estos campos:

- **Versión:** Campo de 4 bits, como en IPv4. Este contiene el número 6 para IPv6, en lugar del 4 para IPv4.

- **Clase de Tráfico:** Campo de 8 bits similar al campo de tipo de servicio (ToS) en IPv4. Este etiqueta el paquete con una clase de tráfico que usa en servicios diferenciados (DiffServ). Esta funcionalidad es la misma para IPv6 e IPv4.

- **Etiqueta de Flujo:** Campo de 20 bits que permite un flujo particular de tráfico a ser etiquetado. Puede ser usado para técnicas de conmutación de múltiples capas y el rápido cumplimiento de intercambio de paquetes.

- **Longitud de Carga Útil:** Similar al campo de longitud total en IPv4.Especifica la longitud de carga útil, en bytes, que el paquete encapsula.

- **Siguiente Encabezado:** Especifica cual cabecera sigue el paquete de encabezado IPv6. Este puede ser un paquete de la capa de transporte, como TCP o UDP, o puede ser una extensión del

[7] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 695.

encabezamiento. Este campo es similar al campo de protocolo en IPv4.

- **Límite de Salto:** Especifica el máximo número de saltos que un paquete IP puede atravesar. Cada salto o Router disminuye este campo en uno (similar al campo de tiempo de vida [TTL] en IPv4). Como no hay cheksum en el encabezado IPv6, el Router puede disminuir el campo sin recalcular el cheksum. El recálculo cuesta un valioso tiempo de proceso en los Routers con IPv4.

- **Dirección de Origen:** Campo de 16 octetos o 128 bits. Identifica el origen del paquete.

- **Dirección de Destino:** Campo de 16 octetos o 128 bits. Identifica el destino del paquete.

- **Encabezados de Extensión:** Sigue los últimos 8 campos. El número de encabezados de extensión no es fijo, con lo que la longitud total de la cadena del encabezado es de extensión variable.

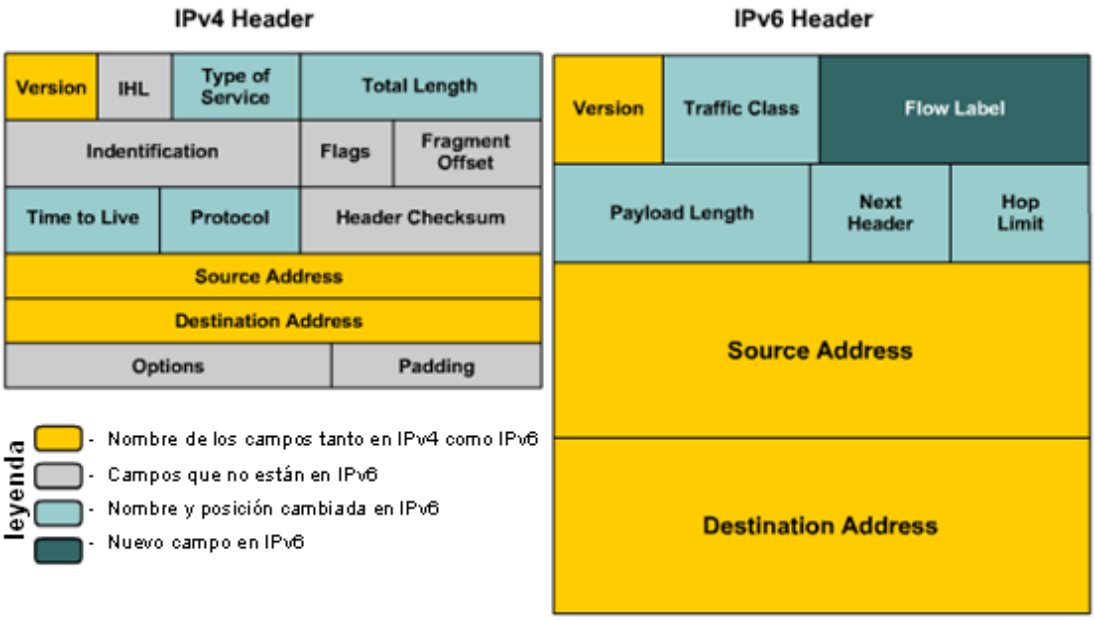


Fig. 5 IPv4 e IPv6 Comparación de Cabecera[8]

2.3 Encabezados de Extensión IPv6

Hay muchos tipos de encabezados de extensión. Cuando múltiples encabezados de extensión son usados en el mismo paquete, el orden de los encabezados deben ser los siguientes:

1. **Encabezado IPv6:** Encabezado básico descrito en la anterior figura.

[8] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 695.

2. **Opciones de Encabezado hop-by-hop (salto por salto):** Cuando es usado por la alerta del Router (protocolo de reservación de recurso [RSVP] y el descubrimiento del receptor multicast versión 1 [MLDv1]) y el paquete jumbograma, este encabezado (valor = 0) es procesado por todos los saltos en el camino de un paquete. Cuando se presenta el encabezado de opciones hop-by-hop (salto por salto) es siempre inmediatamente después del encabezado de paquete básico IPv6.

3. **Encabezado de Opciones de Destino (cuando se utiliza el encabezado de enrutamiento):** Este encabezado (el valor = 60) puede seguir a un encabezado de opciones hop-by-hop (salto por salto), en este caso el encabezado de opciones de destino se procesa en el destino final y también en cada dirección visitada específicamente por un encabezado de enrutamiento.

   Alternativamente, el encabezado de opciones de destino puede seguir a cualquier encabezado de encapsulamiento de seguridad de carga útil (Encapsulating Security Payload - ESP), en cuyo caso el encabezado de opciones de destino se procesa solo en el destino final. Por ejemplo, IP móvil utiliza este encabezado.

4. **Encabezado de Enrutamiento:** Se utiliza para el enrutamiento de origen y el IPv6 móvil (valor=43).

5. **Fragmento de Encabezado:** Se utiliza cuando una fuente debe fragmentar un paquete que es más grande que la MTU de la ruta de acceso entre ella y un dispositivo de destino. El fragmento encabezado se utiliza en cada paquete particionado.

6. **Autenticación y Encabezado de Encapsulación de Seguridad de Carga Útil:** Se utiliza en IPsec para proporcionar autenticación, integridad, y confidencialidad de un paquete. El encabezado de autenticación (valor = 51) y el encabezado ESP (valor = 50) son idénticos para IPv4 e IPv6.

7. **Encabezado de Capa Superior:** Encabezados típicos utilizados dentro de un paquete para el transporte de los datos. Los dos principales son los protocolos de transporte TCP (valor = 6) y UDP (valor = 17).

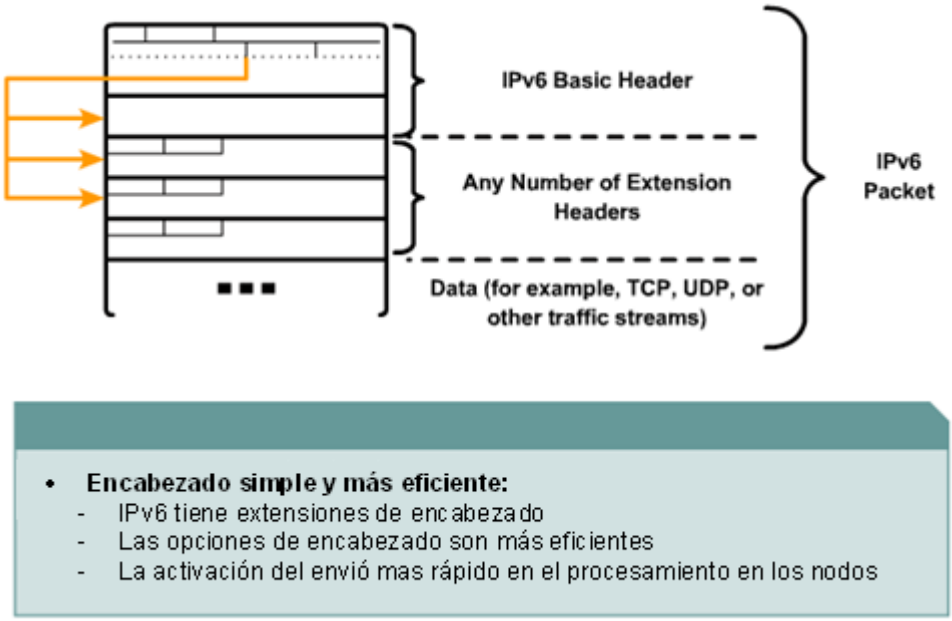


Fig. 6 IPv6 Cabecera de Extensión[9]

2.4 Definición de Representación de Direcciones

Los 128 bits de direccionamiento IPv6 son representados por su ruptura en 8 segmentos de 16 bits. Cada segmento está escrito en hexadecimal entre 0x000 y 0xFFF, separado por dos puntos.

Los dígitos hexadecimales A, B, C, D, E y F representados en IPv6 no distinguen entre mayúsculas y minúsculas.

IPv6 no requiere explícitamente la notación de dirección de cadena. Utilice las siguientes pautas para anotaciones de cadena de direcciones IPv6:

- Los ceros a la izquierda en un campo son opcionales, así 09C0 = 9C0 y 0000 = 0.
- Los campos sucesivos de ceros se pueden representar como "**::**" solo una vez en una dirección.
- Una dirección no específica se escribe como "**::**" porque solo contiene ceros.

Usando la notación "**::**" reduce considerablemente el tamaño de la mayoría de direcciones. Por ejemplo, FF01**::**0:0:0:0:0:0:1 se convierte en FF01**::**1.

[9] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 697.

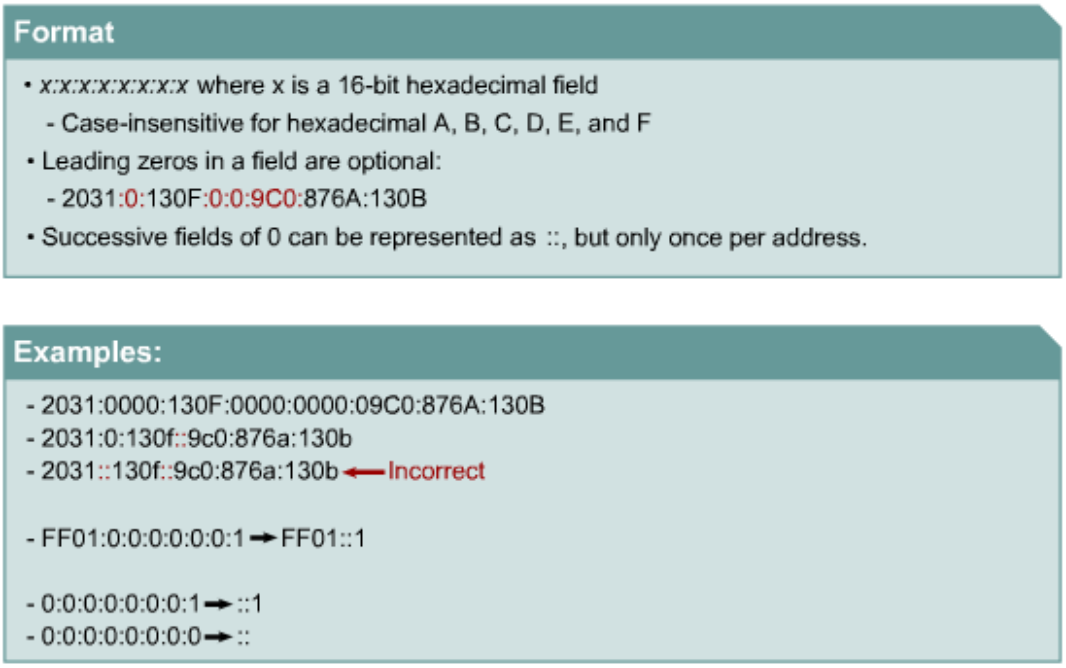


Fig. 7 Representación de Direcciones IPv6[10]

2.5 Tipos de Direcciones IPv6

La estructura de direccionamiento IPv6 se define en múltiples RFCs, incluyendo RFC 3513 y la nueva RFC 4291.

Cada RFC define 3 tipos de direcciones IPv6:

- Dirección Unicast
- Dirección Multicast
- Dirección anycast

[10] Tomado del curriculum de CCNA Exploration.

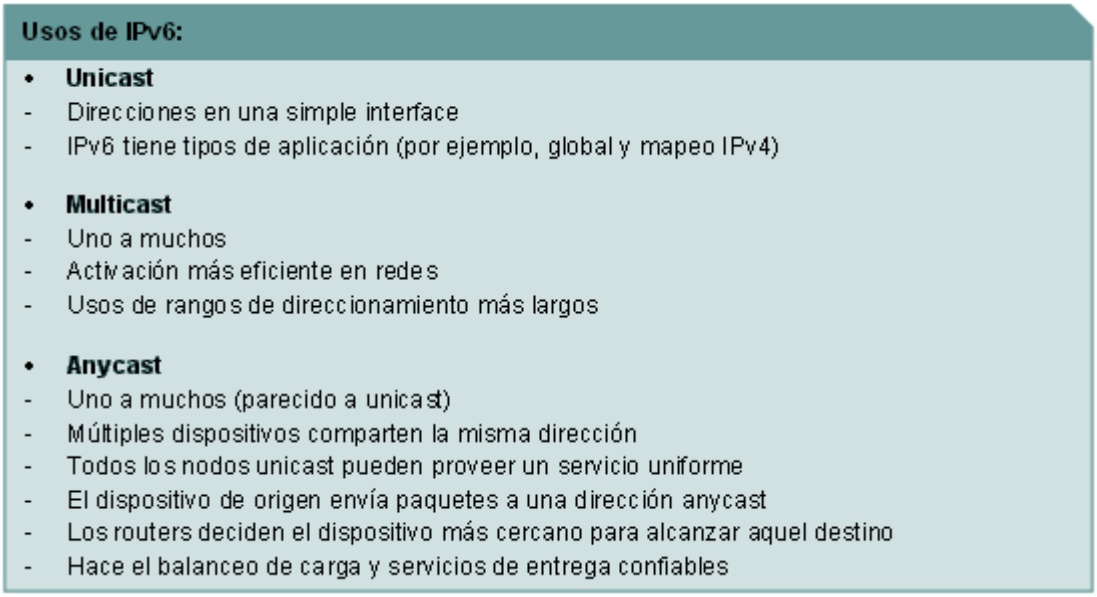


Fig. 8 Tipos de Direcciones IPv6[11]

Dirección Unicast

Una dirección unicast identifica un solo dispositivo. Un paquete enviado a una dirección unicast es entregado a la interfaz identificada por la dirección. Hay dos tipos de direcciones unicast:

- **Dirección Unicast de Enlace Local**: El alcance se configura a un solo enlace. La dirección es únicamente para ese enlace, y no es enrutable fuera de el.

- **Dirección Unicast Global**: Única globalmente, de modo que se pueden enrutar mundialmente sin ninguna modificación. Una dirección global tiene un alcance ilimitado en el internet a nivel mundial. Los paquetes con direcciones de origen y destino globales son enrutados a sus destinos designados por los Routers en el internet.

Todas las interfaces requieren tener al menos una dirección de enlace local unicast. Sin embargo, una característica fundamental de IPv6 es que una sola interfaz también puede tener múltiples direcciones IPv6 de cualquier tipo (unicast, anycast, y multicast).

[11] Tomado del curriculum de CCNP versión 5 Traducido por el autor de la monografía.

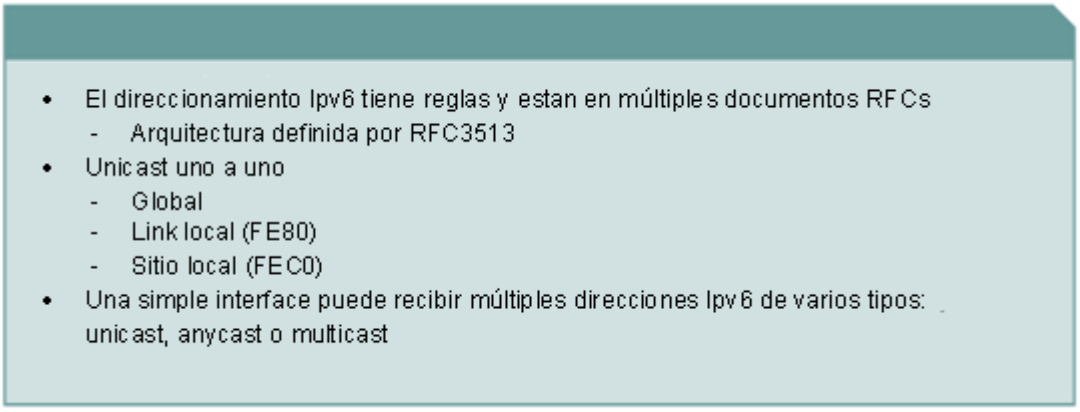


Fig. 9 Direccionamiento Unicast IPv6[12]

Nota: También hay una dirección unicast de punto local; sin embargo, el IETF está actualmente trabajando en eliminar o reemplazar las direcciones de punto local. Por eso, este módulo no incluye este tipo de direcciones.

Direcciones Multicast

IPv6 no tiene direcciones de broadcast (Difusión). El broadcasting en IPv4 tiene como consecuencia varios problemas: genera un número de interrupciones en cada computador de la red y, en algunos casos, provoca malfuncionamiento que puede detener completamente una red entera. Este evento desastroso de red se llama tormenta de broadcast.

El broadcast es reemplazado por las direcciones multicast. Multicast activa la operación de la red eficientemente por el uso funcional de grupos específicos multicast para enviar solicitudes a un número limitado de computadores en la red. Un paquete enviado a una dirección multicast es enviado a todas las interfaces identificadas por esa dirección.

El rango de direcciones multicast en IPv6 es mayor que en IPv4. Para un futuro previsible, la asignación de grupos multicast no será limitado.

Direcciones Anycast

IPv6 también define un nuevo tipo de direcciones llamadas anycast. Una dirección anycast identifica una lista de dispositivos o nodos; por lo tanto una dirección anycast identifica múltiples interfaces.

Un paquete enviado a una dirección anycast es enviado a las interfaces más cercanas, según la definición de los protocolos de enrutamiento en uso.

Las direcciones anycast son sintácticamente indistinguibles de las direcciones globales unicast, porque las direcciones anycast son asignadas del espacio de direcciones globales unicast.

[12] Tomado del curriculum de CCNP versión 5 Traducido por el autor de la monografía.

Nota: Las direcciones anycast no puede ser usadas como direcciones de origen de un paquete IPv6.

Direcciones Especiales

Hay un número de direcciones con significados especiales en IPv6. Algunas de estas se representan en la figura.

::/128	esta es una dirección no especificada de puros ceros y se usa solamente basada en software
::1/128	es la dirección de loopback de los host. en una aplicación los host envían paquetes a esa dirección; en el stack de Ipv6 hace un loop y envía paquetes a si mismo (corresponde a la dirección 127.0.0.1 de Ipv4)
2001:db8::/32	este prefijo es típicamente usado como ejemplo en la documentación (RFC 3849), se usa donde se explican las direcciones IPV6
fe80::/10	este prefijo de enlace local especifica la dirección del enlace local físico. Esta analogía es muy parecido a la auto configuracion de las direcciones IPv4 que asigna el sistema operativo como la dirección 169.254.X.X.
ff00::/8	el prefijo multicast es usado direccionamiento multicast

Fig. 10 Direcciones Especiales de IPv6[13]

2.6 Direcciones IPv6 Globales Unicast y Anycast

Las direcciones globales anycast y unicast comparten el mismo formato. El espacio de direcciones unicast asigna las direcciones anycast. Estas direcciones aparecen como direcciones unicast para los dispositivos que no están configurados para anycast.

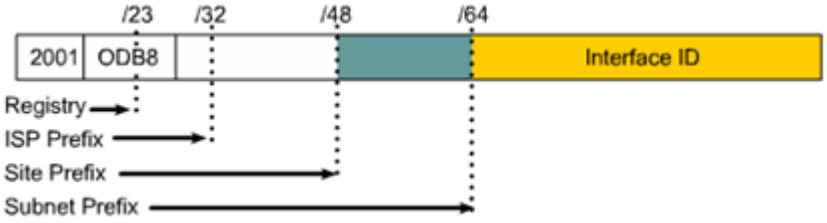


Fig. 11 Direcciones Globales IPv6 Unicast (Y Anycast)[14]

Cuando una dirección unicast es asignada a más de una interfaz, convirtiéndola así en una dirección anycast, los nodos a los cuales la dirección es asignada deberán configurarse explícitamente para usar y reconocer la dirección anycast.

[13] Tomado del curriculum de CCNP versión 5 Traducido por el autor de la monografía.
[14] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 706.

Un paquete que es enviado a las rutas de dirección de anycast al dispositivo más cercano o a la interfaz que comparte la dirección. Un emisor crea un paquete con el anycast como dirección de destino y lo envía a los Routers más cercanos. El origen puede utilizar las direcciones anycast para controlar la ruta a través de la cual fluye el tráfico.

Un ejemplo del uso del anycast en un protocolo de pasarela de frontera (Border Gateway Protocol - BGP[15]) en redes multihomed es cuando un cliente tiene múltiples ISPs con múltiples conexiones entre sí. El cliente puede configurar una dirección anycast diferente para cada ISP. Cada Router para un ISP dado tiene la misma dirección anycast configurada. El dispositivo origen puede elegir cual ISP (proveedor de servicios de Internet) enviará el paquete. Sin embargo, los Routers a lo largo de la ruta determinan el Router mas cercano para llegar a ese proveedor de Internet mediante la dirección IPv6 anycast.

Otro uso para un anycast es cuando una LAN está vinculada a múltiples Routers. Estos Routers pueden tener la misma dirección anycast IPv6 de manera que cada dispositivo remoto necesita identificar solo la dirección anycast. Dispositivos intermedios pueden elegir la mejor ruta para alcanzar el punto más cercano de entrada a la subred.

La dirección global unicast IPv6 es el equivalente de la dirección global unicast IPv4. La estructura de dirección permite que los prefijos de enrutamiento se agreguen, limitando así el número de entradas de la tabla de enrutamiento en la tabla de enrutamiento global. La dirección global unicast usada en estos enlaces se adicionan ascendentemente a través de organizaciones y finalmente a los ISPs.

Las direcciones Unicast globales son definidas por un prefijo de enrutamiento global, un ID (identificación) de subred, y un ID de interfaz. El espacio de direcciones anycast IPv6 abarca el rango de direcciones entrantes IPv6, a excepción de FF00**::/**8 (1111 1111), el cual se utiliza para direcciones multicast.

Las actuales direcciones unicast globales asignadas por la Autoridad de Asignación de Números de Internet (Internet Assigned Numbers Authority - IANA) utiliza el rango de direcciones que inician con el valor binario 001 (2000**::/**3), el cual es una octava parte del espacio total de direcciones IPv6 y es el mayor bloque de las direcciones de bloques asignadas.

Las direcciones con prefijo de 2000**::/**3 (001) a través de E000**::/**3 (111), a excepción de la FF00**::/**8 (1111 1111) direcciones Multicast, requieren tener un identificador de interfaz de 64 bits en el formato de identificación universal extendido (Extended Universal Identifier - EUI)-64.

La dirección global unicast normalmente consta de 48 bits de prefijo de enrutamiento global y de 16 bits de ID de subred. En el ahora obsoleto RFC

[15] http://www.faqs.org/rfcs/rfc2545.html

2374, IPv6 agrega un formato de dirección unicast global, el prefijo de enrutamiento global incluye dos campos más de estructura jerárquica llamados agregador de nivel superior y agregador de nivel siguiente. Debido a que estos campos fueron basados en políticas, el IETF decidió sacarlos del RFC, Sin embargo, algunas redes IPv6 existentes empleadas inicialmente pueden aun estar empleando redes basadas en esta antigua arquitectura. Un campo de subred de 16 bits llamado ID de subred puede ser utilizado por organizaciones individuales para crear su propio direccionamiento global jerárquico y para identificar subredes. Este campo permite a una organización utilizar hasta 65.535 subredes individuales. (RFC 2374 ha sido sustituida por RFC 3587).

3.0 Direcciones Dinámicas IPv6

3.1 Definición de Direcciones de Interfaz de Host

Una dirección IPv6 consta de dos partes:

- Un prefijo de subred en representación de la red a la que está conectada la interfaz. El prefijo de subred es una longitud fija de 64 bits para todas las definiciones actuales.

- Un identificador local, a veces llamado token, que identifica el host en la red local. El identificador local siempre es de 64 bits y se crea dinámicamente en la base del medio de comunicación y encapsulado de capa 2. En el caso simple de un medio Ethernet, el identificador local se deriva usualmente de la dirección MAC EUI-48.

El identificador local de 64 bits en una dirección IPv6 identifica una interfaz única en un enlace. Un enlace es un medio de red a través de la cual los nodos de la red se comunican usando la capa de enlace. El identificador de interfaz también puede ser único en un ámbito más amplio. En muchos casos, un identificador de interfaz es la misma o se basa en la dirección de capa de enlace (MAC) de una interfaz. Al igual que en IPv4, un prefijo de subred en IPv6 está asociado con un enlace.

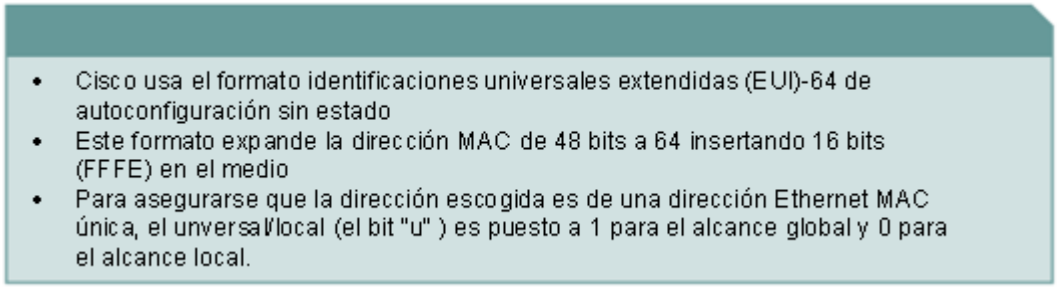


Fig. 12 Direcciones Unicast Globales Agregables[16]

[16] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 707.

3.2 Dirección de Enlace Local

Los identificadores de interfaz en direcciones IPv6 identifican interfaces en un enlace. Una dirección de enlace local puede ser considerada como la parte del host de una dirección IPv6.

La dirección es única solo en este enlace, y no es enrutable fuera del enlace. Los paquetes con un enlace local de destino deben permanecer en el enlace donde se generaron. Los Routers que podría transmitir a otros enlaces no están permitidos porque no hay verificación de unicidad fuera del contexto del enlace de origen.

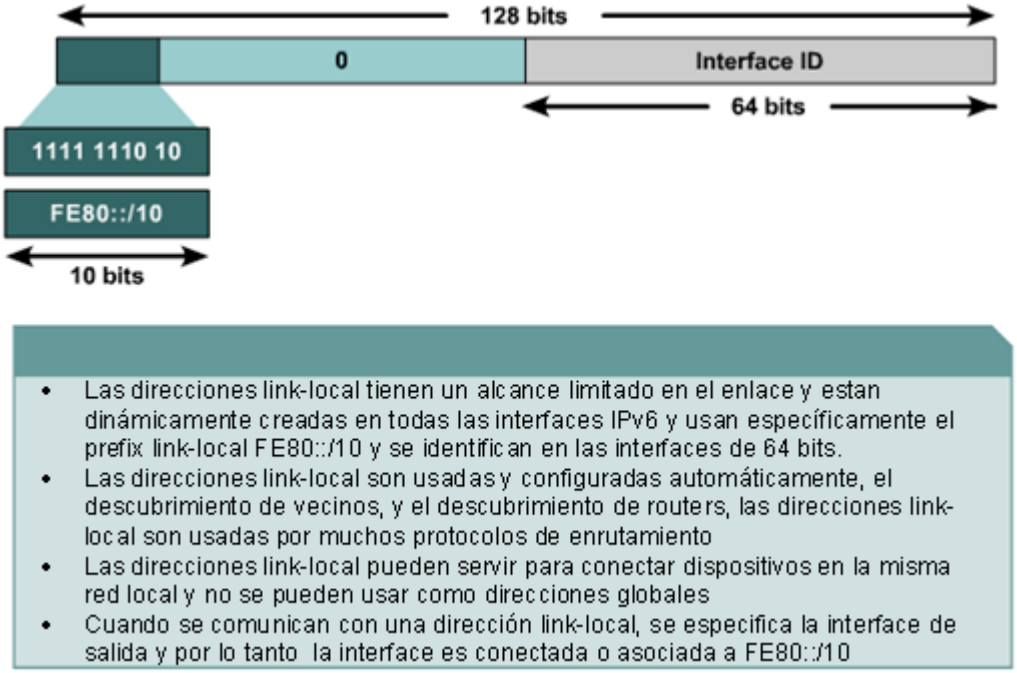


Fig. 13 Dirección de Enlace Local[17]

Las direcciones de enlace local se crean dinámicamente utilizando un prefijo de enlace local de FE80**::/**10 y un identificador de interfaz de 64 bits en un proceso llamado autoconfiguración sin estado.

