UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERIA

"GUIA DE IMPLEMENTACION DE REDES UTILIZANDO EL PROTOCOLO IPV6"

PARA OPTAR AL GRADO DE :

INGENIERO EN CIENCIAS DE LA COMPUTACION

PRESENTADO POR:

JOSÉ ISAAC ESCALANTE RENDÓN

ASESOR:

ING. RAFAEL ADALBERTO COBOS MELÉNDEZ

OCTUBRE DE 2005

EL SALVADOR, CENTROAMÉRICA.

UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERIA
ESCUELA DE COMPUTACION

COMITÉ EVALUADOR DEL TRABAJO DE GRADUACION

ING. RAFAEL ADALBERTO COBOS MELENDEZ
ASESOR

ING. MARCO VINICIO LUNA
JURADO

ING. CARLOS LOPEZ
JURADO

ING. RAFAEL CRISTOBAL HERNANDEZ
JURADO

DEDICATORIA

En primer lugar, quiero agradecer a Dios todopoderoso por la oportunidad que me ha dado de realizar mis estudios y llegar a la culminación de mi carrera de una forma exitosa.

Por consiguiente, quiero dedicarle este éxito a Dios, porque sin su ayuda, nada hubiera sido posible. En segundo lugar quisiera dedicárselo a mis padres, porque desde pequeño, siempre han estado pendientes de mis estudios y me ha n respaldado económicamente para su realización.

Al mismo tiempo quisiera agradecerle a cada una de las personas que hayan formado parte de mi desarrollo estudiantil y profesional, desde los maestros de educación básica hasta los de educación superior. También a todos mis amigos, compañeros de estudio y de trabajo que me han apoyado de gran manera.

ÍNDICE

INTRODUCCION

Con el correr de los años, el Protocolo de Internet versión 4 (IPv4) ha demostrado su robustez. Es así que desde la publicación del RFC 921 (Solicitud para Comentarios, Request for Comments) en el año de 1981, Ipv4 no ha cambiado sustancialmente.

Hoy lo encontramos funcionando y dando soporte de conectividad, en pequeñas redes hogareñas, en grandes redes empresariales y en el mismo Internet.

Este constituye todo un éxito para sus desarrolladores y las personas que lo adoptaron en sus instalaciones. Sin embargo este éxito no ha estado ajeno a problemas que se enfrentan en la actualidad:

- El crecimiento explosivo de Internet asociado a una mala asignación de direcciones ha provocado agotamiento en las direcciones de Internet Ipv4 y ha generado un crecimiento en las tablas de enrutamiento de los routers troncales de Internet.

- Gran desarrollo del mercado de dispositivos que pueden utilizar Ip como protocolo de comunicaciones, asociado a la generación de nuevos servicios comerciales sobre la red.

- Generación y aumento del uso de aplicaciones que requieren calidad de servicio garantizado (QoS).

- Necesidad de emplear configuraciones automáticas para hacer más fácil el uso del mismo.

Ipv4 no fue diseñado para ser seguro, ya que originalmente fue creado para una red militar aislada, que posteriormente se convirtió en una red pública para la investigación y educación.

En 1992, el IETF llegó a la conclusión de que haría falta un sustituto del IPv4 y formó un grupo de trabajo con el nombre de IPNG que tendría la misión de desarrollar la siguiente generación del protocolo IP.

De esta manera, en 1994 , el RFC 1752 "Recomendación para el IP de Nueva Generacion" se convirtió en un estándar para el sucesor de Ipv4, que fue llamado Ipng conocido actualmente como IPv6.

Hoy en día, IPv6 esta empezando a ser una realidad. Todas las redes de Investigación y Educación del mundo soportan IPv6, e incluso algunos grandes operadores.

El presente documento esta orientado a fundamentar los conocimientos sobre el nuevo protocolo de Internet y a la implementación práctica del mismo, como una guía de referencia para su configuración.

ANTECEDENTES

Las redes de comunicación de datos son de gran importancia para las Empresas, Instituciones Gubernamentales, Organizaciones, etc. Actualmente la comunicación entre las mismas es posible gracias al Protocolo de Internet (IPv4), el cual es el protocolo más básico de Internet, y provee todos los servicios necesarios para el transporte de datos. El surgimiento del protocolo Ipv6 se debió a la necesidad de satisfacer las demandas de comunicación y las exigencias de los servicios de nueva generación. De esta manera:

- Para el invierno de 1992 la comunidad del Internet había desarrollado cuatro propuestas diferentes para el IPng que eran: CNAT, IP Encaps, Nimrod y Simple CLNP.
- Después para diciembre del mismo año, aparecieron tres propuestas más: El Protocolo P de Internet (PIP), El Protocolo Simple de Internet (SIP) y el TP/IX .
- En la primavera de 1992 el CLNP simple se desarrolló en el TUBA (TCP y UDP con Direcciones Grandes) , y el IP Encaps en IPAE (Encapsulacion de Direcciones IP) .
- Para el verano de 1993, IPAE se combinó con el SIP aunque mantuvo el nombre SIP, que posteriormente se fusionó con la PIPA, y al grupo de trabajo resultante se le llamó "SIPP" (Protocolo Simple de Internet Mejorado). Casi al mismo tiempo el grupo de trabajo TP/IX cambió su nombre por el de "CATNIP" (Arquitectura común para el Internet)
- Posteriormente, en la reunión del IETF del 25 de julio de 1994 en Toronto Canadá, los directores de área del mismo organismo recomendaron el uso del IPng (IP de Nueva Generación) y lo documentaron en el RFC 1752, (la recomendación para el protocolo IP de siguiente generación)
- El 17 de noviembre del mismo año fue aprobada esta recomendación por el IESG (Grupo de Ingenieria de Internet) que elaboró una propuesta de Estandar.

Desde sus orígenes, hace 10 años, la versión 6 ha madurado al robustecerse y expandir su uso y aplicaciones de forma tal que el 2004, marca el despliegue de IPv6 con exposiciones y conferencias realizadas (al menos una al mes) en todo el mundo. Así, en Enero y Octubre del 2004, se llevaron a cabo dos eventos trascendentes: el de "Lanzamiento del Servicio Global de IPv6" en Bruselas, Bélgica, y el del "Futuro de la Sociedad del Conocimiento" en la Haya, Holanda, con la participación y el soporte de entidades de los cinco continentes, donde se presentaron demostraciones reales del gran potencial de la nueva versión, dentro de las cuales destacan las siguientes:

- IPv6 en el espacio (vía satélite usando tecnologías como DVB-S/MPEG-2).

- Televisión de alta definición con IPv6 y calidad de servicio (HDTV/IPv6 y QoS).
- Multicast con IPv6 mediante la red llamada M6Bone.
- Control remoto y vigilancia del hogar (electrodomésticos, cámaras, cortinas, etcétera).
- Ambientes de colaboración a distancia.
- Aplicaciones de videoconferencia y VoIP usando IPv6.
- Canal de televisión digital (EuroNews).
- Control remoto de instrumentos y video digital (microscopios, telescopios, entre otros).
- Demostraciones del Protocolo de Seguridad IP (IPSec) con IPv6.
- Automóvil con IPv6, usando tecnologías como GPRS (Servicio de Radio de Paquete General), Bluetooth y WiFi (Confiabilidad inalambrica, norma 802.11 para redes locales inalámbricas).
- Herramientas de administración y monitoreo con soporte IPv6.
- Transmisión de IPv6 sobre enlaces PLC, etcétera.

Estos eventos mostraron, sin lugar a dudas, que los principales impulsores de IPv6 son los usuarios de una gran parte del espacio de direccionamiento, además de los proveedores de servicios siempre activos (always-on).

En Latinoamérica, por ejemplo, en Marzo y Octubre del 2004 se formalizó el trabajo que llevan a cabo varias Universidades e Instituciones, con la integración del Grupo de Trabajo IPv6 para Latinoamérica y el Caribe con siglas en inglés "LAC IPv6 TF", respaldado por LACNIC (Registro de Direcciones de Internet para América Latina y el Caribe), y varios NICs (Centros de Información de la Red) nacionales e institucionales. Los antecedentes de IPv6 en la región Latinoamericana datan de finales de 1998, cuando instituciones como RNP (Red Nacional de Pesquisa) de Brasil y la UNAM en México, iniciaron sus investigaciones en la materia.

En El Salvador el desarrollo de Ipv6 ha sido muy limitado, hasta el momento solo se han hecho estudios de investigación sobre el protocolo en diferentes Universidades; pero hasta el momento no existen nodos Ipv6 nativos. Solamente la Universidad Francisco Gavidia por el momento tiene un enlace hacia Internet2 independiente de 2MB el cual esta conectado a la Universidad Internacional de Florida (FUI).

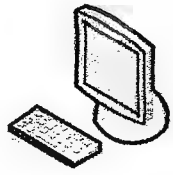
La Organización RAICES de El Salvador esta trabajando actualmente junto con Telecom para la integración de diferentes Universidades del pais a la red de Internet2, la cual utiliza el protocolo Ipv6. Esta integración se pretende realizar a finales del año 2005.

Para el desarrollo de este proyecto Telecom ha determinado: objetivos, equipo a utilizar, las caracteristicas de los mismos, aspectos de seguridad, monitoreo de red, costos, etc. Para una mayor referencia remitirse al documento detallado en los anexos.

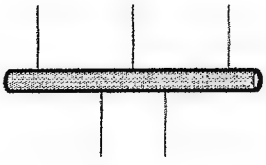
SIMBOLOGIA.

Enrutador

Nube de Red



Terminal 1



Red de Area Local (LAN)

Terminal 2

Enlace Serial

Servidor DNS

Servidor Web

CAPITULO 1

Situación Actual de IPv6

1. SITUACION ACTUAL DE IPV6.

Como una solución a las demandas provocadas por el crecimiento exponencial de Internet, el Grupo de Trabajo de Ingeniaría de Internet (IETF), creó el proyecto IPng (Protocolo de Internet de Nueva Generación), también conocido como Ipv6.

Esta nueva versión del protocolo de Internet, tiene nuevas e importantes características que permiten superar las limitaciones de Ipv4. Entre las características más importantes se destaca el gran espacio de direcciones, la posibilidad de autoconfiguración de host, la movilidad, eficaz soporte para la seguridad, calidad de servicio, transición gradual de Ipv4 a Ipv6, etc. Estas serán retomadas posteriormente en este documento.

1.1 SITUACIÓN ACTUAL DE IPV6 A LO LARGO DEL MUNDO.

Podemos identificar cinco regiones diferenciadas en lo que al estado de desarrollo de IPv6 se refiere:

Asia: En esta área, el impacto de la falta de direcciones IPv4 ha sido más obvio, y APNIC, la entidad de registro regional de Internet para esta región espera agotar su rango de direcciones IPv4 en muy pocos meses. En correspondencia, la presión para encontrar soluciones adecuadas es muy alta, y se han iniciado gran número de actividades, particularmente en Japón.

Europa: La industria de la telefonía móvil es un soporte muy fuerte para la transición a IPv6. En correspondencia, el Instituto de Estándares de Telecomunicación Europea (ETSI) y el Foro IPv6 han establecido un acuerdo de cooperación para aunar sus fuerzas; este movimiento de ETSI ha sido impulsado por el fuerte deseo de los operadores inalámbricos. Además de este acuerdo de cooperación con ETSI, el Foro IPv6 ha estrechado fuertes lazos con el Foro UMTS (Sistema Universal de Telecomunicación Móvil) y la Asociación GSM (Comunicación Móvil para Sistemas Globales), y hay conversaciones con el grupo 3GPP (Protocolo de Tercera Generación).

Norteamérica: Muchas actividades relacionadas con IPv6, tanto en términos de estandarización, despliegue y verificación, tienen sus orígenes en esta región. Muchas de estas actividades pueden ser localizadas en torno al 6bone, la plataforma de pruebas internacional de IPv6.

Otras actividades relacionadas con IPv6 que incluyen importante participación norteamericana son 6REN, que es una iniciativa de coordinación para IPv6 en redes de investigación y educación, 6TAP que es una iniciativa para proporcionar un router IPv6 central en Chicago para facilitar la interconexión entre redes IPv6, y Freenet/Viagénie que es una iniciativa de túneles automáticos.
En cualquier caso, el despliegue comercial de IPv6 en esta región se ha iniciado muy despacio; sólo hay 2 rangos de direcciones IPv6 comerciales en Norteamérica, de un total de 22 en el mundo.
Esto refleja la apariencia de que el despliegue operacional de IPv6 puede no llegar primero a ésta área, ya que los problemas de la falta de direcciones IPv4 aún no han emergido como una urgencia en esta región.

Rusia: Existen fuertes relaciones entre el Foro IPv6, el Foro IPv6 local Ruso, y FREEnet (red académica y de investigación Rusa). El objetivo es crear una comunidad rusa de usuarios de IPv6 y proveedores de servicios.

Resto del Mundo: En la actualidad se están desarrollando proyectos e investigaciones sobre Ipv6 en México, Corea, India, Australia y Singapur. No es tan extraño dado que son países con alto nivel tecnológico o están situados entre dos grandes áreas de desarrollo. En Singapur la razón es el alto grado de comunicaciones inalámbricas, por medios muy diversos.

La necesidad de direcciones se convertirá en una gran fuerza según aumente el número de dispositivos de usuario final, como teléfonos móviles y adaptadores de televisión por cable, que requieren direccionamiento IP, lo que obligará a los desarrolladores a escoger IPv6 frente a IPv4 para permitir direcciones únicas para cada dispositivo. Este paso también supondrá, en muchos casos, el uso de NAT's (Traducción de Direcciones de Red), para permitir el transporte de paquetes IPv6 sobre troncales IPv4.

1.1.1 Usuarios Actuales y Furturos de Ipv6.

Los mejores objetivos para la aplicación de IPv6 son lugares donde hoy no es posible obtener direcciones IPv4, por añadido, países en desarrollo y crecimiento, dado que los mayores ISP's norteamericanos aún mantienen reservas sobre el resto del espacio de direcciones IPv4.
IPv6 resuelve el problema de espacio de direcciones, el cual no tiene ninguna otra solución real, y puede ser de beneficio para cualquier nueva aplicación con grandes necesidades de espacio de

direcciones, como la telefonía IP móvil. Actualmente el número de teléfonos móviles ya ha crecido por encima del número de conexiones a Internet.

Cualquier aplicación que actualmente corre sobre IPv4, lo hará mejor sobre IPv6, con muchos recursos adicionales, y ofreciendo mejores métodos para Calidad de Servicio. Esto favorece mucho a las tecnologías de voz sobre Ip (VoIP) .

Según aumente el número de Intranets que lo usen y empleen túneles entre ellas, y se incremente el número de fabricantes que comercialicen productos con IPv6, y el Foro IPv6 vaya haciendo su trabajo, los ISP's y los operadores irán sintiéndose más cómodos, y al mismo tiempo más obligados a migrar a IPv6.

Esta migración no será posible si no se dispone de productos certificados para el uso de Ipv6, por esto mismo, muchos de los grandes fabricantes se han comprometido al desarrollo de productos comerciales con soporte para Ipv6.

1.1.2 El Obstáculo de Ipv6.

El procesamiento de las opciones de la cabecera sigue siendo una ventaja insuperable de IPv6 sobre cualquier otra solución. Por el momento no hay ninguna propuesta real para otros protocolos; ya que fueron rechazadas durante el proceso de selección de IPng.

Por tanto, existe un obstáculo que puede representar un inconveniente para el proceso de desarrollo y expansión del protocolo Ipv6; este es el Traductor de Direcciones de Red (NAT), que es un estándar de Internet que le permite a una Red de Área Local usar un grupo de direcciones IP para el tráfico interno y otro grupo de direcciones para el tráfico externo. Una tabla de NAT ubicada en el lugar donde la LAN se conecta a Internet, se encarga de realizar todas las traducciones necesarias de IPs.

El NAT sirve para:

- Proveer un tipo de firewall al ocultar las direcciones de IP internas.

- Permitirle a una empresa usar más direcciones de IP internas. Dado que son direcciones internas, no hay posibilidad de conflicto con IPs usadas por otras empresas u organizaciones.

NAT se utiliza para obtener un mayor espacio de direcciones; pero representa una desventaja en cuanto a la complejidad para su gestión, este punto terminará eliminando esta práctica a largo plazo. NAT aísla intranets de Internet trabajando en contra de la carencia de direcciones. De esta manera se da lugar a múltiples convertidores NAT para proporcionar conectividad global. Sin embargo, esta aproximación esta violando el concepto general de Internet, que es la transparencia en el ámbito de la red. NAT incrementa la complejidad de la configuración y crea puntos únicos de fallo en las conexiones a redes. Además rompe el modelo de conexión extremo a extremo, por lo tanto rompe el esquema de seguridad extremo a extremo y predispone a situaciones erróneas en la red.

NAT es una ayuda para resolver los problemas de IPv4, pero no deja de ser un vendaje y se va a coexistir con él hasta que IPv6 lo haga innecesario.

1.1.3 Crecimiento de Internet en el Mundo.

Las cifras del Internet hasta Julio del 2005 muestran gran dinamismo y un crecimiento constante en muchas partes del mundo. Otras lamentablemente muestran una muy baja tasa de penetración, reflejo del estado de atraso y pobreza de algunos países.