3.3 Autoconfiguración sin Estado

La autoconfiguración sin estado es una característica plug-and-play que permite a los dispositivos conectarse automáticamente a una red IPv6 sin necesidad configuración manual y sin ningún tipo de servidor (como servidores DHCP). DHCP y DHCPv6[18] son conocidos como protocolos de estado completo porque mantienen tablas sin servidores dedicados.

[17] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 707.
[18] ftp://ftp.rfc-editor.org/in-notes/rfc3315.txt

El protocolo de autoconfiguración sin estado no necesita de ningun servidor o retardos porque no tiene un estado que mantener. Todos los sistemas IPv6 (diferentes a routers) pueden construir sus propias direcciones globales unicast, las cuales habilitan nuevos dispositivos, como teléfonos celulares, dispositivos inalámbricos, electrodomésticos, redes domesticas, que se implementa en Internet.

Como la longitud del prefijo es fija y también conocida, el sistema construye automáticamente una dirección de enlace local durante la fase de inicialización de las tarjetas de red (NICs) IPv6. Después de verificar la unicidad, este sistema puede comunicarse con otros hosts de IPv6 en ese enlace, sin ninguna otra intervención manual.

Para un sistema conectado a un enlace Ethernet, la construcción y validación de la dirección local de vínculo se realiza en las siguientes fases.

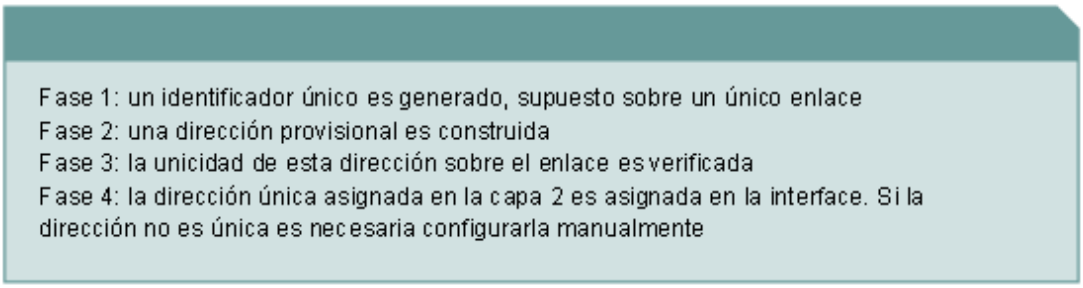


Fig.14 Las Fases de la Autoconfiguración Apátridas[19]

Fase 1

Aunque es configurable manualmente, el método más común de obtener un identificador único en un enlace Ethernet es mediante el uso de la EUI-48 dirección MAC y aplicando el modificado algoritmo estándar IEEE EUI-64.

Por ejemplo, transformando la dirección MAC 00-0C-29-C2-52-FF utilizando la EUI-64 las normas conducen a 00-0C-29-**FF-FE**-C2-52-FF. Si esta dirección debe seguir siendo local, la notación IPv6 seria 000C**:**29FF**:**FEC2**:**52FF. Sin embargo, si la dirección es una dirección unicast global, el formato correcto es 0**2**0C**:**29FF**:**FEC2**:**52FF.

Nota: Para la dirección con alcance global, la parte inicial de la dirección MAC será alterada de 00-0C a 02-0C. Este proceso se describe en el siguiente tema.

Fase 2

También se conoce al prefijo de enlace local fe80**::/**64 se antepone al identificador de 64 bits de la fase 1 para crear la dirección de enlace local de

[19] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 708.

128 bits, por ejemplo, fe80**::**20c**:**29ff**:**fec2**:**52ff. Esta dirección esta asociada con la interfaz y es etiquetado como “provisional”.

Fase 3

Antes de la asociación final, es necesario verificar la unicidad de la dirección en el enlace, denominado detección de dirección duplicada (Duplicate Address Detection - DAD). La probabilidad de tener una dirección duplicada en el mismo enlace no es nula, porque se reconoce que algunos proveedores han enviado lotes de tarjetas con la misma dirección MAC.

El sistema envía paquetes ICMPv6 en el enlace donde la detección tiene que ocurrir. Estos paquetes contienen los mensajes de solicitud de vecinos. Esta dirección origen es la dirección indefinida “**::**”, y la dirección designada es la dirección provisional. Un nodo que ya usa una dirección provisional responde con un mensaje de alerta de vecino. En este caso, la dirección no puede ser asignada a la interfaz. Si no hay respuesta, se asume que la dirección es única y puede asignarse a la interfaz. Si la dirección no es única deberá manipularse manualmente.

Fase 4

Esta fase remueve la etiqueta provisional y asigna formalmente la dirección a la interfaz de red. El sistema puede ahora comunicarse con sus vecinos en el enlace.

Para intercambiar información con sistemas arbitrarios en el internet global, es necesario obtener un prefijo global. Por lo general, pero no necesariamente, el identificador construido durante la primera fase del proceso de autoconfiguración de enlace local automático es añadido al prefijo global en la fase 2.

Generalmente, los prefijos globales son distribuidos a las compañías o a los usuarios finales por los ISPs.

3.4 Identificador EUI-64 para IPv6

Una dirección MAC (IEEE 802) tiene 48 bits de longitud. El espacio para el identificador local en la dirección IPv6 es de 64 bits. El estándar EUI-64 explica cómo se extiende las direcciones IEEE 802 de 48 a 64 bits mediante la inserción de 16 bits 0xFFFE en medio del bit 24 de la dirección MAC. Este crea un identificador de interfaz único de 64 bits.

Por ejemplo, transformando la dirección MAC 00-90-27-17-FC-0C utilizando el estándar EUI-64 resulta en 00-90-27-**FF-FE**-17-FC-0C.Convirtiéndolo en la notación IPv6 se generará 0090:27FF:FE17:FC0C.

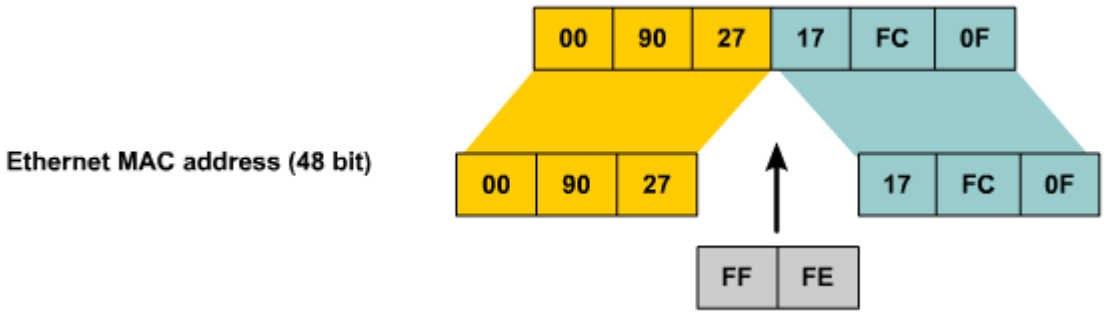


Fig. 15 Identificador de Interfaz EUI-64 a IPv6[20]

Cuando el identificador de interfaz es creado de una dirección MAC Ethernet, se asume que la dirección MAC es universalmente única y, por eso, el identificador de interfaz es universalmente único.

Universal/local (U/L)

El séptimo bit en un identificador de interfaz IPv6 se refiere al bit universal/local o U/L bit. Este bit identifica si el identificador de interfaz es administrado universalmente o localmente.

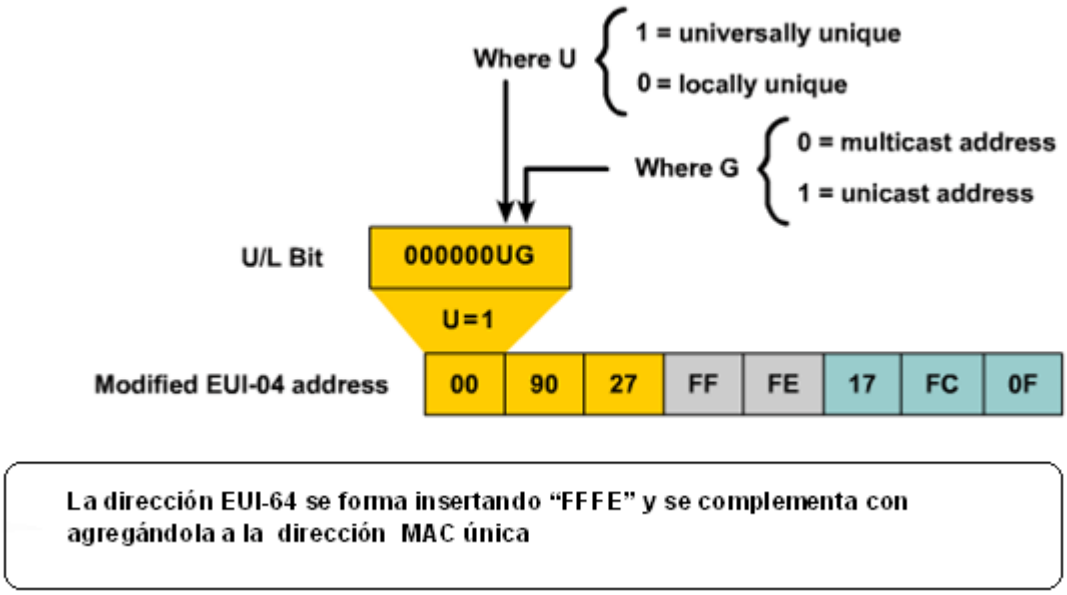


Fig. 16 EUI-64 Universal / Local Bit[21]

- Si el bit U/L es ajustado a 0, la dirección es locamente administrado. El administrador de red ha anulado la dirección de fábrica y especifica una dirección diferente.

[20] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 703.
[21] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 703.

- Si el bit U/L se establece en 1, el IEEE, mediante la designación de un ISP, ha administrado la dirección.

Sin embargo, para hacer de esta dirección una dirección administrada universalmente, nuestra dirección IPv6 0090:27FF:FE17:FC0C realmente se convertiría en 0290:27FF:FE17:FC0C.

Individual/grupal (I/G)

El bit I/G es el bit de menor orden del primer byte y determina si la dirección es una dirección individual (unicast) o una dirección grupal (multicast). Cuando se establece en 0, es una dirección unicast. Cuando se establece en 1 es una dirección multicast (multidifusión).

Para un típico adaptador de red de dirección 802.x, ambos bits U/L e I/G se establecen en 0, correspondiente a la dirección MAC unicast administrada universalmente.

Debido a la privacidad y algunos problemas de seguridad, la aplicación de configuración automática por una multitud también puede crear una interfaz de identificación al azar usando la dirección MAC como base. Esto se considera una extensión de privacidad porque, sin ella, la creación de un identificador de interfaz de una dirección MAC ofrece la posibilidad de rastrear la actividad y el punto de conexión.

Microsoft Windows XP actualmente soporta la implementación de esta capacidad y se usa preferiblemente esta dirección para la comunicación saliente, porque la dirección tiene un corto tiempo de vida y se regenera periódicamente.

3.5 Capas de Enlace de Datos a Través de IPv6

Aunque el comando **redistribution** esta disponible para todos los protocolos de enrutamiento IP, este se comporta diferente dependiendo de los protocolos reales de enrutamiento del IP implicado. Sin embargo, los principios fundamentales son los mismos. Por lo tanto, los ejemplos en esta sección pueden ser usados como punto de partida para el esquema de redistribución.

La capa de enlace de datos define, como el identificador de interfaz IPv6 es creado y como el descubrimiento de vecinos con la resolución de la dirección de capa de enlace de datos.

IPv6 está definido en la mayoría de las capas de enlace de datos actuales, incluyendo las siguientes:

- Ethernet*
- PPP*
- High-Level Data Link Control (HDLC)*
- FDDI
- Token Ring
- Attached Resource Computer Network (ARCNET)
- Nonbroadcast multiaccess (NBMA)
- ATM**
- Frame Relay***
- IEEE 1394

*Cisco ofrece soporte para estas capas de enlace de datos.
**Cisco apoya sólo ATM circuito virtual permanente (PVC) y ATM LAN Emulation (LANE).
***Cisco apoya sólo Frame Relay PVC.

Un RFC describe el comportamiento de IPv6 en cada una de estas capas de enlace de datos específicos, pero el software Cisco IOS no es necesariamente soportado por todos ellos.

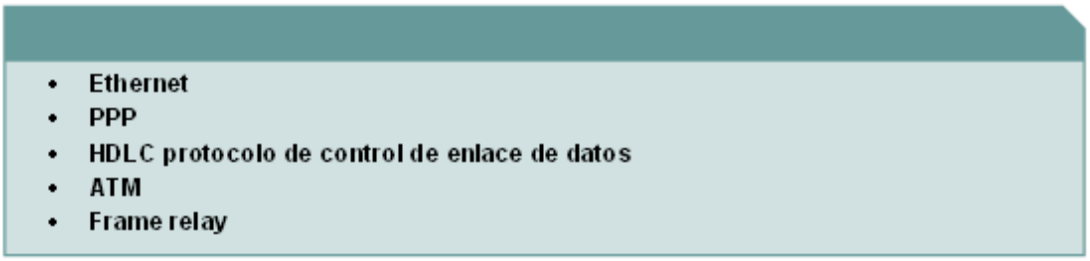


Fig. 17 Cisco Apoya Ipv6 Capas de Enlace de Datos[22]

3.6 Multicasting (Multidifusión) IPv6

Una dirección multicast identifica un grupo de interfaces. El tráfico enviado a una dirección multicast viaja a múltiples destinos al mismo tiempo. Una interfaz puede pertenecer a cualquier número de grupos multicast. El multicasting es extremadamente importante para IPv6, porque este es el núcleo de muchas funciones de IPv6.

El formato de la dirección multicast es la siguiente:

[22] Tomado del curriculum CCNP versión 5 traducido por el autor de la monografía.

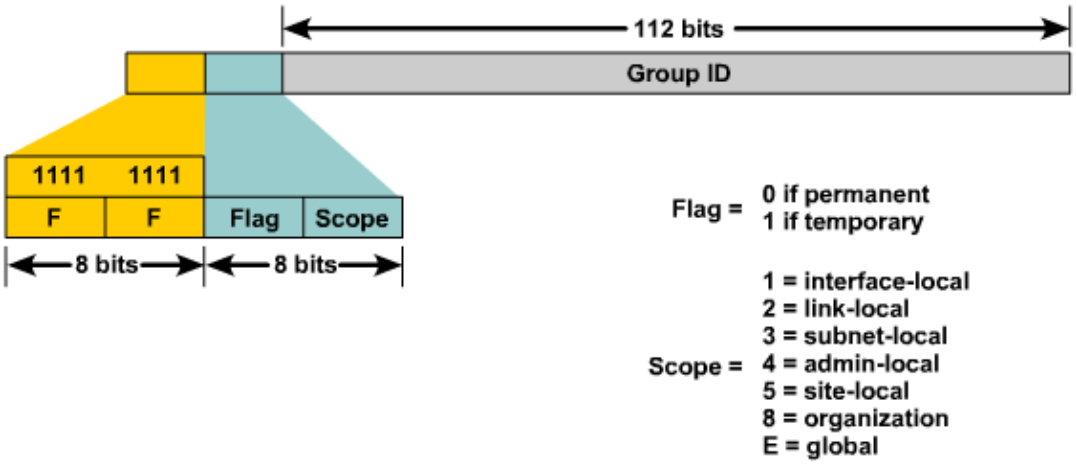


Fig. 18 Multidifusión[23]

- Las direcciones IPv6 multicast son definidas por el prefijo FF00**::/**8. El segundo octeto define el tiempo de vida (bandera) y el alcance de la dirección multicast.

    - El parámetro de bandera es igual a 0 para una dirección multicast permanente, o bien conocido, la dirección de multidifusión. Para obtener una dirección de multicast temporal, la bandera es igual a 1.

    - El parámetro de ámbito de aplicación es igual a 1 para el alcance de la interfaz (transmisión loopback), 2 para el ámbito de aplicación de enlace (similar al alcance de un enlace local unicast), 3 para el alcance local de subred donde las subredes pueden abarcar múltiples enlaces, 4 para el ámbito local admin (administrativamente configurado), 5 para el alcance del sitio, 8 para el alcance organizacional (múltiples sitios), y E para el alcance global. Por ejemplo, una dirección multicast inicia con FF02**::/**16 una dirección multicast permanente con un alcance de enlace local.

- El grupo multicast ID consiste de 112 bits inferiores de la dirección multicast.

El multicast es frecuentemente usado en IPv6 y reemplaza el broadcast. No hay broadcast en IPv6. No a hay tiempo de vida (TTL) en IPv6 multicast. El alcance es definido en la dirección.

[23] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 709.

3.7 Direcciones Multicast Permanentes

Las direcciones multicast, FF00**::** a FF0F**::**, son reservadas. Dentro de ese rango, los siguientes son algunos ejemplos de asignación de direcciones. Las asignaciones son rastreadas por la IANA[24].

	Meaning	Scope
FF02::1	All nodes	Link-local
FF02::2	All routers	Link-local
FF02::9	All RIP routers	Link-local
FF02::1:FFXX:XXXX	Solicited-node	Link-local
FF05::101	All NTP Servers	Site-local

Fig. 19 Direcciones Multicast Permanentes[25]

- **FF02::1--** Todos los nodos en el enlace (alcance de enlace local – link local scope).

- **FF02::2 --** Todos los routers en el enlace.

- **FF02::9--** Todos los routers con el protocolo de enrutamiento de información (RIP) en el enlace IPv6.

- **FF02::1:FFXX:XXXX --** Nodo multicast solicitado en el enlace, donde XX**:**XXXX son los 24 bits mas a la derecha de la dirección correspondiente unicast o anycast del nodo. (Mensajes de solicitud Vecino se envían en un enlace local, cuando un nodo desea determinar la dirección de enlace de capa de otro nodo en el vínculo local mismo, similar a Address Resolution Protocol [protocolo de resolución de dirección - ARP] en IPv4).

- **FF05::101--** Todos los servidores del protocolo de tiempo de red (NTP) en el sitio (alcance de sitio local).

[24] http://www.iana.org/
[25] Tomado del libro CISCO CCNP Route 642-902 Oficial Certification Guide pagina 554.

El alcance de sitio local multicast tiene un radio administrativamente asignado y no tiene correlación directa al prefijo unicast de sitio local (ahora obsoleto) de FEC0**::/**10.

3.8 Las Direcciones que No son Únicas

En casos muy raros, los 24 bits más a la derecha de la dirección unicast del objetivo no son únicos en el enlace. La dirección del nodo multicast solicitante se utilizan en IPv6 para la resolución de direcciones de una dirección IPv6 a una dirección MAC en un segmento LAN.

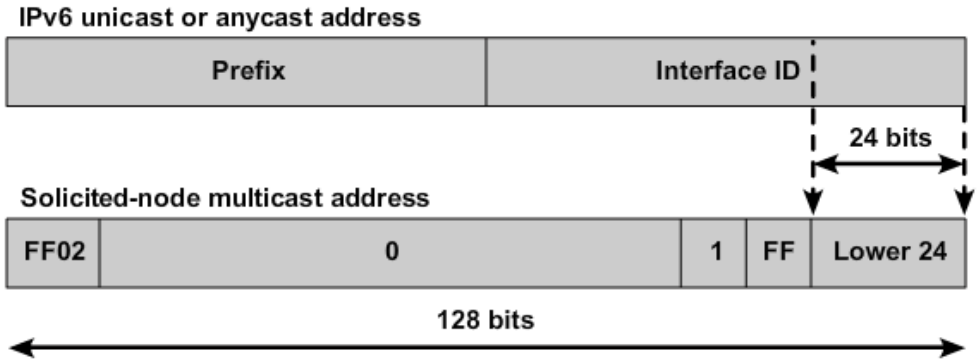


Fig. 20 Dirección IPv6 Unicast o Anycast [26]

Por ejemplo, considerando dos nodos con direcciones 2001**:**DB8**:**200**:**300**:**400**:**500**:**aaaa**:**bbbb y 2001**:**DB8**:**200**:**300**:**400**:**501**:**aaaa**:**bbbb, donde el prefijo de enlace es 2001**:**DB8**:**200**:**300**::/**64.

Estos dos nodos estarían escuchando la misma la dirección multicast solicitando el nodo. Cada uno recibiría el paquete multicast, pero solamente el nodo cuya dirección completa coincide con la dirección de destino completa de los paquetes multicast (integrado en el campo de datos del paquete multicast) responderá con un anuncio de vecino (que incluye la dirección MAC real).

Los otros nodos deberán recibir el paquete multicast, pero en la inspección de la dirección de destino implícito cuenta de que no era el destinatario de la solicitud y no respondía.

A continuación se describe cómo funciona esta situación.

El nodo A tiene esta característica:

- dirección 2001**:**DB8**:**200:300**:**500**:**1234**:**5678

[26] Tomado del Curriculum CCNp versión 5.

El nodo B tiene estas características:

- dirección 2001:DB8:200:300:400:500:AAAA:BBBB
- dirección de nodo multicast solicitante FF02:0:0:0:0:1:FFAA:BBBB (el mismo que el nodo C)

El nodo C tiene estas características:

- dirección 2001:DB8:200:300:501:AAAA:BBBB
- la dirección del nodo solicitante multicast FF02:0:0:0:0:1:FFAA:BBBB (el mismo que el nodo B)

1. el nodo A desea intercambiar paquetes con el nodo B. el nodo A envía un paquete de descubrimiento de vecino para la dirección del nodo solicitante multicast de B, FF02:0:0:0:0:1:AAAA:BBBB. Dentro del paquete, además de otros datos, esta la dirección completa IPv6 que el nodo A busca (2001:DB8:200:300:500:AAAA:BBBB). Se conoce como la dirección de destino.

2. Tanto el nodo B y el nodo C escuchan la misma dirección multicast, entonces ambos reciben y procesan el paquete.

3. El nodo B observa que la dirección de destino dentro del paquete es el suyo y responde.

4. El nodo C observa que la dirección destino en el interior del paquete no es la suya y no responde.

De esta manera, los nodos pueden tener la misma dirección del nodo de solicitud multicast en el enlace sin causar el descubrimiento de vecinos, solicitud de vecinos, o advertencia vecina de malfuncionamiento.

3.9 Anycast

Una dirección anycast IPv6 es una dirección global unicast que es asignada a mas de una interfaz.

Fig. 21 Anycast[27]

[27] Tomado del Curriculum CCNpo versión 5.

Cuando un paquete es enviado a una dirección anycast, es enrutado a la interfaz más cercana que tenga dicha dirección.

En un ámbito de aplicación WAN, la interfaz más cercana es encontrada de acuerdo a la métrica de distancia del protocolo de enrutamiento. En un ámbito de aplicación LAN, la interfaz más cercana es encontrada de acuerdo al primer vecino aprendido.

A continuación se describen las características de una dirección anycast:

- Las direcciones anycast son asignadas a partir del espacio de direcciones por lo que son indistinguibles de las direcciones unicast. Cuando se le asigna a un nodo de interfaz, el nodo debe ser configurado explícitamente para saber que la dirección es una dirección anycast.

- La idea de anycast en IP fue propuesta en 1993. Para IPv6, anycast se define como una forma de enviar un paquete a la interfaz más cercana que es miembro del grupo anycast, que permite un tipo de mecanismo de descubrimiento al punto más cercano.

- Hay poca experiencia con el uso generalizado de anycast. Pocas direcciones anycast están actualmente asignadas, incluyendo el router anycast de subred y el agente inicial anycast móvil IPv6.

- Una dirección anycast no debe ser usada como una dirección de origen de un paquete IPv6.

3.10 Movilidad IPv6

La movilidad es una característica muy importante en las redes actualmente. IP móvil es un estándar IETF[28] disponible tanto para IPv4 como para IPv6. IP móvil habilita dispositivos móviles para moverse sin interrumpir las conexiones actuales.

En IPv6, la movilidad está incorporada, lo que significa que cualquier nodo IPv6 se puede utilizar según sea necesario. Sin embargo, en IPv4, la movilidad es una nueva función que se debe añadirse.

Los encabezados de enrutamiento de IPv6 hacen a IPv6 móvil más eficiente para los nodos terminales que IPv4 móvil. La movilidad toma ventajas de la flexibilidad de IPv6. Por ejemplo, binding (unión) usa algunas opciones de encabezamiento (destino) que son obligatorias para todos los dispositivos IPv6. Además, la movilidad IPv6 crea un nuevo encabezado de extensión de "movilidad".

[28] http://www.ietf.org/

La movilidad IPv6 es diferente de la movilidad IPv4 de varias formas:

- El espacio de direcciones IPv6 permite el despliegue de IP móvil empleado en cualquier clase de ambiente extenso.

- Debido al gran espacio de direcciones IPv6, no se requieren grandes agentes externos. Las infraestructuras no necesitan actualizarse para aceptar los nodos IPv6 móviles, así la dirección de custodia (CoA) puede ser una dirección enrutable global IPv6 para todos los nodos móviles.

- El modelo IPv6 móvil toma algunas ventajas del protocolo IPv6. Los ejemplos incluyen encabezados de opción, el descubrimiento de vecinos, y la configuración automática.

- En muchos casos, se elimina el triangulo de enrutamiento, porque la optimización de la ruta IPv6 móvil permite a los nodos móviles y nodos correspondientes comunicarse directamente. El soporte para la optimización de ruta es una parte fundamental del protocolo, en lugar de un juego no estándar de extensiones. El soporte está integrado en IPv6 móvil para permitir la optimización de ruta para coexistir de manera eficiente con los Routers que realizan el filtrado de entrada. La optimización de ruta IPv6 móvil puede operar con seguridad incluso sin las asociaciones de seguridad acordados. Esto específica que la optimización de ruta puede ser empleada a escala global entre todos los nodos móviles y sus correspondientes nodos.

- Los nodos móviles trabajan de manera transparente incluso con los demás nodos que no soportan la movilidad (igual que movilidad IPv4).

- El mecanismo de descubrimiento de dirección del agente inicial (home) en IPv6 móvil regresa una única respuesta al nodo móvil. La aproximación broadcast directa usada en IPv4 regresa respuestas separadas de cada agente inicial.

- La mayoría de paquetes enviados a nodos móviles mientras está lejos del home en IPv6 móvil son enviados usando un encabezado de enrutamiento IPv6 en lugar de un encapsulamiento IP, reduciendo la cantidad de gastos generales comparados con IPv4 móvil.

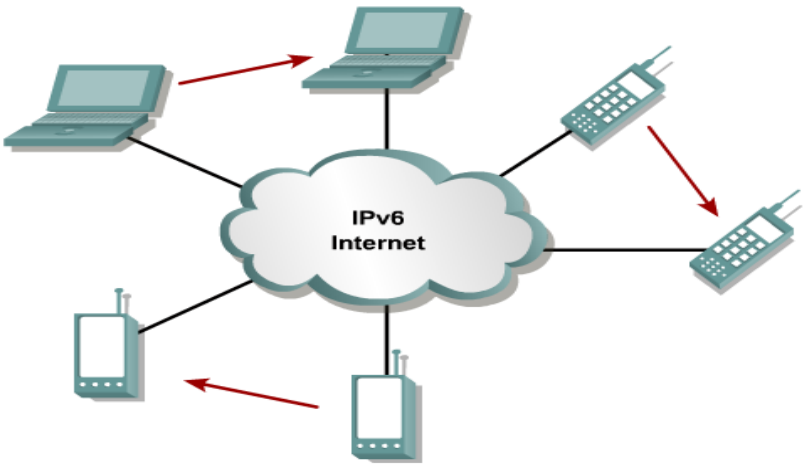


Fig. 22 Movilidad IPv6[29]

4.0 Enrutamiento IPv6.

4.1 Descripción del Enrutamiento IPv6.

Similar a IP versión 4 (IPv4) de enrutamiento entre dominios sin clase (CIDR), IPv6 utiliza el prefijo más extenso de enrutamiento asociado. Las versiones recientes del protocolo manejan direcciones IPv6 extendidas y diferentes estructuras de encabezado. Actualmente, las actualizaciones disponibles de los protocolos de enrutamiento se muestran en la figura.