El Internet es el mayor medio de comunicación en el mundo, con una audiencia de mas de 938 millones de personas. Esto significa que uno de cada diez habitantes del planeta utiliza esta espectacular herramienta de alcance global para la cultura, la educación a distancia, los negocios y el entretenimiento. (Ver Tabla 1.1)

Cada día aumenta la necesidad de direcciones IP para satisfacer las necesidades de comunicación de nuevos usuarios de Internet, a esto hemos de sumar los innumerables dispositivos que se van creando, o los ya existentes a los que damos nuevas o mejoradas aplicaciones, mediante su conexión a la Red. Como ejemplo se podría mencionar a los propios teléfonos, pues la siguiente generación, sin duda, utilizará la tecnología IP (VoIP); la televisión y la radio, también basados en tecnologías IP; o los sistemas de seguridad, tele vigilancia y control. Además otros dispositivos de entretenimiento como los Walkman MP3, que a través de Internet nos permiten recuperar y almacenar creaciones musicales.
Nuevas tecnologías emergentes, como Bluetooth, WAP, las redes inalámbricas o las redes domésticas, hacen más patente esta necesidad de crecimiento, al menos, en lo que al número de direcciones se refiere. Por ejemplo, la última tendencia es la de permitir a cualquier dispositivo serie ser conectado a una LAN o WAN, y por qué no a Internet.

Podríamos hablar, en general, de casi cualquier dispositivo, tanto doméstico como industrial, integrado en la Gran Red, pero también de dispositivos de control médico, como los marcapasos, entre otros muchos.

A continuación se presenta el cuadro resumen del estado del Internet en el mundo

ESTADISTICAS DE LA POBLACIÒN MUNDIAL Y EL USO DE INTERNET						
REGION	**POBLACION (2005)**	**% DE POBLACION MUNDIAL**	**USUARIOS**	**CRECIMIENTO (2000-2005)**	**%POBLACION (PENETRACION)**	**% USUARIOS MUNDIAL**
ÁFRICA	896,721,874	14.0%	16,174,600	258.3%	1.8%	1.7%
ASIA	3,622,994,130	56.4%	323,756,956	183.2%	8.9%	34.5%
EUROPA	731,018,523	11.4%	269,036,096	161.0%	36.8%	28.7%
MEDIO ORIENTE	260,814,179	4.1%	21,770,700	311.9%	8.3%	2.3%
NORTE AMÉRICA	328,387,059	5.1%	223,392,807	106.7%	68.0%	23.8%
LATINO AMÉRICA/ CARIBE	546,723,509	8.5%	68,130,804	277.1%	12.5%	7.3%
OCEANÍA /AUSTRALIA	33,443,448	0.5%	16,448,966	115.9%	49.2%	1.8%
TOTAL MUNDIAL	6,420,102,722	100%	938,710,929	160.0%	14.6%	100%

Tabla 1.1 Estadísticas de Población Mundial y Usuarios de Internet. (Datos Provenientes de Internet World Stats).

En cuanto al número de los usuarios por regiones, las cifras son muy elocuentes. A continuación se presentan algunas conclusiones:

- El crecimiento global del Internet en el mundo ha sido del 80.8% desde Diciembre del año 2000 hasta Julio del 2005.

- La gran mayoría de usuarios esta concentrada en América, Asia y Europa.

- Oceanía es la región mas penetrada, donde Australia y Nueva Zelanda han logrado un acercamiento e integración con los países angloparlantes de Europa y América por medio del Internet.

- La región del Medio Oriente fue la de mayor crecimiento relativo (311.9%) desde el año 2000 hasta Julio del 2005.

- En algunos países de Europa disminuyo la población y a la vez subió el número de usuarios, elevando aun mas la tasa de penetración.

- En algunos países del tercer mundo creció la población a mayor ritmo que los usuarios del Internet, reduciendo aun más la tasa de penetración.

1.2 IPV6 Y EL 6BONE.

Es una red mundial experimental utilizada para probar los conceptos y la puesta en practica de Ipv6, mediante una red virtual compuesta por islas, las cuales son un conjunto de equipos y computadoras que utilizan el protocolo Ipv6 para comunicarse entre si, estas islas se encuentran unidas por conexiones punto a punto llamadas túneles.

Actualmente se hacen grandes esfuerzos para reemplazar los túneles por enlaces nativos sobre Ipv6. Hasta la fecha, el 6Bone esta formado por 58 países de los cinco continentes, estos se describen en la Tabla 1.2 .

PAIS	NUMERO DE ISLAS	PAIS	NUMERO DE ISLAS
Argentina	11	Luxemburgo	2
Australia	8	Malasia	3
Austria	33	Malta	2
Bélgica	22	México	16
Brasil	13	Holanda	41
Canadá	20	Nueva Zelanda	3
Chile	3	Noruega	5
China	13	Perú	2
Colombia	6	Filipinas	1
Cuba	1	Polonia	88
Republica Checa	7	Portugal	9
Dinamarca	4	Rumania	8
Rep. Dominicana	3	Rusia	6
Estonia	5	Senegal	1
Finlandia	49	Singapur	5
Francia	51	Eslovaquia	2
Alemania	142	Eslovenia	8
Grecia	14	Sur África	4
Hong Kong	4	España	25
Hungría	40	Suecia	109
India	2	Suiza	21
Indonesia	2	Taiwán	7
Irlanda	4	Tailandia	5
Israel	1	Tunes	1
Italia	73	Turquía	2
Japón	51	Ucrania	3
Korea	14	Reino Unido	30
Latvia	1	Estados Unidos	158
Lithuania	5	Yugoslavia	2

Tabla 1.2. Paises miembros del 6Bone

A continuación se presenta un diagrama ejemplo de algunas de las conexiones que existen en el 6Bone actualmente.

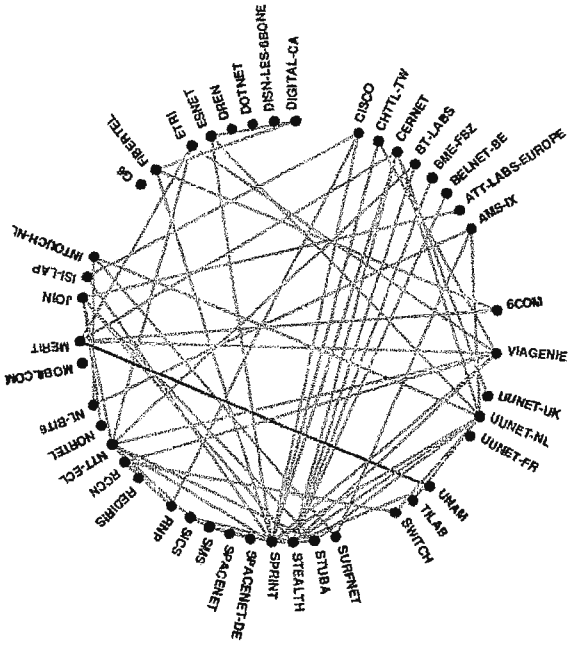


Figura 1.1 Diagrama de Enlaces en el 6Bone.

Con la red de 6Bone se posibilitan los enlaces a páginas web construidas bajo el protocolo Ipv6.
Para poder acceder a una pagina web Ipv6 se debe pertenecer a una red implementada bajo dicho protocolo y tener una conexión hacia el 6bone a través de túneles o de forma nativa.
Algunos ejemplos de instituciones que poseen páginas web Ipv6 son:

- Proyecto Kame de Japón.
  http://www.kame.net

- Universidad de Muenster's
  http://www.uni-muenster.de

- Departamento de computo de la Universidad de Lancaster.
  http://www.lancs.ac.uk

- Bussines Internet Inc.'s
  http://www.ipng.net

- Centro Técnico de Virginia.
  http://www.vt.edu IPv6 Web Pages

- Politécnico de Torino
  http://www.polito.it IPv6 Web Pages

1.3 EL FORO IPV6 (IPV6 FORUM).

Es un consorcio mundial de proveedores líderes de Internet, Redes de Educación e Investigación, con la clara misión de promocionar IPv6 mejorando dramáticamente el reconocimiento de IPv6 por parte del mercado y los usuarios, creando la Nueva Generación de Internet con calidad y seguridad y permitiendo el acceso equitativo mundial al conocimiento y la tecnología, abrazando una responsabilidad moral del mundo.

Para este fin, el Foro IPv6 debe:

- Establecer un Foro internacional y abierto de experiencia en IPv6.
- Compartir los conocimientos y experiencias de IPv6 entre los miembros.
- Promocionar nuevas aplicaciones basadas en IPv6 y soluciones globales.
- Promocionar la interoperabilidad de implementaciones normalizadas de IPv6.
- Cooperar para alcanzar Calidad de Servicio extremo a extremo.
- Resolver problemas que creen barreras para el uso de IPv6.

El Foro IPv6 no tiene la capacidad para desarrollar el protocolo, dado que la única autoridad competente para esta misión es el IETF .

1.3.1 Estructura del Foro.

El Foro IPv6 ha sido organizado en dos cuerpos principales, ambos dependiendo del Consejo del Foro IPv6:

1.3.1.1 Directiva Técnico de Despliegue de IPv6.

Esta directiva tiene plena autonomía en sus decisiones respecto del grupo de promoción, garantizando soluciones técnicas objetivas e independientes de fabricantes.
Esta disponible para la asistencia a los miembros del Foro en cuestiones y oportunidades técnicas, de despliegue e implementación.

La directiva consiste en unos 20 miembros contribuidores activos, con el fin de cubrir una amplia experiencia en áreas como seguridad, routing, movilidad, QoS, entornos de PC, software de fuentes abiertas, gestores de redes, desarrolladores de aplicaciones, verificación y prueba, telefonía IP, etc.

1.3.1.2 Grupo de Promoción del Foro IPV6.

El Grupo de Promoción se compone de los siguientes Grupos de Trabajo (siempre abiertos a nuevos grupos):

- **Proyectos:** Casos de Negocios de la Vida Real, Historias Exitosas de IPv6, Proyectos Nacionales e Internacionales, etc. El objetivo es demostrar la evolución positiva hacia la Nueva Internet con proyectos colaborativos trabajando sobre tecnología IPv6, facilitando el intercambio de información entre proyectos y la creación de otros nuevos.

- **Educación, Promoción y Relaciones Públicas.** El objetivo es crear y promover, por cualquier medio, mensajes de calidad, documentos, presentaciones, y herramientas, para educar acerca de IPv6 y asegurarse destacar una imagen limpia y poderosa de las ventajas de Ipv6.

- **Conferencias Globales de IPv6:** Encuentros/Conferencias Internacionales y Regionales de IPv6, Conferencias de Asociados, etc. El objetivo es crear eventos mundiales y locales para promocionar diversos aspectos de IPv6.

- **Programa de Embajadores:** Forma alternativa, sin costo, para individuos que desean participar en la promoción del protocolo IPv6. Destinado a gente interesada en escribir artículos, realizar presentaciones, discursos, u otras actividades promocionales/educacionales, fundamentalmente locales.

1.3.2 Miembros del Foro Ipv6.

El estado actual de los miembros del Foro IPv6, fechado a 10 de Julio del 2005, es de 73 compañías/organizaciones:

1 - Case Technology, UAE
2 - Thomson-CSF Detexis, France
3 - Ericsson Telebit, Denmark
4 - Eurocontrol, France
5 - Gigabell, Germany
6 - Hitachi, Japan
7 - Hewlett-Packard, US
8 - DFN, Germany
9 - Canarie-Viagenie, Canada
10- NTT, Japan
11- WIDE, Japan
12- BT, UK
13- CSELT, Italy
14- Mentat, US
15- SUN, US
16- Netmedia, Finland
17- Trumpet Software, Australia
18- Intracom, Greece
37- Motorola, US
38- Telia Networks Services, Sweden
39- Centre for Wireless Communications, Singapore
40- Siemens, Germany
41- IBM, US
42- BellSouth, US
43- Teleglobe, US
44- Silicon Graphics, Inc (SGI), US
45- Etisalat, UAE
46- SwitchCore AB, Sweden
47- UCAID - Internet2, US
48- University College of London (UCL), UK
49- University of Southampton, United Kingdom
50- University of Lancaster, United Kingdom
51- Royal Philips - The Netherlands
52- Royal KPN (Royal Dutch Telecom) - The Netherlands
53- The Open Group - UK
54- CIAC, France
55- UNINETT, Norway
56- NEC, Japan
57- ETRI, Korea
58- INTAP, Japan
59- Alpha Group, US
60- Korea Telecom, Korea
61- CNRS, France
62 -YDC (Yokogawa Digital Computer Corporation), Japan
63 - Alcatel, France
64 - GITEP, France
65 - ISI, US - UK
66 - Nortel Networks - US
67 - ISOC
68 - Stardust.com, US
19- Cisco, US
20- COMPAQ, US
21- SPRINT, US
22- NOKIA, US
23- AT&T, US
24- Teldat, Spain
25- Deutsche Telekom, Germany
26- Qwest, US
27- IABG, Germany
28- ESnet-6REN, US
29- MCI WorldCom, US
30- Ericsson, Sweden
31- Microsoft, US
32- 3Com, US
33- Advanced Systems Consulting, Inc., US
34- Consulintel, Spain
35- The Business Internet, US
36- NTT Software Corporation, Japan
69 - Telefonica Spain
70 - Telscom, CH
71 - NFP, Finland
72 - Lucent, EU/US
73 - IMAG, France

1.4 ADMINISTRACION DE IPV6 EN LACNIC

1.4.1 Definicion de LACNIC.

El Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC), es la organización que administra el espacio de direcciones IP, Números de Sistemas Autónomos (ASN), Resolución Inversa y otros recursos para la región de América Latina y el Caribe (LAC) en nombre de la comunidad Internet.

Tiene como objetivos representar y promover los puntos de vista de la comunidad de la región así como contribuir al desarrollo y crecimiento de Internet en la misma, además de promover oportunidades educacionales y políticas públicas relativas a la Internet.
Entre sus pautas LACNIC pretende ofrecer un servicio neutral, participativo, democrático y no lucrativo de calidad con un directorio elegido por sus miembros. En este contexto, la membresía se atendrá a reglas específicas, de acuerdo a la ubicación geográfica y al carácter de ISPs. Los miembros se eligen por un sistema de votación según el tamaño del espacio de direcciones que administren.
Las políticas y los procedimientos se basan en las RFCs relacionadas con la administración de IP, números de sistemas autónomos y Resolución Inversa. Así mismo se implementan permanentemente mecanismos de participación y discusión con respecto a la actualización y modificación de las políticas.
LACNIC es una organización sin fines de lucro, basada en membresía y establecida jurídicamente en el Uruguay.

1.4.2 Objetivos.

- Proveer servicios de registro de direcciones IP, Numeros de Sistema Autonomo (ASN), Resolución Inversa y sus recursos asociados, con el propósito de permitir y facilitar las comunicaciones a través de redes informáticas.

- Representar y promover los puntos de vista e intereses de la región ante organismos internacionales, en el área de su competencia.

- Colaborar en el crecimiento de Internet en Latinoamérica y el Caribe.

- Asistir a la comunidad Latinoamericana y Caribeña en el desarrollo de procedimientos, mecanismos y estándares para la asignación eficiente de recursos de Internet.

- Promover oportunidades educacionales a sus miembros en áreas técnicas y políticas de su competencia.

- Proponer y desarrollar las políticas públicas en el área de su competencia.

1.4.3 Área de Cobertura:

LACNIC brinda sus servicios en 29 territorios de América Latina y el Caribe, donde están incluidos.

Antillas Holandesas
Argentina
Aruba
Belice
Bolivia
Brasil
Chile
Colombia
Costa Rica
Cuba
Ecuador
El Salvador
Guyana Francesa
Guatemala
Guyana
Haití
Honduras
Islas Falkland (Malvinas)
México
Nicaragua
Panamá
Paraguay
Perú
República Dominicana
Sur Georgia y Sur Sandwich
Islandia
Surinam
Trinidad y Tobago
Uruguay
Venezuela

1.4.4 Recursos Administrados por LACNIC.

LACNIC administra actualmente en su región los siguientes recursos:

- Bloques de direcciones Ipv4.
  200/8 y 201/8 + Bloques ERX.

- Bloque de direcciones Ipv6.
  2001:1200::/23

- ASN (Números de Sistema Autónomo).
  27648 – 28671 Recibidos de IANA.
  26592 – 26623 Recibidos de ARIN (Transición)
  Total de ASN = 1056.

1.4.5 Asignaciones Ipv6 Realizadas por LACNIC.

Hasta el año 2005 LACNIC ha realizado 21 asignaciones de rangos Ipv6 en algunos países de Latino América y el Caribe.

El número de asignaciones por país se muestra en el siguiente grafico.

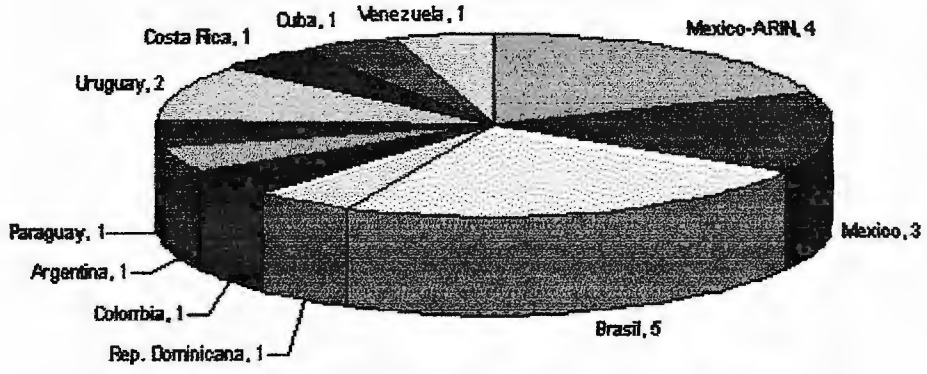


Figura 1.2 Rangos Ipv6 Asignados por LACNIC.

En la Figura 1.3 se muestra la cantidad de asignaciones de bloques Ipv6 realizados por LACNIC por cada año, desde el año 2000 hasta el 2005.