- Tipos de enrutamiento IPv6
  - Estatico
  - RIPng (RFC2080)
  - OSFv3 RFC (2740)
  - IS-IS para IPv6
  - MP-BGP4 RFC 2545/2858
  - EIGRP para Ipv6
- El comando ipv6 unicast routing se debe habilitar antes de los protocolos de enrutamiento configurados

Fig. 23 Protocolo de Enrutamiento IPv6[30]

[29] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 699.
[30] Tomado del curriculum CCNP versión 5.

Los siguientes son resúmenes de varios protocolos de enrutamiento usados con IPv6.

Enrutamiento Estático

El enrutamiento estático con IPv6 es usado y configurado de la misma forma que en IPv4. Hay un requerimiento específico IPv6 por el RFC 2461: un router debe ser capaz de determinar la dirección de enlace local de cada uno de sus vecinos para asegurar que la dirección objetivo de un mensaje redireccionado identifique el Router vecino por su dirección local.

Este requerimiento básicamente significa que el uso de una dirección global unicast como la dirección de siguiente salto con el enrutamiento no es recomendable.

RIPng

Protocolo de enrutamiento de información de siguiente generación (RIPng, RFC 2080) es un protocolo de enrutamiento de vector distancia con un límite de 15 saltos que usa el horizonte dividido y envenenamiento reversivo para prevenir los loops (bucles) de enrutamiento.

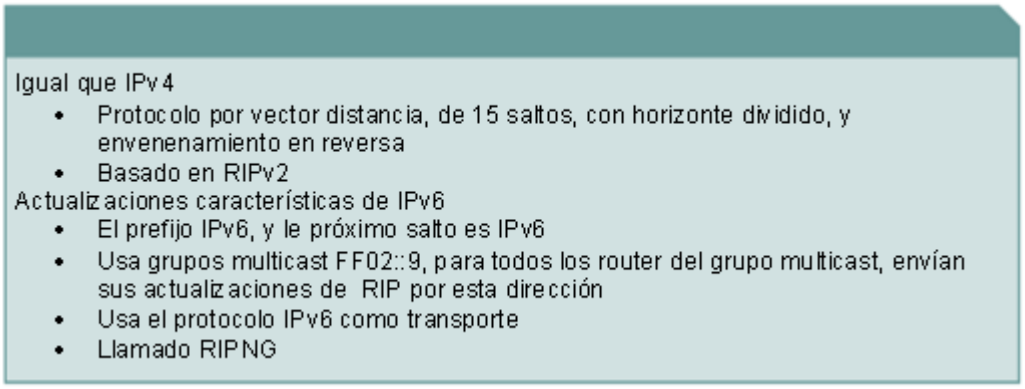


Fig. 24 RIPng[31]

La implementación del protocolo para IPv6 incluye estas características:

- Basado en IPv4 RIP versión 2 (RIPv2) y similar a esta.
- Usa IPv6 para el transporte
- Prefijo IPv6, dirección de siguiente salto IPv6
- Usa el grupo multicast FF02**::**9, de todos los router RIP del grupo multicast, como la dirección de destino para actualizaciones RIP.
- Envía actualizaciones por el puerto UDP 521

[31] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 751.

OSPFv3

La implementación del protocolo para IPv6 incluye estas características:

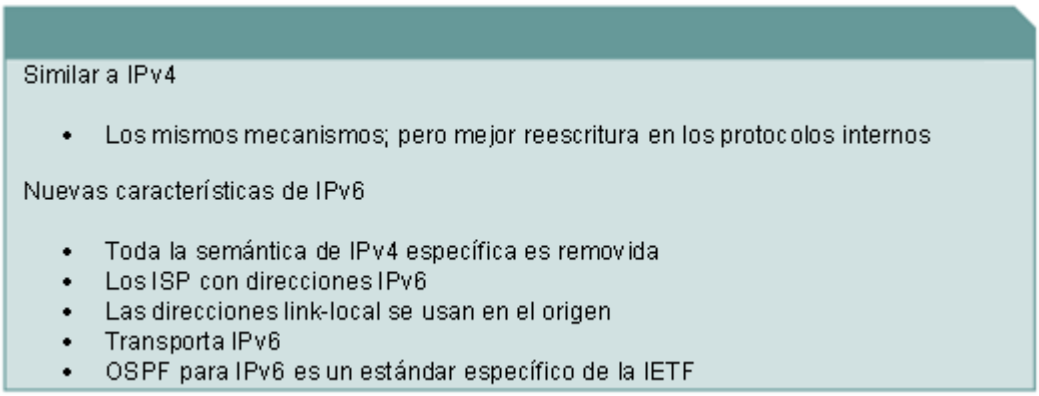


Fig. 25 OSPFv3[32]

- Basada en la versión 2 (OSPFv2), con mejoras
- Distribuye prefijos IPv6
- Se ejecuta directamente en IPv6

Esta aplicación agrega estos atributos específicos a IPv6:

- Direcciones de 128 bits
- Dirección de enlace local
- Múltiples direcciones y peticiones por interfaces
- Autenticación (ahora usa IPsec)
- OSPFv3 corre en un enlace en lugar de una subred.

EIGRP

El protocolo de enrutamiento de pasarela interior mejorado (Enhanced Interior Gateway Routing Protocol - EIGRP) puede usarse para prefijos IPv6 de ruta. EIGRP IPv4 se ejecuta sobre un transporte IPv4, solo se comunica con sus compañeros de IPv4, y advierten solo las rutas IPv4. EIGRP para IPv6 sigue el mismo modelo. EIGRP para IPv4 y EIGRP para IPV6 se configuran y manejan separadamente. Sin embargo, la configuración de EIGRP para IPv4 e IPv6 es similar y proporciona familiaridad operacional y continuidad.

4.2 OSPFv3 e IPv6.

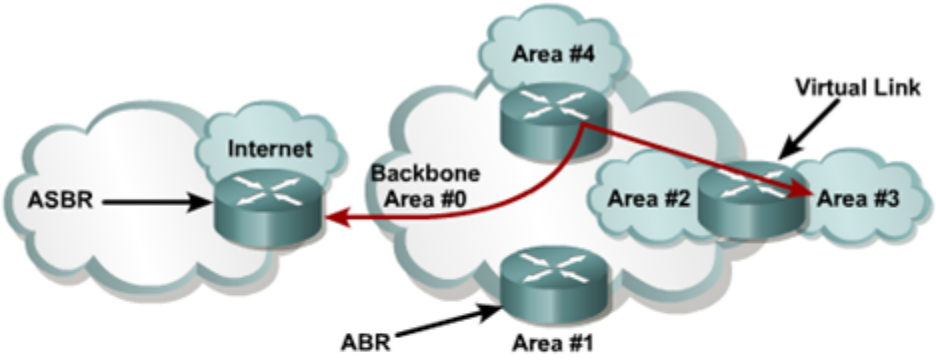
OSPF es un protocolo de estado de enlace de enrutamiento IP. Piensa en un enlace como una interfaz en un dispositivo de red. Un protocolo de estado de enlace toma decisiones de enrutamiento basado en el estado del enlace que conecta las maquinas de origen y destino.

[32] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 760.

El estado de enlace es una descripción de la interfaz y su relación con sus dispositivos de red vecinos. La información de interfaz incluye el prefijo IPv6 de la interfaz, la máscara de red, el tipo de red a la que se conecta, los Routers conectados a la red, y así sucesivamente.

Esta información se propaga en diversos tipos de anuncios de estado de enlace (link-state advertisements - LSAs). Una colección de datos LSA en un Router es almacenado en una base de datos de estado de enlace (link-state database - LSDB). El contenido de la base datos, cuando es sometido al algoritmo Dijkstra, resulta en la creación de la tabla de enrutamiento OSPF.

La diferencia entre la base de datos y la tabla de enrutamiento es que la base de datos contiene una completa colección de datos puros. La tabla de enrutamiento contiene una lista más corta de caminos para conocer los destinos específicos a través de puertos de interfaz del Router.OSPFv3, que se describe en RFC 2740, soporta IPv6.



La topologia en el área es invisible para fuera del área:
- La inundación de LSA es delimitado por el área
- El cálculo de SPF es realizado para cada área

El backbone está contiguo

Todas las áreas tienen conexión con el backbone
- Se puede utilizar un enlace virtual para conectarse al backbone

Fig. 26 Estructura Jerárquica - OSPFv3[33]

4.3 Similitudes entre OSPFv2 y OSPFV3

Muchas de las características OSPF para IPv6 son iguales en OSPFv2. OSPFv3 para IPv6 descrito en el RFC 2740, se expande en OSPFv2 para

[33] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 762 y 767.

proveer soporte para los prefijos de enrutamiento IPv6 y el mayor tamaño de direcciones IPv6.

Otras similitudes con OSPFv2 incluyen lo siguiente:

- Los mecanismos para el descubrimiento de vecinos y la formación de adyacencias son los mismos.

- La operación de OSPFv3 conforme el RFC soportan los modos multiacceso de **no difusión** (NBMA) y topología punto a multipunto. OSPFv3 también soporta otros modos de Cisco, como punto a punto y broadcast, incluyendo la interfaz.

- el flujo y el tiempo de vida de los LSA son iguales para OSPFv2 y OSPFv3.

- OSPFv3 utiliza los mismos tipos de paquetes básicos como OSPFv2, como los paquetes hello, descripción de la base de datos (también llamada paquete de descripción de la base de datos), petición de estado de enlace (LSR), actualización de estado de enlace (LSU), y LSA.

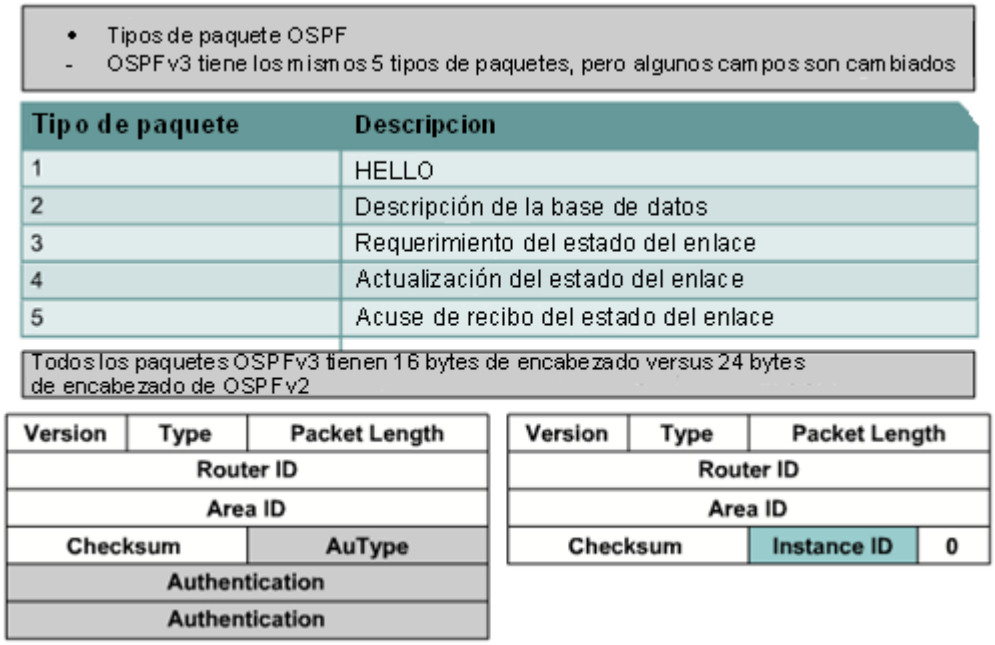


Fig. 27 Mejora de las Diferencias y Apoyo de Protocolo de Enrutamiento OSPFv2[34]

Todas las capacidades opcionales de OSPF para IPv4, incluyendo el soporte a la demanda de circuitos, áreas not-so-stubby (NSSAs), y las extensiones para el Multicast OSPF (MOSPF) son también soportadas en OSPF para IPv6.

[34] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 761.

4.4 Diferencias entre OSPFv2 y OSPFv3

Las diferencias entre OSPFv2 y OSPFv3 incluyen lo siguiente:

- **Ospfv3 Corre Sobre un Enlace**

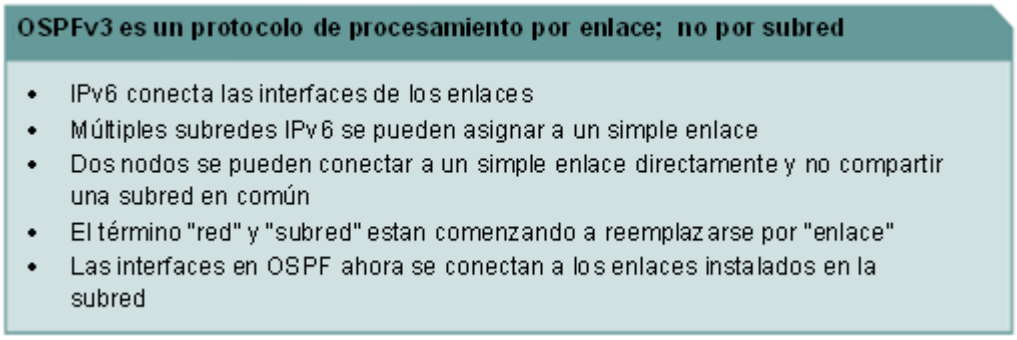


Fig. 28 OSPFv3 Por Procesos De Enlace[35]

  - OSPF para IPv6 se ejecuta en un enlace en lugar del comportamiento de IPv4 por subred IP. IPv6 usa el término "vínculo" para indicar "una facilidad de comunicación o medio sobre el cual los nodos pueden comunicarse en la capa de enlace." Por lo tanto, los términos "red" y "subred", utilizada en la especificación OSPF IPv4 se sustituyen por "vínculo".

  - La declaración **network** en el modo de subcomando del router OSPFv2 es reemplazado por el comando de interfaz **ipv6 ospf** process-id area area-id [**instance** instance-id].

- **Se Usan Direcciones de Enlace Local**

  - OSPFv3 utilizan direcciones de enlace local IPv6 para identificar las adyacencias de vecinos OSPFv3. Por lo tanto, cuando se configura el comando **IPv6 ospf neighbor,** la dirección **IPv6** que se debe utilizar es la dirección local de vínculo del vecino.

- **Soporte para Múltiples Instancia Ospfv3**

  - Separa los sistemas autónomos, cada uno de OSPF en ejecución, utilizan un vínculo común. Un único enlace puede pertenecer a múltiples áreas.

  - OSPFv3 utiliza un nuevo campo, llamado lD (identificador) de la instancia, para permitir múltiples instancias por enlace. Para tener 2 instancias de conversaciones unos con otros, deben

[35] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 765 y 766.

compartir la misma instancia ID. Por defecto, el identificador de instancia se establece en 0.

- **Direcciones Multicast[36]**

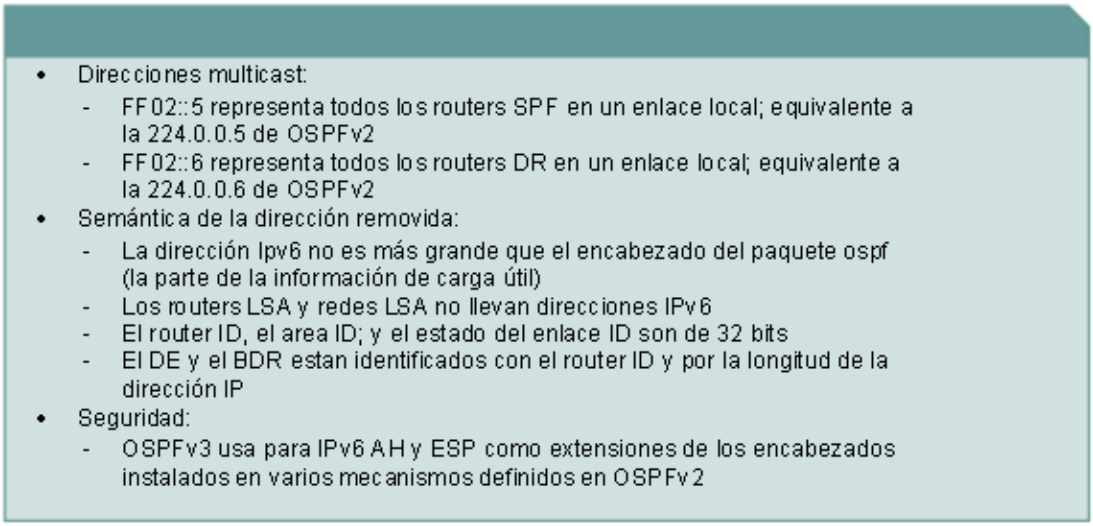


Fig. 29 Otras Diferencias entre OSPFv2 y OSPFv3[37]

  - FF02**::**5 representa primero la ruta más corta de todos los Routers (shortest path first - SPF) en el alcance de enlace local, equivalente a 224**.**0**.**0**.**5 en OSPFv2.

  - FF02**::**6 representa todos los Routers designados (designated routers - DRs) en el alcance de enlace local, equivalente a 224**.**0**.**0**.**6 en OSPFv2.

- **Supresión de la Semántica de Dirección**

  - Las direcciones IPv6 no están más presentes en el encabezado del paquete OSPF (parte de la información de carga útil).

  - Los Routers LSA y las redes LSA no llevan direcciones IPv6.

  - El Router ID, área ID, y el ID de enlace permanecen en 32 bits.

  - El Router DR y el router de respaldo designado (backup designated router - BDR) son identificados por su router ID y no por su dirección IP.

[36] http://www.faqs.org/rfcs/rfc1112.html
[37] Tomado del curriculum de CCNp versión 5.

- **Seguridad**

    - OSPFv3 utiliza el encabezado de autenticación IPv6 (Authentication Header - AH) y los encabezados de extensión de seguridad de carga útil (Encapsulating Security Payload - ESP), en lugar de la variedad de mecanismos definidos en OSPFv2.

    - La autenticación ya no forma parte de OSPF. Ahora es el trabajo de IPv6 asegurar que el nivel correcto de autenticación este en uso.

4.5 Tipos de LSA para IPv6

LSA OSPFv3 incluyen las siguientes Las características:

- El LSA se compone de un Router ID, área ID, e ID de estado de enlace. Son Cada uno de 32 bits. Aunque, estén escritos en notación decimal, no son derivados de una dirección IPv4.

- Las LSAs de Router y LSAs de red contienen solo IDs de 32 bits. No contienen direcciones.

- Las LSAs tienen alcance de transmisión que define el diámetro hacia donde deben transmitir:

    - **Enlace local:** Fluye a todos los Routers en la red.
    - **Área:** Fluye a todos los Routers dentro de un área OSPF.
    - **Sistema Autónomo:** Fluye a todos los Routers en un sistema autónomo entero OSPF.

- OSPFv3 soporta el envío de LSAs desconocidos basado en el alcance de transmisión. Esto puede ser útil en una NSSA.

- OSPFv3 toma las ventajas del multicasting IPv6, usando FF02**::**5 para todos los Routers OSPF, y FF02**::**6 para el DR y BDR OSPF.

Los dos LSAs renombrados son los siguientes:

- **LSAs de Prefijo Interárea para los Routers de Área de Frontera (ABRs) (tipo 3):** Las LSA de tipo 3 anuncian las redes internas de los Routers en otras áreas (rutas interárea). Las LSAs tipo 3 pueden representar una única red o un grupo de redes sumarizadas en una advertencia. Solo los ABRs generan LSAs sumarizadas. En OSPF para IPv6, las direcciones para estas LSAs son expresadas como prefijos, prefijos de longitud en vez de dirección, máscara. La ruta por defecto se expresa como un prefijo con longitud 0.

- **LSAs de Router Interárea para Sistemas Autónomos de Routers de Frontera (ASBRs) (tipo 4):** Las LSAs tipo 4 advierten la ubicación de un ASBR. Los Routers que tratan de alcanzar una red externa utilizan estas advertencias para determinar la mejor ruta al siguiente salto. Los ASBRs generan LSAs tipo 4.

Las dos nuevas LSAs en IPv6 son las siguientes:

- **LSAs de enlace (tipo 8):** Las LSAs de tipo 8 tienen un alcance de enlace local y nunca se transmiten más allá del enlace con el cual están asociados. Las LSAs de enlace proveen la dirección de enlace local del Router para todos los demás Routers ligados al enlace. Las LSAs de enlace también informan a los otros Routers ligados al enlace de una lista de prefijos IPv6 para asociarlos con el enlace, y permitir al Router afirmar una colección de bits opcionales para asociarlo con la red LSA que se originada por el enlace.

- **LSAs de Prefijo Intra-Área (tipo 9):** Un Router puede originar múltiples LSAs de prefijo intra-área para cada Router o red de tránsito, cada uno con un único ID de estado de enlace. El ID de estado de enlace para cada prefijo intra-área LSA describe su asociación a la LSA de Router o LSA de red. El ID de estado de enlace también contiene prefijos para redes stub y de tránsito.

	LSA Function Code	LSA type
Router-LSA	1	0x2001
Network-LSA	2	0x2002
Inter-Area-Prefix-LSA	3	0x2003
Inter-Area-Router-LSA	4	0x2004
AS-External-LSA	5	0x2005
Group-membership-LSA	6	0x2006
Type-7-LSA	7	0x2007
Link-LSA	8	0x2008
Intra-Area-Prefix-LSA	9	0x2009

Fig. 30 Descripcion LSA.[38]

[38] Tomado de la versión de CCNP versión 5 y del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 761..

4.6 Prefijo de Dirección y LSAs

Un prefijo de dirección se produce en casi todas las nuevas LSAs definidas. El prefijo es representado por tres campos: prefijo de longitud, prefijo de opciones, y prefijo de dirección. En OSPF para IPv6, las direcciones para las LSAs son expresadas como prefijos, prefijo de longitud en vez de dirección, máscara.

La ruta por defecto se expresa como un prefijo con longitud 0.

Las LSAs de tipo 3 y 9 llevan toda la información del prefijo IPv6, la cual, en IPv4 se incluye en las LSAs de Router y de red.

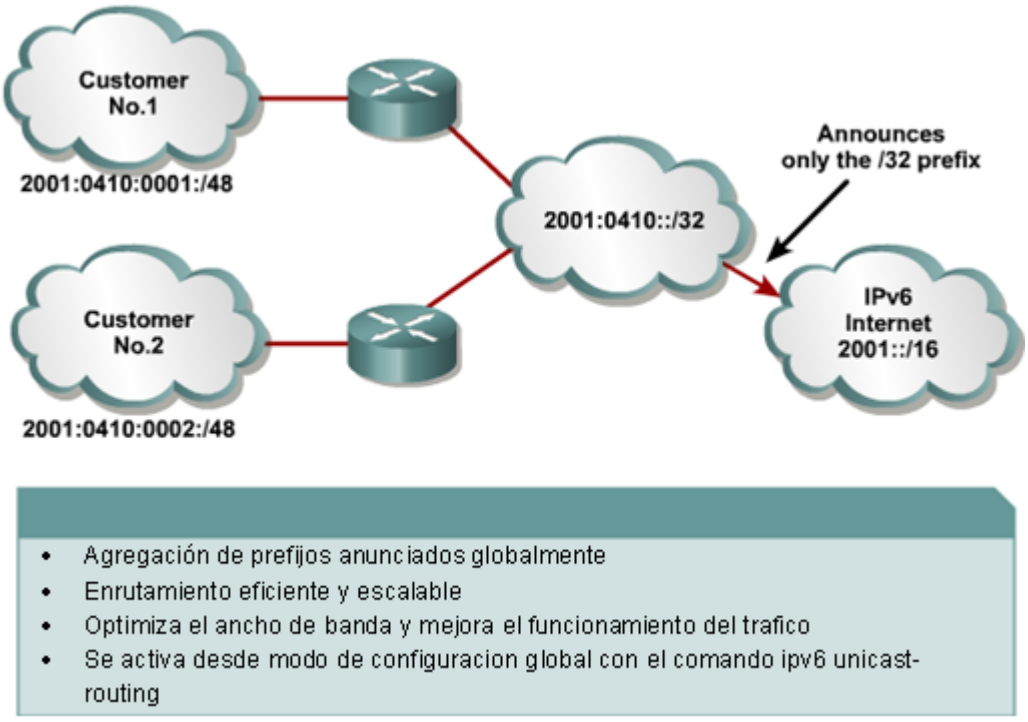


Fig. 31 Mayor Espacio de Direcciones Permite Agregación de Direcciones[39]

5.0 Implementación y Verificación OSPFv3

5.1 Configuración de OSPFv3 en IPv6

Muchos comandos OSPFv3 son similares a los de OSPFv2. En muchos casos, simplemente debe reemplazar cada prefijo **ip** en el comando OSPF con **ipv6**. Por ejemplo, en vez de usar el comando **ip address** para asignar una dirección IPv6 use el comando **ipv6 address.** Para ver las rutas IPv6, use el comando de emisión **show ipv6 route.**

[39] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 762 y 767.

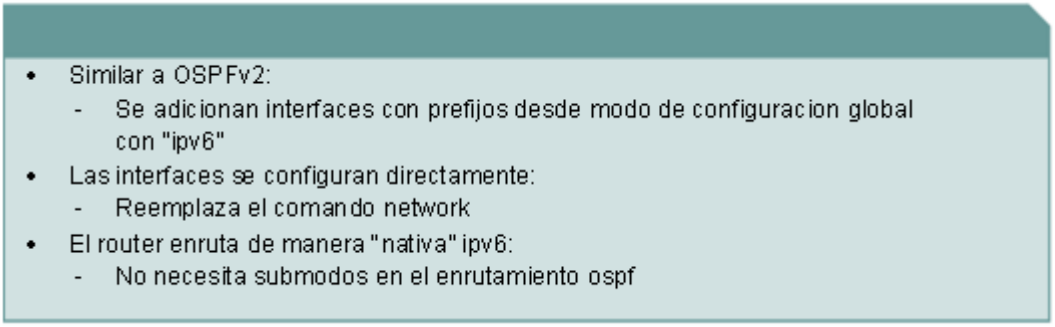


Fig. 32 Configurar OSPFv3 en el Software Cisco IOS

La configuración de OSPFv3 no es un modo de subcomando del comando **router ospf** como en la configuración de OSPFv2. Por ejemplo, en vez de utilizar el comando **network area** para identificar redes que forman parte de la red OSPFv3, las interfaces se configuran directamente para especificar que las redes IPv6 son parte de la red OSPFv3.

A continuación se describen los pasos para configurar OSPF para IPv6:

Paso 1 Completa la estrategia de red de OSPF y la planeación para la red IPv6. Por ejemplo, se debe decidir si se requieren múltiples áreas.

Paso 2 Habilitar el enrutamiento unicast IPv6 utilizando el comando **ipv6 unicast-routing.**

Paso 3 Habilitar IPv6 en la interfaz usando el comando **ipv6 ospf area.**

Paso 4 (opcional) Configurar OSPFv3 en la interfaz con las específicas configuraciones, incluyendo área, prioridad del Router, y costo de la ruta OSPFv3.

Paso 5 (opcional) Configurar los detalles de enrutamiento del modo de configuración del Router, incluyendo la prioridad del Router, sumarización de ruta, y demás.

5.2 Habilitando OSPFv3 en una Interfaz

La mayor parte de la configuración de OSPFv3 se realiza en la interfaz. La figura 33 muestra un ejemplo de configuración que permite una dirección IP IPv6, área, la prioridad del router y costo de la ruta.

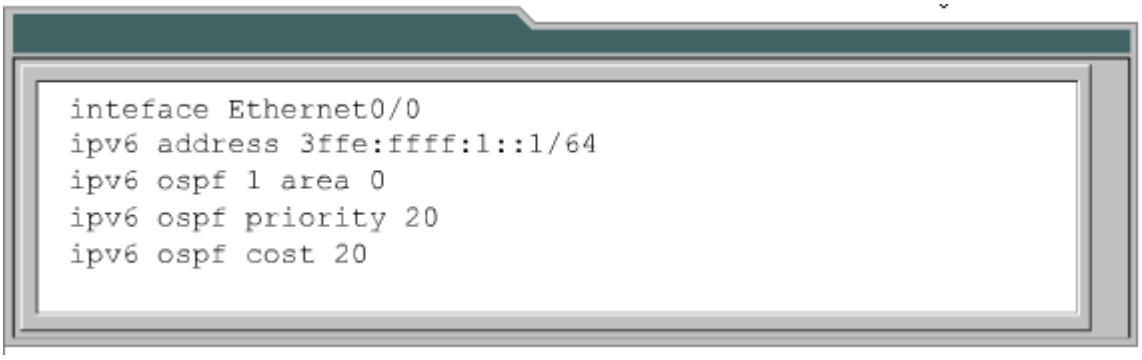


Fig. 33 Permite OSPFv3 en una Interfaz

La figura 34 proporciona descripciones de los comandos de interfaz necesarios y opcionales incluyendo la prioridad del Router y el costo de la ruta OSPFv3.