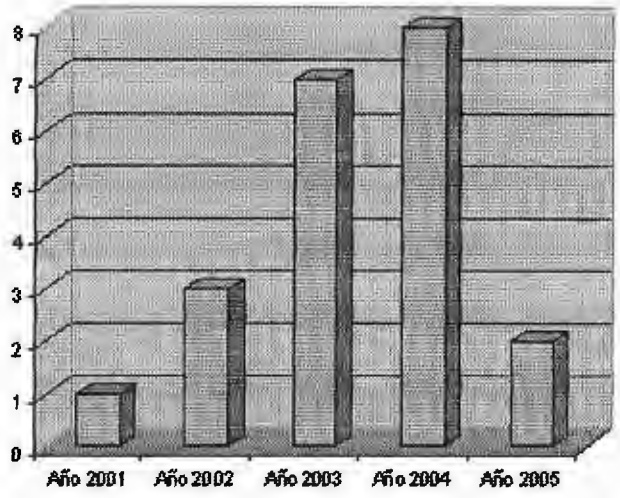


Figura 1.3 Asignaciones de Rangos Ipv6 por Año

Como se puede observar en la figura anterior, la asignación de rangos de direcciones Ipv6 fue superior en los años 2003 y 2004.

1.4.6 Promoción de Ipv6 en la Región Latinoamericana y el Caribe.

LACNIC basa su estrategia de promoción de Ipv6 en la región, en cinco puntos básicos.

1.4.6.1 Adaptación de Políticas.

Estas son políticas adoptadas por los Registros Regionales de Internet para la asignación de bloques Ipv6. La ultima política regional adoptada fue en el año 2003, la cual comprende los siguientes aspectos para la asignación de bloques Ipv6:

- Ser un Proveedor de Servicios de Internet (ISP).
- No ser un sitio final (usuario final).

- Documentar un plan detallado sobre los servicios y la conectividad en IPv6 a ofrecer a otras organizaciones (clientes).

- Anunciar en el sistema de rutas inter-dominio de Internet un único bloque, que agregue toda la asignación de direcciones IPv6 recibida, en un plazo no mayor de 12 meses.

- Ofrecer servicios en IPv6 a clientes localizados físicamente en la región del LACNIC en un plazo no mayor de 24 meses.

Las organizaciones que cumplan con el criterio anterior pueden recibir un mínimo de asignación de un prefijo /32.

1.4.6.2 Suspensión de Tarifas:

- Una primera resolución del Directorio de LACNIC en el año 2003 establece que las asignaciones de bloques IPv6 no tienen costo por los primeros dos años. (2003-2005)

- Una segunda resolución del directorio establece que se ha suspendido el cobro de las asignaciones IPv6 a aquellas organizaciones que han cumplido ya el periodo de 2 años, por tiempo indefinido y hasta nuevo aviso.

1.4.6.3 Financiamiento para la Investigación:

El financiamiento de la investigación esta respaldado por el Fondo Regional para la Innovación Digital en America Latina y el Caribe (FRIDA), que es una iniciativa conjunta de LACNIC, el Instituto de Conectividad para las Américas (ICA), El Centro Internacional de Investigación y Desarrollo (IDRC), la y Sociedad de Internet (ISOC).
LACNIC es el administrador del fondo total de $480,000 destinados a proyectos de Tecnologías de Información en América Latina y el Caribe.

1.4.6.4 Actividades de Promoción:

- LAC IPv6 Task Force (Fuerza de Trabajo Ipv6).

Tiene como objetivo fomentar la adopción de IPv6 en la región. Para ello, el LAC IPv6 TF coordina la cooperación entre las distintas partes relacionadas con la adopción de IPv6 en Latinoamérica y el

Caribe, así como actividades de sensibilización, divulgación y educación acerca de IPv6 y tecnologías afines. Es posible visitar el sitio Web a través de la URL: http://www.lac.ipv6tf.org/

- FLIP – 6. (Foro Latinoamericano de Ipv6)

El objetivo del Foro Latinoamericano de IPv6 es intercambiar experiencias obtenidas en la implementación de servicios y aplicaciones basadas en IPv6 en la región. El Tercer Foro se realizó en conjunto durante LACNIC VIII, en Junio del 2005.

- IPV6 TOUR.

Seminario de un día para promoción y divulgación sobre IPv6.

Primera fase en Agosto.
1) 22 Agosto del 2005 Montevideo, Uruguay
2) 26 Agosto del 2005 Buenos Aires, Argentina
3) 28 Agosto del 2005 Santiago, Chile

Segunda Fase en Noviembre
1) Sao Paulo, Brasil
2) Ciudad de México, México

- IPV6 TF DE LACNIC.

Actualmente existen tres grupos de trabajo constituidos en América Latina y el Caribe
1) Cuba. Con el sitio Web: http://www.cu.ipv6tf.org/
2) Brasil. Con el sitio Web: http://www.br.ipv6tf.org/
3) México. Con el sitio Web: http://www.cu.ipv6tf.org/

1.4.6.5 Capacitación y Entrenamiento:

- Tutoriales sobre IPv6.

En el marco de las reuniones de LACNIC se organizan tutoriales orientados a IPv6. En la última reunión LACNIC VIII, realizada del 27 al 30 de Junio del 2005, se lanzaron los siguientes tutoriales.
1) DNSSEC e IPv6 en DNS
2) IPv6 Start – Up

- Anteriores tutoriales

1) IPv6 101
2) Implementación y producción en IPv6

1.4.7 Solicitud de Bloques Ipv6 en LACNIC.

Para solicitar un bloque IPv6 la organización interesada debe llenar un formulario de solicitud y enviarlo después a la dirección de correo hostmaster@lacnic.net. Una vez verificado el formulario sin encontrar ningún error, se genera un número de control que identifica la solicitud.

Una vez aprobada la solicitud de asignación inicial, LACNIC envía un e-mail con información sobre el pago y el acuerdo que deber ser firmado. La asignación solamente será efectiva después de la recepción del pago y del acuerdo firmado.

Las solicitudes de asignación adicional solamente serán completadas en los casos que no hayan pagos ni documentaciones pendientes.

El bloque mínimo asignado por LACNIC es un /32 y para calificar para la asignación inicial, la organización debe:

- Ser un LIR (Registro de Internet Local), o sea, organización que asigna direcciones para usuarios de los servicios de red que provee. Son, en general, los proveedores de acceso (ISP), cuyos clientes son los usuarios finales u otros proveedores de acceso.

- No ser un sitio final (usuario final).

- Documentar un plan detallado sobre los servicios y la conectividad en IPv6 a ofrecer a otras organizaciones (clientes).

- Anunciar en el sistema de rutas inter-dominio de Internet un único bloque, que agregue toda la asignación de direcciones IPv6 recibida, en un plazo no mayor de 12 meses.

- Ofrecer servicios en IPv6 a clientes localizados físicamente en la región del LACNIC en un plazo no mayor de 24 meses.

1.4.7.1 Adjudicaciones adicionales.

LACNIC concede adjudicaciones adicionales, cuando la organización (ISP/LIR) alcanza una alta tasa de utilización del último bloque asignado. La tasa de utilización es calculada en términos de bloques de prefijo /48 asignados a usuarios finales.

Para calcular la tasa de utilización se utiliza la metodología HD-Ratio (RFC3194). Según esta metodología, una tasa de 0.8 es considerada aceptable en términos de utilización de direccionamiento, lo cual justificará la adjudicación adicional.
LACNIC utiliza la información obtenida de su sistema de registro (Servidor WHOIS) para calcular el HD-Ratio.

En caso de que la organización interesada pruebe una buena utilización del espacio anteriormente asignado, según el criterio mencionado, estará habilitada para recibir un nuevo espacio de direccionamiento de tamaño igual al recibido anteriormente.
Siempre que sea posible, el espacio adicional a ser asignado a una organización, será adyacente al último espacio asignado.

El solicitante debe tener claro que existe una tarifa asociada a la renovación del servicio de registro de los recursos asignados por LACNIC.

1.4.7.2 Formulario de Solicitud de Bloques Ipv6.

A continuación se presenta el formato del formulario que se debe utilizar para solicitar un bloque de direcciones Ipv6:

LACNIC IPV6 Template 20040930-1-SP (Esta linea es Fija).

1) Información sobre la organización que esta solicitando el bloque IPv6.
Si la organización ya tiene algún recurso registrado con LACNIC, informar solamente su "ownerID".
Nota: En caso de no saber cual es el "ownerID" consulte algún recurso adjudicado a su organización en el servidor WHOIS de LACNIC [whois://whois.lacnic.net]

a. ID. de la Organización (OwnerID):
b. Nombre de la Organización:

c. Dirección Postal:

d. Ciudad:

e. Estado:

f. País:

g. Código Postal:

2) Puntos de contacto en la organización.

Será necesario informar contacto técnico, de facturación y de membresía. Los contactos de facturación y membresía son internos y por esto no son visibles en las consultas whois. Informar solamente el "userID" de los puntos de contacto. En el caso que los tenga aun, se deben crear en: http://lacnic.net/cgi-bin/lacnic/idmng?lg=SP

a. ID contacto técnico (UserID):

b. ID contacto facturación (UserID):

c. ID contacto membresía (UserID):

3) Brindar información sobre la organización que solicita el bloque IPv6.

a) Información de la Organización:

4) Informar el plan para despliegue de la red IPv6 en la organización, el plan de utilización de las direcciones IPv6 y plan de sub asignaciones de direcciones IPv6 para los clientes.

a. Fecha:

b. Plan de utilización:

c. Plan de Asignación:

5) Brindar información sobre la estructura de la red IPv6 y tipo de servicio que serán ofertado para los clientes.

En el caso que se este solicitando un prefijo mas largo que /32, se debe brindar también información que justifique esta necesidad.

6) Información Adicional:

Final del formulario

1.4.8 Costo por Asignación de Bloque Ipv6.

A continuación se muestran los costos para la asignación de bloques Ipv6.

TAMAÑO DEL BLOQUE	MONTO INICIAL	RENOVACIÓN	RENOVACIÓN 10% BONIFICACIÓN
/32	$ 2,500	$ 2,500	$ 2,250
Mayor>/32	$ 20,000	$ 20,000	$ 18,000

Tabla 1.3 Costos de Asignación de Bloques Ipv6.

Se debe considerar que por el momento para Ipv6 el pago inicial y la primera renovación se encuentran exonerados.

1.5 IPV6 SOBRE INTERNET 2

Internet2 es un proyecto que agrupa un gran número de Universidades y Centros de Investigación a nivel mundial con el objetivo principal de promover las tecnologías de redes de alta velocidad, que contribuyan al desarrollo de las aplicaciones con alta demanda de recursos tecnológicos, requeridas por el sector académico, científico y tecnológico en el ámbito de la cooperación Nacional e Internacional.

El eje de Internet2 es un consorcio formado por aproximadamente 200 Universidades de Estados Unidos con apoyo del gobierno y algunas de las empresas líderes del sector informático y de telecomunicaciones (IBM, Intel Corporation, Cisco Systems, AT & T, Microsoft, Juniper Networks, Lucent Technologies, Qwest Communications, Sun Microsystems, por ejemplo). A este eje se le han incorporado Universidades, Organizaciones no gubernamentales relacionadas con el trabajo de redes y corporaciones interesadas en participar en el proyecto. Los usuarios finales son grupos de investigadores en diversas partes del mundo que desarrollan servicios y aplicaciones que requieren acceso a redes de alta velocidad.

Internet2 es administrada por la Corporacion Universitaria para el Desarrollo de Redes Avanzadas (UCAID), y entre otras características, opera sobre una de las redes de mayor velocidad en el mundo denominada Abilene que puede alcanzar 2,4 Gigabits por segundo, recientemente fue actualizada a 10 Gigabits por segundo.

La red de Internet 2 se encuentra basada sobre el protocolo Ipv6, el cual agrega características importantes para la eficiencia de la misma. Internet2 no pretende reemplazar a la Internet actual, ni

tampoco se ha propuesto como principal objetivo construir una infraestructura paralela. Los participantes tienen enlaces al Internet tradicional para servicios como la web, noticias, correo electrónico y similares. La meta del proyecto es unir a las instituciones académicas, científicas y tecnológicas nacionales y regionales con los recursos necesarios para desarrollar nuevas tecnologías y aplicaciones, que serán las utilizadas en la futura Internet.

1.5.1 Objetivos Principales de Internet2

- Promover el desarrollo de redes de altas prestaciones (de altas velocidades, baja latencia, con enlaces de gran capacidad, calidad de servicio, seguridad, etc.) y ponerlas al servicio de la comunidad científica y de investigación.

- Facilitar el desarrollo de aplicaciones avanzadas con alta demanda de recursos.

- Asegurar la transferencia rápida de los nuevos servicios, tecnologías y aplicaciones a la comunidad Internet.

1.5.2 Aplicaciones Sobre Internet2:

- Video-conferencia de alta velocidad.

- Telemedicina. La distribución de datos con garantía de calidad de servicio (QoS) y la transmisión de imágenes en alta resolución, pilares de la llamada medicina remota o telemedicina. Además, los resultados de búsquedas en grandes bases de datos en línea permitirán al médico comparar imágenes, historiales y otras opiniones para hacer un diagnóstico altamente fiable.

- Computación en gran escala con procesos de bases de datos en múltiples sitios. Integración de diversos recursos de computación independientes, generalmente heterogéneos y distribuidos geográficamente a través de un middleware (software que traduce la información de una compañía a un formato entendible por otra empresa diferente), para brindar capacidad de cómputo y almacenamiento a gran escala, de forma transparente para el usuario.

- Ambientes de colaboración interactiva en los que se pueda intercambiar información con otros sin las barreras de las distancias. Por ejemplo: investigación e instrucción interactiva basada en redes.

- Enrutamiento Multidifusion (Multicast), el cual se puede explicar de la siguiente manera: si hay 6 usuarios que desean ver una videoconferencia que se estuviera mandando por Internet, ocurriría que los datos tendrían que salir 6 veces desde el servidor, y esto se multiplicaría hacia otros usuarios, es decir se estaría multiplicando la cantidad de veces que se manda el evento por usuario que lo quiera ver. En cambio por medio del multicast se enviaría una sola vez desde el servidor y se iría distribuyendo por la ruta que lo lleva a cada usuario, sin duplicar la información sobre el mismo camino, de esta forma se aprovecha mejor la red. Con esto se demuestra que no sólo es importante el ancho de banda de Internet2, sino también que es necesario una utilización más eficiente de este ancho de banda con la finalidad de no saturarlo de inmediato.

- Teleinmersión, la cual permite a participantes geográficamente distantes compartir un entorno virtual que recrea su ambiente real, e interactuar en tiempo real. La teleinmersión tiene gran aplicación en entornos académicos y científicos pues permite el trabajo en grupos.

- Aplicaciones que requieran comunicación a muy alta velocidad entre computadores, con garantía de Calidad de Servicio (QoS).

- Aplicaciones que requieran interacción hombre-computadora en tiempo real.

- Modelos en tiempo real basados en sensores. Acceso a recursos remotos, como telescopios o microscopios.

- Transmisión de imágenes de alta resolución.

- Laboratorios virtuales.

- Bibliotecas digitales.

1.5.3 Estructura de Internet2.

La red de Internet2 esta formada por varias redes de alta velocidad, que representan los backbones principales de los continentes o países mas desarrollados. Estas redes se caracterizan por ser de alto rendimiento para la investigación y el desarrollo de aplicaciones. Al mismo tiempo se están desarrollando proyectos para la interconexión entre las grandes redes ya existentes.
A continuación se describen las redes y proyectos más importantes que forman parte de Internet2.

1.5.3.1 Red ABELINE.

Abilene es un backbone que posee tecnología avanzada que representa el soporte para el desarrollo y expansión de las nuevas aplicaciones que se desarrollan dentro de la comunidad de Internet2.
Abilene conecta los puntos de agregación de red regionales, llamados GigaPoPs, para soportar el trabajo de las Universidades miembros de Internet2, ya que ellas desarrollan aplicaciones avanzadas de Internet. Abilene complementa a otras redes de investigación de alto rendimiento.

Los conectores de Abilene son instituciones educativas y de investigación que se conectan directamente con la red de Abilene. Los conectores de Abilene pueden ser GigaPoPs, Universidades, miembros del afiliado u otras redes regionales.
GigaPoPs son puntos regionales de agregación de la red formados por las universidades de Internet2 para conectar con una variedad de redes de alto rendimiento, y otros tipos de redes.

La red de Abilene apoya el desarrollo de usos tales como laboratorios virtuales, bibliotecas digitales, educación de la distancia y tele-inmersión. La red de Abilene se ha desarrollado en sociedad con Internet2, Qwest Comunications, Cisco Systems, Nortel Network y la Universidad de Indiana.
Hasta la fecha la red ya ha experimentando un incremento de velocidad de 2.5 Gigabits/sec a 10 Gigabits/sec.

A continuación se muestra el diagrama de la red Abilene.

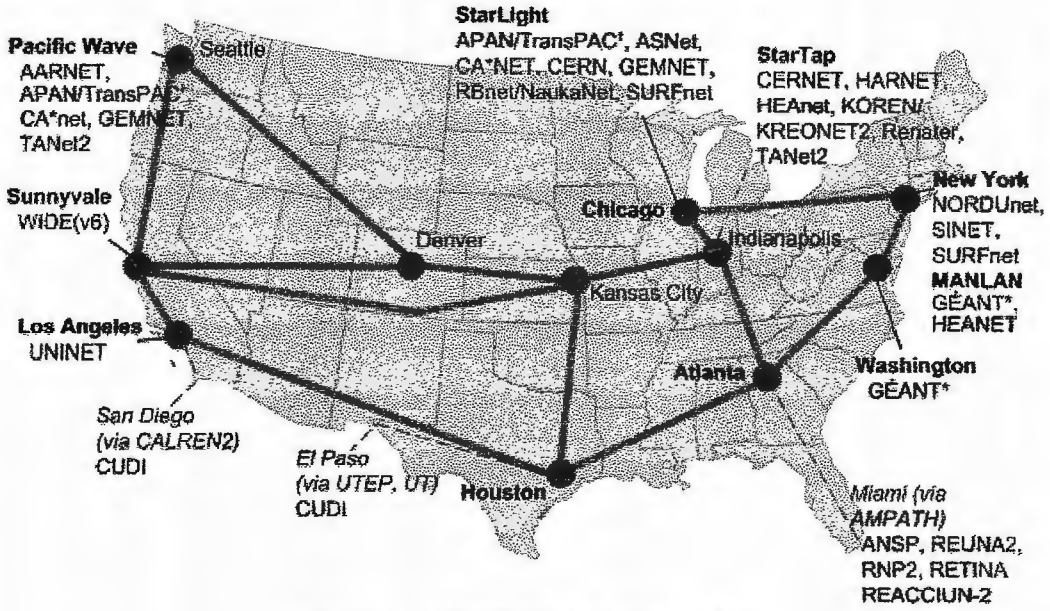


Figura 1.4 Diagrama de la Red Abilene

1.5.3.2 Red GEANT (Red Europea Multi-Gigabit)

GEANT proporciona la capacidad más alta y ofrece la cobertura geográfica más grande de cualquier red de su clase en el mundo.