Paso	Comando o acción	Propósito
1	Router(config)# **interface** *type number*	Especifica el tipo y numero de la interface, y se accesa al router para esa interfaz desde modo de configuracion global
2	Router(config-if)# **ipv6 address** *address/prefix-length* [**eui-64**]	Configura las direcciones ipv6 en la interface y activa el procesamiento de ipv6. Los parámetros eui-64 forzan al router a completar la dirección con los parámetros de 64 bits con la dirección de la interface si usa este parámetro EUI-64 como interface ID
3	Router(config-if)# **ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*]	Activa ospf con ipv6 para la interface
4	Router(config-if)# **ipv6 ospf priority** *priority number*	El numero de prioridad que se usa para la eleccion del router designado
5	Router(config-if)# **ipv6 ospf cost** *cost*	El costo de envio de los paquetes en la interface expresa el estado del enlace con su métrica

Fig. 34 Comandos de Configuración de la Interfaz OSPFv3

5.3 Características de la Configuración de Enrutamiento OSPFv3

Las características de enrutamiento OSPFv3 son configurados en el modo de configuración del Router. Para ingresar al modo de configuración del Router, utilice el comando **ipv6 router ospf** process-id. Este comando activa un proceso OSPF en el Router. El parámetro de ID de proceso identifica un único proceso OSPFv3.

Para un sólo Router IPv6, un parámetro de Router ID debe definirse en la configuración de OSPFv3 como una dirección IPv4 utilizando el comando de configuración del Router **router-id** *router-id.* OSPFv3 utiliza un número de 32 bits para el Router ID. El Router ID OSPFv3 puede expresarse en decimal punteado, permitiendo una fácil superposición de una red OSPFv3 en una red existente OSPFv2. La figura 35 muestra un ejemplo de configuración.

Fig. 35 Configuración de la ID del Router

Si IPv4 está configurado en el Router, por defecto, el Router ID se elige de la misma manera como lo es con OSPFv2. La dirección más alta IPv4 configurada en una interfaz de loopback será el Router ID. Si no se configuran las interfaces de loopback, la dirección más alta en cualquier otra interfaz se convierte en el ID del Router.

5.4 Sumarización de Rutas OSPFv3

La figura 36 muestra un ejemplo de rutas OSPFv3 antes de la sumarización.

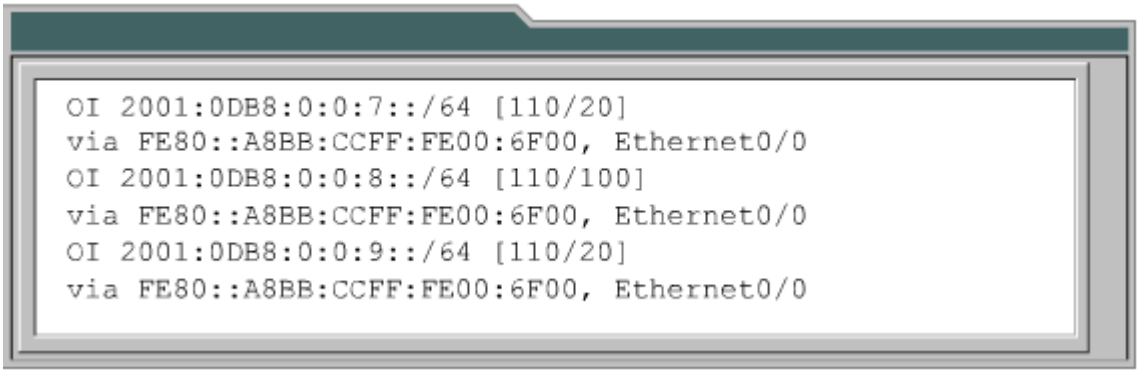


Fig. 36 Rutas Antes de la Sumarizacion OSPFv3

Para agrupar y sumarizar rutas en un área de frontera, utilice el comando del router OSPF IPv6 the **area** *area-id* **range** *ipv6-prefix/prefix-length* [**advertise** | **not-advertise**] [**cost** *cost*]. La figura 37 da un ejemplo de configuración.

```
Router(config)#ipv6 router ospf 1
Router(config-rtr)#area range 1 2001:0DB8::/48
```

Fig. 37 Sumarizacion de Rutas OSPFv3

El costo de las rutas sumarizadas es el mas alto costo de las rutas que se sumarizan. Por ejemplo, las rutas mostradas en la figura 36 llegan a ser una ruta sumarizada como se muestra en la figura 38.

```
OI 2001:0DB8::/48 [110/100]
via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
```

Fig. 38 Rutas Después de la Sumarizacion OSPFv3

5.5 Ejemplo de Configuración OSPFv3

El ejemplo en la figura 39 muestra una red OSPF de 2 Routers, con área 0 y área 1. El comando especifico de interfaz **ipv6 ospf 100 area 0** crea el proceso “ospf 100 del router ipv6” dinámicamente, como lo hace el comando **ipv6 ospf 100 area 1.**

```
Router1#
interface S1/1
 ipv6 address 2001:410:FFFF:1::1/64
 ipv6 enable
 ipv6 ospf 100 area 0

interface S2/0
 ipv6 address 3FFE:B00:FFFF:1::2/64
 ipv6 enable
 ipv6 ospf 100 area 1

ipv6 router ospf 100
 router-id 10.1.1.3

Router2#
interface S3/0
 ipv6 address 3FFE:B00:FFFF:1::1/64
 ipv6 enable
 ipv6 ospf 100 area 1

ipv6 router ospf 100
 router-id 10.1.1.4
```

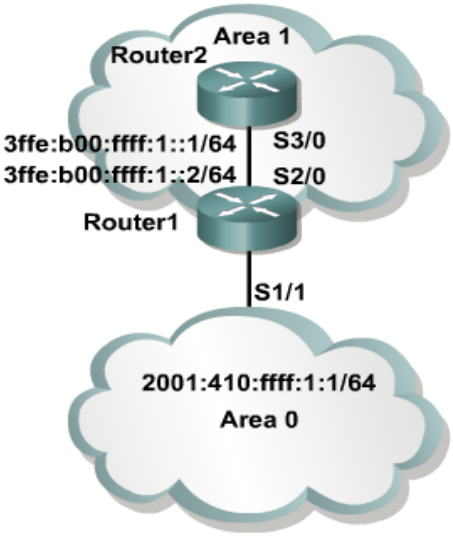


Fig. 39 Ejemplo de Configuración OSPFv3[40]

[40] Tomado del curriculum CCNP versión 5 y del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 768.

5.6 Verificación OSPFv3

Hay diversos comandos **show** OSPFv3 usados comúnmente, incluyendo el comando **show ipv6 ospf** [*process-id*] [*area-id*] **interface** [*interface*]. Este comando genera la información de interfaz OSPF relacionada, como se muestra en la figura 40.

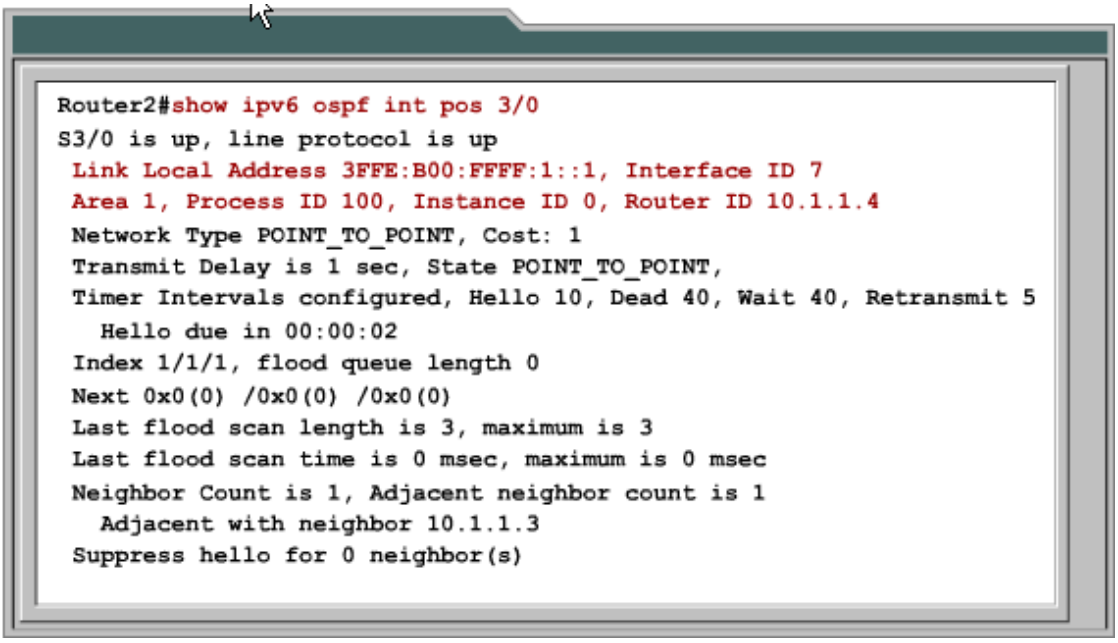
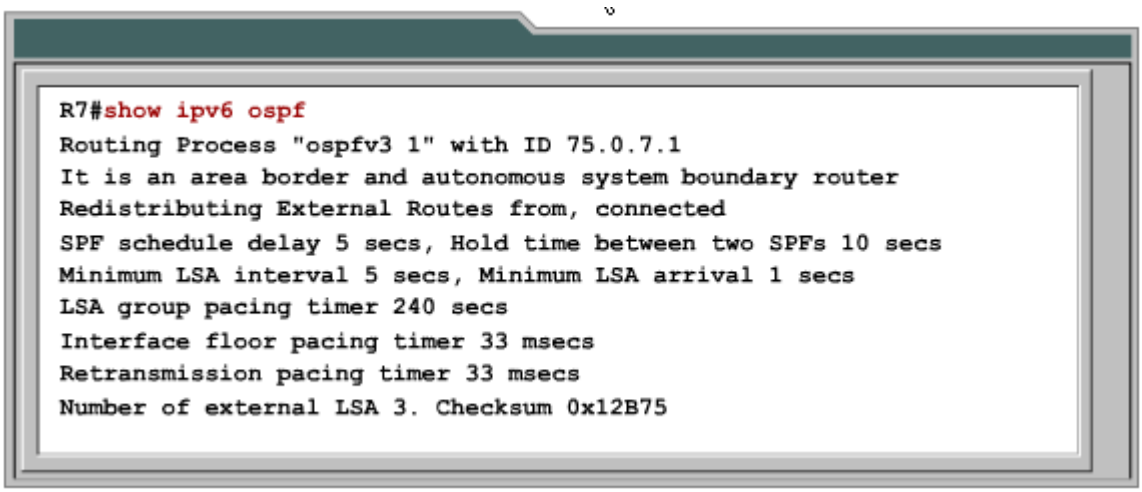


Fig. 40 Cisco IOS Verificar OSPFv3[41]

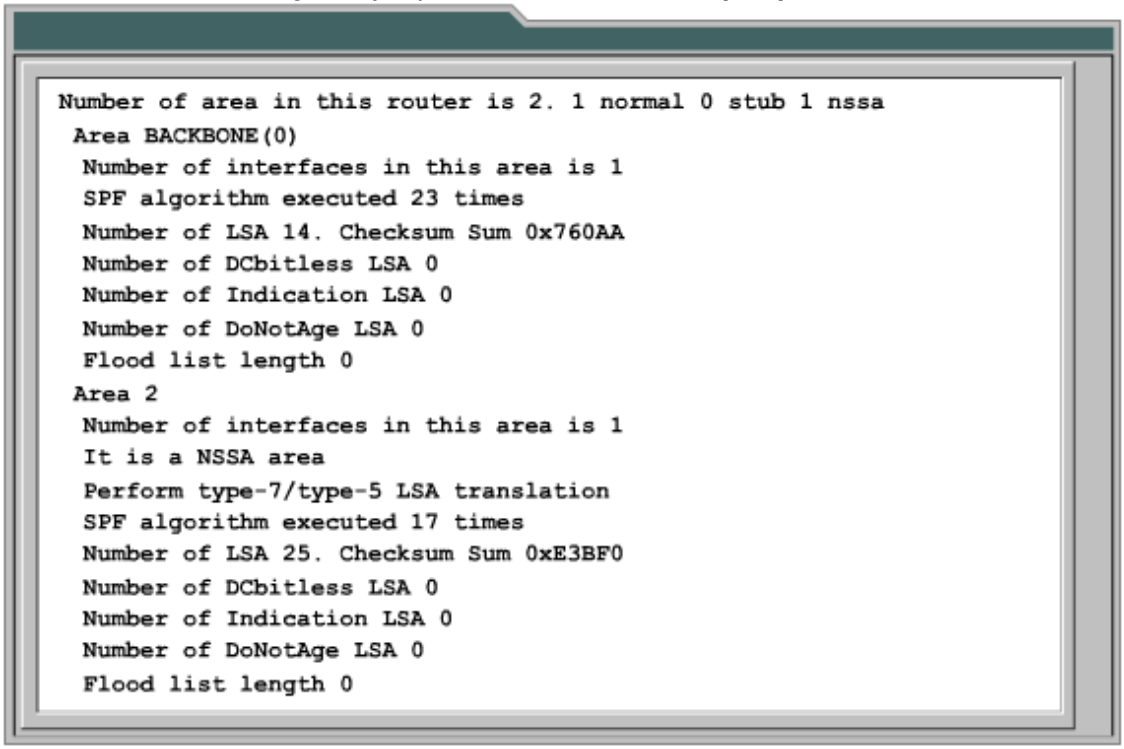
El comando **clear ipv6 ospf** [*process-id*] {**process** | **force-spf** | **redistribution** | **counters** [**neighbor** [*neighbor-interface* | *neighbor-id*]]} activa el recálculo SPF y la repoblación de la base de información de enrutamiento (RIB).

El comando **show ipv6 ospf** [process-id] [area-id] muestra información general sobre los procesos OSPF, como se muestra en las figuras 41 y 42.



[41] Tomado del curriculum CCNP versión 5.

Fig. 41 Ejemplos del Comando **show ip ospf**[42]



```
Number of area in this router is 2. 1 normal 0 stub 1 nssa
 Area BACKBONE(0)
  Number of interfaces in this area is 1
  SPF algorithm executed 23 times
  Number of LSA 14. Checksum Sum 0x760AA
  Number of DCbitless LSA 0
  Number of Indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0
 Area 2
  Number of interfaces in this area is 1
  It is a NSSA area
  Perform type-7/type-5 LSA translation
  SPF algorithm executed 17 times
  Number of LSA 25. Checksum Sum 0xE3BF0
  Number of DCbitless LSA 0
  Number of Indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0
```

Fig. 42 Ejemplos del Comando **show ip ospf** (Cont.)[43]

La figura 43 lista algunas de las salidas de los campos y descripciones del comando **show ipv6 ospf.**

Campo	Descripción
Proceso de enrutamiento "ospfv3" con ID 172.16.3.3	Proceso ID y OSPF router ID
Grupo temporizador de tiempo	Se configura el grupo temporizador de tiempo en segundos
Interface de tiempo de inundación	Se configura el tiempo de inundación de temporizador en milisegundos
Tiempo de temporizador de retransmisión	Se configura el tiempo de retransmisión en milisegundos
Numero de áreas descripción	Numero de áreas en el router; área de direcciones y así sucesivamente

Fig. 43 Descripciones de los Campos **show ipv6 ospf**[44]

[42] Tomado del curriculum CCNP versión 5
[43] Tomado del curriculum CCNP versión 5
[44] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 738 y 748.

5.7 Verificación de Vecinos OSPFv3

Para mostrar la información de vecino OSPF en función de cada interfaz, utilice el comando **show ipv6 ospf neighbor** en el modo EXEC de usuario o EXEC privilegiado. El comando **show ipv6 ospf neighbor detail** provee información detallada sobre los vecinos OSPF IPv6, como se ilustra en la Figura 44.

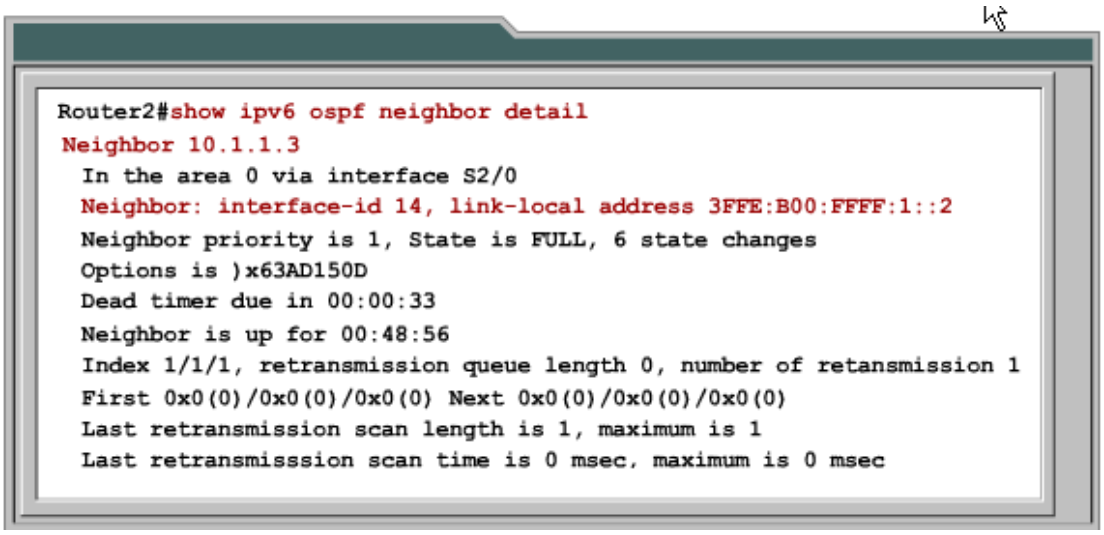


Fig. 44 Ejemplo del Comando **show ipv6 ospf neighbor detail** [45]

La figura 45, muestra las salidas de los campos y descripciones del comando **show ipv6 ospf neighbor.**

Campo	Descripción
Vecinos ID; vecinos	Router con el ID del vecino
En el área	El área y la interface están relacionados directamente con los vecinos conocidos
Pri; prioridad de vecino	Prioridad del router vecino; y estado del vecino
Estado	Estado de ospf
Cambios de estado	Numero de cambios de estado desde que los vecinos fueron adicionados
Opciones	Las opciones de los paquetes hello tiene varios campos. Solamente un bit externo (e-bit). Posibles valores están entre 0 a 2; el 2 indica que es un área no stub. Y el cero indica que es un área stub

Fig. 45 Descripción de Campo **show ipv6 ospf neighbor detail**[46]

[45] Tomado del curriculum CCNP versión 5.
[46] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 738.

Intervalo de tiempo muerto	Especifica el intervalo de tiempo muerto antes de que se considere el vecino eliminado
Vecino desde arriba	Especifica el tiempo en horas, minutos y segundos desde que se estableció la adyacencia en el formato (HH:MM:SS)
Índice	Localización del vecino si dentro del área o interarea y retransmisión en cola
Longitud de retransmisión en cola	Numero de elementos en la cola retransmitidos
Numero de retransmisión	Número y tiempo de la actualización de los paquetes y tiempo durante la retransmisión
Primero	Localización en la memoria y detalles de la inundación
Siguiente	Localización en la memoria y detalles de la inundación
Ultima retransmisión y nuevo escaneo	Numero de LSAs durante la última retransmisión
Numero de retransmisión	Numero de tiempo y de paquetes de actualización durante la reciente inundación
Primero	Localización en la memoria y detalles de la inundación
Siguiente	Localización en la memoria y detalles de la inundación

Fig. 45 Descripcion de Campo **show ipv6 ospf neighbor detail** (Cont.)[47]

5.8 Verificación de la Base de Datos OSPFv3

Para mostrar la lista de información relacionada a la base de datos OSPF para un Router especifico, utilice el comando **show ipv6 ospf database** en el modo EXEC de usuario o EXEC privilegiado. Las diversas formas de este comando entregan información sobre diferentes advertencias de estado de enlace OSPF (link-state advertisements - LSAs).

Las figuras 46 y 47 ilustran una muestra parcial de la salida del comando **show ipv6 ospf database.**

[47] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 748.

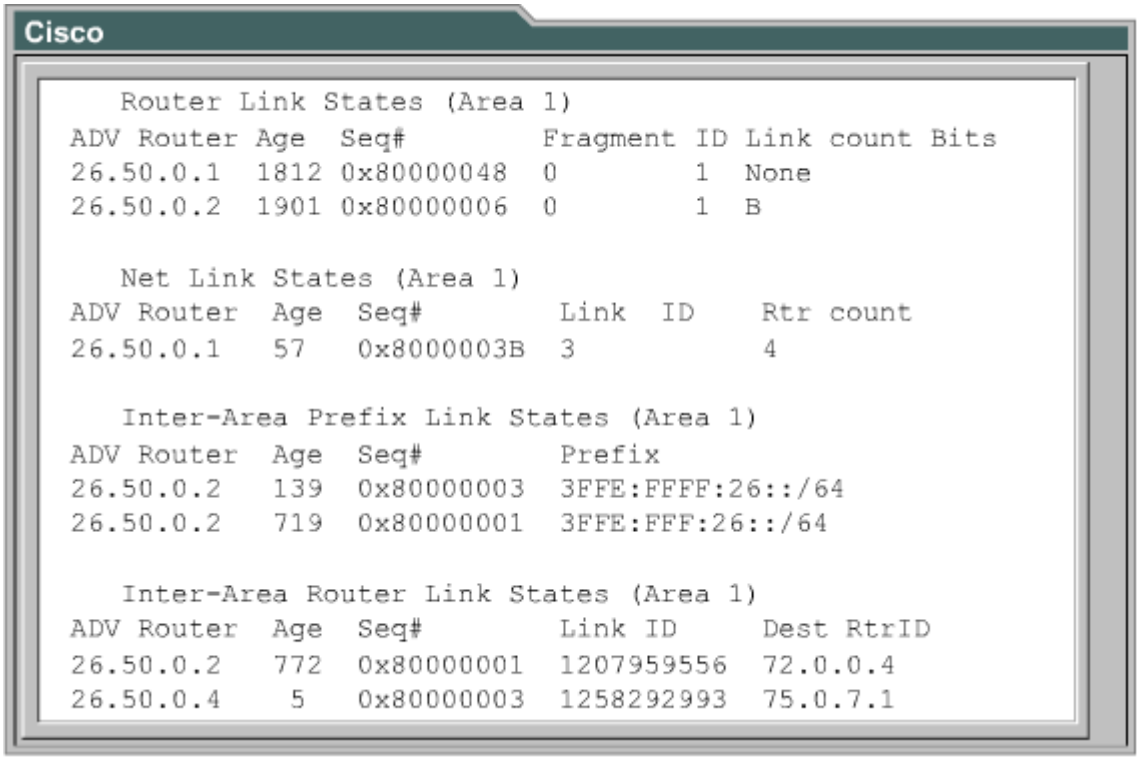


Fig. 46 Comando **show ipv6 ospf database** [48]

La figura 47 provee las descripciones de las salidas de los campos del comando **show ipv6 ospf database.**

Campo	Descripción
Router AVD	Anuncia el router ID
Tiempo	Tiempo del estado del enlace
Numero de secuencia	Numero de secuencia del estado del enlace (detecta el antiguo y el siguiente LSAs)
Enlace ID	Numero de la interface ID
Ref-lstype	Se refiere al tipo del enlace con su estado

Fig. 47 Descripcion de Campo **show ipv6 ospf database**[49]

La figura 48 ilustra muestras de las salidas del comando **show ipv6 ospf database database-summary.**

[48] Tomado del curriculum CCNP versión 5.
[49] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 766

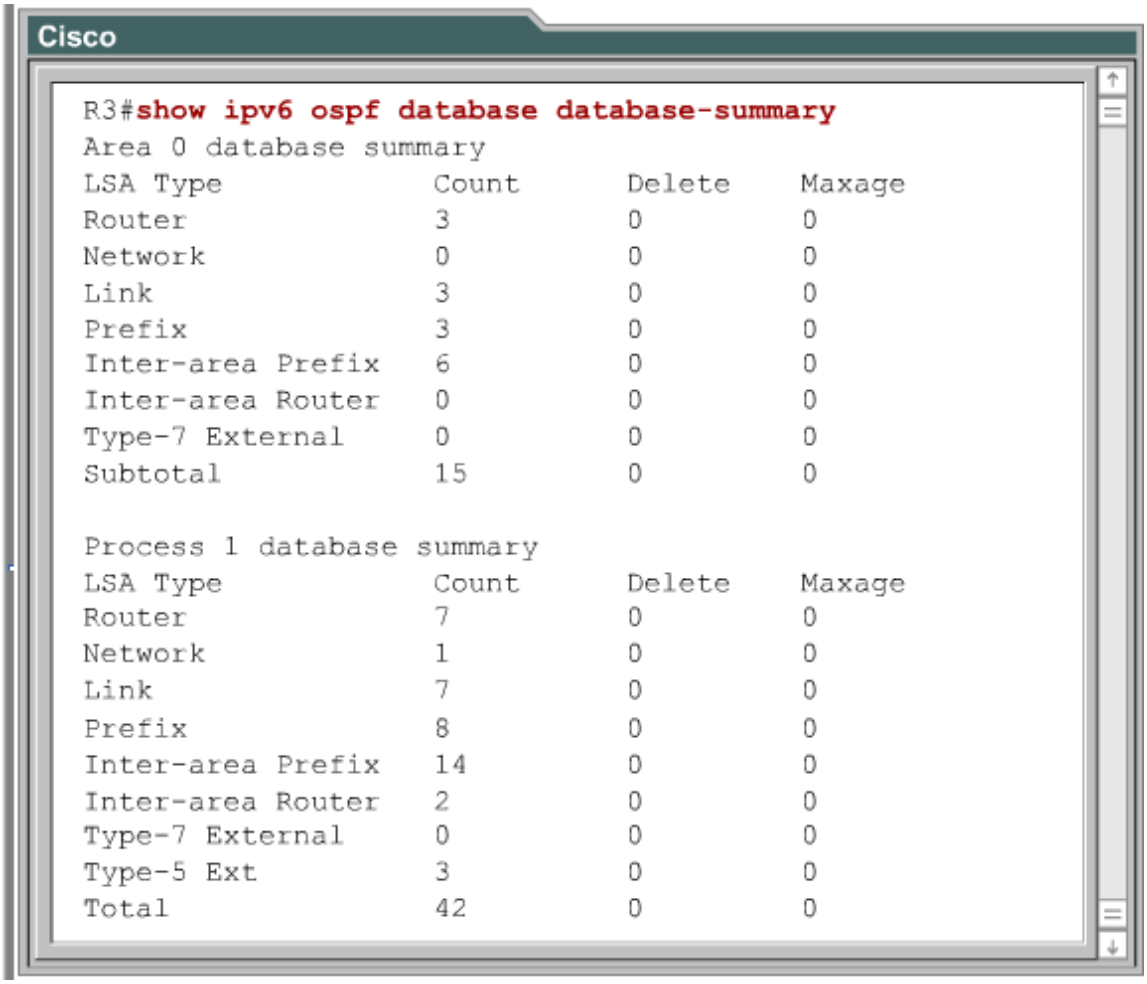


Fig. 48 comandos **show ipv6 ospf database database-summary**[50]

6.0 EIGRP para IPv6

Cisco creó originalmente EIGRP para anunciar los protocolos enrutados IPv4, IPX y AppleTalk. Esta arquitectura básica de EIGRP permitió crear fácilmente otro protocolo de capa 3, IPv6 para ser agregado. Como resultado, Cisco no tiene que hacer cambios a EIGRP de manera significativa para soportar IPv6, existen tantas similitudes entre las versiones de EIGRP para IPv4 e IPv6.

La cobertura restante de EIGRP se centra en los cambios a la configuración de EIGRP y la verificación en apoyo de IPv6.

6.1 EIGRP para IPv4 e IPv6 conceptos teóricos y comparativos.

En su mayor parte, EIGRP para IPv4 e IPv6 contienen muchas similitudes. A continuación se enumeran algunas de las principales diferencias:

[50] Tomado del curriculum CCNP versión 5.

■ EIGRP para IPv6 anuncia prefijos y longitudes para IPv6, en lugar de información de las mascaras de subred de IPv4.

■ EIGRP para IPv6 utiliza la dirección de enlace local del vecino como la dirección IP del siguiente salto; EIGRP para IPv4 no aplica este concepto.

■ EIGRP para IPv6 encapsula sus mensajes en paquetes IPv6, en lugar de paquetes IPv4.

■ La autenticación de EIGRP para IPv6 se basa en la incorporación de características de autenticación y confidencialidad propias de IPv6.

■ EIGRP para IPv4 por defecto utiliza automáticamente sumarización de rutas en los límites de las redes IPv4 con clase; IPv6 no tiene ningún concepto de las redes con clase, por lo que EIGRP para IPv6 no puede realizar ninguna sumarización automática.

■ EIGRP en IPv6 no requiere vecinos en la misma subred IPv6 como requisito para convertirse en vecinos.

Aparte de estas diferencias, la mayoría de los detalles de EIGRP para IPv6 funcionan como EIGRP para IPv4. Como se muestra en la Figura 49 se comparan las características de cada uno.

Características	EIGRP para IPv4	EIGRP para IPv6
Anuncia rutas	IPv4	IPv6
Protocolo de capa 3 EIGRP con mensajes	IPv4	IPv6
Tipo de encabezado del protocolo capa 3	88	88
Puertos UDP	No aplica	No aplica
Uso de sucesor, y sucesor factible	Si	Si
Uso de dual	Si	Si
Soporta VLSM	Si	Si
Puede garantizar sumarización automática	Si	No aplica
Usa actualizaciones disparadas	Si	Si
Uso una métrica compuesta, por defecto ancho de banda y retardo	Si	Si
Métrica de significado infinito	$2^{32} - 1$	$2^{32} - 1$
Soporta etiquetado de rutas	Si	Si
Destino de las actualizaciones multicast	224.0.0.10	FF02::10
Autenticacion	Especifico de EIGRP	IPv6 usa AH/ESP

Fig.49 Tabla comparativo de EIGRP para IPv4 e IPv6[51]

[51] Tomado del libro CCNP ROUTE 642-902 Guia de certificacion oficial pagina 581.

6.2 CONFIGURANDO EIGRP PARA IPv6

EIGRP para IPv6 sigue el mismo concepto básico de configuración para RIPng, además de unos pocos pasos adicionales, como se indica a continuación:

1. Habilitar el enrutamiento IPv6 desde modo de configuración global con el comando **ipv6 unicast-routing**.

2. Habilitar EIGRP desde modo de configuración global con el comando **ipv6 router eigrp** (1-65535).

3. Habilitar IPv6 en la interfaz, básicamente con uno de los siguientes dos métodos:

- Configure una dirección unicast IPv6 en cada interfaz, usando el comando de interfaz **ipv6 address** *address/prefix-length* [**eui-64**].

- Configure el comando **ipv6 enable**, IPv6, habilita IPv6 y hace que el router obtenga su dirección de enlace local.

4. Habilitar EIGRP en la interfaz con el modo de subinterfaz **ipv6 eigrp** *asn* (donde el nombre coincide con el comando de configuración global **ipv6 router eigrp** *asn*).

5. Habilitar EIGRP para IPv6 con el comando **no shutdown** en la interfaz mientras está configurando EIGRP.

6. Si no hay un router ID de EIGRP configurado automáticamente, debe tener al menos una interfaz configurada con una dirección IPv4 activa, configure un router ID de EIGRP con el comando **eigrp router-id** *rid* en el modo de configuración de EIGRP.

La siguiente lista define cómo EIGRP para IPv6 recoge su RID, que figuran en el orden de preferencia:

1. Utilice el valor configurado (usando el subcomando EIGRP **eigrp router-id** *a.b.c.d* bajo el comando **ipv6 router eigrp**).

2. Use la dirección IPv4 más alta de un enlace activo sobre una interfaz de loopback configurada

3. Use la dirección Ipv4 más alta de un enlace activo sobre una interface que no tenga una interface de loopback.

Tenga en cuenta que la mayoría de instalaciones ya han configurado las direcciones IPv4, es posible que el proceso de EIGRP para IPv6 no pueda derivar un valor RID. Si el router no tiene interfaces funcionando que tengan direcciones IPv4, el RID EIGRP para IPv6 no está explícitamente configurado, entonces el proceso de EIGRP para IPv6 simplemente no funciona. Así, el proceso de configuración de seis pasos incluye una mención del RID EIGRP; de manera más general, puede ser prudente configurar un RID explícitamente como una cuestión de habilidad.

Después de haber sido habilitado en una interfaz, EIGRP para IPv6 realiza las mismas dos funciones básicas que EIGRP para IPv4: descubre los vecinos y anuncia subredes conectadas. EIGRP para IPv6 utiliza el mismo concepto para encontrar vecinos igual que lo hacen los routers EIGRP para IPv4, excepto que EIGRP para IPv6 no requiere que los routers IPv6 vecinos tengan direcciones IPv6 en la misma subred.

También, como con EIGRP para IPv4, EIGRP para IPv6 anuncia una o todas las subredes conectadas en la interfaz, con la excepción de las direcciones de enlace local y las rutas locales (las rutas de host para una propia dirección de interfaz del router IPv6).

El Siguiente Ejemplo muestra un como es la configuración en el Router R1 en la figura 50. Todos los routers vecinos deben usar el mismo ASN; ASN 9 será utilizado en este caso.

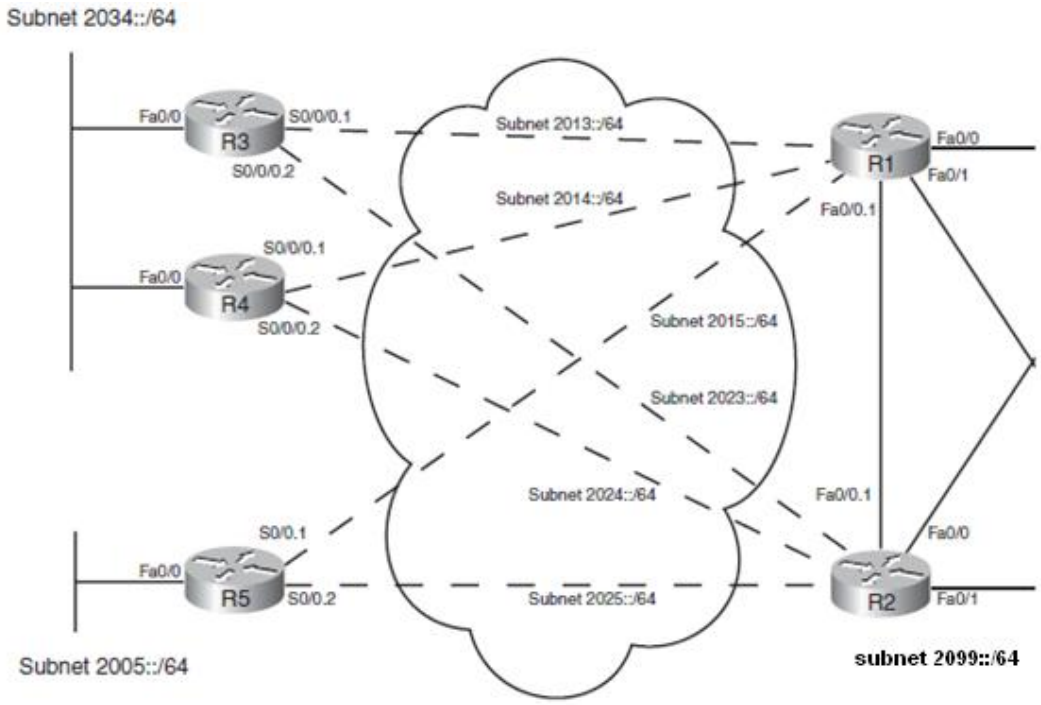


Fig.50 Ejemplo de configuración EIGRP para IPv6.[52]

Ejemplo: Configuración de EIGRP para IPv6 Enrutamiento y protocolos de enrutamiento en R1

R1# **show running-config**
! Configuracion paso 1: habilite el enrutamiento IPv6
ipv6 unicast-routing

! La siguiente, configuracion de los paso 3 y 4, en las 5 interfaces

interface FastEthernet0/0.1
ipv6 address 2012::1/64

[52] Tomado del libro CCNP ROUTE 642-902 guia de certificacion official pagina 577.

ipv6 eigrp 9
!
interface FastEthernet0/0.2
ipv6 address 2017::1/64
ipv6 eigrp 9
!
interface FastEthernet0/1.18
ipv6 address 2018::1/64
ipv6 eigrp 9
!
interface Serial0/0/0.3
ipv6 address 2013::1/64
ipv6 eigrp 9
!
interface Serial0/0/0.4
ipv6 address 2014::1/64
ipv6 eigrp 9
!
interface Serial0/0/0.5
ipv6 address 2015::1/64
ipv6 eigrp 9
!
!
Configuracion de los paso 2, 5, y 6
Debe subir las interfaces fisicas
no shutdown
ipv6 router eigrp 9
router eigrp 10.10.34.3

6.3 Verificando EIGRP para IPv6.

Los comandos **show** de EIGRP para IPv6 generalmente muestran, la misma información equivalente de EIGRP para IPv4, incluso más que RIPng. En la mayoría de los casos, basta con utilizar el mismo comando **show ip...** comandos aplicables con IPv4; y EIGRP. Esto sustituye IPv6 en lugar de IP.

El siguiente cuadro enumera un comparativo de referencia de los comandos más populares con EIGRP para ambas versiones. Note que en la tabla se asume que los comandos comienzan ambos con **show ip** o **show ipv6** en todo menos en la última fila de la tabla.

Function	show ip...	show ipv6...
All routes	... route	... route
All EIGRP learned routes	... route eigrp	... route eigrp
Details on the routes for a specific prefix	... route *subnet mask*	... route *prefix/length*
Interfaces on which EIGRP is enabled, plus metric weights, variance, redistribution, max-paths, admin distance	... protocols	... protocols
List of routing information sources	... protocols ... eigrp neighbors	... eigrp neighbors
Hello interval	... eigrp interfaces detail	... eigrp interfaces detail
EIGRP database	... eigrp topology [all-links]	... eigrp topology [all-links]
Debug that displays sent and received Updates	debug ip eigrp notifications	debug ipv6 eigrp notifications

Fig.51 Tabla Comparativo de EIGRP **show ip** y **show ipv6 ...**[53]

El ejemplo siguiente muestra algunos ejemplos tomados de los comandos SHOW en el router R3 de la red interna que se mostro en el grafico anterior. Los comentarios explicativos se muestran en el ejemplo de este caso.
Ejemplo 1 IPv6 EIGRP comandos **SHOW**[54]

En R3, la dirección del siguiente salto es la dirección local de vínculo del siguiente router.

R3# **show ipv6 route 2099::/64**
Routing entry for 2099::/64
Known via **"eigrp 9"**, distance 90, metric 2174976, type internal
Route count is 2/2, share count 0
Routing paths:
FE80::22FF:FE22:2222, Serial0/0/0.2
Last updated 00:24:32 ago
FE80::11FF:FE11:1111, Serial0/0/0.1
Last updated 00:07:51 ago

Tenga en cuenta que el siguiente comando lista únicamente las rutas EIGRP aprendidas. En él se enumeran dos de los próximos saltos para 2099:: 64. Note la información de la lista del siguiente salto son direcciones de enlace local.

R3# **show ipv6 route eigrp**

IPv6 Routing Table - Default - 19 entries

[53] Tomado del libro CCNP ROUTE 642-902 guia de certificacion official pagina 585.
[54] Tomado del libro CCNP ROUTE 642-902 guia de certificación oficial pagina 585.

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
EX - EIGRP external
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D 2005::/64 [90/2684416]
via FE80::11FF:FE11:1111, Serial0/0/0.1
via FE80::22FF:FE22:2222, Serial0/0/0.2
D 2012::/64 [90/2172416]
via FE80::22FF:FE22:2222, Serial0/0/0.2
via FE80::11FF:FE11:1111, Serial0/0/0.1
D 2014::/64 [90/2681856]
via FE80::11FF:FE11:1111, Serial0/0/0.1
D 2015::/64 [90/2681856]
via FE80::11FF:FE11:1111, Serial0/0/0.1
! lines omitted for brevity...
D 2099::/64 [90/2174976]
via **FE80::22FF:FE22:2222,** Serial0/0/0.2
via **FE80::11FF:FE11:1111,** Serial0/0/0.1

R3# **show ipv6 eigrp neighbors**

IPv6-EIGRP neighbors for process 9

H	Address	Interface	**Hold Uptime**	SRTT	RTO	Q	Seq
			(sec)	(ms)		Cnt	Num
1	Link-local address: FE80::22FF:FE22:2222	Se0/0/0.2	**14 01:50:51**	3	200	0	82
0	Link-local address: FE80::11FF:FE11:1111	Se0/0/0.1	13 01:50:52	14	200	0	90

La siguiente lista de comando muestra la base de datos de la topología EIGRP, incluyendo los cálculos viables de distancia, reporte de distancia, y el listado de todas las rutas de los sucesores y sucesores factibles.

R3# **show ipv6 eigrp topology**

P 2005::/64, 2 successors, FD is 2684416
via FE80::11FF:FE11:1111 (2684416/2172416), Serial0/0/0.1
via FE80::22FF:FE22:2222 (2684416/2172416), Serial0/0/0.2
P 2012::/64, 2 successors, FD is 2172416
via FE80::11FF:FE11:1111 (2172416/28160), Serial0/0/0.1
via FE80::22FF:FE22:2222 (2172416/28160), Serial0/0/0.2
P 2013::/64, 1 successors, FD is 2169856
via Connected, Serial0/0/0.1
! lines omitted for brevity

P 2099::/64, 2 successors, FD is 2174976
via FE80::11FF:FE11:1111 (2174976/30720), Serial0/0/0.1
via FE80::22FF:FE22:2222 (2174976/30720), Serial0/0/0.2
Finalmente la dirección del enlace local del vecino R1 es identificada.

R3# **show cdp entry R1**
————————————-
Device ID: R1
Entry address(es):
IP address: 10.10.13.1
IPv6 address: 2013::1 (global unicast)
IPv6 address: FE80::11FF:FE11:1111 (link-local)
Platform: Cisco 1841, Capabilities: Router Switch IGMP
Interface: Serial0/0/0.1, Port ID (outgoing port): Serial0/0/0.3
! lines omitted for brevity
El hecho más notable que figura en el ejemplo es que se confirma que existe poca diferencia con los comandos show para EIGRP para IPv4 contra IPv6.

7.0 RIP de Próxima Generación (RIPng)

Protocolo de enrutamiento de la información (RIP) inicio su vida como uno de los primeros protocolos de enrutamiento dinámico IP. Y con el tiempo se convirtió en el primer protocolo de enrutamiento dinámico para los protocolos IP emergentes en los años 1970. Más tarde, a mediados de la década de 1990, aparece RIP versión 2 (RIP-2.

A mediados de la década de 1990, el proceso para la definición de IPv6 se acercaba hacia la terminación, al menos para los estándares originales de IPv6. Para soporte de IPv6, el comité IETF define una nueva versión de RIP para la compatibilidad con IPv6.

Pero en lugar de llamar a RIP; como RIP, versión 3, los creadores seleccionaron un número para este nuevo protocolo conocido como versión 1, tratándolo como un nuevo protocolo. Sin embargo, nadie se molestó en poner "versión 1" en el nombre, simplemente lo llamaron RIP de próxima generación (RIPng), o simplemente RIP. Hasta la fecha, no hay ninguna nueva versión de RIPng, haciendo que RIPng todavía sea la versión más reciente de este protocolo.

7.1 Protocolo de enrutamiento RIPng

Las rutas de IPv6 usan los mismos protocolos y las mismas técnicas que IPv4. Si bien las direcciones son más largas, los protocolos utilizados en el enrutamiento IPv6 son simplemente extensiones lógicas de los protocolos utilizados en IPv4.

RFC 2080 define el protocolo de información de routing de siguiente generación (RIPng, Routing Information Protocol Next Generation) como un

protocolo de enrutamiento simple basado en RIP. RIPng no es ni más ni menos potente que RIP, pero proporciona una manera sencilla de crear una red IPv6 sin necesidad de crear un nuevo protocolo de enrutamiento.
RIPng es un protocolo de enrutamiento vector distancia con un límite de 15 saltos que usa Actualizaciones de envenenamiento en reversa y horizonte dividido para evitar routing loops. Su simplicidad proviene del hecho de que no requiere ningún conocimiento global de la red. Sólo los routers vecinos intercambian mensajes locales.

RIPng incluye las siguientes características:

- Basado en IPv4 RIP versión 2 (RIPv2) y es similar a RIPv2
- Usa IPv6 para el transporte
- Incluye el prefijo IPv6 y la dirección IPv6 del siguiente salto
- Usa el grupo multicast FF02::9 como dirección de destino para las actualizaciones de RIP (similar a la función de broadcast que realiza RIP en IPv4)
- Envía actualizaciones por el puerto UDP 521
- Es compatible con Cisco IOS Release 12.2(2)T y posteriores

En implementaciones de stack doble, se necesitan RIP y RIPng.

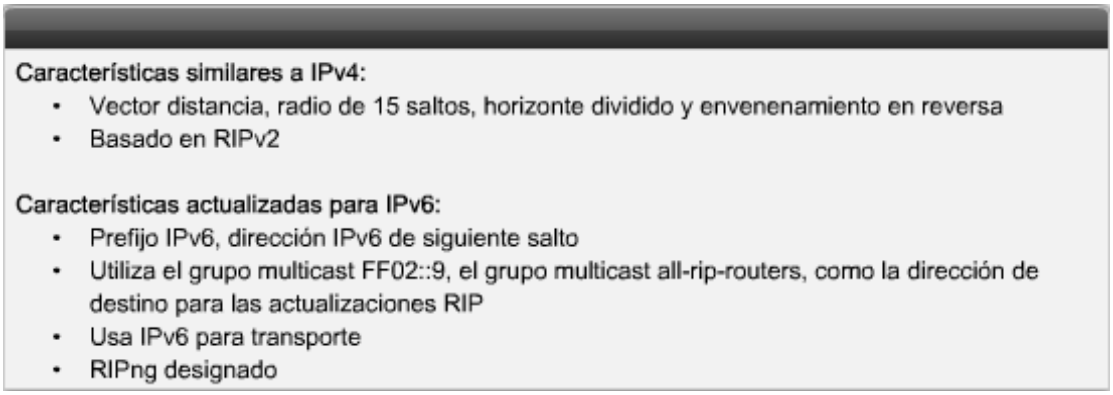


Figura 52: características entre IPv4 e IPv6[55]

7.2 RIPng- Teoría y comparaciones con RIP – 2

RIPng establece que el protocolo utiliza iguales conceptos y convenciones de las especificaciones originales de RIP-1, además de algunos conceptos de RIP-.2. Sin embargo, sabiendo que muchos de ustedes no recuerdan las especificaciones al detalle de RIP-2, en la Tabla 53 hay una lista variada de factores acerca de RIP-2 y RIPng.

[55] Tomado del curriculum de CCNA Exploration

Características	RIP-2	RIPng
Anuncio de rutas	IPv4	IPv6
los mensajes de RIP usan protocolos de la capa 3 y 4	IPv4; UDP	IPv6, UDP
puerto UDP	520	521
usa vector distancia	si	si
distancia administrativa por defecto	120	120
soporta VLSM	si	si
Can perform automatic summarization	Yes	N/A
usa horizonte dividido	si	si
usa envenenamiento en reversa	si	si
envía actualizaciones periódicas full cada 30 seg	si	si
usa actualizaciones disparadas	si	si
usa conteo de saltos	si	si
usa una métrica infinita	16	16
soporta rutas etiquetadas	si	si
direcciones multicast de actualizaciones	224.0.0.9	FF02::9
usa Autenticacion	RIP-specific	uses IPv6 AH/ESP

Figura 53: Tabla comparativa entre RIPv2 y RIPng[56]

El funcionamiento total de RIPng se acerca RIP-2. En tanto, los routers envían actualizaciones periódicas completas a todas las rutas, excepto para las rutas omitidas debido a las normas Horizonte dividido. No hay relación con los vecinos que producen actualizaciones periódicamente, en un tiempo variable de 30 segundos, también sirve con el propósito de confirmar que el router vecino todavía funcione. La métrica funciona exactamente igual. Cuando un router deja de ver una ruta en las actualizaciones recibidas, recibe una ruta envenenada (métrica 16), y converge, de manera lenta en comparación con EIGRP y OSPF.

Algunas diferencias se refieren específicamente a IPv6. Primero, los mensajes propios lista los prefijos y longitudes IPv6, En lugar de mascaras y subredes.

En RIP-1 y 2, RIP encapsula mensajes de actualización de RIP dentro de un encabezado en IPv4 con UDP; con IPv6, la encapsulación se utiliza para paquetes IPv6, de nuevo con un encabezado UDP.

Algunas pequeñas diferencias en el formato de mensaje de actualización también existen, con la diferencia obvia que en la lista de actualizaciones IPv6 van los prefijos y la longitud del prefijo.

[56] Tomado del libro CCNP ROUTE 642-902 guia de certificación oficial pagina 574.

Otra diferencia es que IPv6 soporta la autenticación usando la IPsec como encabezado de autenticación (AH), RIPng no admite de forma nativa la autenticación compatible, sino que depende de IPsec.

7.3 Configuración RIPng

RIPng usa un estilo nuevo de comandos para la configuración básica, pero la mayoría tiene características opcionales y los comandos de verificación se parecen mucho a los utilizados en RIP para IPv4. Esta sección da un vistazo a la configuración básica RIPng, aceptando los valores por defecto en lo posible.

La gran diferencia entre RIP-2 y la configuración RIPng es que RIPng descarta el comando **network** de RIP a diferencia del subcomando de la interfaz **ipv6 rip *nombre* enable**, que permite que RIPng se active para la interfaz.

Otra diferencia se relaciona con el enrutamiento de IPv4 e IPv6: las rutas de IPv4 con un IOS por defecto (tiene el comando **ip routing**), pero estos IOS no establecen una ruta IP6 por defecto (**no ipv6 unicast routing**).

Por último, RIPng permite que realice varios procesos RIPng se lleven a cabo en un solo router, así que el IOS requiere que cada proceso RIPng se le de un nombre de texto que identifica a cada proceso de RIPng para que un Router es otra diferencia con respecto a RIP-2.

La siguiente lista muestra los pasos de configuración básicos para RIPng, incluidos los pasos para habilitar enrutamiento IPv6 y habilitar el IPv6 en las interfaces.

Paso 1: Habilitar enrutamiento IPv6 desde modo de configuración global **ipv6 unicast-routing**

Paso 2: Habilitar RIPng desde modo de configuración global **ipv6 router rip** *nombre*. El nombre debe ser único en un router, pero no tiene por qué coincidir con los routers vecinos.

Paso3: Habilitar IPv6 en la interfaz, normalmente con uno de estos dos métodos:

- Configure una dirección unicast IPv6 en cada interfaz usando el comando de interfaz **ipv6 address** *address/prefix-length* [**eui-64**].

- Configure el comando **ipv6 enable**, que permite que el router obtenga su dirección de enlace local.

Paso4: Habilitar RIP en la interfaz con el comando **ipv6 rip** *nombre* **enable** (donde el nombre coincide con el escrito en el paso 2 es decir **ipv6 router rip** *name*).

La lista sólo incluye algunos comandos de configuración sencillos, además los pasos relacionados directamente para RIPng (Pasos 2 y 4), además de otras medidas relativas de cómo opera en sí IPv6 (los pasos 1 y 3). También tiene dos pasos dependientes entre sí, de la siguiente manera:

■ Paso 2 se basa en el paso 1 porque IOS rechaza el comando en el paso 2 (**ipv6 router rip** *name*) si el comando en el Paso 1 (**ipv6 unicast-routing**) se ha omitido.

■ Paso 4 se basa en el paso 3 porque IOS rechaza el comando en el paso 4 si IPv6 se ha habilitado en la interfaz, ya sea de forma estática como se menciona en el paso 3 o con uno de los otros métodos enumerados.

Por último, tenga en cuenta que, aunque el comando de interface **ipv6 rip** *process-name* **enable** del (Paso 4) se refiere al nombre del proceso configurado en el Paso 2, el IOS crea el proceso de RIP en relación al comando de interfaz **ipv6 rip** *process-name* **enable** si ese proceso de RIPng aún no existe.

En otras palabras, si has seguido los pasos anteriores en orden, pero se le olvidó hacer el paso 2, el comando en el paso 4 causa que el IOS cree automáticamente el comando en el paso 2.

Al igual que con RIP-1 y RIP-2, para cualquier interfaz en la que RIPng se ha habilitado, el proceso de RIP tiene tres acciones principales. En primer lugar, empieza a enviar actualizaciones RIP en la interfaz. También empieza a procesar las actualizaciones RIP recibidas en esa interfaz. Por último, se anuncia sobre las rutas conectadas en esa interfaz. IPv6 permite la configuración de varias direcciones unicast IPv6 en una interfaz, RIP anuncia sobre la mayoría de los prefijos IPv6 unicast asociados con la interfaz.

Las excepciones notables son que RIP no hace anuncios sobre cualquier enlace de las direcciones locales, ni RIP anuncia sobre las rutas locales aprendidas, las rutas con un prefijo de longitud /128 creado para cada interfaz de direcciones IPv6. En resumen, RIP anuncia todas las subredes enrutables asociada con la interfaz.

La figura 50 citada anteriormente, muestra un ejemplo de una red interna con IPv6 de unidifusión global y subredes. El ejemplo de interconexión de redes utiliza valores de dirección que son memorables y hacen más cortas las direcciones IPv6. Todo las subredes usan el prefijo de longitud 64, con cuartetos de 2, 3, 4 y compuesto por todos los valores 0. El ID de interfaz parte de que cada dirección utiliza todos los 0 hexadecimales en los tres primeros cuartetos (cuartetos de 5, 6 y 7 en la dirección general), con el dígito final en el cuarteto final utilizado para identificar cada router. Este último dígito coincide con el nombre de cada router en la mayoría de los casos.

Por ejemplo, todas las direcciones IPv6 de R1 los últimos cuatro octetos son 0000:0000:0000:0001. La subinterface de R1 S0/0/0.3, la cual conecta el PVC al router R3, usa un prefijo de 2003:0000:0000:0000::/64, haciendo completa la dirección IPv6 en esta interface, cuando abreviada, es 2003::1/64 un valor conveniente para minimizar a todas las salidas como se ve en la figura.

Ejemplo: se muestra la configuración RIPng en el router R1 en el diseño. El nombre del proceso de RIP es fred.[57]

R1# **show running-config**

! 1 paso: habilite eñ enrutamiento IPv6
ipv6 unicast-routing

! enseguida, las 5 interfaces, de los pasos 3 y 4: se configuran con direcciones IPv6 y habilite RIPng con un proceso llamado Fred,

interface FastEthernet0/0.1
ipv6 address 2012::1/64
ipv6 rip fred enable
!
interface FastEthernet0/0.2
ipv6 address 2017::1/64
ipv6 rip fred enable
!
interface FastEthernet0/1.18
ipv6 address 2018::1/64
ipv6 rip fred enable
!
interface Serial0/0/0.3
ipv6 address 2013::1/64
ipv6 rip fred enable
!
interface Serial0/0/0.4
ipv6 address 2014::1/64
ipv6 rip fred enable
!
interface Serial0/0/0.5
ipv6 address 2015::1/64
ipv6 rip fred enable
!
! siguiente paso, cree el enrutamiento para RIPng llamado fred.

ipv6 router rip fred

[57] Tomado del libro CCNP ROUTE 642-902 guia de certificación oficial pagina 577.

Habilitación de IPv6 en routers Cisco

Hay dos pasos básicos para activar IPv6 en un router. Primero, debe activar el reenvío de tráfico IPv6 en el router y, a continuación, debe configurar cada una de las interfaces que requiere IPv6.

De forma predeterminada, el reenvío de tráfico IPv6 está deshabilitado en los routers Cisco. Para activarlo entre interfaces, debe configurar el comando global ipv6 unicast-routing.

El comando ipv6 address puede configurar una dirección IPv6 global. La dirección link-local se configura automáticamente cuando se asigna una dirección a la interfaz. Debe especificar la dirección IPv6 completa de 128 bits o debe especificar el uso de un prefijo de 64 bits con la opción eui-64.