GEANT es un proyecto de colaboración entre 28 redes nacionales de educación e investigación, que representan a 30 países en Europa. Su principal propósito ha sido el desarrollo de una red multi-gigabit de comunicación de datos paneuropea reservada específicamente para uso de la investigación y la educación. El proyecto también cubre otras actividades relacionadas con la investigación en el área de redes: pruebas en redes, desarrollo de nuevas tecnologías y apoyo a otros proyectos relacionados con el área de redes.

GEANT ha estado en funcionamiento desde diciembre de 2001. Nueve redes operan a velocidades de 10 Gbps y 11 operan a 2,5 Gbps.

A continuación se muestra el diagrama de conexión de la red GEANT en Europa.

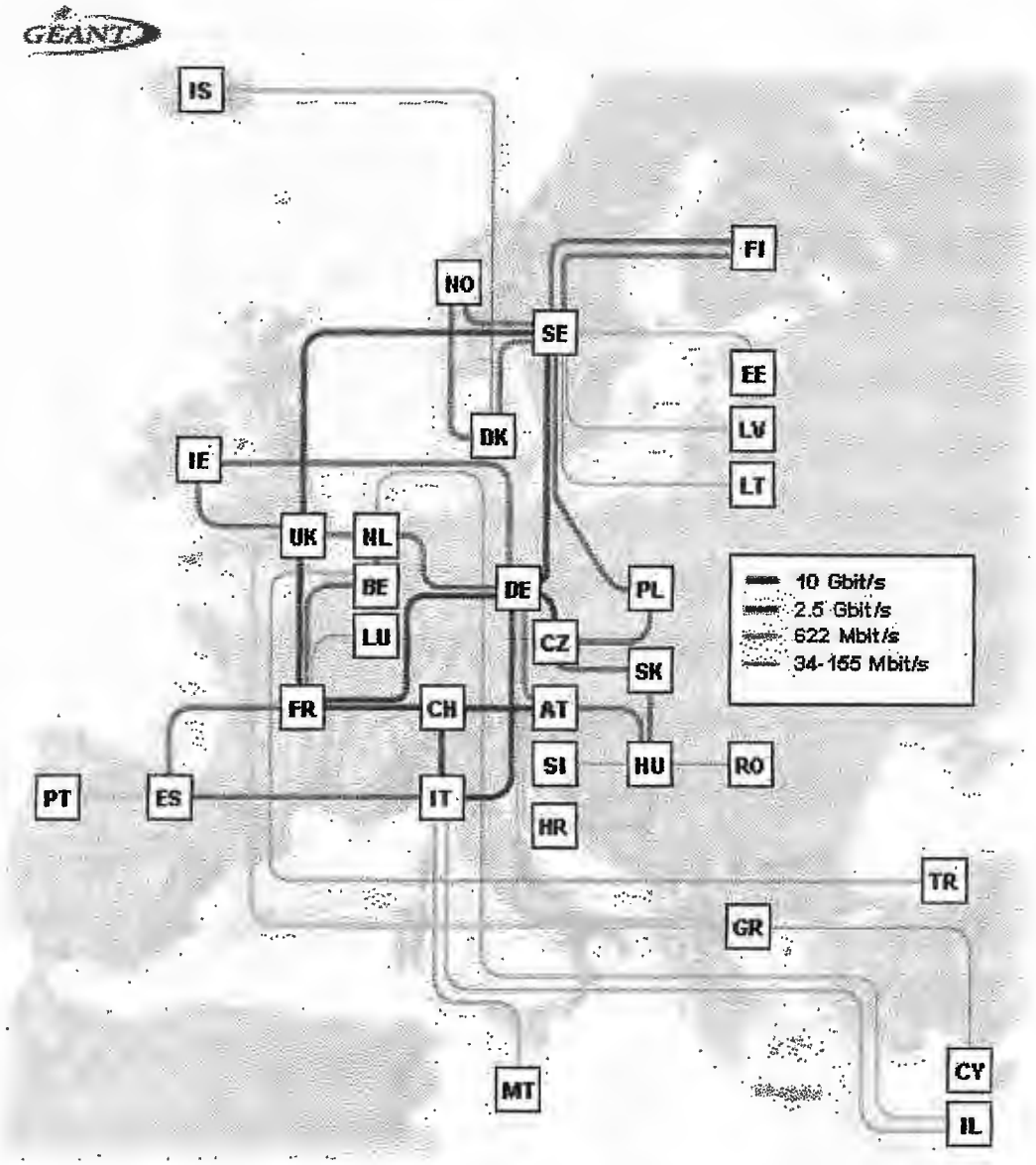


Figura 1.5. Diagrama de la Red GEANT en Europa.

1.5.3.3 Red AmericasPATH (AMPATH)

La red de AmericasPATH (AMPATH) es un proyecto de La Universidad Internacional de Florida (FIU) en colaboración con GC (Global Crossing). Utilizando la red terrestre y de fibra óptica submarina de GC, AMPATH interconectará las redes de educación e investigación en el sur y América Central, el Caribe y México a las redes de investigación y educación de los EEUU y fuera de los EEUU vía la red Abilene de Internet2.

AMPATH utiliza las redes de fibra óptica submarina y terrestre de Global Crossing para interconectar las redes de investigación y educación de cada país participante, a las redes de Internet2 en los EEUU y otros países. FIU mantiene y administra el proyecto AMPATH y ofrecerá soluciones económicas para anchos de banda y servicios operativos.

El propósito del proyecto de AMPATH es permitir que los países que participan contribuyan a la investigación y al desarrollo de las aplicaciones para el adelanto de tecnologías Internet. El proyecto de AMPATH intenta avanzar la meta del proyecto Internet2 de animar y de permitir el desarrollo de las aplicaciones avanzadas de la red. La misión de AMPATH es servir como el camino para el establecimiento de una red de investigación y educación en las Américas y al mundo.

A continuación se muestra el diagrama de conexión de la red AMPATH.

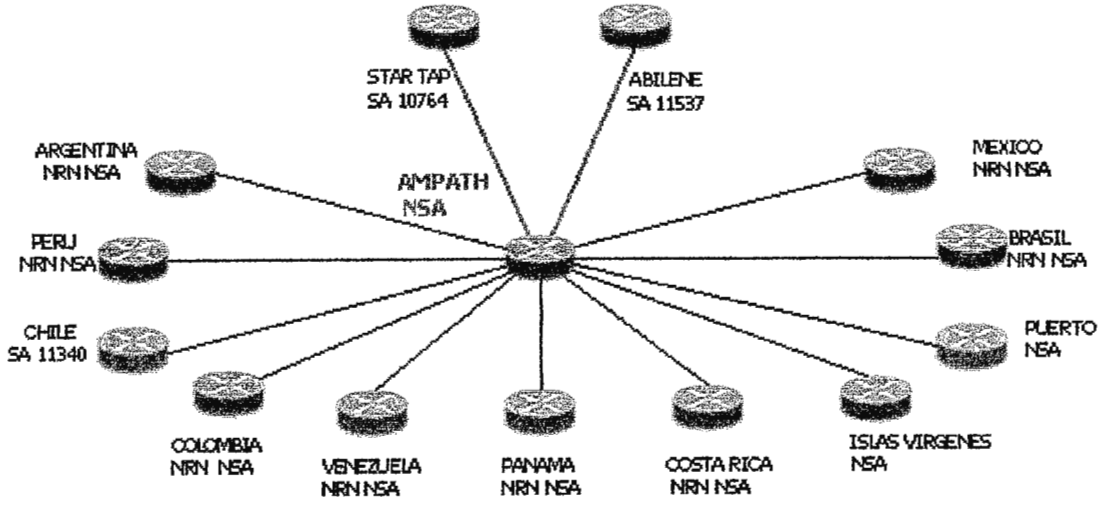


Figura 1.6 Díagrama de Red AMPATH.

1.5.3.4 Proyecto ALICE (América Latina Interconectada Con Europa).

El proyecto ALICE se ha establecido para crear una infraestructura de redes de investigación utilizando el protocolo IP dentro de América Latina y su interconexión con Europa. ALICE se enmarca dentro de las acciones que forman parte del programa Alianza para la Sociedad de la Información (@LIS), que es un programa de cooperación con Latinoamérica, cuyo objetivo es promocionar la Sociedad de la Información y combatir la brecha digital existente en Latinoamérica.

@LIS proporcionará la infraestructura necesaria a través del financiamiento del proyecto ALICE, apoyando con ello la creación de una infraestructura de redes de investigación en América Latina y su enlace con la red de investigación paneuropea GEANT.

La coordinación del proyecto ALICE corre a cargo de DANTE (Tecnología de Red Avanzada para Europa), una organización sin fines de lucro domiciliada en el Reino Unido, que se creo en 1993 con el fin de organizar los servicios internacionales de redes avanzadas para la comunidad de investigación y académica europea. En la actualidad, la principal función de DANTE es gestionar el funcionamiento de la red de investigación paneuropea GEANT.

Para el proyecto ALICE, DANTE se ha asociado con 4 NREN europeas que tienen un estrecho vínculo histórico y social con Latinoamérica. Se trata RENATER (Francia), GARR (Italia), FCCN (Portugal) y RedIRIS (España).
En Latinoamérica y el Caribe, ALICE se ha asociado con las NREN de 18 países que están agrupadas en CLARA.
La Comisión Europea respalda el proyecto ALICE de forma activa, además de financiarlo con 10 millones de euros que constituyen el 80% de la financiación del proyecto.

El proyecto ALICE durará hasta abril de 2006, tras el cual la organización CLARA, Cooperación Latinoamericana de Redes Avanzadas, garantizará la sostenibilidad de la red intra-regional y la continuación de su conexión.

Los socios del proyecto ALICE se muestran en la siguiente tabla.

DANTE	Coordinador, UK	http://www.dante.net
CLARA	LA	http://www.redclara.org/
RETINA	Argentina	http://www.retina.ar
BolNet	Bolivia	http://www.bolnet.bo
RNP	Brasil	http://www.rnp.br
REUNA	Chile	http://www.reuna.cl
Univ. del Cauca	Colombia	http://www.ucauca.edu.co/
Crnet	Costa Rica	http://www.crnet.cr
RedUniv	Cuba	http://www.mes.edu.cu/
FUNDACyT	Ecuador	http://www.reicyt.org.ec
RAICES	El Salvador	http://www.raices.org.sv
RAGIE	Guatemala	http://www.ragie.org.gt
UNITEC	Honduras	http://www.unitec.edu
CUDI	México	http://www.cudi.edu.mx
UNA	Nicaragua	http://www.unan.edu.ni/
RedCyT	Panamá	http://www.redcyt.org.pa
ARANDU	Paraguay	http://www.arandu.net.py/id19.htm
RAP	Perú	http://www.rap.org.pe
RAU	Uruguay	http://www.rau.edu.uy
REACCIUN	Venezuela	http://www.reacciun.ve
RENATER	Francia	http://www.renater.fr
GARR	Italia	http://www.garr.it
FCCN	Portugal	http://www.fccn.pt
RedIRIS	España	http://www.rdiris.es

Tabla 1.4 Instituciones Asociadas al Proyecto ALICE

1.5.3.5 Red APAN (Asia-Pacific Advanced Network).

Es un consorcio internacional, sin fines de lucro, establecido el 3 de Junio de 1997. APAN conforma una red de alto rendimiento para la investigación y el desarrollo en aplicaciones y servicios avanzados, que

enlaza a varios de los países de la región asiática. Los miembros primarios son: Australia, Japón, Corea, Singapur y USA (Universidad de Indiana), los miembros asociados: Malasia y China.

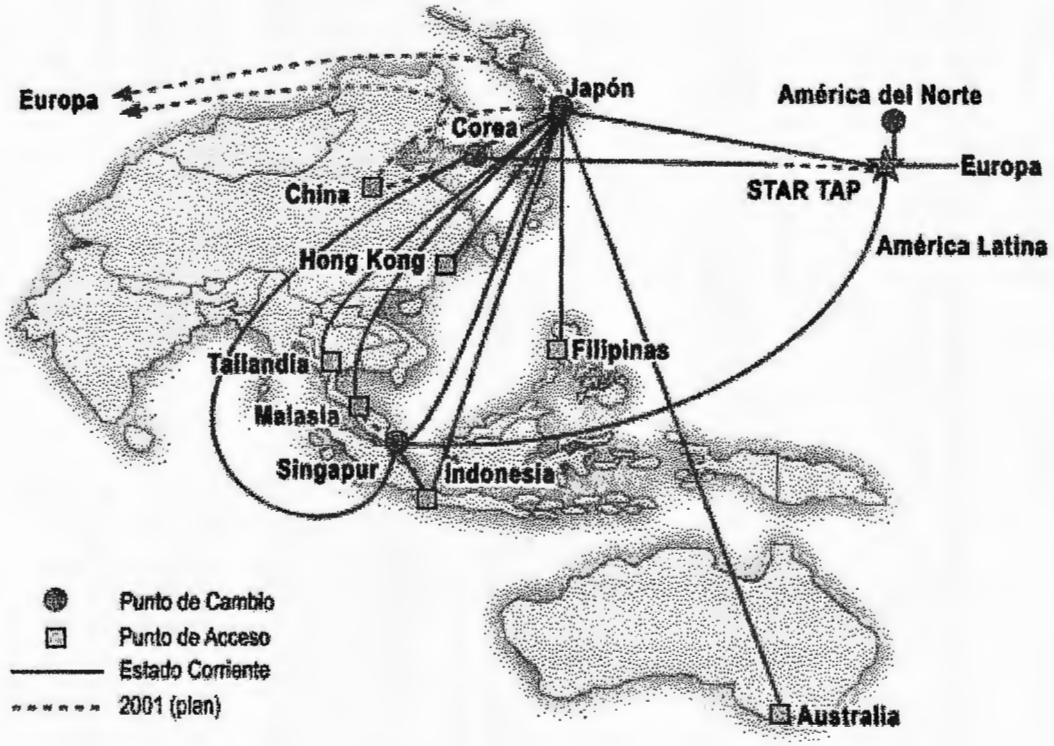


Figura 1.7 Estructura de la Red APAN

1.5.3.6 CANARIE (Desarrollo Avanzado de Internet en Canada).

Es la organización Canadiense para el desarrollo de la Internet avanzada. Fue establecida en 1993 y ha trabajado con el gobierno, la industria y las comunidades de investigación y educación para realzar la infraestructura canadiense de Internet, el desarrollo de aplicaciones y su uso. Es una organización privada, sin fines de lucro, apoyada por la industria de Canadá.

CANARIE fundó en 1994 la National Test Network, una de las redes ATM más extensas del mundo, que en 1997 se transformó en CANetII, una red de nueva generación para ser usada por los miembros del consorcio.

CANet II fue la primera red Internet Óptica basada en Multicanalización por División de Longitud Onda (tecnología capaz de aumentar en más de dos órdenes de magnitud el ancho de banda de un solo hilo de fibra óptica y mejorar el medio físico de transmisión), que luego, en 1998, se transformó en Ca*Net3, la red nacional que interconecta a las Universidades y Centros de Investigación de Canadá, y que a partir del 2002 pasa a llamarse CANet4.