Comando	Propósito
`RouterX(config)# ipv6 unicast-routing`	Habilita el reenvío de tráfico IPv6
`RouterX(config-if)# ipv6 address ipv6prefix/prefix-length eui-64`	Configura las direcciones IPv6 de la interfaz

Figura 54: configuración de RIPng[58]

Ejemplo de configuración de dirección IPv6

Puede especificar la dirección IPv6 por completo o calcular el identificador del host (los 64 bits del extremo derecho) a partir del identificador EUI-64 de la interfaz. En el ejemplo, la dirección IPv6 de la interfaz se configuró con el formato EUI-64.

De manera alternativa, puede especificar la dirección IPv6 completa de la interfaz de un router con el comando ipv6 addressipv6-address/prefix-length en el modo de configuración de la interfaz.
La configuración de una dirección IPv6 en una interfaz configura automáticamente la dirección link-local para esa interfaz.

[58] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 769, 749 y 794

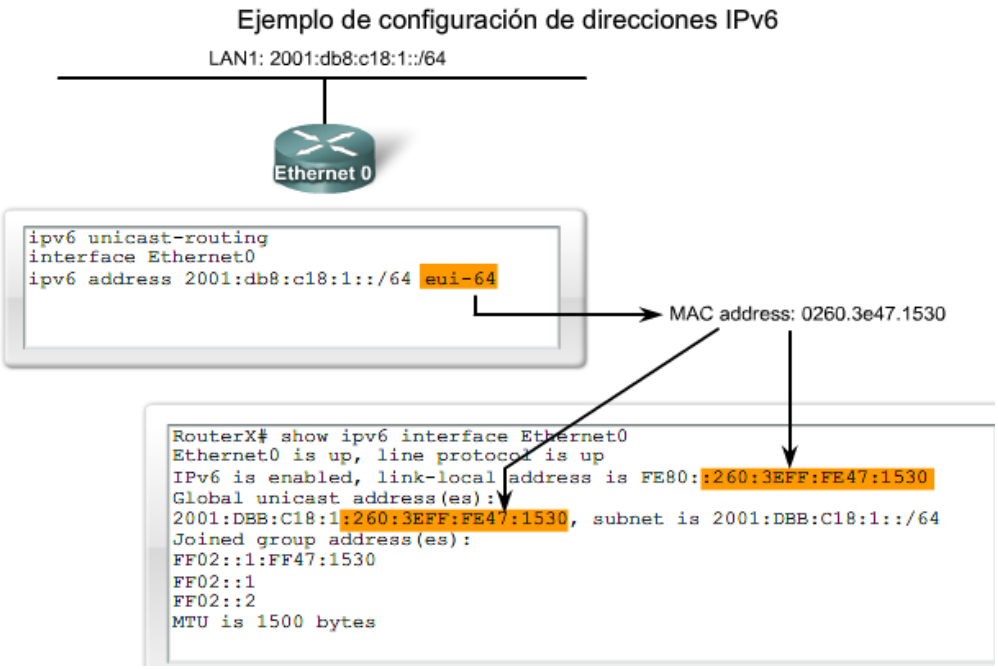


Figura 55: ejemplo de configuraciones de IPv6.[59]

Resolución de nombres IPv6 de IOS de Cisco

Hay dos maneras de realizar la resolución de nombres desde el proceso de software IOS de Cisco:

- Definición de un nombre estático para una dirección IPv6 mediante el comando ipv6 host name [port] ipv6-address1 [ipv6-address2...ipv6-address4]. Puede definir hasta cuatro direcciones IPv6 para un nombre de host. La opción del puerto hace referencia al puerto Telnet que se utilizará para el host asociado.

- Especificación del servidor DNS utilizado por el router con el comando ip name-serveraddress. La dirección puede ser IPv4 o IPv6. Con este comando puede especificar hasta seis servidores DNS.

Comando	Propósito
RouterX(config)# **ipv6 host** *name* [*port*] *ipv6addr* [{*ipv6addr*} ...] RouterX(config)# **ipv6 host router1 3ffe:b00:ffff:b::1**	Define un nombre estático para direcciones IPv6
RouterX(config)#**ip name-server** *address* RouterX(config)#**ip name-server 3ffe:b00:ffff:1::10**	Configura un servidor o servidores DNS para consultar

Figura 56: Configuración de RIPng con IPv6[60]

[59] Tomado del curriculum de CCNA Exploration.
[60] Tomado del curriculum de CCNP versión 5.

Al configurar los protocolos de enrutamiento admitidos en IPv6, debe crear el proceso de enrutamiento, habilitar el proceso de enrutamiento en las interfaces y personalizar el protocolo de enrutamiento para su red en particular.

Antes de configurar el router para que ejecute IPv6 RIP, habilite IPv6 de manera global con el comando de configuración global ipv6 unicast-routing y habilite IPv6 en las interfaces en las que haya que habilitar IPv6 RIP.

Para habilitar el enrutamiento RIPng en el router, use el comando de configuración global ipv6 router ripname. El parámetro name identifica el proceso RIP. Este nombre de proceso se utiliza más adelante al configurar RIPng en las interfaces participantes.

Para RIPng, en lugar de utilizar el comando network para identificar qué interfaces deben ejecutar RIPng, se utiliza el comando **ipv6 rip name enable** en el modo de configuración de la interfaz para habilitar RIPng en una interfaz. El parámetro name debe coincidir con el mismo parámetro en el comando ipv6 router rip.

La habilitación dinámica de RIP en una interfaz crea un proceso de "router rip" si es necesario.

Comando	Propósito
RouterX(config)#**ipv6 router rip** *name*	Crea e ingresa al modo de configuración de router RIP.
RouterX(config-if)#**ipv6 rip** *name* **enable**	Configura RIP en una interfaz.

Figura 57: RIPng para la configuración de IPv6

El ejemplo muestra una red de dos routers. El router R1 está conectado a la red predeterminada. Tanto en el router R2 como en el router R1, el nombre RT0 identifica el proceso RIPng. RIPng está habilitado en la primera interfaz Ethernet del router R1 mediante el comando ipv6 rip RT0 enable. El router R2 muestra que RIPng está habilitado en ambas interfaces Ethernet mediante el comando ipv6 rip RT0 enable.

Esta configuración permite que las interfaces Ethernet 1 del router R2 y Ethernet 0 de ambos routers intercambien información de enrutamiento RIPng.

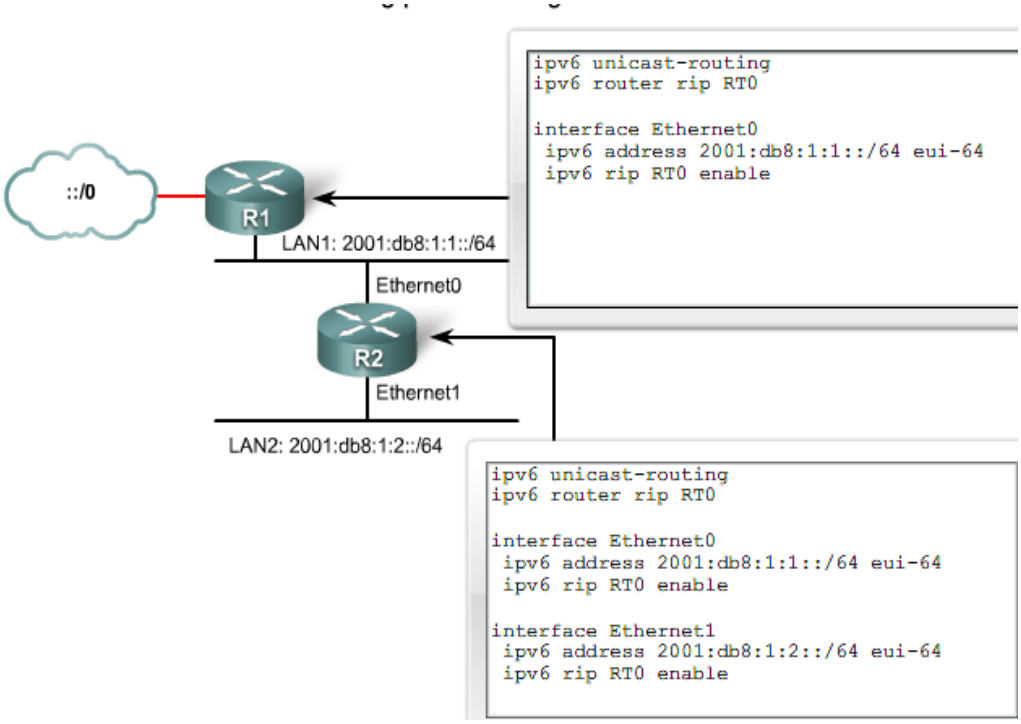


Figura 58: ejemplo de configuración RIPng[61]

7.4 Verificación de RIPng

El comando show relacionado con RIPng tiene el mismo tipo de información general como se ha visto con RIP-2. Sin embargo, algunos de los comandos que se utilizan para obtener una parte de la información pueden ser diferentes, por supuesto, existen algunas diferencias obvias debido a la diferente estructura de direcciones IPv6.

Tabla 59 muestra una lista de referencia que compara todos los comandos relacionados de RIP que empieza ya sea con **show ip** o **show ipv6.** También se enumeran los comandos de depuración similares utilizadas para mostrar la información de enrutamiento RIP.

Function	IPv4	IPv6
All routes	... route	... route
All RIP learned routes	... route rip	... route rip
Details on the routes for a specific prefix	... route *subnet mask*	... route *prefix/length*
Interfaces on which RIP is enabled	... protocols	... protocols
List of routing information sources	... protocols	... rip next-hops
Debug that displays sent and received Updates	debug ip rip	debug ipv6 rip

Fig.59 Tabla comparativa Verificación de comandos: **Show ip** y **Show ip v6.**[62]

[61] Tomado del curriculum de CCNP verison 5.

Las diferencias más notables se producen cuando la información se ve con IPv4 con el comando **show ip protocols.** Este comando **show ip protocols** muestra una amplia variedad de información para IPv4 RIP, mientras que los comandos IPv6 difunden la información sobre un par de comandos diferentes, como se indica en la Tabla anterior. El Ejemplo muestra algunos de los comandos, tomado del router R3 de la figura 50.

Las notas explicativas se muestran en el ejemplo en este caso. Tenga en cuenta que R3 utiliza un nombre de proceso RIPng como Barney.

Ejemplo: comandos IPv6 RIPng con **show**[63]

R3# **show ipv6 route 2099::/64**

Routing entry for 2099::/64
Known via "**rip barney",** distance 120, metric 3
Route count is 2/2, share count 0
Routing paths:
FE80::22FF:FE22:2222, Serial0/0/0.2
Last updated 00:27:12 ago
FE80::11FF:FE11:1111, Serial0/0/0.1

! Note que el siguiente commando solamente lista el proceso proceso RIP aprendiendo rutas.
! Los siguientes 2 saltos para la diraccion 2099::64. Note que el próximo salto se lista con la información de la dirección link-local.

R3# **show ipv6 route rip**
IPv6 Routing Table - Default - 19 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, M - MIPv6, **R - RIP**, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
EX - EIGRP external
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R 2005::/64 [120/3]
via FE80::11FF:FE11:1111, Serial0/0/0.1
via FE80::22FF:FE22:2222, Serial0/0/0.2
R 2012::/64 [120/2]
via FE80::11FF:FE11:1111, Serial0/0/0.1
via FE80::22FF:FE22:2222, Serial0/0/0.2
! lines omitted for brevity...
R 2099::/64 [120/3]
via FE80::22FF:FE22:2222, Serial0/0/0.2
via FE80::11FF:FE11:1111, Serial0/0/0.1

---

[62] Tomado del libro CCNP ROUTE 642-902 guia de certificación oficial pagina 578.
[63] Tomado del libro CCNP ROUTE 642-902 guia de certificación oficial pagina 579.

! los comandos **show ip protocols**, **show ipv6 protocols** muestran mas información.

R3# **show ipv6 protocols**
IPv6 Routing Protocol is “connected”
IPv6 Routing Protocol is “rip barney”
Interfaces:
Serial0/0/0.2
Serial0/0/0.1
FastEthernet0/0
Redistribution:
None
! este commando lista los tiempos desplegados para RIP V2.

R3# **show ipv6 rip**

RIP process “barney”, port 521, multicast-group FF02::9, pid 258
Administrative distance is 120. Maximum paths is 16
Updates every 30 seconds, expire after 180
Holddown lasts 0 seconds, garbage collect after 120
Split horizon is on; poison reverse is off
Default routes are not generated
Periodic updates 57, trigger updates 10
Interfaces:
Serial0/0/0.2
Serial0/0/0.1
FastEthernet0/0
Redistribution:
None
! Este commando es equivalente a la informacion desplegada por el comando **Show ip protocols que tambien muestra el encabezado del origen del enrutamiento.**

! note que las direcciones link-local son listadas.

R3# **show ipv6 rip next-hops**
RIP process “barney”, Next Hops
FE80::11FF:FE11:1111/Serial0/0/0.1 [9 paths]
FE80::44FF:FE44:4444/FastEthernet0/0 [3 paths]
FE80::22FF:FE22:2222/Serial0/0/0.2 [9 paths]

Mas allá de la información se destaca los comentarios dentro del ejemplo, el siguiente salto de direcciones IPv6 en el ejemplo deben ser examinados. RIPng direcciones de enlace local IPv6 como la dirección IP del siguiente salto. (Recuerde: las direcciones de enlace local comienzan con FE80.)

Los comandos **show ipv6 route 2099::/64** y **show ipv6 route** son los primeros comandos que muestra el ejemplo, y el comando **show ipv6 rip next-hops** se observa al final del ejemplo, todo ello muestra el siguiente salto de direcciones IP que comienzan con FE80, confirmando que

efectivamente se utiliza link de direcciones locales como direcciones del siguiente salto.

Para descubrir qué routers usan direcciones locales, hace que sea más fácil trabajar con direcciones locales. En primer lugar, puede configurar la dirección MAC de cada interfaz LAN. Los routers utilizan cada uno direcciones reconocidas como la MAC:R1 utiliza 0200.1111.1111, R2 utiliza 0200.2222.2222, y así sucesivamente.

Por otra parte, usted puede configurar la dirección de enlace local con el comando **ipv6 address**, usando la palabra clave **link-local** al final, y hacer que cada dirección local sea más reconocible. De todos modos, para encontrar el router cuyo vínculo dirección local se muestra en la tabla de enrutamiento IPv6, el comando **show cdp entry** *nombre* puede ser útil porque muestra las direcciones IPv4 e IPv6, incluyendo enlace del vecino dirección local.

Verificación y resolución de problemas de RPIng para IPv6
Después de configurar RIPng, es necesario hacer una verificación. La figura enumera los diferentes comandos que puede utilizar.

Comando	Propósito
`show ipv6 interface`	Muestra el estado de las interfaces configuradas para IPv6.
`show ipv6 interface brief`	Muestra el estado resumido de las interfaces configuradas para IPv6.
`show ipv6 neighbors`	Muestra la información en caché de la detección de vecinos IPv6.
`show ipv6 protocols`	Muestra los parámetros y el estado actual de los procesos del protocolo de enrutamiento activo IPv6.
`show ipv6 rip`	Muestra información acerca de la actual
`show ipv6 route`	Muestra la tabla de enrutamiento IPv6 actual.
`show ipv6 route summary`	Muestra la forma resumida de la tabla de enrutamiento IPv6 actual.
`show ipv6 routers`	Muestra información de publicación del router IPv6 que se recibe de otros routers.
`show ipv6 static`	Muestra sólo las rutas IPv6 estáticas instaladas en la tabla de enrutamiento.
`show ipv6 static 2001:db8:5555:0/16`	Muestra información sólo de la ruta estática en cuanto a la dirección específica que se suministró.
`show ipv6 static interface serial 0/0`	Muestra información sólo de la ruta estática con la interfaz especificada como la interfaz de salida.
`show ipv6 static detail`	Muestra una entrada más detallada para las rutas IPv6 estáticas.
`show ipv6 traffic`	Muestra estadísticas sobre el tráfico IPv6.

Figura 60: comandos de verificación de IPv6.[64]

[64] Tomado del curriculum de CCNA Exploration.

Si durante la verificación detecta que RIPng no está funcionando bien, debe resolver el problema.

Comando	Propósito
`clear ipv6 rip`	Borra rutas de la tabla de enrutamiento RIP IPv6 y, si están instaladas, las rutas de la tabla de enrutamiento IPv6.
`clear ipv6 route *`	Borra todas las rutas de la tabla de enrutamiento IPv6. NOTA: La eliminación de todas las rutas de la tabla de enrutamiento generará un alto índice de uso de la CPU mientras se reconstruye la tabla de enrutamiento.
`clear ipv6 route 2001:db8:c18:3::/64`	Elimina esa ruta específica de la tabla de enrutamiento IPv6.
`clear ipv6 traffic`	Restablece los contadores de tráfico IPv6.
`debug ipv6 packet`	Muestra mensajes de debug para paquetes IPv6.
`debug ipv6 rip`	Muestra mensajes de debug para transacciones de enrutamiento RIP IPv6.
`debug ipv6 routing`	Muestra mensajes de debug para actualizaciones de la tabla de enrutamiento IPv6 y actualizaciones de la caché de ruta.

Figura 61: comandos de verificación.[65]

8.0 Usando IPv6 e IPv4

8.1 Mecanismo de Transición IPv6 a IPv4

La transición de IPv4 a IPv6 no requiere una actualización en todos los nodos al mismo tiempo. Muchos de los mecanismos de transición permiten la integración uniforme de IPv4 a IPv6. Hay mecanismos disponibles que permiten a los nodos IPv4 comunicarse con los nodos IPv6. Todos estos mecanismos pueden aplicarse a diferentes situaciones.

Las dos técnicas más comunes para la transición de IPv4 a IPv6 son las siguientes:

- Pila (stack) dual[66]
- Túneles de IPv6 a través de IPv4 (6to4)[67]

Para la comunicación entre redes IPv4 e IPv6, las direcciones IPv4 pueden encapsularse en direcciones IPv6.

La figura 62 muestra un ejemplo de un mecanismo de transición e integración. Los Routers 6to4 automáticamente encapsulan el tráfico IPv6 dentro de paquetes IPv4.

---

[65] Tomado del curriculum de CCNA Exploration.
[66] http://www.faqs.org/rfcs/rfc2767.html
[67] http://www.ietf.org/rfc/rfc4380.txt

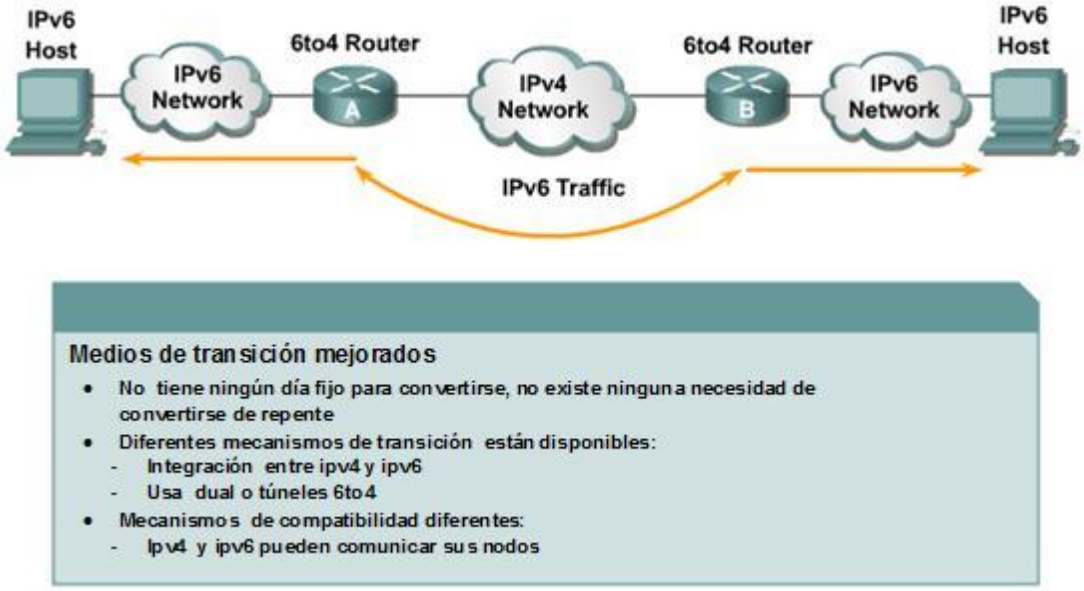


Fig. 62 Transición de IPv4 a IPv6 [68]

8.2 Estado Dual Cisco IOS

La mayoría de las versiones más recientes del software Cisco IOS están preparadas para IPv6. Tan pronto como las configuraciones básicas de IPv4 e IPv6 se completan en la interfaz, la interfaz hace doble pila (dual-stacked), y envía el tráfico IPv4 e IPv6.

Usar IPv6 en un Router Cisco IOS requiere usar el comando de configuración global **ipv6 unicast-routing.** Este comando activa el envió de datagramas IPv6.

Fig. 63 Cisco IOS Dual Stack (doble pila)[69]

[68]Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 829.
[69] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 832.

Todas las interfaces que transmitan el tráfico IPv6 deben tener una dirección IPv6. El comando **ipv6 address** [*IPv6-address*] [/*prefix length*] específica una red IPv6 asignada a la interfaz y permite el procesamiento de IPv6 en la interfaz.

El estado dual es un método de integración cuando un nodo tiene la implementación y conectividad de las redes IPv4 e IPv6, y así el nodo tiene dos pilas (stacks). Esta configuración puede llevarse a cabo en la misma interfaz o en múltiples interfaces. Las consideraciones para el estado dual incluyen lo siguiente:

- Un nodo de estado dual elige cual pila usar basándose en la dirección de destino. Un nodo de estado dual prefiere IPv6 cuando es disponible. La aproximación de estado dual para la integración IPv6 en la que los nodos tienen ambas pilas IPv4 e IPv6 es uno de los métodos de integración más comúnmente utilizados. Viejas aplicaciones IPv4 continúan trabajando como antes. Aplicaciones nuevas y modificadas toman las ventajas de ambas capas IP.

- Una nueva interfaz de programación de aplicaciones (application programming interface - API) es definida para soportar ambas direcciones IPv4 e IPv6 y peticiones del sistema de nombre de dominio (DNS[70]). El API reemplaza las llamadas **gethostbyname y gethostbyaddr.** Una aplicación convertida puede hacer uso tanto de IPv4 e IPv6. Una aplicación puede ser convertida al nuevo API mientras aun usa solo IPv4.

- La experiencia en portar aplicaciones de IPv4 a IPv6 sugiere que para la mayoría de las aplicaciones es un cambio mínimo en algunos lugares localizados en el interior del código fuente. Esta técnica es bien conocida y ha sido aplicada en el pasado para otras transiciones de protocolos. Esto habilita gradualmente las actualizaciones de aplicaciones, una por una, a IPv6.

[70] http://www.faqs.org/rfcs/rfc1035.html

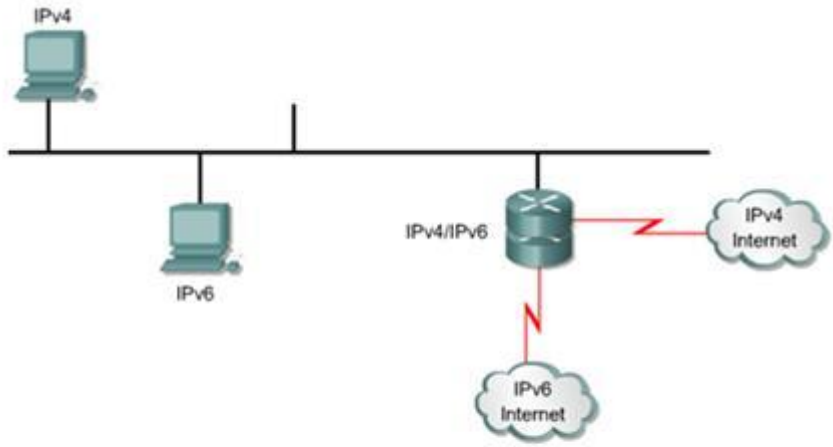


Fig. 64 Dual Stack (doble pila)[71]

8.3 Superposición de Túneles

La creación de redes a menudo utiliza los túneles de la superposición con una funcionalidad incompatibles en una red existente. Hacer túnel del tráfico IPv6 sobre una red IPv4 requiere un Router de frontera para encapsular los paquetes IPv6 dentro de un paquete IPv4 y otro Router para desencapsularlo.

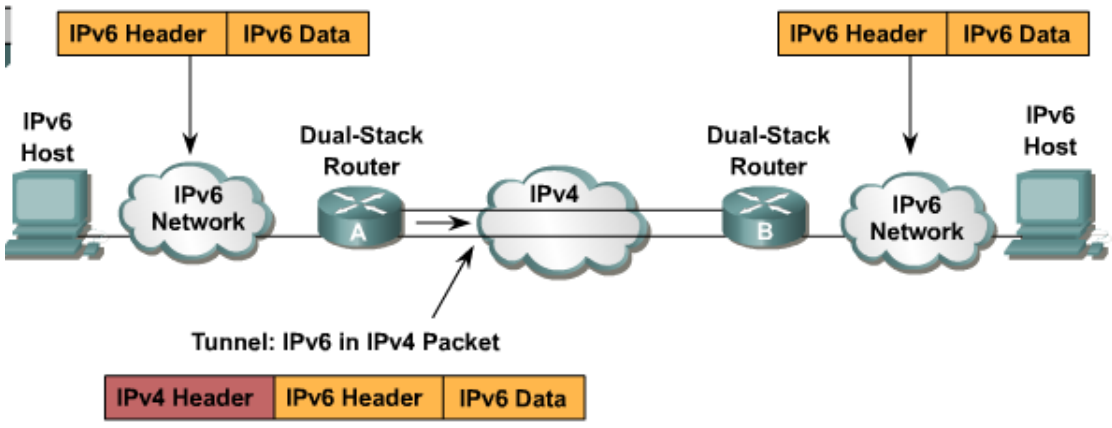


Fig. 65 Superposiciones de los Túneles[72]

Este proceso le permite conectar las islas de IPv6 sin necesidad de convertir toda la red para IPv6.

[71] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 836.
[72] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 829.

Tunneling es un método de integración donde un paquete IPv6 es encapsulado dentro de otro protocolo, como IPv4.

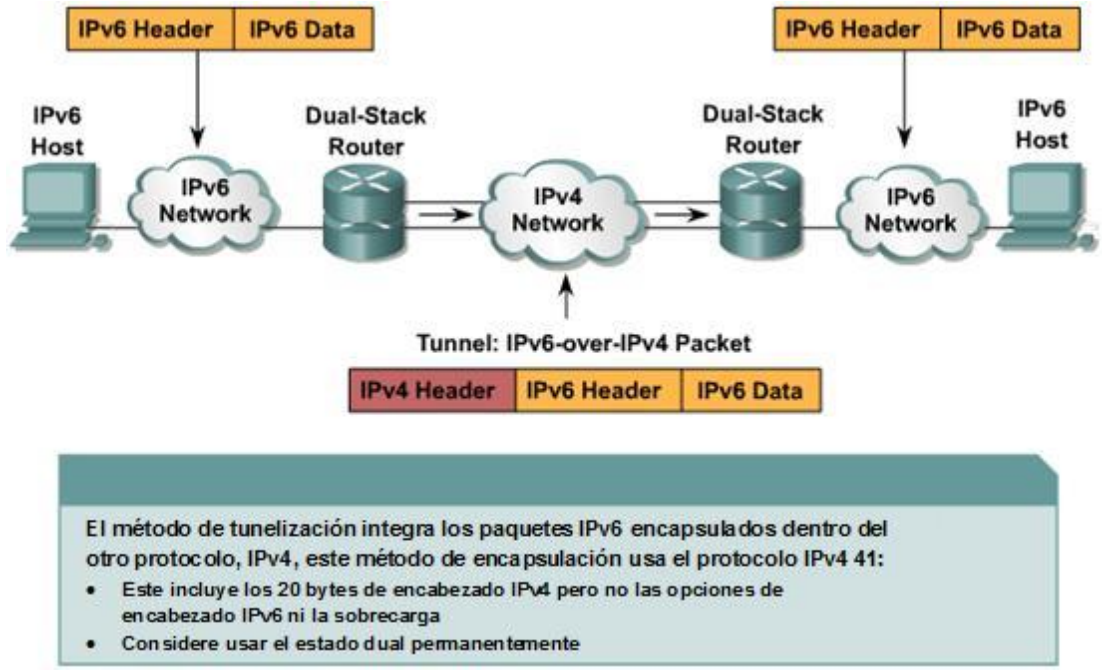


Fig. 66 Tunneling (Túnel)[73]

Este método de encapsulación es el protocolo 41 de IPv4 y tiene las siguientes características:

- Incluye un encabezado de 20 bytes con IPv4 sin opciones, un encabezado IPv6 y una carga útil.
- Considera una pila dual la cual permite la conexión de las islas IPv6 sin necesidad de convertir una red intermediarios para IPv6.
- Tunneling presenta estos problemas:
    - La MTU se reduce en 20 octetos (si el encabezado IPv4 no contiene ningún campo opcional).
    - Dificultad para solucionar problemas.