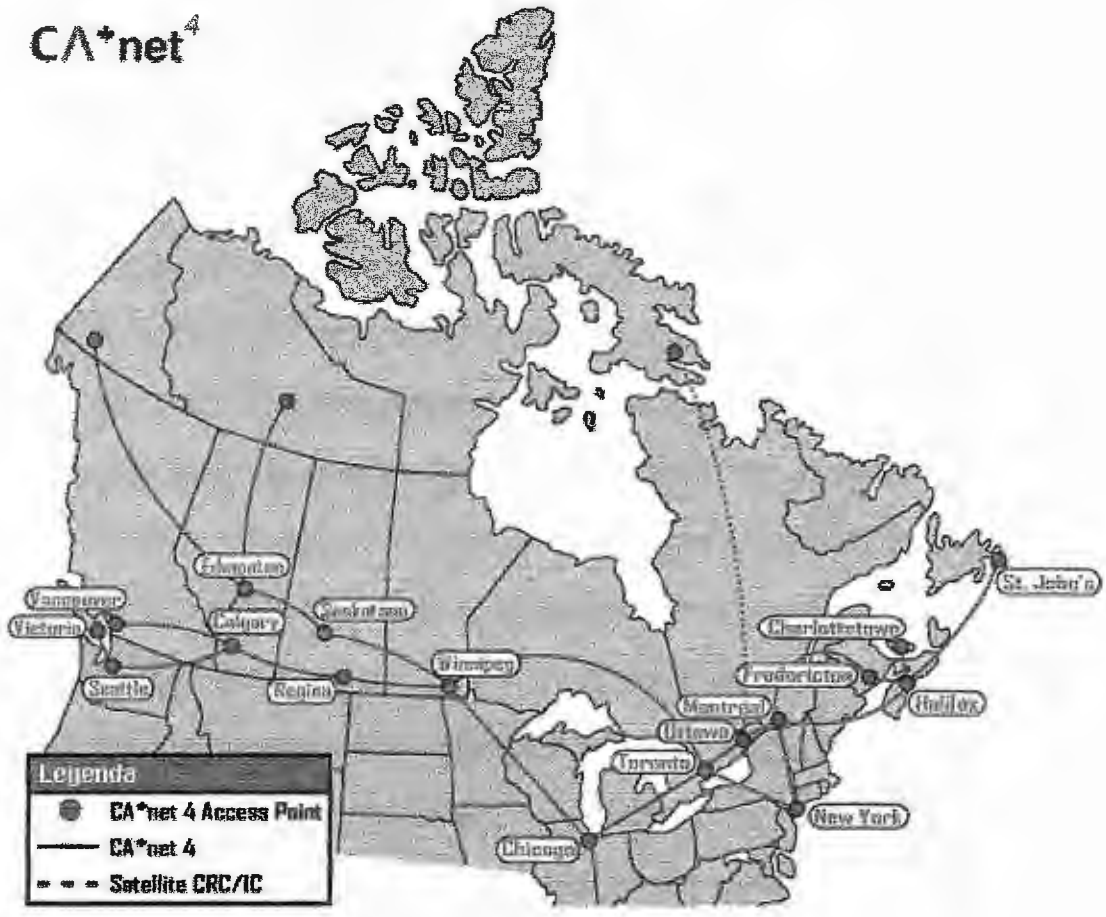


Figura 1.8 Estructura de la Red CANARIE.

CA*Net4 es la red Internet2 de Canadá, que interconecta redes de alta velocidad de cada una de las provincias canadienses en backbones de fibra óptica a lo largo y ancho de ese país. Fue lanzada en el 2002 con un presupuesto de 110 millones de dólares y constituye una de las redes de investigación más importantes que existen en la actualidad.

1.5.3.7 CLARA (Cooperación Latinoamericana de Redes Avanzadas)

CLARA, la Cooperación Latinoamericana de Redes Avanzadas, es una asociación sin fines de lucro registrada en Montevideo, Uruguay. Fue creada por 16 Redes Nacionales de Investigación y Educación Latinoamericanas, las cuales se muestran a continuación:

Univ. de Cauca (Colombia)
RAP (Perú)
RNP (Brasil)
RAGIE (Guatemala)
RETINA (Argentina)
REACCIUN (Venezuela)
BolNet (Bolivia)
RedUniv (Cuba)
REUNA (Chile)
RedCyT (Panamá)
Crnet (Costa Rica)
RAU (Uruguay)
RAICES (El Salvador)
UNITEC (Honduras)
Arandu (Paraguay)
CUDI (México)
REICyT (Ecuador)
RENIA(Nicaragua)

La red de Red CLARA y su conexión a GÉANT (Europa) fueron ejecutadas por el proyecto ALICE, América Latina Interconectada Con Europa. La meta de ALICE es proveer conexiones de Internet dedicadas para las comunidades de investigación y educación de la región latinoamericana, hacia Europa. El proyecto está financiado hasta mayo del 2006 con 10 Millones de Euros aportados por el Programa @LIS de Cooperación de la Comisión Europea, que persigue promover la Sociedad de la Información en la región.

La siguiente figura muestra la estructura de la red CLARA a lo largo de Latinoamérica y el Caribe.

Figura 1.9 Estructura de la Red Clara.

1.6 REGISTROS DE INTERNET.

Un organización conocida como RI o Registro de Internet, es aquella que tiene la responsabilidad de administrar globalmente los recursos de Internet; ya sea direcciones IP, nombres de dominios, servidores raiz,etc.

Como ejemplo de RI se pueden mencionar a dos instituciones:

- **ICANN:** Internet Corporation for Assigned Names and Numbers o Corporación de Internet para Nombres y Números Asignados. Es una organización sin fines de lucro que asume la responsabilidad de alojar los espacios para las direcciones IP, asignar parámetros protocolares,

administrar los sistemas de nombres de dominio y administrar los servidores raíz. Fue creada por Jon Postel, en 1998, en respuesta a un pedido iniciado por el Departamento de Comercio de los Estados Unidos. Este pedido solicitaba la formación de un ente privado sin fines de lucro que administrara las políticas del sistema de nombres y direcciones de Internet.

- **IANA:** Internet Assigned Numbers Authority o Autoridad de Números Asignados en Internet. Es una organización que trabaja bajo la supervision del Internet Architecture Board (IAB), responsable de asignar las nuevas direcciones de IP de Internet.

1.6.1 Registros Regionales de Internet (RIR).

Instituciones encargadas de distribuir y administrar el espacio de direcciones público de Internet dentro grandes regiones geográficas. Actualmente existen cinco Registros Regionales de Internet, los cuales están bajo la supervisión de la IANA.
Estos son:

- ARIN: Registro Americano para los Números de Internet.
- APNIC: Centro de Información de Red de Asia y el Pacifico.
- RIPE: Centro de Coordinación de Redes para Europa.
- LACNIC: Registro de Direcciones de Internet para América Latina y el Caribe.
- AFRINIC: Registro de direcciones Ip de Internet para África.

1.6.2 Registros Nacionales de Internet (NIR).

Instituciones encargadas de asignar espacios de direcciones Ip a sus miembros, que por lo general son Proveedores de Servicios de Internet (ISP) a nivel nacional. También se encarga de asignar espacios de direcciones Ip a usuarios finales. Los NIR existen mayormente en Asia Pacifico; en Latinoamérica son México y Brasil.

1.6.3 Registros Locales de Internet/Proveedores de Servicios de Internet (LIR/ISP).

Institución encargada de asignar espacios de direcciones a los usuarios de sus servicios de red. Por lo general son ISPs cuyos clientes son usuarios finales u otros ISPs. Ejemplo: Telmex, Telgua, Telecom, etc.

A continuación se muestra una grafica que muestra la distribución jerárquica de los diferentes Registros de Internet, ya sean Nacionales, Locales o Regionales.

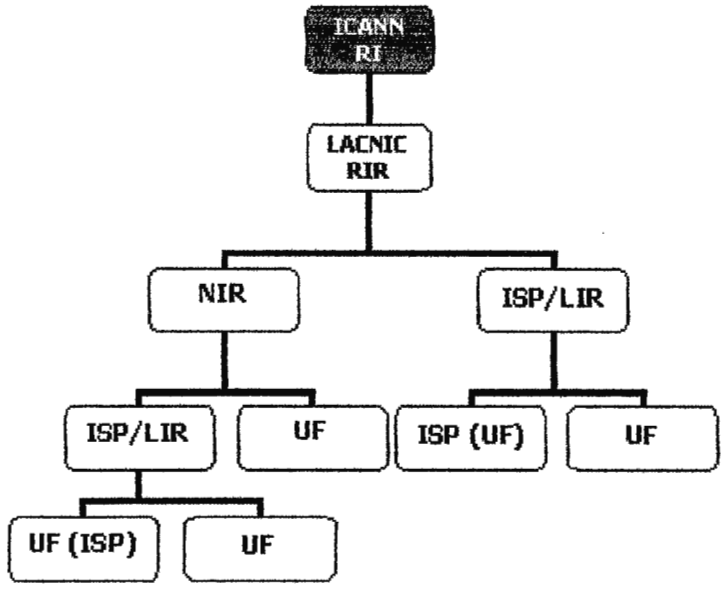


Figura 1.10. Diagrama Jerárquico de los Registros de Internet.

1.7 DIRECCIONES IPV6 GLOBALES ASIGNADAS HASTA LA FECHA.

La siguiente tabla muestra una lista de direcciones Globales Unicast Ipv6 que ya han sido asignadas a los Registros Regionales de Internet para su administración dentro de su área y además se presenta la fecha en que fueron asignadas.

PREFIJO GLOBAL UNICAST	INSTITUCION	FECHA
2001:0000::/23	IANA	01/Jul/99 Nota(1)
2001:0200::/23	APNIC	01/Jul/99
2001:0400::/23	ARIN	01/Jul/99
2001:0600::/23	RIPE NCC	01/Jul/99
2001:0800::/23	RIPE NCC	01/May/02
2001:0A00::/23	RIPE NCC	02/Nov/02
2001:0C00::/23	APNIC	01/May/02 Nota(2)
2001:0E00::/23	APNIC	01/Ene/03
2001:1200::/23	LACNIC	01/Nov/02
2001:1400::/23	RIPE NCC	01/Feb/03
2001:1600::/23	RIPE NCC	01/Jul/03
2001:1800::/23	ARIN	01/Abr/03

2001:1A00::/23	RIPE NCC	01/Jun/04
2001:1C00::/22	RIPE NCC	01/May/04
2001:2000::/20	RIPE NCC	01/May/04
2001:3000::/21	RIPE NCC	01/May/04
2001:3800::/22	RIPE NCC	01/May/04
2001:3C00::/22	RESERVADO	11/Jun/04 Nota(3)
2001:4000::/23	RIPE NCC	11/Jun/04
2001:4200::/23	ARIN	01/Jun/04
2001:4400::/23	APNIC	11/Jun/04
2001:4600::/23	RIPE NCC	17/Ago/04
2001:4800::/23	ARIN	24/Ago/04
2001:4A00::/23	RIPE NCC	15/Oct/04
2001:4C00::/23	RIPE NCC	17/Dic/04
2001:5000::/20	RIPE NCC	10 Sep 04
2001:8000::/19	APNIC	30 Nov 04
2001:A000::/20	APNIC	30 Nov 04
2002:0000::/16	6T04	01 Feb 01 Nota(4)
2003:0000::/18	RIPE NCC	12 Jan 05
2400:0000::/19	APNIC	20 May 05
2400:2000::/19	APNIC	08 Jul 05
2600:0000::/22	ARIN	19 Apr 05
2604:0000::/22	ARIN	19 Apr 05
2608:0000::/22	ARIN	19 Apr 05
2606:0000::/22	ARIN	19 Apr 05
2A00:0000::/21	RIPE NCC	19 Apr 05
2A01:0000::/23	RIPE NCC	14 Jul 05
3FF3:0000::/16	6BONE	01 Dec 98 Nota(5)

Tabla 1.5. Direcciones Globales Unicast Ipv6 Asignadas a RIR`s.

El espacio de las direcciones Unicast Asignables esta definido en el RFC3513, el bloque esta definido por el prefijo 2000::/3. Todo el espacio no listado en la tabla anterior esta reservado para futuras asignaciones.

Nota 1: El prefijo 2001:0000::/23 esta asignado a IANA y es para propósitos de prueba y experimentación de la misma (RFC2928).

Nota 2: El prefijo 2001:0DB8::/32 ha sido asignado como un rango no ruteable para ser utilizado con propósitos de documentación.

Nota 3: El prefijo 2001:3C00::/22 esta reservado para posibles asignaciones futuras al RIPE NCC.

Nota 4: El prefijo 2002::/16 esta reservado para el desarrollo de túneles 6to4 (RFC3056).

Nota 5: El prefijo 3FFE::/16 es una asignación experimental al 6Bone (RFC2471). El prefijo será retornado al bloque de direcciones no utilizadas el 6 de Junio del 2006 (RFC3701).

1.8 ESTANDARES PROBADOS PARA IPV6.

Hasta el momento se ha probado el funcionamiento y la operabilidad de diferentes dispositivos y software con soporte para Ipv6. Para la realización de estas pruebas se necesita seguir un estandar que especifica el tipo de caracteristicas que deben ser evaluadas en los equipos.

1.8.1 Tipos de Pruebas Realizadas.

Principales.

- Interoperabilidad: Es la posibilidad que posee el sistema de proveer servicios y aceptar los servicios de otro sistema heterogeneo y de esta manera operar juntos efectivamente.

- Conformidad: Determina si una pieza en particular del sistema satisface el criterio especificado en un documento de control.

Soporte.

- Funcionamiento: Es la evaluacion de la calidad, que usualmente se cuantifica con un valor especifico el cual caracteriza un aspecto especial, capacidad o atributos de un sistema. Ejemplo: El retardo, paquetes perdidos, tiempo de falla, etc.

- Simulación: Crear el ambinete necesario para evaluar el funcionamiento del sistema como si fuera en la realidad.

- Robustez: Probar la resistencia y consistencia del sistema ante situaciones adversas.

1.8.2 Estandares de Ipv6 Probados.

Nucleo Ipv6. (Core)

- Especificación de Ipv6. (RFC2460)
- Descubrimiento de vecinos para Ipv6. (RFC2461)

- Autoconfiguracion de direccion sin estado en Ipv6. (RFC2462)
- Protocolo de Mensajes de control de Internet. (RFC2463)
- Descubrimiento de ruta MTU para Ipv6. (RFC1981)
- Arquitectura de direccionamiento Ipv6. (RFC3513)
- Transmisión de paquetes Ipv6 sobre redes Ethernet. (RFC2464)
- Ipv6 sobre PPP. (RFC2472)

Enrutamiento Ipv6.

- RIPng. (RFC2080)
- BGP4+. (RFC2545)
- OSPFv3. (RFC2740)
- Opciones de alerta de Router en opciones de salto. (RFC2711)
- Renumeracion de Router. (RFC2894)

IPSecurity (Seguridad IP).

- Arquitectura de seguridad para el protocolo de Internet. (RFC3168)
- IPSec AH. (RFC2402)
- IPSec ESP. (RFC2406)
- RADIUS e IPV6. (RFC3162)
- Utilizando IPSec para proteger la Señalización Ipv6 de Seguridad entre nodos moviles y agentes de casa. (RFC3776)

Movilidad.

- Soporte para Movilidad en Ipv6 MIPv6. (RFC3775)
- Usando IPSec para proteger la señalización Ipv6 movil entre nodos moviles y agentes de casa. (RFC3776)
- Administración de Movilidad Ipv6 Jerarquica.
- Requerimientos de Soluciones de Calidad de Servicio (QoS) para Ip movil. (RFC3583)
- Tuneles para Ipv6. (RFC2473)

Multicast.

- Selección de la ruta de origen para el protocolo MLD (Multicast Listener Discovery. (RFC3590)
- MIB (Magnament Information Base) Ipv6 para MLD. (RFC3019)
- Source Especific Mutlticast (Multicast de Origen Especifico) SSM. (RFC3569)
- Soporte de Movilidad en Ipv6 MIPv6. (RFC3775)
- MLDv2 para Ipv6. (RFC3810)

Mecanismos de transición.

- Túneles sobre Ipv6. (RFC2473)
- Transmisión de Ipv6 sobre dominios Ipv4 sin túneles explícitos. (RFC2529)
- Mecanismos de transición para host Ipv6 y Routers. (RFC2893)
- Conexión de Dominios Ipv6 a traves de nubes Ipv4. (RFC3056)
- Extensiones DNS para Soportar Ipv6. (RFC3596)

Calidad de Servicio.

- Funcionamiento del campo tipo de Trafico. (RFC2474)
- Adicion de la Notificación de Congestion Explicita para Ip. (RFC3168)
- Compresión de los Encabezados Ipv6 base y de Extensión, Encabezados Ipv4, Encabezados TCP y UDP. Encapsulacion de encabezados Ipv4 e Ipv6. (RFC2507)
- Compresión del encabezado IP/UDP/RTP. (RFC2508)
- Agregación RSVP. (RFC3175)
- Especificación del Etiquetado de Flujo Ipv6. (RFC3697)
- Requerimientos de Soluciones de Calidad de Servicio (QoS) para Ip movil. (RFC3583).

DHCPv6 (Protocolo de Configuración Dinamica de Host).

- Protocolo de Configuración Dinamica de Host para Ipv6. (RFC3315)
- Opciones de Prefijo Ipv6 para DHCPv6. (RFC3633)
- Opciones de Configuración DNS para DHCPv6. (RFC3646)
- Servicio sin estado de DHCPv6. (RFC3736)

- Opciones DHCP para Servidores SIP (Session Initiation Protocol). (RFC3319)
- Opciones de Configuración del Servicio de Información de la Red para DHCPv6. (RFC3898)
- Opciones de Configuración de Tiempo para DHCPv6.

1.8.3 Eventos de Prueba Realizados para Ipv6.

A continuación se muestra una tabla que contiene información sobre las pruebas de interoperabilidad realizadas para Ipv6. Ademas se muestran los organizadores de los eventos y las fechas de los mismos.

EVENTO	RESPONSABLE	URL	RECIENTE	FUTUROS
IPv6 Plugtests 	ETSI	http://www.etsi.org/plugtests/Ipv6.htm	5º. Encuentro Ipv6 Plugtests Octubre del 2004. Cannes Francia	6º. Encuentro Ipv6 Plugtests 17-21 Octubre del 2005. Sophia Antiopolis, Francia
Evento de Prueba de Interoperabilidad Ipv6 	TAHI	http://www.tahi.org/	6º. Evento de Prueba de Interoperabilidad de TAHI Ipv6. Enero del 2005. Chiba, Japon.	Enero del 2006, Japon.
Proyecto Moonv6 	Laboratorio de la Universidad New Hampshire	http://moonv6.sr.unh.edu/	3º. Fase, Noviembre del 2004	4º. Fase No Definida.

Tabla 1.6 Preubas realizadas con Ipv6.

CAPITULO 2

Atributos de IPv6

2. ATRIBUTOS DE IPV6.

2.1 DEFINICION DE IPV4

La comunicación entre las redes de computadoras es posible a través de un protocolo conocido como IP (Protocolo de Internet). Ipv4 es la versión 4 del Protocolo IP y fue la primera versión del protocolo que se implemento extensamente, y forma las bases para la actual Internet.
IPv4 usa direcciones de 32 bits, limitándose a 4,294,967,296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs).
Ipv4 es la base actual de la comunicación IP; pero posee algunas limitaciones en cuanto a las exigencias de las redes contemporáneas, como:

- Inminente saturación del espacio de direcciones.
- La seguridad es opcional, ya que IPv4 no fue diseñado para ser seguro en un principio. Las aplicaciones de seguridad surgieron posteriormente.
- El encabezado de trama para el protocolo Ipv4 posee pocos bits para establecer la calidad de servicio.

Una de las limitaciones más importantes es la escasez de las direcciones IP, de este modo:

- Existen menos direcciones disponibles.
- Limita el crecimiento del Internet.
- Obstaculiza el uso de Internet a nuevos usuarios.
- Hace necesario el uso del NAT (Network Address Traslation).

2.2 DEFINICION DE IPV6

En 1992, el IETF llegó a la conclusión de que haría falta un sustituto del IPv4 y formó un grupo de trabajo con el nombre de Protocolo de Nueva Generacion, que tendría la misión de desarrollar la siguiente generación del protocolo IP.
De esta manera, en 1994 , el RFC 1752 "Recomendación para la Nueva Generacion de IP" se convirtió en un estándar para el sucesor de Ipv4, que fue llamado Ipng conocido actualmente como IPv6

(Internet Protocol Version 6). IPv6 posee mejores características en comparación con Ipv4. Esta es otra de las razones que despiertan interés para su implementación

2.2.1 Características de Ipv6.

El protocolo Ipv6 incorpora nuevas características con respecto a su predecesor Ipv4 entre las cuales podemos mencionar son:

Nuevo Formato de Encabezado:

El encabezado de Ipv6 presenta un nuevo formato diseñado para que la carga de trabajo del encabezado sea mínima. Para ello, se mueven los campos de opciones y los que no son esenciales, hacia encabezados de extensión que se colocan tras el encabezado de Ipv6. El encabezado optimizado de Ipv6 proporciona un procesamiento más eficiente en los routers intermedios.

Gran Espacio de Direcciones:

Ipv6 tiene direcciones Ip de origen y destino de 128 bits (16 bytes). Con 128 bits se pueden expresar más de 1000 millones de combinaciones posibles, el gran espacio de direcciones Ipv6 se ha diseñado para permitir varios niveles de subredes y asignaciones de redes de la red troncal de Internet a las subredes individuales de una organización.
Aunque actualmente solo se asigna un pequeño numero de las direcciones posibles para los host, hay muchas direcciones disponibles para uso en el futuro. Con un numero de direcciones disponibles mucho mayor, dejan de ser necesarias las técnicas de conservación de direcciones, como la distribución de NAT.

Direccionamiento Jerárquico e Infraestructura de enrutamiento eficientes:

Las direcciones globales de Ipv6 utilizadas en la parte Ipv6 de Internet están diseñadas para crear una infraestructura de enrutamiento jerárquica eficiente que se puede resumir, basada en la aparición de múltiples niveles de proveedores de servicios de Internet. En Internet Ipv6, los routers troncales tienen tablas de enrutamiento mucho más pequeñas.

Configuración de direcciones sin estado y con estado:

Para simplificar la configuración de hosts, Ipv6 permite la configuración de direcciones con estado, como la configuración de direcciones en presencia de un servidor DHCP, y la configuración de direcciones sin estado (configuración de direcciones en ausencia de un servidor DHCP).
Con una configuración de direcciones sin estado, los host de un vinculo se configuran automáticamente con direcciones Ipv6 para el vinculo (que se denominan direcciones de enlace local) y con direcciones derivadas de prefijos anunciados por routers locales. Incluso en ausencia de un router, los host del mismo vínculo pueden configurarse automáticamente con direcciones de enlace local y se comunican sin configuración manual.

Seguridad Integrada:

La compatibilidad con IPSec es un requisito del conjunto de protocolos Ipv6. Este requisito proporciona una solución basada en estándares, en respuesta a las necesidades de seguridad de la red y aumenta la interoperabilidad entre distintas implementaciones de Ipv6.

Mayor Compatibilidad con QoS:

Los nuevos campos del encabezado Ipv6 definen como se identifica y se controla el tráfico. La identificación del tráfico mediante un campo Flow Label (Etiqueta de Flujo) en el encabezado Ipv6 permite a los routers identificar y proporcionar un tratamiento especial a los paquetes que pertenecen a un flujo. Como el trafico se identifica en el encabezado de Ipv6, se puede proporcionar compatibilidad con QoS incluso si la carga de paquetes esta cifrada mediante IPSec.

Nuevo Protocolo para Interacción de Nodos Vecinos:

El protocolo de Descubrimiento de Vecino para IPv6 consiste en un conjunto de mensajes ICMPv6 (Protocolo de Mensajes de Control de Internet) que administran la interacción de nodos vecinos (nodos que se encuentran en el mismo vínculo). El Protocolo de Descubrimiento de Vecino reemplaza al Protocolo de resolución de direcciones (ARP) basado en difusión, al protocolo de descubrimiento de enrutadores de ICMPv6 y a los mensajes de Redirección de ICMPv4, con mensajes de Descubrimiento de Vecinos de unidifusión (Unicast) y multidifusión (Multicast).

Capacidad de Ampliación.

IPv6 se puede ampliar fácilmente con nuevas características, si se agregan encabezados de extensión tras el encabezado Ipv6. A diferencia de las opciones del encabezado de Ipv4, que solo permite 40 bytes de opciones, el tamaño de los encabezados de extensión de IPv6 solo esta limitado por el tamaño del paquete de IPv6.

2.3 COMPARACION ENTRE IPV4 E IPV6.

La siguiente tabla muestra en forma comparativa las diferencias más significativas de Ipv4 e Ipv6.

IPV4	IPV6
Las direcciones de origen y de destino tienen una longitud de 32 bits (4 bytes).	Las direcciones de origen y de destino tienen una longitud de 128 bits (16 bytes).
La compatibilidad con IPSec es opcional.	La compatibilidad con IPSec es obligatoria.
No hay identificación de carga para el control de QoS por parte de los router en el encabezado de Ipv4.	La identificación de carga para el control de QoS por parte de los enrutadores se incluye en el encabezado de Ipv6 mediante el campo Flow Label (Etiqueta de Flujo).
La fragmentación es posible en ambos router y en el host de envío.	La fragmentación no es posible en los router. Solo es posible en el host de envío.
El encabezado incluye una suma de comprobación.	El encabezado no incluye una suma de comprobación.
El encabezado incluye opciones	Todos los datos opcionales se mueven a extensiones de encabezado IPv6.
El Protocolo de Resolución de direcciones (ARP) utiliza tramas de solicitud de ARP de difusión para resolver una dirección de IPv4 en una dirección de capa de enlace.	Las tramas de solicitud de ARP se reemplazan por mensajes Neighbor Solicitud de vecino de multidifusion.
Se utiliza el protocolo de administración de grupos de Internet (IGMP) para administrar la pertenencia a grupos de subredes locales.	El protocolo IGMP se reemplaza por mensajes de Descubrimiento de oyentes de multidifusion (MLD).
Para determinar la dirección Ipv4 de la mejor puerta de enlace predeterminada se utiliza el descubrimiento de router ICMP, que es opcional.	El descubrimiento de router de ICMPv4 se reemplaza por los mensajes de Solicitud de router y Anuncio de Router, de ICMPv6, que son necesarios.
Utiliza registros de recursos (A) de dirección de host en el Sistema de nombres de dominio (DNS, Domain Name System) para asignar nombres de host a direcciones IPv4.	Utiliza registros de recursos (AAAA) de dirección de host en el sistema de nombres de dominio (DNS) para asignar nombres de host a direcciones IPv6.

Tabla 2.1 Comparación entre Ip4 e ipv6.

También existen diferencias en cuanto a la estructura del encabezado de los paquetes Ipv4 e Ipv6, así como se muestra en las figuras siguientes:

Figura 2.1 Encabezado Ipv4

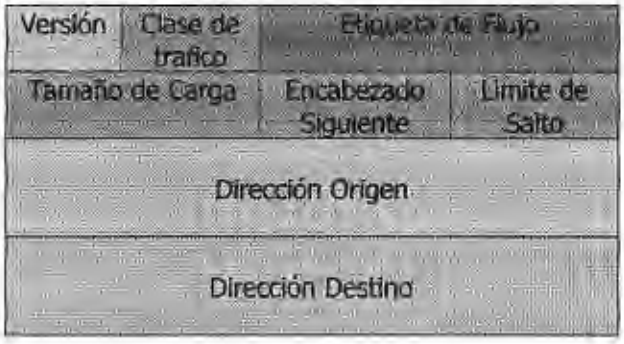


Figura 2.2 Encabezado Ipv6

Donde:

- Campos transferidos de Ipv4 a IPv6.
- Campos nuevos en Ipv6.
- Campos a los que se les ha cambiado Nombre y Posición en IPv6.
- Campos Removidos en IPv6.

2.4 TRANSICIÓN DE IPV4 A IPV6.

La transición de Ipv4 a Ipv6 no es cuestion de un dia, esta se debe realizar poco a poco, empezando a dar servicios en la red IPv6, pero manteniendo los que ya se dan en IPv4. Se debe permitir que los usuarios en las instituciones accedan a la red IPv6 a la vez que siguen conectados a la Internet Ipv4.

Se han diseñado mecanismos para que los clientes que solo tienen IPv4 accedan a servidores que solo manejan Ipv6 y viceversa. A continuación se muestran algunos de los más importantes:

- Doble-Pila (Dual-Stack): Un equipo debe tener instaladas la pila Ipv4 y la pila Ipv6 a la vez, de modo que si esta conectado a los dos tipos de red, puede dar el servicio de ambas.

- Tuneles: Permiten hacer una conexión Ipv6 sobre una red Ipv4 y viceversa. De este modo, si nuestro proveedor solamente nos da conexión Ipv4, podemos unirnos a la red Ipv6 a traves de la misma. Este es el mecanismo habitual de conexión que se utiliza si el proveedor de acceso no proporciona una conectividad Ipv6 nativa y ya se posee un rango de direcciones Ipv6. Una extensión de este mecanismo se conoce como tuneles automaticos, los cuales permiten establecer un tunel automáticamente, para qu equipos duales tengan conectividad Ipv6 a traves de una red Ipv4.

- Traductor de Direcciones de Red (NAT-PT): Protocolo de Traducción de Direcciones y de puertos, es una extensión de NAT que ya se usa en Ipv4 para que ademas de cambiar la direccion, se pueda cambiar la cabecera del protocolo completa, manteniendo los datos de cada paquete intactos.

- 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.

Podemos ver en la figura 2.3 como se espera que sea la transición, partiendo de un mundo solamente con Ipv4, posteriormente van apareciendo algunas redes Ipv6, que poco a poco van interconectandose a veces de forma nativa y a veces utilizando tuneles sobre la red Ipv4 para ello (esta es la situación actual).

Según van apareciendo más redes interconectadas y mas servicios Ipv6, las redes Ipv4 quedan relegadas a un seguno plano, de forma que con el tiempo seran islas en un mundo Ipv6, hasta que acaben desapareciendo.

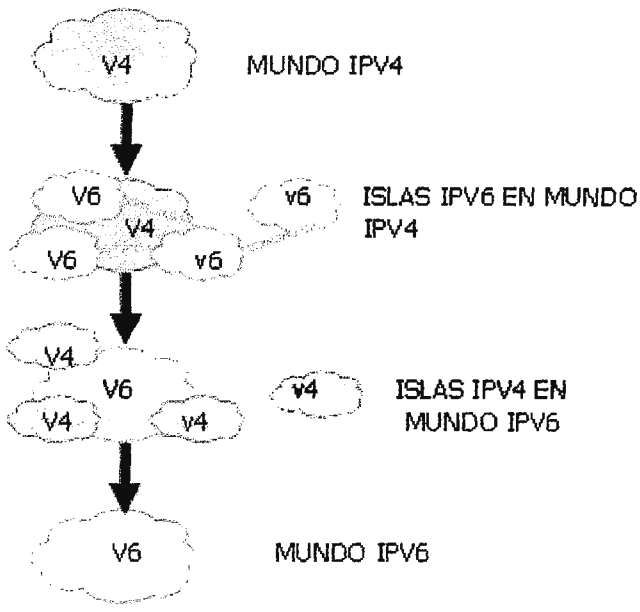


Figura 2.3 Transición de Ipv4 a Ipv6.

CAPITULO 3

Estructura y Direccionamiento en Ipv6

3. ESTRUCTURA Y DIRECCIONAMIENTO EN IPV6.

3.1 ENCABEZADO SIMPLIFICADO DE LOS PAQUETES IPV6.

El encabezado de paquete básico utilizado en IPv4 posee 12 campos que utilizan un tamaño total de 20 octetos (160 bits). Los 12 campos pueden ser sucedidos por un campo de opciones, el cual es sucedido por una porción de datos que usualmente es un paquete de la capa de transporte.

La longitud variable del campo de opciones se agrega al tamaño total del encabezado del paquete IPv4. La figura 3.1 muestra los campos del encabezado Ipv4

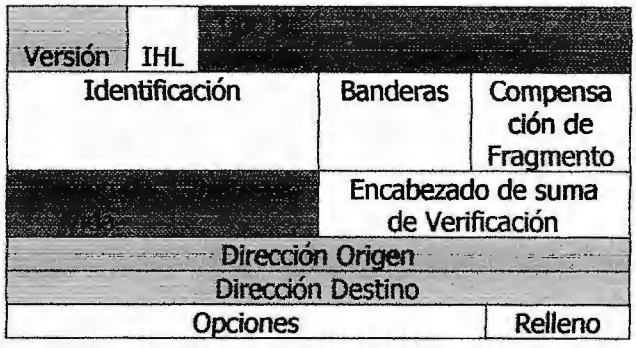


Figura 3.1 Encabezado de Paquetes Ipv4.

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

La cabecera de un paquete IPv4 es variable, por lo que necesita un campo de tamaño. Sin embargo, para simplificar la vida de los routers, IPv6 utiliza un tamaño de cabecera fijo de 40 bytes, que componen un total de ocho campos, asi como lo muestra la figura 12.

Figura 3.2 Encabezado de Paquetes Ipv6

A continuación se muestra la descripción de cada uno de los campos del encabezado Ipv6.

CAMPO	DIRECCIÓN
Versión (4 bits)	Sirve para que el router se entere de que es un paquete IPv6.
Clase de Trafico (8 bits)	Para poder diferenciar entre servicios sensibles a la latencia, como VoIP, de otros que no necesitan prioridad, como trafico http.
Etiqueta de Flujo (20 bits)	Permite la diferenciación de flujos de tráfico. Esto tiene importancia a la hora de manejar la calidad de servicio (QoS)
Tamaño de Carga (16 bits)	Describe el tamaño en octetos de la sección de datos del paquete. Al ser este campo de 16 bits, podremos usar paquetes de hasta mas de 64000 bytes.
Siguiente Cabecera (8 bits)	Este campo permite a routers y hosts examinar con más detalle el paquete. A pesar de que el paquete básico IPv6 tiene cabecera de tamaño fijo, el protocolo puede añadir mas para utilizar otras características como encriptación y autenticación.
Limite de Salto (8 bits)	Especifica el número de saltos de router que puede hacer el paquete antes de ser desechado. Con 8 bits podremos tener un máximo de 255 saltos.
Dirección Origen (128 bits)	Dirección Ipv6 origen del paquete.
Dirección Destino (128 bits)	Dirección Ipv6 destino del paquete.

Tabla 3.1 Campos de la Cabecera Ipv6.

3.2 EL CAMPO DE SIGUIENTE CABECERA (NEXT HEADER FIELD)

Como hemos dicho antes, el tamaño de la cabecera IPv6 básica es fijo. Dentro de esta cabecera existe un campo llamado de siguiente cabecera que permite describir con más detalle las opciones del paquete. Esto quiere decir que en realidad tendremos una cabecera de tamaño fijo por norma general y otra cabecera de tamaño variable en caso de que utilicemos alguna de las características avanzadas. En la tabla 5 se muestran los campos de que posee siguiente cabecera.

Siguiente Cabecera	Valor del Campo
Opciones de Hop-by-Hop	0
Opciones de Destino	60
Encaminamiento	43
Fragmento	44
Autenticación	51
Encapsulaciòn	50
Ninguna	59

Tabla 3.2. Campos de Siguiente Cabecera.

Esta arquitectura es muy flexible, ya que cada cabecera tiene un campo de siguiente cabecera, con lo que podemos tener varias opciones agregadas. Un ejemplo ilustrativo lo podemos ver en las Figuras 3.3 y 3.4.

Con la cabecera de encaminamiento conseguimos la funcionalidad equivalente de IPv4 de Source-Routing, es decir, especificar los nodos intermedios por los que ha de pasar el paquete.

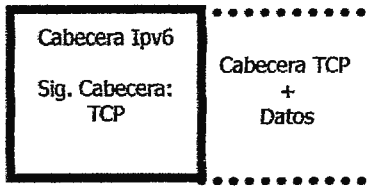


Figura 3.3 Cabecera Ipv6 Básica y Datos.

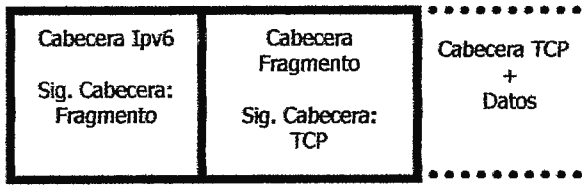


Figura 3.4 Cabecera Ipv6 Básica, Fragmento y Datos.

Una cosa que debe quedar bien clara es que los nodos intermedios o ruteadores no deben examinar más que la cabecera IPv6 básica. Existen excepciones como en el caso de que existan cabeceras de opciones de salto, o como en el caso anterior, que exista una cabecera de enrutamiento en el que sólo los nodos en ella definidos deberían alterar el paquete.