Tunneling es una integración intermedia y una técnica de transición que no debe considerarse una solución definitiva. La arquitectura nativa de IPv6 debe ser el objetivo final.

[73] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 828.

8.4 Aislamiento de Estado Dual de Host

La encapsulación puede hacerse por Routers de frontera entre hosts o entre un host y un Router. El ejemplo en la figura 67 muestra un aislamiento de pila dual de host usando la encapsulación de túnel para conectar al Router de frontera de la red IPv6.

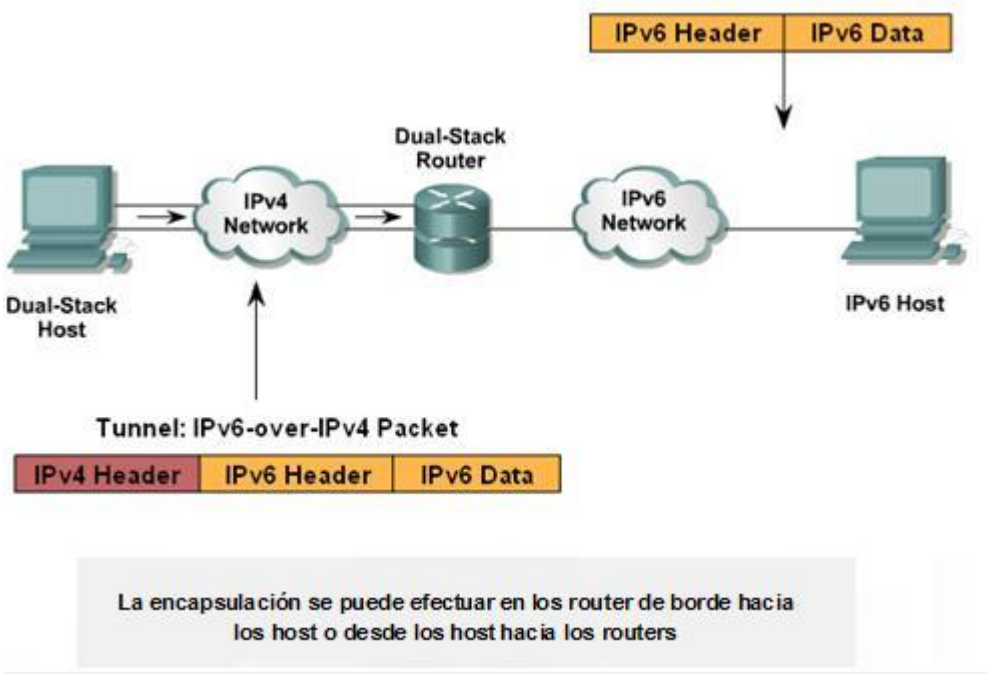


Fig. 67 Doble Pila de Host Aislados[74]

Tunneling no funciona si un nodo intermedio entre los dos extremos del túnel, como un cortafuego (firewall), filtra las salidas del protocolo 41 de IPv4, el cual es IPv6 sobre encapsulación IPv4.

8.5 Configuración de Tunneling (Túnel)

Si se configura manualmente un túnel, se debe configurar ambas direcciones estáticas IPv4 e IPv6. Usted Debe desarrollar esta configuración en los Routers de cada extremo del túnel.

[74] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 829.

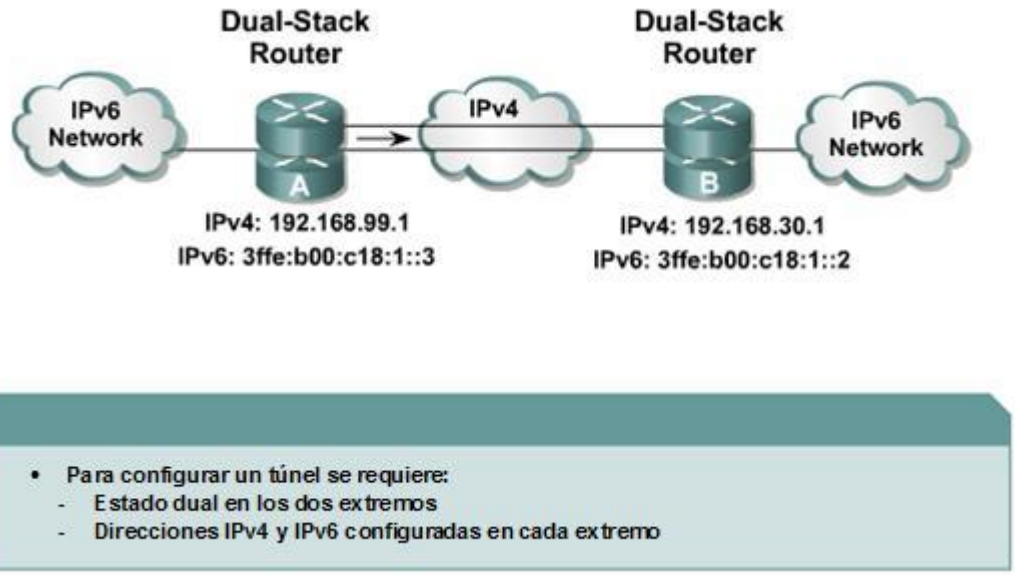


Fig. 68 Túnel Configurado[75]

Estos Routers finales deben ser de doble pila, y la configuración no puede cambiar dinámicamente, como las necesidades de cambio y enrutamiento de la red. El enrutamiento debe ser configurado apropiadamente para enviar un paquete entre las dos redes IPv6.

Los extremos del túnel pueden ser no numerados, pero sin extremos no numerados se hace difícil la solución de problemas. La práctica de guardar direcciones IPv4 para los extremos del túnel ya no es un problema.

8.6 Ejemplo de Configuración del Túnel

El ejemplo en la figura 69 muestra como configurar la superposición de un túnel IPv6 de forma manual. Con la configuración manual de túneles IPv6, una dirección IPv6 se configura en una interfaz de túnel, y se configura manualmente las direcciones IPv4 asignadas al origen y el destino del túnel. El host o Router de cada extremo de la configuración de un túnel deberá soportar ambos protocolos de pila IPv4 e IPv6.

[75] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 844.

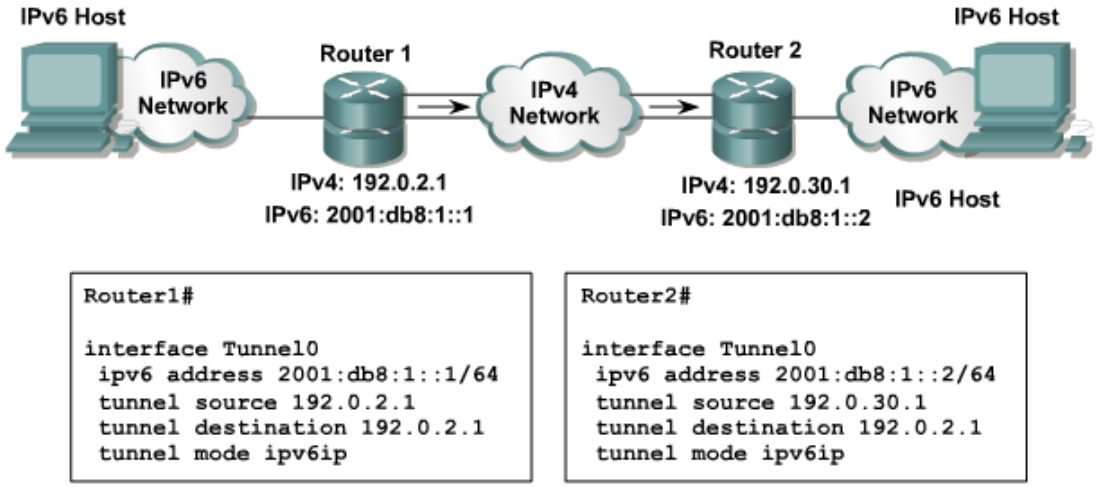


Fig. 69 Ejemplo De Configuración del Túnel Cisco IOS[76]

El comando que permite la superposición de túnel IPv6 es **tunnel mode ipv6ip.** Específicamente, este indica que IPv6 es el protocolo pasajero y que IPv4 será usado como protocolo de transporte y encapsulación.

Existen otros mecanismos de transición automáticos de tunneling, incluyendo los siguientes:

- **6to4:** Utiliza el prefijo reservado 2002**::/**16 para permitir a una conexión de un sitio de internet IPv4 crear y utilizar un prefijo IPv6 **/**48 basado en una única dirección IPv4 globalmente enrutable o accesible.

- **Protocolo de Direccionamiento de Túnel Automático Intra-Sitio (ISATAP):** Permite a una intranet privada IPv4 (que puede o no estar utilizar direcciones RFC 1918) para aplicar gradualmente los nodos IPv6 sin tener que actualizar la red.

Otro mecanismo de transición es Teredo (formalmente conocido como Shipworm). Este mecanismo de túneles IPv6 a datagramas UDP IPv4. Este método provee direcciones privadas IPv4 y NAT transversal IPv4.

8.7 Tunneling y Direcciones IPv6 e IPv4

El método de tunneling 6to4 automáticamente establece la conexión de islas IPv6 a través de una red IPv4. Se aplica un prefijo IPv6 válida para cada isla IPv6, que permite el rápido despliegue de IPv6 en una red corporativa, sin recuperación de la dirección desde el ISPs o registros.

El método de tunneling 6to4 requiere un código especial en los Routers de frontera, pero los hosts IPv6 y los Routers dentro del sitio 6to4 no requieren

[76] Tomado del curriculum de CCNA Exploration y del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 855.

nuevas características para soportar 6to4. Cada sitio 6to4 recibe un prefijo /48, el cual es la concatenación de 0x2002 y la dirección hexadecimal IPv4 del Router de frontera.

En la figura 70, la dirección IPv4 del Router de frontera es 192.168.99.1. Como resultado, el prefijo de la red IPv6 es 2002**:**c0a8**:**6301**::/**48 porque c0a86301 es la representación hexadecimal de 192.168.99.1. La red IPv6 puede sustituir cualquier dirección IP en el espacio después de la primera sección de 16 bits (0x2002).

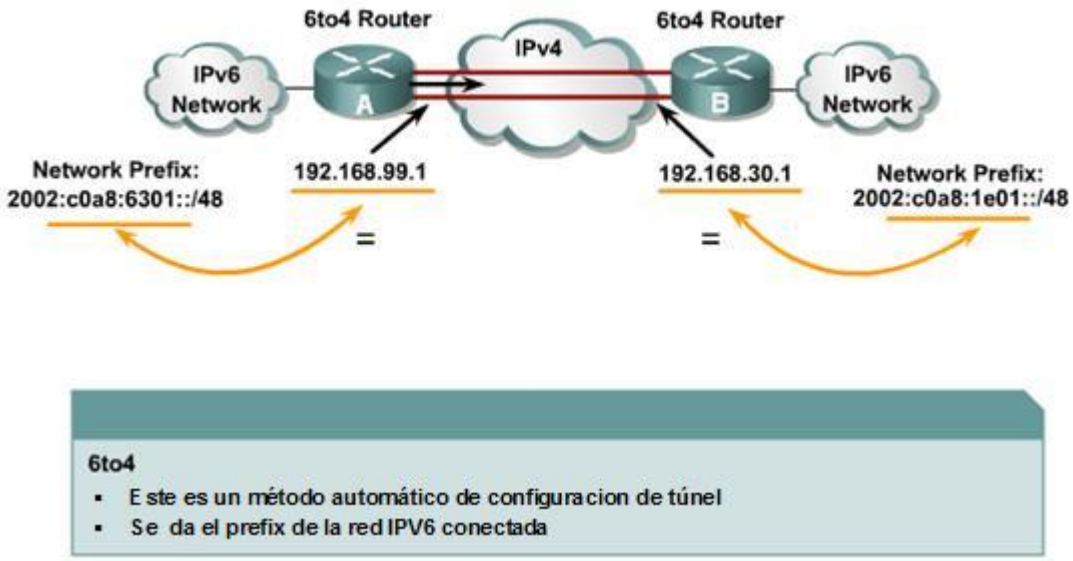


Fig. 70 Túnel 6to4[77]

Cuando un paquete IPv6 con una dirección de destino en el rango de 2002**::/**16 alcanza el Router de destino 6to4, el Router de frontera 6to4 extrae la dirección IPv4 que está en la dirección de destino 2002**::** (insertada entre el tercer y sexto octeto, inclusive). El Router 6to4 entonces encapsula el paquete IPv6 en un paquete IPv4 con la dirección de destino IPv4 que fue extraída dentro de la dirección de destino IPv6.

La dirección IPv4 representa la dirección de otro Router de frontera 6to4 del sitio de destino 6to4. El Router de frontera de destino desencapsula el paquete IPv6 en el paquete IPv4 y entonces envía el paquete nativo hacia su destino final.

Nota: 2002::/16 es el rango de direcciones específicamente asignado a 6to4.

8.8 Traducción de NAT-PT

Para los equipos legados que no será actualizado a IPv6 y para algunos escenarios desplegados, las técnicas que pueden conectar solo nodos IPv4

[77] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 859.

y solo nodos IPv6 están disponibles. La traducción es básicamente una extensión de las técnicas de NAT.

NAT[78]- protocolo de traducción (NAT-PT[79]) es un mecanismo de traducción que se encuentra entre una red IPv6 y una red IPv4. El traductor traduce los paquetes IPv6 en paquetes IPv4 y viceversa.

NAT-PT estático utiliza las reglas de traducción estática para asignar una dirección IPv6 a una dirección IPv4. Los Nodos de la red IPv6 se comunican con los nodos de la red IPv4 utilizando una asignación de IPv6 de la dirección IPv4 configurada en el Router NAT-PT.

La figura 71 muestra como solo el nodo IPv6 (nodo A) puede comunicarse solo con el nodo IPv4 (nodo D) usando NAT-PT. El dispositivo NAT-PT está configurado para asignar la dirección de origen IPv6 para el nodo A de 2001:0db8:bbbb:1:: a la dirección IPv4 192.0.2.2. NAT-PT esta configurado para asignar la dirección origen IPv4 del nodo C, 192.0.30.1 a 2001:0db8::a.

Cuando los paquetes con una dirección origen IPv6 del nodo A se reciben en el Router NAT-PT son traducidos a una dirección destino para asociarse al nodo D en la red única IPv4. NAT-PT solo puede ser configurado para asociar una dirección de origen IPv4 y traducir el paquete para una dirección de destino IPv6 que permita a un host único IPv4 comunicarse con un host único IPv6.

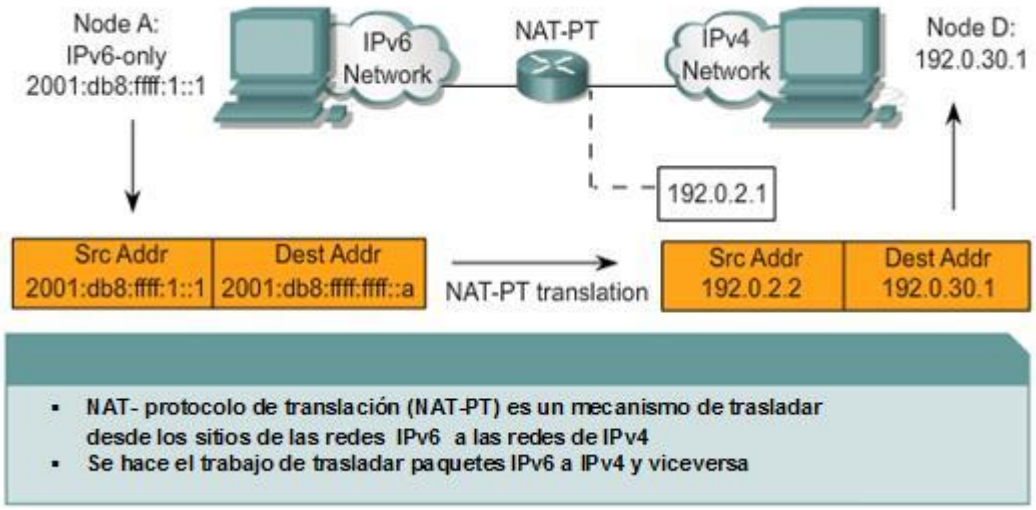


Fig. 71 Traducción - NAT-PT[80]

Desde la perspectiva del nodo A, este establece una comunicación a otro nodo IPv6. Y desde la perspectiva del nodo D, se establece una

[78] http://www.faqs.org/rfcs/rfc1631.html
[79] http://tools.ietf.org/html/rfc4966
[80] Tomado del libro Implementing CISCO IP Routing Fundation Learning Guide pagina 864 y 866.

comunicación IPv4 con su correspondiente. El nodo D no requiere modificación.

Si se tiene múltiples hosts IPv6 único o IPv4 único que necesitan comunicarse, se puede necesitar configurar muchas asignaciones estáticas NAT-PT. NAT-PT estático es útil cuando aplicaciones o servidores requieren acceso a direcciones IPv4 estables. Acceder a un servidor DNS externo IPv4 es un ejemplo donde NAT-PT estático puede ser utilizado.

Las traducciones NAT-PT también pueden ser asignadas dinámicamente basándose en consultas DNS, usando un nivel de aplicación de puerta de enlace DNS (DNS ALG).

Otras posibles soluciones son las siguientes:

- ALGs: Este método usa la aproximación de pila dual y permite a un host en un dominio único IPv6 para enviar datos a otro host en un dominio único IPv4. Esto requiere que todos los servidores de aplicación en un Gateway corran IPv6.

- API: Se puede instalar un modulo especifico en una pila TCP/IP de un host para cada host en la red. El modulo intercepta el tráfico IP a través de un API y lo convierte en el complemento de IPv6.

9.0 Implicacion o problemas de enrutamiento con IPv6.

Al igual que el enrutamiento entre dominios sin clase (CIDR, Classless Interdomain Routing) de IPv4, IPv6 utiliza un enrutamiento de concordancia de prefijo más largo. IPv6 utiliza versiones modificadas de la mayoría de los protocolos de enrutamiento comunes para administrar las direcciones IPv6 más largas y las diferentes estructuras de encabezado.

Los espacios de dirección más grandes permiten asignaciones de direcciones grandes a los ISP y las organizaciones. Un ISP agrupa todos los prefijos de sus clientes en un único prefijo y lo anuncia en Internet IPv6. El mayor espacio de direcciones es suficiente para permitir a las organizaciones definir un único prefijo para toda su red.

¿Pero cómo se ve afectado el rendimiento del router con esto? Un breve resumen del funcionamiento de un router en una red será útil para mostrar cómo IPv6 afecta el enrutamiento. Conceptualmente, un router tiene tres áreas funcionales:

- **El plano de control** administra la interacción del router con los demás elementos de la red y proporciona la información necesaria para tomar decisiones y controlar el funcionamiento general del router. Este plano ejecuta procesos, tales como protocolos de enrutamiento y administración de red. Estas funciones en general son complejas.

- **El plano de datos** administra el reenvío de paquetes de una interfaz física o lógica a otra. Utiliza diferentes mecanismos de conmutación, por ejemplo, la conmutación de procesos y el envío express de Cisco (CEF, Cisco Express Forwarding) en routers con el software IOS de Cisco.

- **Los servicios mejorados** incluyen funciones avanzadas que se aplican al reenviar datos, por ejemplo, filtrado de paquetes, calidad de servicio (QoS, Quality Of Service), encriptación, traducción y contabilidad.

IPv6 presenta nuevos desafíos específicos para cada una de estas funciones.

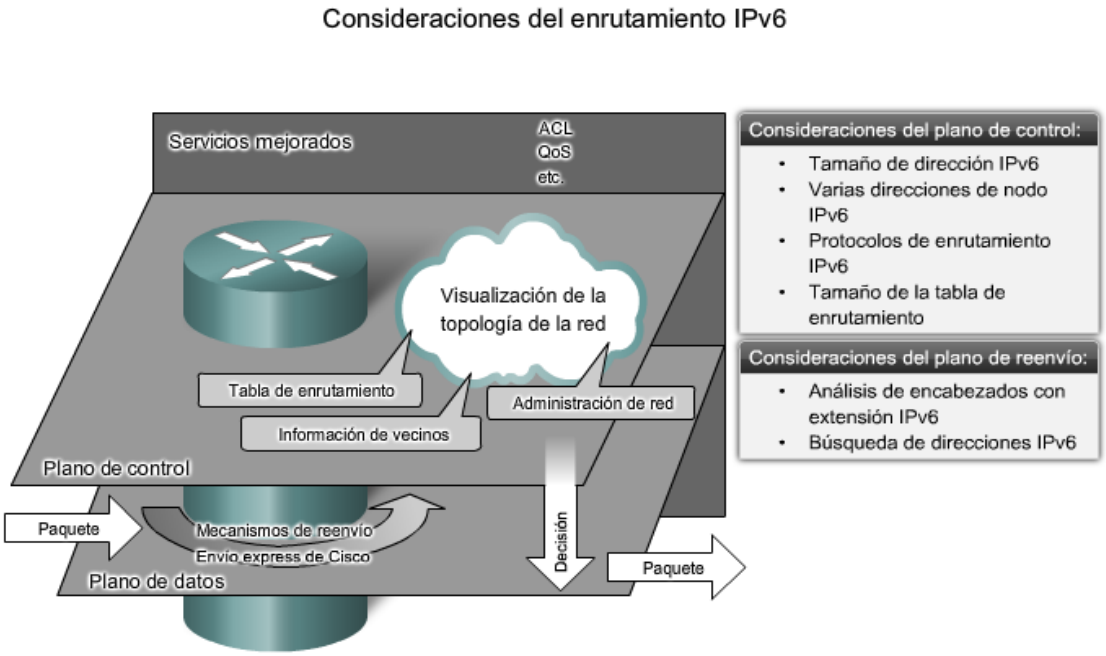


Fig. 72: consideraciones de enrutamiento IPv6[81]

9.1 Plano de control de IPv6

Al habilitar IPv6 en un router se inicia el proceso operativo del plano de control específicamente para IPv6. Las características del protocolo definen el rendimiento de estos procesos y la cantidad de recursos necesarios para operarlos:

[81] Tomado del curriculum CCNA Exploration.

- **Tamaño de la dirección IPv6:** el tamaño de la dirección afecta las funciones de procesamiento de la información de un router. Los sistemas que utilizan una estructura de memoria, bus o CPU de 64 bits pueden transmitir una dirección IPv4 de origen y destino en un único ciclo de procesamiento. Para IPv6, las direcciones de origen y destino requieren dos ciclos cada una, o sea cuatro ciclos, para procesar la información de las direcciones de origen y destino. Como resultado, los routers que utilizan exclusivamente procesamiento de software probablemente tengan un rendimiento más lento que en un entorno IPv4.

- **Varias direcciones de nodos IPv6**: como los nodos IPv6 pueden usar varias direcciones unicast IPv6, el consumo de memoria caché para la detección de vecinos puede verse afectado.

- **Protocolos de enrutamiento IPv6:** los protocolos de enrutamiento IPv6 son similares a sus contrapartes IPv4, pero como un prefijo IPv6 es cuatro veces más grande que un prefijo IPv4, las actualizaciones de enrutamiento deben transportar más información.

- **Tamaño de la tabla de enrutamiento**: el mayor espacio de dirección IPv6 genera redes más grandes y hace que aumente mucho el tamaño de Internet. Esto hace que se necesiten tablas de enrutamiento más grandes y más requisitos de memoria para su funcionamiento.

9.2 Plano de datos.

El plano de datos reenvía paquetes IP en función de las decisiones tomadas por el plano de control.

El motor de reenvío analiza la información relevante del paquete IP y hace una búsqueda para establecer una equivalencia entre la información analizada y las políticas de reenvío definidas por el plano de control. IPv6 afecta el rendimiento de las funciones de análisis y búsqueda:

- **Análisis de los encabezados de extensión IPv6:** las aplicaciones, incluido IPv6 móvil, con frecuencia utilizan información de la dirección IPv6 en los encabezados de extensión, lo que hace que aumenten de tamaño. Estos campos adicionales requieren procesamiento adicional. Por ejemplo, un router que utiliza ACL para filtrar información de Capa 4 necesita aplicar las ACL tanto a los paquetes que tienen encabezados de extensión como a los que no los tienen.

Si la longitud del encabezado de extensión excede la longitud fija del registro de hardware del router, la conmutación por hardware genera un error y los paquetes pueden ser derivados a conmutación por software o descartados. Esto afecta seriamente el rendimiento de reenvío del router.

- **Búsqueda de direcciones IPv6**: IPv6 realiza una búsqueda en los paquetes que ingresan al router para encontrar la interfaz de salida correcta. En IPv4, el proceso de decisión de reenvío analiza una dirección de destino de 32 bits. En IPv6, la decisión de reenvío puede requerir el análisis de una dirección de destino de 128 bits. La mayoría de los routers actuales realizan búsquedas mediante un circuito integrado de aplicación específica (ASIC, Application-Specific Integrated Circuit) con una configuración fija que realiza las funciones para las que fue diseñado originalmente: IPv4. Nuevamente, esto puede dar como resultado que los paquetes sean derivados a un procesamiento por software que es más lento o que sean descartados por completo.

10.0 Simulador GNS3.

GNS3 es un simulador grafico de redes que le permitirá diseñar fácilmente topologías de red y luego ejecutar simulaciones en el. Hasta ahora GNS3 Soporta el IOS de routers, ATM/Frame Relay/switchs Ethernet y PIX firewalls.

Usted puede extender su red propia, conectándola a la topología virtual.
Para realizar esta magia, GNS3 está basado en Dynamips, PEMU (incluyendo el encapsulador) y en parte en Dynagen, fue desarrollado en python a través de
PyQt la interfaz grafica (GUI) confeccionada con la poderosa librería Qt, famosa por su uso en el proyecto KDE. GNS3 también utiliza la tecnología SVG (Scalable Vector Graphics) para proveer símbolos de alta calidad para el diseño de las topologías de red.

10.1 Acerca de Dynamips

Dynamips es un emulador de routers Cisco escrito por Christophe Fillot. Emula a las plataformas 1700, 2600, 3600, 3700 y 7200 , y ejecuta imágenes de IOS
estándar.

Este tipo de emulador será útil para:

- *Ser utilizado como plataforma de entrenamiento, utilizando software del mundo real. Permitirá a la gente familiarizarse con dispositivos Cisco, siendo Cisco el líder mundial en tecnologías de redes.*

- *Probar y experimentar las funciones del Cisco IOS.*

- *Verificar configuraciones rápidamente que serán implementadas en routers reales.*
- *Por supuesto, este emulador no puede reemplazar a un router real, es simplemente una herramienta complementaria para los administradores de redes Cisco o para aquellos que desean aprobar los exámenes de CCNA/CCNP/CCIE.*

Así como Dynamips provee un switch virtual simple, no emula switches Catalyst (aunque si emula la NM-16ESW).

10.2 Acerca de Dynagen

Dynagen es un front end basado en texto para Dynamips escrito por Greg Anuzelli que provee una separada OOP API utilizada por GNS3 para interactuar con Dynamips. GNS3 también utiliza el formato .INI de configuración e integra la consola de administración de Dynagen que permite a los usuarios listar los dispositivos, suspender y recargar instancias, determinar y administrar los valores de idle-pc , realizar capturas, y mucho mas.

10.3 Imágenes IOS

Dynamips ejecuta imágenes de Cisco IOS reales. De Dynamips FAQ:

En Windows, ubique la imagen en C:\Program Files\Dynamips\images. Puede ubicar las imágenes en cualquier ubicación, pero los laboratorios de ejemplo están configurados para buscar en esa locación. En sistemas Linux/Unix ubique las imágenes en los lugares designados (yo prefiero /opt/images).

Las imágenes del Cisco IOS están comprimidas. Estas imágenes comprimidas funcionan bien con Dynamips, aunque el proceso de arranque es significativamente más lento debido a la descompresión (igual que en los routers reales). Es recomendable que descomprima las mismas de antemano asi el emulador no tiene que realizar esa tarea. En sistemas Linux/Inx/Cygwin puede utilizar el utilitario “unzip”:

Unzip –p c7200-g6ik8s-mz.124-2.T1.bin > c7200-g6ik8s-mz.124-2.T1.image
recibira un mensaje de advertencia del unzip, pero puede ignorarlo. En Windows puede descomprimir las imágenes utilizando el WinRAR.