La especificación recomienda además el siguiente orden para las cabeceras adicionales:

- Cabecera IPv6 básica.
- Opciones Hop-by-Hop.
- Opciones de destino.
- Encaminamiento.
- Fragmento.
- Autenticación.
- Encapsulaciòn.
- Opciones de destino.
- Cabecera nivel superior.

Las opciones de destino pueden ser procesadas en momentos distintos dependiendo de si el paquete atraviesa un nodo intermedio o llega al nodo destino.
La única restricción de la especificación es que las opciones de Hop-by-Hop han de ir siempre de la cabecera básica.

3.3 DIRECCIONAMIENTO IPV6.

La motivación principal para la creación de Ipv6 es la de prevenir la demanda de direcciones IP en un futuro. Las aplicaciones como los dispositivos móviles de internet como Asistentes Digitales personales (PDA) y teléfonos, las Redes de Casa (HANs) y los servicios inalámbricos de datos están conduciendo a una gran demanda de direcciones IP.

Ipv6 cuadriplica el numero de bits de direcciones que posee actualmente Ipv4 (32 bits), utilizando 128 bits para crear las direcciones IP, lo cual provee suficientes direcciones IP para cada dispositivo de red en el planeta. Ipv6 habilita inherentemente escalabilidad y seguridad punto a punto para los dispositivos de red. Además, la flexibilidad del espacio de direcciones IPv6 reduce la necesidad de direcciones privadas y del uso del NAT; por lo tanto, IPv6 permite nuevos protocolos de aplicación que no requieren de un procesamiento especial por los routers de borde en las redes fronterizas.
Como ya hemos dicho, las direcciones IPv6 son identificadores de interfaces y/o conjuntos de interfaces de 128 bits. Tenemos tres tipos de direcciones:

- Unicast: Identifica a una sola interfase. Un paquete enviado a una dirección unicast se entregara a una sola interfase.

- Anycast: Identifica a un conjunto de interfaces, probablemente en distintos nodos. Un paquete enviado a una dirección de este tipo será entregado solo a uno de los nodos, que debería ser, en principio, el más cercano.

- Multicast: Igual que en el caso anterior, identificara a un conjunto de interfaces que estarán seguramente en nodos distintos. Pero, en este caso, el paquete será enviado a todos los nodos del conjunto.

En las figuras podemos ver un ejemplo de comunicación entre tres nodos con conjuntos de direcciones A, B y C. Y los distintos comportamientos según el tipo de comunicación.
Con IPv6 dejan de existir las direcciones broadcast, cuya funcionalidad es absorbida por las direcciones multicast.
A continuación se muestran el comportamiento de cada tipo de direcciones :

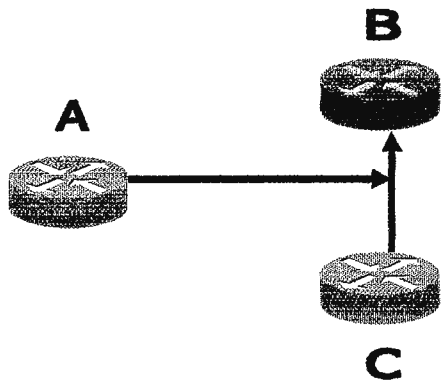


Figura 3.5 Ejemplo comportamiento Unicast

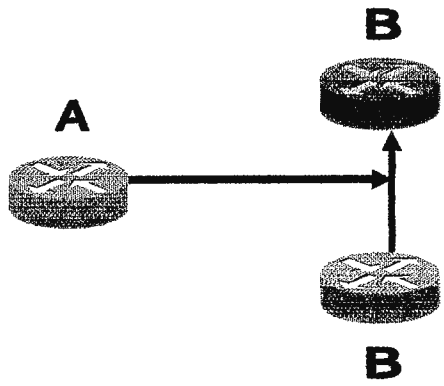


Figura 3.6 Ejemplo comportamiento Anycast

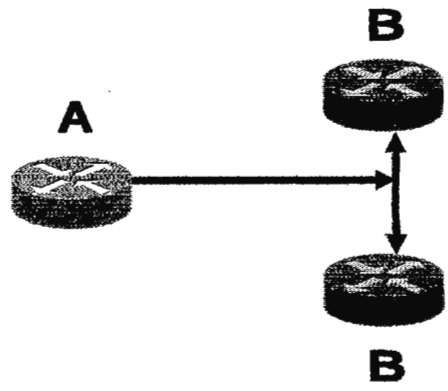


Figura 3.7 Ejemplo comportamiento Multicast

3.3.1 Modelos de direccionamiento.

Cualquier tipo de dirección debe ser asignada a interfases, no a nodos. Esto es algo importante que no hay que olvidar. Todas las interfases han de tener, por los menos, una dirección local de enlace (Link-Local) de tipo unicast. Una misma interfase puede tener asignadas múltiples direcciones de cualquier tipo (unicast, anycast, multicast) o ámbito (scope). Direcciones unicast con ámbito mayor que el de enlace no son necesarias para interfaces que no son usadas como origen y destino de paquetes IPv6 hacia o desde no vecinos. Esto significa que para la comunicación dentro de una LAN no nos hacen falta direcciones IPv6 globales, sino que tenemos más que suficiente con direcciones de ámbito local. De hecho, es lo aconsejable para enlaces punto a punto.
Respecto a los prefijos de subred, IPv6 sigue el mismo modelo que IPv4, es decir, un prefijo se asocia a un enlace, pudiendo haber varios prefijos en un mismo enlace.

3.3.2 Ámbitos de Direcciones Ipv6.

Acabamos de mencionar en la sección anterior el ámbito de una dirección sin saber todavía lo que era. Vamos a explicar en qué consiste. El protocolo IPv6 ánade soporte para direcciones de distintos ámbitos, lo que quiere decir que tendremos direcciones globales y no globales. Si bien con IPv4 ya habíamos empleado direccionamiento no global con la ayuda de prefijos de red privados, con IPv6 esta noción forma parte de la propia arquitectura de direccionamiento.
Cada dirección IPv6 tiene un ámbito, que es un área dentro de la cual esta puede ser utilizada como identificador único de una o varias interfases. El ámbito de cada dirección forma parte de la misma dirección, con lo que vamos a poder diferenciarlos a simple vista.

Para las direcciones unicast distinguimos tres ámbitos:

- Local de enlace (link-local), para identificar interfaces en un mismo enlace.
  Empiezan todas por fe80:.

- Locales de sitio (site-local), para identificar interfaces en un mismo sitio.
  La definición de sitio es un tanto genérica, pero en principio un sitio es el área topológica de red perteneciente a un edificio o un campus, perteneciente a una misma organización.
  Empiezan por fec0:.

- Global, para identificar interfaces en toda Internet. Estas comienzan por 2001: o 3ffe:.

En lo que a ámbito se refiere, las direcciones anycast siguen la misma norma que las unicast. Sin embargo, para las direcciones multicast tenemos catorce posibles ámbitos, que identifican desde un interfaz local a una dirección global.
Nodos de un mismo ámbito y visibles entre si, definen una zona. No se permite que un router encamine tráfico entre diferentes zonas (perderían todo el sentido los ámbitos).
Una de las grandes ventajas de los ámbitos es que permitirá la renumeración de prefijos sin mucha dificultad, ya que las direcciones de ámbito no global se mantendrán. Tenemos que esperar que se produzca alguna renumeración de prefijos globales, ya que según crezca una organización su prefijo se puede quedar pequeño y necesitar más espacio de direcciones. Y como hemos dicho antes, se tratará siempre que sea posible de mantener las tablas de enrutamiento al mínimo. Lo que sólo se consigue dando un prefijo nuevo mayor e invalidando el anterior, porque lo que seguramente sucedería seria que las redes contiguas ya estén asignadas.

3.3.3 Nomenclatura de las direcciones.

Tenemos tres formas comunes de representar direcciones IPv6 en texto:

- x:x:x:x:x:x:x:x donde cada x es el valor en hexadecimal de cada grupo de 16 bits de la dirección.

- x:x::x en el caso de que haya grupos contiguos de 16 bits todos cero.

Es una abreviatura que servirá para hacer más cómodo el uso de algunas direcciones. Podemos ver un ejemplo comparativo de este caso y el anterior
en la tabla 3.3 .

- x:x:x:x:x:x:d.d.d.d, donde las x son los seis grupos de 16 bits en hexadecimal

de mayor peso de la dirección y las d son los valores decimales de
los cuatro grupos de 8 bis de menor peso de la dirección. Esta forma es a veces más conveniente a la hora de manejar entornos mixtos IPv6 e IPv4.
Por ejemplo: 0:0:0:0:0:FFFF:129.144.52.38 y en su forma abreviada
::FFFF:129.144.52.38.

Tipo de Dirección Ipv6	Formato Preferido	Formato Comprimido
Unicast	2001:0:0:0:0DB8:800:200C:417A	2001::0DB8:800:200C:417A
Multicast	FF01:0:0:0:0:0:0:101	FF01::101
Loopback	0:0:0:0:0:0:0:1	::1
No Especificada	0:0:0:0:0:0:0:0	::

Tabla 3.3 Formatos de direcciones Ipv6 Comprimidos.

3.3.4 Nomenclatura de los prefijos.

La representación de los prefijos de direcciones con IPv6 es similar a la que tenemos con CIDR con IPv4, representada por: dirección-ipv6/tamaño-prefijo.
Donde dirección-ipv6 es alguna de las notaciones vistas en la sección anterior y tamaño-prefijo es un valor decimal que especifica cuantos bits de la dirección corresponden al prefijo.
Por ejemplo, el prefijo de la UJI (Universidad Jaume I.) de España, en hexadecimal es 3FFE33300002, que son 48 bits, lo podemos escribir como:

- 3FFE:3330:0002:0000:0000:0000:0000:0000/48
- 3FFE:3330:2:0:0:0:0:0/48
- 3FFE:3330:2::/48

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

3.3.5 Representación de los tipos de direcciones.

El tipo específico de cada dirección IPv6 viene dado por los primeros bits de esta, dentro de lo que se llama el campo de formato de prefijo (FP, format prefix).
El tamaño de este campo es variable. Los prefijos desde 001 a 111 tienen la obligación de tener los identificadores de interfaz de 64 bits en formato EUI-64, descrito en [IEE97], excepto para las direcciones multicast (1111 1111). Las direcciones unicast se distinguen por el valor del octeto de mayor peso, que tiene algún valor distinto de 1.
Como podemos ver, hay mucho espacio no asignado (el 85%), lo que en un futuro permitirá expandir el espacio posible o incluso dar nuevos usos.

3.4 DIRECCIONES IPV6 UNICAST.

Una dirección Ipv6 unicast es un identificador para una sola interfaz, en un solo nodo. Un paquete que se envía a una dirección unicast es entregado a la interfaz identificada con esa dirección. Existen diferentes tipos de direcciones Ipv6 unicast:

- Direcciones Globales Agregables.
- Direcciones Locales de Sitio (site-local).
- Direcciones Locales de Enlace (link-local).
- Direcciones Ipv4 compatibles con Ipv6.

3.4.1 Direcciones Globales Agregables.

Una dirección global agregable es una dirección IPv6 proveniente del prefijo unicast de agregación global. La estructura de estas direcciones permite la agregación de prefijos de enrutamiento que limitan el número de las entradas de las tablas de enrutamiento en la tabla de enrutamiento global. Las direcciones de agregación global se utilizan en los enlaces que se agregan dentro organizaciones, y en los Proveedores de Servicio de Internet. Las direcciones globales de agregación IPv6 son definidas por un prefijo de enrutamiento gobal, un identificador de subred y un identificador de la interfaz. A excepción de las direcciones que comienzan con 000 binarios, todas las direcciones globales unicast tienen un identificador de la interfaz de 64 bits. La asignación de las direcciones globales unicast actuales utiliza el rango de direcciones que comienzan con el valor binario 001 (2000::/3).

La figura 3.8 demuestra la estructura de una dirección global de agregación.

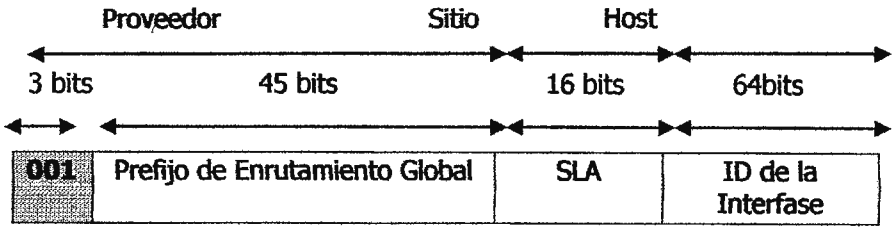


Figura 3.8 Estructura de una dirección global de agregación.

La IANA (Internet Assigned Numbers Authority) asigna el espacio de direcciones IPv6 en el rango de 2000::/16 a los registros regionales. La dirección global de agregación consiste típicamente en un prefijo global de enrutamiento de 48-bit y un identificador de subred de 16 bits o un Site-Level Aggregator (SLA) de 16 bits.

Un campo de subred de 16 bits llamado identificador de subred podría ser utilizado por organizaciones individuales para crear su propia jerarquía local de la dirección y para identificar subredes. Un identificador de subred es similar a una subred en IPv4, con la diferencia de que una organización con un identificador de subred Ipv6 pueda soportar hasta 65,535 subredes individuales. Un identificador de interfaz se utiliza para identificar interfaces sobre un enlace. El identificador de la interfaz debe ser único para el enlace. También pueden ser únicos sobre un alcance amplio (broader scoupe). En muchos casos, un identificador de interfaz será igual o basado en la dirección de la capa de enlace de la interfaz. Los identificadores de interfaz usados en direcciones globales unicast de agregación y otros tipos de direcciones Ipv6 deben tener 64 bits de longitud y deben ser construidos en el formato EUI-64 modificado.

Los identificadores de interfase se construyen en el formato EUI-64 modificado en una de las siguientes maneras:

• Para las interfaces de tipo IEEE 802 (por ejemplo, Ethernet, y las interfaces FDDI), los primeros tres octetos (24 bits) se toman del identificador único de la organización (OUI), que forman parte de los 48 bits de la dirección de la capa de enlace (dirección MAC) del interfaz, el cuarto y quinto octeto (16 bits) es un valor hexadecimal fijo igual a FFFE, y los tres octetos restantes (24 bits) se toma de los tres

octetos restantes de la dirección MAC. La construcción del identificador de interfaz es terminada al establecer el bit de Universal/Local (U/L) (séptimo bit del primer octeto) con un valor de 0 o 1. Un valor de 0 indica un identificador localmente administrado; un valor de 1 indica un identificador global único del interfaz IPv6.

• Para el resto de tipos de interfaces (por ejemplo, serial, loopback, ATM, Frame Relay y tipos de interfaces túnel) excepto las interfaces de túneles recubiertos usadas con Ipv6 (Overlay Tunnels), el identificador de la interfaz se construye de la misma manera que el identificador de interfaz para interfaces de tipo IEEE ; sin embargo, la primera dirección MAC del rango de las direcciones MAC en el router se utiliza para construir el identificador (porque la interfaz no posee una dirección MAC).

• Para las interfaces de tipo Ipv6 Overlay Tunnels, el identificador de la interfaz es la dirección IPv4 asignada al interfaz del túnel, con todos los ceros en los 32 bits de la parte alta del identificador.

Si no hay interfaces de tipo IEEE 802 en el router, se generan direcciones locales de enlace IPv6 en las interfaces del router, de la siguiente manera:

1. El router consulta las direcciones MAC (del rango (pool) de direcciones MAC dentro del router).

2. Si no hay direcciones MAC disponibles en el router, el número de serie del mismo es utilizado para formar las direcciones locales de enlace.

3. Si el número de serie del router no se puede utilizar para formar las direcciones locales de enlace, el router utiliza un Message Diggest 5 (MD5) para determinar la dirección MAC del router.

3.4.2 Dirección Local de Sitio (Site-Local Address)

Una dirección local de sitio es una dirección unicast IPv6 que utiliza el prefijo FEC0::/10 (1111 1110 11) y concatena el identificador de subred (el campo SLA de 16-bit) con el identificador de interfaz en el formato EUI-64 modificado. Las direcciones locales de sitio se pueden utilizar para numerar un sitio completo sin usar un prefijo global único. Estas se pueden considerar como direcciones privadas porque pueden ser utilizadas para restringir la comunicación a un dominio limitado.

La figura 3.9 muestra la estructura de una dirección sitio-local. Los routers IPv6 no deben enviar los paquetes que poseen direcciones locales de sitio ya sea de fuente o destino, que se encuentren fuera del sitio.

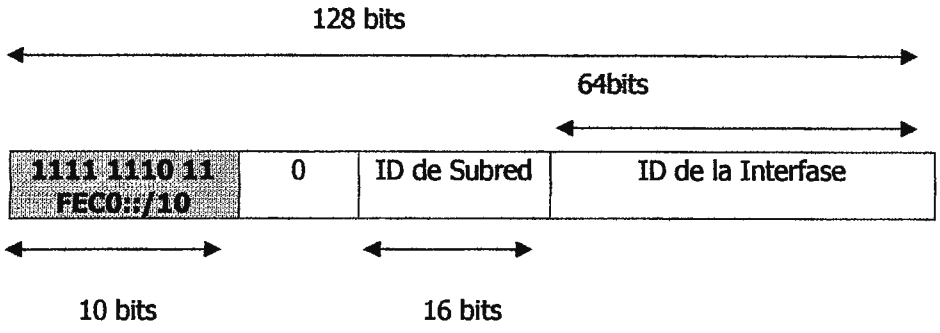


Figura 3.9 Estructura de una dirección local de sitio

3.4.3 Dirección Local de Enlace (Link-Local Address).

Una dirección local de enlace es una dirección unicast IPv6 que se puede configurar automáticamente en cualquier interfaz usando el prefijo local de enlace FE80::/10 (1111 1110 10) y el identificador de la interfase en el formato EUI-64 modificado. Estas direcciones se utilizan en el Protocolo de Descubrimiento de Vecinos (Neighbors Discovery Protocol) y el proceso de auto configuración sin estado. Los nodos en un enlace local pueden utilizar direcciones locales de enlace para comunicarse; los nodos no necesitan las direcciones locales de sitio o globales únicas para comunicarse. La figura 3.10 muestra la estructura de una dirección local de enlace. Los routers IPv6 no deben enviar los paquetes que tienen una dirección local de enlace ya sea fuente o destino hacia otros enlaces.