Tenga en cuenta que las imágenes actuales de los routers 1700 y 2600 deben ser descomprimidas antes de utilizarlas en Dynamips.

Por favor, siempre pruebe sus imágenes directamente con Dynamips antes de usarlas con GNS3: *./Dynamips –P <chassis> <path-to –the-ios-image>*

10.4 Utilizacion de Recursos

Dynamips hace uso intensivo de memoria RAM y CPU en orden de lograr la magia de la emulación. Si su intención es de ejecutar una imagen de IOS que requiere 256 MB de RAM en un router 7200 real, y dedica 256 MB de RAM a la instancia de su router virtual, este utilizara 256 MB de memoria para funcionar. Dynamips

También utiliza (por defecto) 64 MB de RAM por cada instancia en un sistema
Unix (16 MB en Windows) para cachear (cache) las transacciones JIT. Este será el tamaño total de trabajo; esto se debe a que Dynamips archivos para trazar un mapa de la memoria virtual de los routers. En el directorio de trabajo usted hallara archivos temporarios “ram” cuyo tamaño es igual a la memoria RAM de los routers virtuales. Su SO cacheara en la RAM las secciones de los archivos nmap que están siendo utilizados. (Vea en la sección Optimización del Uso de Memoria las opciones de configuración, estas pueden reducir en forma significativa la utilización de memoria.

Si usted posee mucha RAM, y sabe lo que esta haciendo, desmarque la opción
“Habilitar la función nmap” en las Preferencias de Dynamips.

Dynamips también hace uso intensivo de CPU, porque esta emulando la CPU de un router instrucción-por-instrucción. En principio no tiene manera de saber
cuando el router virtual está en estado ocioso (idle), por esa razón ejecuta diligentemente todas las instrucciones que constituyen las rutinas de idle del IOS, igualmente que las instrucciones que conforman el “real” funcionamiento. Pero una vez que haya ejecutado el proceso de “Idle-PC” para una determinada imagen de IOS, la utilización de CPU decrecerá en forma drástica.

11.0 Packet Tracert

Es un programa de simulación muy realista.

11.1 PACKET TRACER™

Es un simulador gráfico de redes desarrollado y utilizado por Cisco como herramienta de entrenamiento para obtener la certificación CCNA14. Packet Tracert es un simulador de entorno de redes de comunicaciones de fidelidad media, que permite crear topologías de red mediante la selección de los dispositivos y su respectiva ubicación en un área de trabajo, utilizando una interfaz gráfica.

Packet Tracert 5.3 es la última versión del simulador de redes de Cisco Systems, herramienta fundamental para los estudiantes que estan cursando el CCNA o se dedican al mundo de networking.

11.2 Características generales.

Packet Tracert es un simulador que permite realizar el diseño de topologías, la configuración de dispositivos de red, así como la detección y corrección de errores en sistemas de comunicaciones. Ofrece como ventaja adicional el análisis de cada proceso que se ejecuta en el programa de acuerdo a la capa de modelo OSI que interviene en dicho proceso; razón por la cuál es una herramienta de gran ayuda en el estudio y aprendizaje del funcionamiento y configuración de redes de comunicaciones y aplicaciones telemáticas

En este programa se crea la topologia física de la red simplemente arrastrando los dispositivos a la pantalla. Luego dando click en ellos entras a sus consolas de configuración. Allí estan soportados todos los comandos del Cisco IOS e incluso funciona el "tab completion". Una vez completada la configuración física y lógica de la red puedes hacer simulaciones de conectividad (pings, traceroute, etc) todo ello desde las propias consolas incluidas.

Principales Funcionalidades

- Entre las mejoras del Packet Tracert 5.3 encontramos:
- Soporte para Windows (2000, XP, Vista) y Linux (Ubuntu y Fedora).
- Permite configuraciones multiusuario y colaborativas en tiempo real.
- Soporte para IPv6, OSPF multitarea, redistribución de rutas, RSTP, SSH y Switchs multicapa.

Soporta los siguientes protocolos:

- HTTP, Telnet, SSH, TFTP, DHCP y DNS.
- TCP/UDP, IPv4, IPv6, ICMPv4 e ICMPv6.
- RIP, EIGRP, OSPF Multiárea, enrutamiento estático y redistribución de rutas.
- Ethernet 802.3 y 802.11, HDLC, Frame Relay y PPP.
- ARP, CDP, STP, RSTP, 802.1q, VTP, DTP y PAgP.

Nuevas recursos, actividades y demostraciones:

- OSPF, IPv6, SSH, RSTP, Frame Relay, VLAN's, Spanning Tree, etc.

Nota: No soporta IGRP y los archivos hechos con Packet Tracer 5.3 no son compatibles con las versiones anteriores, pero estas si con el 5.

11.3 Interfaz gráfica del usuario.

Este software ofrece una interfaz basada en ventanas, que le ofrece al usuario facilidades para el modelado, la descripción, la configuración y la simulación de redes. Packet Tracert tiene tres modos de operación: el primero de estos es el modo topology (topología), que aparece en la ventana de inicio cuando se abre el programa, el otro es el modo simulation (simulación), al cual se accede cuando se ha creado el modelo de la red; finalmente aparece el modo realtime (tiempo real), en donde se pueden programar mensajes SNMP para detectar los dispositivos que están activos en la red y si existen algún problema de direccionamiento o tamaño de tramas entre las conexiones. A continuación se describirá brevemente cada uno de los modos de operación de Packet Tracert.

11.4 Modo de operación de topología.

En el modo “Topology”, se realizan tres tareas principales, la primera de ellas es el diseño de la red mediante la creación y organización de los dispositivos; por consiguiente en este modo de operación se dispone de un área de trabajo y de un panel de herramientas en donde se encuentran los elementos de red disponibles en Packet Tracert.

11.5 Modo de operación de simulación.

En el modo simulation, se crean y se programan los paquetes que se van a transmitir por la red que previamente se ha modelado. Dentro de este modo de operación se visualiza el proceso de transmisión y recepción de información haciendo uso de un panel de herramientas que contiene los controles para poner en marcha la simulación. Una de las principales características del modo de operación simulation, es que permite desplegar ventanas durante la simulación, en las cuales aparece una breve descripción del proceso de transmisión de los paquetes; en términos de las capas del modelo OSI.

11.6 Modo de operación en tiempo real.

Este modo de operación está diseñado para enviar pings o mensajes SNMP, con el objetivo de reconocer los dispositivos de la red que están activos, y comprobar que se puedan transmitir paquetes de un hosts a otro(s) en la red. Dentro del modo Realtime, se encuentra el cuadro de registro Ping log, en donde se muestran los mensajes SNMP que han sido enviados y se detalla además el resultado de dicho proceso; con base en este resultado se puede establecer cuál o cuáles de los terminales de la red están inactivos, a causa de un mal direccionamiento IP, o diferencias en el tamaño de bits de los paquetes.

12.0 Resumen

Este estado del arte es una descripción del protocolo enrutado IP versión 6 (IPv6), y del porque se convertirá en el protocolo de elección en el futuro y los beneficios de esa elección. Los cambios en el formato de direccionamiento y el formato de encabezado de paquete fueron abordados en detalle, incluyendo la configuración automática y el rol de la dirección multicast.

La mayor parte de este estado del arte es una descripción dedicada del enrutamiento IPv6.

Todos los protocolos de enrutamiento posibles se definieron, como (Open Shortest Path First Protocol - OSPF) para IPv6 se tratan con más detalle. Igual de EIGRP junto con el protocolo de próxima generación como RIPNG.

Además se incluyeron algunas estrategias de transición para la migración de IPv4 a IPv6 también fueron definidos sus pro y contra con cada protocolo de enrutamiento utilizado y configurado en el laboratorio.

Los comandos de configuración, verificación, y de solución de problemas Cisco IOS también son tratados al detalle en cada laboratorio.

13.0 BIBLIOGRAFIA

Implementing Cisco IP Routing (ROUTE) Fundation Learning Guide.

CCNP Route Oficcial Certification Guide.

IPV6: the new internet protocol HUITEMA, Christian segunda edicion. Editorial pretice hall 1998

IPV6: the complete reference HENRICKSON, hethe, hofmann, scott. Editorial mcgraw-hill/Osborne 2003

Cisco Networking Academy Program CCNA 1 and 2 Companion Guide Pearson educación de México 2003, España

Cisco Networking Academy Program CCNP Pearson educación de México 2009, España

Comunicaciones y redes de computadores, STALLINGS William, quinta edición. Editorial prentice hall 1997

Privacy Extensions for Stateless Address Autoconfiguration in IPv6, RFC 3041, Jan 2001, Narten, T. and R. Draves.http://www.ietf.org/rfc/rfc3041.txt

6net, Deliverable 2.2.2: Initial IPv4 to IPv6 migration Cookbook for organizational/ISP (NREN) and backbone networks, T. Chown and M. Feng, Mar 2003.http://www.6net.org/publications/deliverables/D2.2.2.pdf.

6net, Deliverable 2.3.2: Initial IPv4 to IPv6 transition cookbook for end site networks/universities, C. Schild and T. Strauf, Feb 2003.http://www.6net.org/publications/deliverables/D2.3.2.pdf

Manual de laboratories de IPV6; en_ROUTE_ILM_v6000.pdf

RFC"s

RFC 1752: the recommendation for the IP next generation protocol. BRADNER S, mankin a, network working group enero 1995

RFC 2460: especificacion protocol internet IP, version 6 (IPV6); DEERING S, hinden r. network working group Julio 1998

RFC 2464: transmission of IPV6 packets over Ethernet networks CRAWFORD M, network working group diciembre de 2008

RFC 2893: transition mechanisms for IPV6 hosts and routers. GILLIGAN R, nordmark e. network working group, agosto 2000

RFC3056: Connection of IPv6 Domains via IPv4 Clouds, B. Carpenter, K. Moore, IETF RFC, February 2001

RFC3142: An IPv6-to-IPv4 Transport Relay Translator, J. Hagino, K. Yamamoto,
RFC 3142; June 2001.

RFC3068: An Anycast Prefix for 6to4 Relay Routers, C. Huitema, RFC 3068; June
2001.

GNS3: http://www.gns3.net
Dynamips: http://www.ipflow.utc.fr/index.php/Cisco_7200_Simulator

Dynamips Blog (donde se encuentra mucha acción): http://www.ipflow.utc.fr/blog
Dynagen (front-end basado en texto al emulador):http//dyna-en.sourceforge.net
GNS3 / Dynamips /Dynagen seguimiento de fallos: http://www.ipflow.utc.fr/bts
Foro de Hacki Dynamips / Dynagen / GNS3 :http:// 7200emu.hacki.at/index.php

URL"s

http://www.ipv6.org

http://www.go6.net

http://protocols.com/

http://www.wikipedia.org

info@citel.mht

http://portalipv6.lacnic.net

www.ciscopress.com/ccnp

http://www.programaswarez.com/appz-programas-gratis/14789-packet-tracer-v5-0-espanol-software-simulador-de-redes-con-la-tecnologia-cisco.html

14.0 Glosario

NUMERALES

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

ABR
Tasa de bits disponible. Clase QoS definida para redes ATM. ABR se utiliza para las conexiones que no requieren de las relaciones temporales entre origen y destino. ABR no ofrece garantías en términos de pérdida de células o el retraso, proporcionando sólo el mejor servicio posible. Fuentes de tráfico para ajustar su velocidad de transmisión en respuesta a la

información que se describa en el estado de la red y su capacidad para entregar con éxito los datos.

Enrutador de la Zona Fronteriza. Enrutador ubicado en la frontera de una o más áreas OSPF que conecta las zonas de la red principal. ABRs se consideran miembros de una columna vertebral OSPF y las zonas adjunta. Por lo tanto, mantener las tablas de enrutamiento que describen tanto la topología de red troncal y la topología de las otras áreas.

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.

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.

Anycast
Un tipo de red IPv6 direccionamiento y enrutamiento sistema por el cual se transportan los datos a la "más cercano" o "mejor" destino tal como se ven por la topología de enrutamiento. Un paquete enviado a una dirección Anycast se entrega a la interfaz más cercana, según la definición de los protocolos de enrutamiento en uso, identificada por la dirección Anycast. Comparte el mismo formato de dirección como una dirección global Unicast IPv6.

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 Enrutado
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.

Checksum de la Capa Superior
Cálculo del checksum realizado en ICMPv6, TCP y UDP que utiliza la pseudo-cabecera IPv6.

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.

Configuración automática sin estado (Stateless autoconfiguration)
Autoconfiguración sin estado es una función plug-and-play IPv6 que permite que los dispositivos se conecten a la red sin configuración y sin ningún tipo de servidores (como servidores DHCP). Esta característica clave permite el despliegue de nuevos dispositivos en la Internet, tales como teléfonos celulares, dispositivos inalámbricos, electrodomésticos, y las redes domésticas.

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 enlace local unicast (link-local unicast address)
IPv6 usa direcciones de enlace local para identificar las interfaces en un enlace que están destinados a permanecer dentro de una emisión de dominio determinado. También pueden ser considerados como la parte "host" de una dirección IPv6. Estas direcciones se utilizan para funciones como la autoconfiguración apátridas. Direcciones locales de vínculo comienza con el prefijo FE80:: / 10, y luego incluir una interfaz de identificación.

Dirección de Lazo Local
Es la dirección IPv6 ::1, que se asigna a la interfaz local.

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.

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.

Estructura de datos o convención lógica utilizada para identificar una entidad única, como un proceso particular o dispositivo de red.

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 el 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.

Dirección unicast global (Global unicast address)
Una dirección IPv6 unicast que es único globalmente. Puede ser encaminada a nivel mundial sin ninguna modificación. Comparte el mismo formato de la dirección como una dirección IPv6 anycast. Las direcciones unicast globales son asignadas por la Internet Assigned Numbers Authority (IANA).

Dirección unicast locales **(Local unicast address)**
Una dirección IPv6, cuyo alcance está configurado para un solo vínculo. La dirección es única sólo en este enlace y no es enrutable fuera del vínculo.

DNS
(Domain Name System.) Ver sistema de nombres de dominio

Doble pila
Un mecanismo de transiciones comunes que permitan una integración sin problemas de IPv4 a IPv6.

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 ejemplo, 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).

EUI-64
Identificador Extendido Universal (EUI) -64 de direcciones. Este es un formato de direcciones IPv6 creado por tomar la dirección MAC de una interfaz (es de 48 bits de longitud) y la inserción de otra cadena hexadecimal de 16-bit (FFFE) entre la OUI (primeros 24 bits) y número de serie único (últimos 24 bits) de la dirección MAC. Para asegurarse de que la dirección elegida es de una única dirección MAC de Ethernet, el séptimo bit en el byte de orden superior se establece en 1 (equivalente a la IEEE G / L bits) para indicar la unicidad de 48 bits de dirección.

F

FF02::1
Dirección IPv6 multicast es la identificación de todos los nodos en un enlace.

FF02::2
Dirección IPv6 multicast es la identificación de todos los routers en un enlace.

FF02::5

Dirección IPv6 multicast es la identificación de todos los routers OSPF en el ámbito de aplicación linklocal. Es equivalente a la dirección multicast 224.0.0.5 en OSPFv2.

FF02::6
Dirección IPv6 multicast es la identificación de todos los routers OSPF designados en el enlace de ámbito local. Es equivalente a la dirección multicast 224.0.0.6 en OSPFv2.

FF02::9
Dirección IPv6 multicast es la identificación de toda la información de enrutamiento IPv6 (Protocolo de RIPng) enrutadores en el enlace.

FF05::1:FF*XX:XXXX*
IPv6 multicast es la dirección utilizada para crear mensajes de solicitud vecino que se envían en un enlace local, cuando un nodo desea determinar la dirección de enlace de capa de otro nodo en el vínculo local mismo. Similares a Address Resolution Protocol [ARP] en IPv4.

FF05::101
Dirección IPv6 multicast identificar todos Network Time Protocol (NTP) en el sitio (site-ámbito local).

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.

H

HELLO
Protocolo de enrutamiento interior utilizada principalmente por los nodos NSFnet. HELLO permite que paquete en particular cambien al descubrir las rutas de plazo mínimo. No debe confundirse con el protocolo Hello.

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.

Interface
1) Conexión a entre dos sistemas o dispositivos.
2) En la terminología de enrutamiento, una conexión de red.
3) En telefonía, un límite compartido definido por las características comunes de interconexión física, características de la señal, y los significados de las señales intercambiadas.
4) El límite entre las capas adyacentes del modelo OSI.

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.

IP address
1) 32-bits de direcciones asignadas a los ejércitos a través de TCP / IP. Una dirección IP pertenece a una de las cinco clases (A, B, C, D o E) y está escrito como 4 octetos separados por puntos (formato decimal de puntos). Cada dirección consiste en un número de red, un número de subred opcional, y un número de host. La red y los números de subred se utilizan conjuntamente para el encaminamiento, mientras que el número de host se utiliza para hacer frente a un host individual dentro de la red o subred. Una máscara de subred se utiliza para extraer información de red y subred de la dirección IP. También se llama una dirección de Internet.
2) Comando utilizado para establecer la dirección de red lógica de esta interfaz. Véase también la IP y la máscara de subred.

IPng
Protocolo de Internet de próxima generación.

IPv4
Protocolo de Internet versión 4. Protocolo de capa de red en la pila TCP / IP que ofrece un servicio de red interna a la conexión. IPv4 proporciona características para abordar, tipos de especificación de servicios, la fragmentación y el montaje, y la seguridad. Documentados en RFC 791.

IPv6
Protocolo de Internet versión 6 es un estándar de la capa de red IP que utiliza dispositivos electrónicos para intercambiar datos a través de una interconexión de redes packetswitched. De ello se deduce IPv4 como la segunda versión del Protocolo Internet, a ser formalmente adoptada para uso general. IPv6 incluye soporte para el flujo de identificación en la cabecera del paquete, que puede ser utilizada para identificar los flujos. Anteriormente llamados IPng (IP de próxima generación).

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.

IPv6-over-IPv4 tunnels (6to4) IPv6 sobre túneles IPv4 (6to4)
También se llama túneles 6to4, es un mecanismo de transición común que permita una integración sin problemas de IPv4 a IPv6. Este mecanismo utiliza el prefijo reservados 2002:: / 16 para permitir una conexión de Internet IPv4 sitio para crear y utilizar un prefijo / 48 basada en IPv6 en una sola dirección IPv4 globalmente enrutable o alcanzable.

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)
Dentro del sitio Protocolo de direccionamiento automático de túnel permite una intranet IPv4 privada (que puede o no estar usando direcciones RFC 1918) para aplicar gradualmente los nodos IPv6 sin tener que actualizar la red.

IS-IS
Intermediate System-to-Intermediate System. Enlace OSI protocolo de estado de enrutamiento jerárquico basado en DECnet fase V por el cual la ISS (routers) el intercambio de información de enrutamiento basado en una única métrica para determinar la topología de red. Comparar con IS-IS integrado.

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

LSA
Link-anuncio de estado. Paquete de difusiones utilizadas por los protocolos de estado de enlace que contiene información acerca de los vecinos y los costos de ruta. LSA son utilizados por los routers que reciben para mantener sus tablas de enrutamiento. A veces llamado un paquete de estado de enlace (LSP).

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
Multicast Listener Discovery (MLD) v1 realiza las funciones de IGMPv2 en IPv6. MLDv2 es equivalente a IGMPv3 en IPv6.

Mobile IP
Un estándar de IETF para IPv4 e IPv6, permite a los dispositivos móviles para desplazarse sin romper las conexiones actuales. En IPv6, la movilidad está incorporada, lo que significa que cualquier nodo IPv6 puede utilizar según sea necesario.

MOSPF
Multicast OSPF. Intradomain protocolo de enrutamiento de multidifusión utilizado en las redes OSPF. Las extensiones se aplican a la base del protocolo OSPF para apoyar IPv4 unicast y multicast de enrutamiento 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.

MP-BGP
Multiprotocolo BGP se utiliza para habilitar BGP4 para llevar la información de otros protocolos, por ejemplo, conmutación de etiquetas multiprotocolo (MPLS) e IPv6.

MPLS
Multiprotocol Label Switching (MPLS) es una técnica de etiquetado utilizado para aumentar la velocidad de flujo de tráfico. Cada paquete se ha marcado con la secuencia de ruta de acceso al destino. Esto ahorra tiempo al no tener que hacer una búsqueda de la tabla de enrutamiento. En otra palabra de la conmutación de paquetes se realiza en la capa 2 en lugar de capa 3. MPLS apoyo de múltiples protocolos como IP, ATM y Frame Relay. Véase también MPLS / TE.

MTU
Unidad de transmisión máxima. Tamaño máximo de paquete, en bytes, que una interfaz particular puede manejar

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.

Multicast
Paquetes individuales copiados por la red y enviados a un subconjunto específico de direcciones de red. Estas direcciones se especifican en el campo de dirección de destino.

Multihoming
Esquema de direccionamiento en el IS-IS routing que apoya la asignación de direcciones de área múltiples.

N

NAT
Network Address Translation. Sólo a nivel mundial único en términos de la Internet pública. Un mecanismo para traducir las direcciones privadas en direcciones públicamente utilizables para su uso en la Internet públicas. Un medio eficaz para ocultar el dispositivo real de abordar dentro de una red privada. También conocido como traductor de direcciones de red.

NAT-PT
NAT-traducción de protocolo (NAT-PT) es un mecanismo de traducción que se encuentra entre una red IPv6 y una red IPv4. El trabajo del traductor es traducir los paquetes IPv6 en paquetes IPv4 y viceversa.

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.

Octeto
8 bits. En la creación de redes, el término octeto se utiliza con frecuencia (en lugar de byte) ya que algunas arquitecturas de máquinas emplean bytes que no son de 8 bits de longitud.

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.

OSPFv2
Open Shortest Path First version 2. OSPFv2 es una dirección IPv4 linkstate, el algoritmo de enrutamiento IGP jerárquico propuesto como sucesor de RIP en la comunidad de Internet. Las características de OSPF incluyen por lo menos-cost

routing, ruteo múltiple, y balanceo de carga. OSPF se derivó de una primera versión del protocolo de ISIS.

OSPFv3
Open Shortest Path First versión 3 es la implementación del protocolo para IPv6. Se basa en OSPF versión 2 (OSPFv2), con mejoras.

P

PDAs
Asistentes personales digitales son dispositivos de mano. Dependiendo del modelo y la versión, que pueden ofrecer una cantidad variable de características que incluyen algunos de los siguientes: los organizadores personales, agenda, calculadora, reloj y funciones de calendario, juegos de ordenador, acceso a Internet, correo electrónico, la radio y la reproducción de MP3, de vídeo la grabación, GPS, teléfonos móviles (teléfonos inteligentes), navegadores o reproductores multimedia.

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.

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 e 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

PVC
Circuito virtual permanente. Circuito virtual que se estableció de manera permanente. PVCs ahorra ancho de banda asociada con el establecimiento de circuitos y derribar en situaciones en que determinados circuitos virtuales deben existir en todo momento. Llama una conexión virtual permanente en la terminología de ATM. Comparar con SVC.

Q

QoS
Calidad del servicio. Medida del rendimiento de un sistema de transmisión que refleja su calidad de transmisión y disponibilidad del servicio.

R

Red **(Network)**
1) Colección de computadoras, impresoras, routers, switches y otros dispositivos que son capaces de comunicarse entre sí a través de algún medio de transporte.
2) Comando que asigna un NIC-con el que el router está conectado directamente mediante una dirección.
3) Comando que especifica cualquier red conectada directamente a ser incluidos.

Redistribución
Permitiendo que la información de enrutamiento descubierto a través de un protocolo de enrutamiento que se distribuirán en los mensajes de actualización de otro protocolo de enrutamiento. A veces se llama redistribución de la ruta.

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 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.

RFC
Petición de Comentarios. Serie de documentos utilizados como medio principal para comunicar información acerca de la Internet. Algunas RFC son designadas por el IAB como estándares de Internet. La mayoría de las RFC documentan especificaciones de protocolos tales como Telnet y FTP, pero algunas son humorísticas o históricas. RFC están disponibles en línea de numerosas fuentes.

RIPng
Routing Information Protocol de próxima generación (RIPng, RFC 2080) es un protocolo de enrutamiento de vector de distancia con un límite de 15 saltos que utiliza horizonte dividido y revertir veneno para evitar bucles de enrutamiento. Se basa en IPv4 RIP versión 2 (RIPv2) y similar a RIPv2, pero usa IPv6 para el transporte. La dirección del grupo multicast FF02:: 9 identifica todos los RIPng permitido routers.

Route
Camino a través de una interconexión de redes.

Router
Dispositivo de capa de red que utiliza uno o más parámetros para determinar el camino óptimo a lo largo de la cual el tráfico de red debe ser reenviado. Los Routers reenvían paquetes de una red a otra basada en la información de capa

de red. De vez en cuando llama una puerta de enlace (aunque esta definición de la puerta de enlace se está convirtiendo cada vez más obsoletas).

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.

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.

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.

Sitio dirección local unicast **(site-local unicast address)**
Una dirección IPv6 que es muy similar en función a lo privado del espacio de direcciones IPv4, que incluye las gamas. Estas direcciones son para las comunicaciones internas y no son enrutables en la Internet pública. Sitio local de direcciones FEC0:: / 10 de comenzar con el prefijo.

Show IP route
Comando que muestra el contenido de una tabla de enrutamiento IP.

Subred
En IPv6 uno o más enlaces que utilizan el mismo prefijo de 64 bits.

T

TCP
Protocolo de Transmisión de Control. Orientado a la conexión de protocolo de capa de transporte que proporciona una solución confiable de datos dúplex completo de transmisión. TCP es parte del protocolo TCP / IP stack.

TCP/IP
Protocolo de Transmisión de Control / Protocolo de Internet. Nombre común para el conjunto de protocolos desarrollados por el Departamento de Defensa de EE.UU. en la década de 1970 para apoyar la construcción de Internetworks en todo el mundo. TCP e IP son los dos más conocidos protocolos en la suite.

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.

Teredo
Anteriormente conocido como carcoma, Teredo es un mecanismo que los túneles IPv6 en datagramas IPv4 Protocolo de datagramas de usuario (UDP). Este método proporciona para uso privado de direcciones IPv4 e IPv4 Network Address Translation (NAT).

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).

Token Ring
Token-passing LAN desarrollado y apoyado por IBM. Token Ring se ejecuta en 4 o 16 Mbps a través de una topología de anillo. Similar a IEEE 802.5.

ToS
Tipo de servicio. Campo dentro de un datagrama IP que indica cómo el datagrama debe ser manejado.

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

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.

Tunneling
Arquitectura de túnel que está diseñado para proporcionar los servicios necesarios para poner en práctica cualquier punto estándar de sistema de encapsulación punto.

U

Unicast
Mensaje enviado a un solo destino de red
UDP
Protocolo de datagramas de usuario. La capa de protocolo de transporte orientado a la conexión en el protocolo TCP / IP stack. UDP es un protocolo simple que intercambia datagramas sin acuses de recibo o la entrega

garantizada, que requiere que el tratamiento de errores y la retransmisión por ser manejados por otros protocolos. UDP se define en RFC 768.

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
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).

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.

Vínculo (Link)
Comunicaciones de la red de canales que consiste en un circuito o ruta de transmisión y todo el equipo entre un emisor y un receptor. La mayoría utiliza a menudo para referirse a una conexión WAN. A veces se refiere como una línea o un enlace de transmisión.

VoD
De vídeo bajo demanda (VOD), estos sistemas permiten a los usuarios seleccionar y visualizar contenidos de vídeo a través de una red como parte de un sistema de televisión interactiva. Los sistemas VOD o flujo de contenido, permiten ver el vídeo mientras se descarga, o "descargar" el programa en que es llevado en su totalidad a un set-top box antes de verlo este se inicia.

VoIP
Voz sobre IP. La capacidad de llevar a la telefonía normal sobre un estilo de voz basada en IP, Internet con POTS-como funcionalidad, fiabilidad y calidad de voz. VoIP permite a un router realizar el tráfico de voz (por ejemplo, llamadas telefónicas y faxes) sobre una red IP. En VoIP, los segmentos de DSP de la señal de voz en marcos, que luego se juntan en grupos de dos y

almacenados en los paquetes de voz. Estos paquetes de voz son transportados mediante la propiedad intelectual en el cumplimiento de las especificaciones UIT-T H.323.