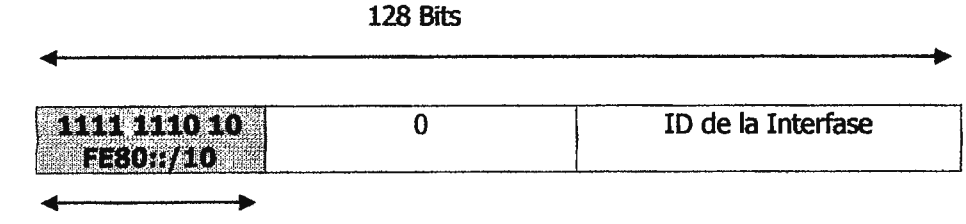


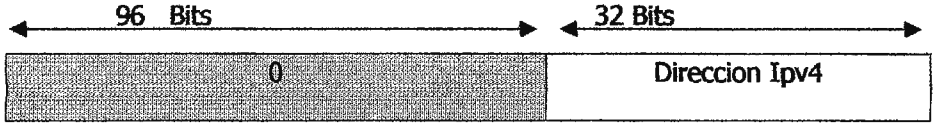
Figura 3.10. Estructura de una dirección local de enlace.

3.4.4 Direcciones Ipv4-Ipv6 Compatibles.

Una dirección Ipv4-Ipv6 compatible es una dirección unicast IPv6 la cual posee ceros en los 96 bits de la parte alta de la dirección y posee una dirección Ipv4 en los 32 bits de la parte baja de la dirección.

El formato de una dirección IPv4-IPv6 compatible es: 0:0:0:0:0:0:A.B.C.D o ::A.B.C.D.

Esta dirección funciona como la dirección IPv6 del nodo y la dirección IPv4 encajada en los 32 bits de la parte baja se utiliza como la dirección IPv4 del nodo. Las direcciones de IPv4-Ipv6 compatibles se asignan a los nodos que soportan el stack de protocolos Ipv4 e Ipv6 y se utilizan en túneles automáticos. La figura 3.11 muestra la estructura de una dirección Ipv4-Ipv6 compatible y algunos formatos aceptables para la dirección.



::192.168.30.1 = C0A8:1E01

Figura 3.11 Estructura de una dirección Ipv4-Ipv6 compatible.

3.5 DIRECCIONES IPV6 ANYCAST.

Una dirección anycast es una dirección que se asigna a un conjunto de interfaces que pertenecen típicamente a diferentes nodos. Un paquete enviado a una dirección anycast se entrega al interfaz más cercana (según lo definido por los protocolos de enrutamiento en uso) identificada por la dirección anycast. Las direcciones Anycast son sintácticamente indistinguibles de las direcciones unicast porque las direcciones anycast estan alojadas en el espacio de las direcciones unicast. Al asignar una dirección unicast a más de una interfase, se transforma en anycast. Los nodos a los cuales se asigna una dirección anycast se deben configurar explícitamente para reconocer que la dirección es una dirección anycast.

Las direcciones Anycast se pueden utilizar solamente en los routers y no en los host. Las direcciones anycast no se deben utilizar como las direcciones de origen en los paquetes IPv6.

La figura 3.12 muestra el formato de una dirección de subred anycast del router; la dirección tiene un prefijo concatenado por una serie de ceros (el identificador de interfase).

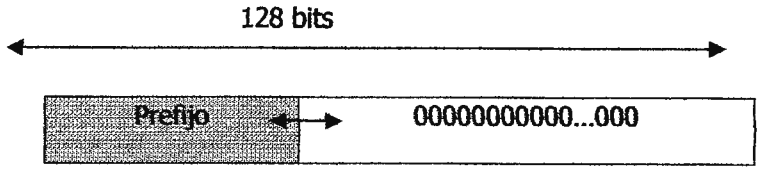


Figura 3.12 Estructura de una dirección Anycast.

A continuación se muestra la configuración para un prefijo anycast

```
interface Tunnel0
no ip address
ipv6 address 2002:A00:1::1/64
ipv6 address 2002:c058:6301::/128 anycast
tunnel source Ethernet0
tunnel mode ipv6ip 6to4
!
interface Ethernet0
ip address 10.0.0.1 255.255.255.0
ip address 192.88.99.1 255.255.255.0 secondary
!
ipv6 route 2002::/16 Tunnel0
!
```

3.6 DIRECCIONES IPV6 MULTICAST.

Una dirección multicast IPv6 es una dirección IPv6 que tiene un prefijo de FF00::/8 (1111 1111). Una dirección multicast IPv6 es un identificador para un conjunto de interfaces que pertenecen típicamente a diferentes nodos.

Un paquete enviado a una dirección multicast se entrega a todas las interfaces identificadas por la dirección multicast. El segundo octeto del prefijo define el tiempo de vida y el alcance de la dirección

multicast. Una dirección multicast permanente posee un parámetro de tiempo de vida igual a 0; una dirección multicast temporal posee un parámetro de tiempo de vida igual a 1.
Una dirección multicast que tiene el alcance de un nodo, de un enlace, de un sitio, de una organización, o un alcance global, tiene un parámetro de alcance igual a 1, 2, 5, 8, o de E, respectivamente. Por ejemplo, una dirección multicast con el prefijo FF02::/16 es una dirección multicast permanente con un alcance de enlace.

La figura 3.13 muestra el formato de una dirección multicast Ipv6.

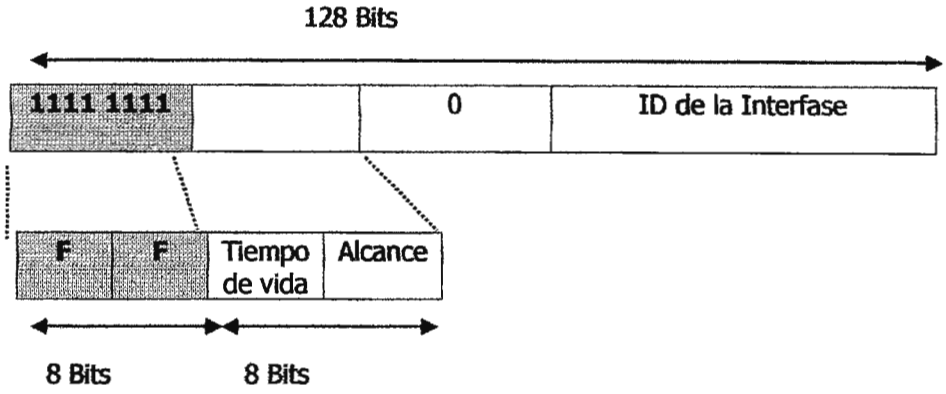


Figura 3.13 Formato de una dirección multicast Ipv6.

Donde:

CAMPO	VALOR
Tiempo de Vida	0= Permanente
	1= Temporal
Alcance	1= Nodo
	2= Enlace
	5= Sitio
	8= Organización
	E= Global

3.7 SALIDAS EN PANTALLA DE DIRECCIONES IPV6.

Cuando los comandos Ipv6 o Ipv4 muestran en pantalla una dirección Ipv6, una dirección Ipv6 demasiado larga se puede desbordar sobre los campos vecinos, provocando una difícil lectura en pantalla.

Los campos de la salida fueron diseñados para trabajar con la dirección Ipv4 más larga posible, que tiene 15 caracteres.

Las direcciones IPv6 pueden tener hasta 39 caracteres de largo. El esquema siguiente se ha adoptado en los comandos IPv4 e IPv6 para permitir que la longitud apropiada de la dirección Ipv6 pueda ser mostrada completamente, esto se logra moviendo los campos restantes de una dirección Ipv6 muy larga a la línea siguiente, en caso de ser necesario.

Los campos que son movidos se mantienen alineados con el encabezado de la columna. Para tener un ejemplo mas claro podemos utilizar el comando "where"; el cual nos muestra las conexiones existentes en un router. En el siguiente codigo se muestran ocho conexiones existentes. Las primeras seis conexiones son a través de direcciones Ipv6 y las ultimas dos conexiones son a través de direcciones Ipv4.

```
Router# where

Conn Host                 Address             Byte  Idle Conn Name
   1 test5                1111:2222:3333:4::5    6    24 test5
   2 test4                1111:2222:3333:44::5
                                                 6    24 test4
   3 1111:2222:3333:4::5 1111:2222:3333:4::5    6    24 1111:2222:3333:4::5
   4 1111:2222:3333:44::5
                          1111:2222:3333:44::5
                                                 6    23 1111:2222:3333:44::5
   5 1111:2000:3000:4000:5000:6000:7000:8001
                          1111:2000:3000:4000:5000:6000:7000:8001
                                                 6    20 1111:2000:3000:4000:5000:6000:
   6 1::1                 1::1                   0     1 1::1
   7 10.1.9.1             10.1.9.1               0     0 10.1.9.1
   8 111.222.111.222      111.222.111.222        0     0 111.222.111.222
```

La conexión 1 contiene una dirección IPv6 que utiliza la longitud máxima permitida en el campo de dirección. La conexión 2 posee una dirección Ipv6 que se desborda del campo de dirección y provoca que los campos siguientes se muevan a la línea siguiente, pero siempre en línea con el registro que representan. La conexión 3 contiene una dirección IPv6 que llena la longitud máxima del campo de nombre de host y de dirección, sin provocar ningún desbordamiento de campos. La conexión 4 muestra el resultado del desbordamiento de los campos de nombre de host y de dirección; la salida se muestra sobre tres líneas que guardan la alineación del registro que representan. La conexión 5 exhibe un efecto similar al de la conexión 4 con una dirección Ipv6 muy larga en los campos del nombre de host y la dirección. Observe que el campo "Conn Name" se encuentra invadido realmente. La conexión 6 muestra una dirección Ipv6 muy corta que no provoca ningún cambio en pantalla. Las conexiones 7 y 8 muestran direcciones Ipv4 cortas y largas respectivamente.

CAPITULO 4

Implementación del Protocolo IPv6

4. IMPLEMENTACION DEL PROTOCOLO IPV6.

Ipv6, llamado formalmente Ipng (Internet Protocol Next Generation) es la última versión del Protocolo de Internet (IP). IP es un protocolo que utiliza paquetes para intercambiar tráfico de datos, voz y video sobre redes digitales. Ipv6 fue propuesto cuando se determino que los 32 bits que forman las direcciones Ipv4 no eran suficientes para las demandas de crecimiento del Internet. Ipv6 provee un mayor espacio de direcciones y posee mejoras como un encabezado principal simplificado y encabezados de extensión. Este se describe inicialmente en el RFC 2460 por el IETF (Internet Engineering Task force). Los RFCs describen la arquitectura y servicios soportados por Ipv6.
La arquitectura de Ipv6 ha sido diseñada para permitir que los usuarios existentes de Ipv4 puedan tener una fácil transición mientras se proveen servicios como la Seguridad Punto a Punto y Calidad de Servicio (QoS). El abundante espacio en las direcciones Ipv6 permiten escalabilidad y un mayor número de direcciones para utilizar. El formato del encabezado de paquetes Ipv6 manipula los paquetes de una forma más eficiente. Ipv6 soporta ampliamente los protocolos de enrutamiento mas destacados como RIP, IS-IS, OSPFv3 y el multiprotocolo BGP (Protocolo de Enrutamiento de Borde).

4.1 PRERREQUISITOS PARA IMPLEMENTAR CONECTIVIDAD BÁSICA UTILIZANDO IPV6

- Conocimientos previos sobre la estructura y funcionamiento de Ipv4.

- Para el envío de trafico Ipv6 usando CEFv6 (Cisco Express Forwarding) o dCEFv6 (Distributed Cisco Express Forwarding), se debe configurar el envió de datagramas unicast Ipv6 globalmente en el router usando el comando de configuración **ipv6 unicast-routing**, además se debe configurar una dirección ipv6 en una interfase utilizando el comando de configuración **ipv6 address.**

- Se debe habilitar CEF para ipv4 (CEFv4) globalmente en el router utilizando el comando de configuración **ip cef** antes de habilitar CEFv6 globalmente en el router utilizando el comando de configuración **ipv6 cef.**

- En plataformas de arquitectura distribuida que soportan CEFv6 and dCEFv6, como los routers de la serie Cisco 7500, se debe habilitar dCEFv4 globalmente en el router utilizando el comando de configuración **ip cef distributed** antes de habilitar dCEFv6 globalmente en el router utilizando el comando **ipv6 cef distributed.**

Como se menciono anteriormente en el anteproyecto de tesis se ha definido el uso de plataformas Cisco para la implementación del protocolo Ipv6. Cisco ha creado una serie de Sistemas Operativos para sus plataformas los cuales dan soporte a características importantes de Ipv6. A continuación se muestra la tabla 4.1, la cual muestra las características a las que dan soporte según el tipo de Cisco IOS (Sistema Operativo).

CARACTERISTICAS	CISCO IOS REQUERIDO
Caracteristicas Basicas de IPv6 para Cisco IOS	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3,12.3(2)T
Formato de direcciones Ipv6	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3,12.3(2)T
Direcciones Unicast Ipv6	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3,12.3(2)T
Direcciones Anycast Ipv6	12.3(4)T, 12.2(25)S
Conmutacion CEF and Distributed CEF para Ipv6	12.0(21)ST, 12.0(22)S, 12.2(13)T, 12.2(14)S, 12.3, 12.3(2)T
Unicast Reverse Path Forwarding (Unicast RPF)strict mode	12.2(13)T, 12.2(14)S
Unicast Reverse Path Forwarding (Unicast RPF)loose mode	12.2(25)S
NetFlow (Control de Flujo) para IPv6	12.3(7)T
DNS for IPv61	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
Map host names para IPv6 addresses	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
AAAA DNS lookups sobre transporte Ipv4	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
DNS lookups sobre transporte Ipv6	12.2(8)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
Descubrimiento de ruta MTU Ipv6	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
ICMPv6	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
ICMPv6 redirect	12.2(4)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
ICMPv6 rate limiting	12.2(8)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
Descubrimiento de vecinos Ipv6	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S,

	12.3, 12.3(2)T
Detección de direcciones duplicadas de vecinos, para Ipv6	12.2(4)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
IPv6 stateless autoconfiguration	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 2.3(2)T
Prefijos de delegación DHCP para Ipv6	12.3(4)T
Stateless DHCP for IPv6	12.3(4)T
DHCP para IPv6 Relay Agent	12.3(11)T
ATM PVC y ATM LANE	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
Frame Relay PVC	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
FDDI	12.2(2)T, 12.2(14)S, 12.3, 12.3(2)T
Servicio PPP sobre packet over SONET, ISDN, e interfaces seriales (sincronas y asincronas)	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
Ethernet, Fast Ethernet, Gigabit Ethernet, y 10-Gigabit Ethernet	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
Cisco High-Level Data Link Control (HDLC)	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
Cisco High-Level Data Link Control (HDLC) Dynamic packet transport (DPT)	12.0(23)S
Remote bridged encapsulation (RBE)	12.3(4)T
Dual IPv4 y IPv6 protocol stacks	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 2.3(2)T
Configurando direccionamiento Ipv6 y enrutamiento.	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
Soporte CISCO-IP-MIB	12.2(15)T, 12.3, 12.3(2)T
Soporte CISCO-IP-FORWARDING-MIB	12.0(22)S, 12.2(14)S, 12.2(15)T, 12.3, 12.3(2)T

Tabla 4.1 Características de Ipv6 soportadas por Cisco IOS.

Las versiones de IOS 12.2(2)T y 12.2(14)S son las que soportan las principales características de Ipv6. Por lo tanto es recomendable que el equipo a utilizar posea las versiones de IOS anteriormente mencionadas. La Tabla 4.2 muestra las plataformas de Router Cisco que soportan estas versiones de IOS.

PLATAFORMA	12.2 T Releases	
	12.2(2)T	12.2(14)S
Cisco 800 series	Si	Si
Cisco 1400 series	Si	Si
Cisco 1600 series	Si	Si
Cisco 1700 series	Si	Si
Cisco 2500 series	No	Si
Cisco 2600 series	Si	Si

Cisco 3600 series	Si	Si
Cisco 4000 series (4500, 4500-M, 4700, 4700-M)	Si	No
Cisco 7100 series	Si	Si
Cisco 7200 series	Si	Si
Cisco 7500 series	SI	No
Cisco 1200 series	No	No

Tabla 4.2 Plataformas Cisco que soportan IOS 12.2(2)T o 12.2(4)T

4.1.1. Justificación del Equipo a Utilizar.

Para la realización de pruebas sobre el protocolo Ipv6 se necesitan equipos de red específicos, como routers, switches, PC`s etc.
Estas pruebas se realizaran utilizando plataformas Cisco, las cuales se muestran a continuación:

- 2 Enrutadores Cisco 2620.
- 1 Enrutador Cisco 1700
- 1 Switch Cisco 2950.

Por lo tanto, los ejemplos de configuración e implementación mostrados en este documento, se encuentran basados en el Sistema Operativo Cisco; aclarando que no hay ningún tipo de preferencia con la marca.

Las razones por las que se utiliza equipo Cisco son:

1) Facilidad de acceso a este tipo de equipos, que por lo general tienen un precio elevado. Por lo tanto no se incurrirá en ningún gasto para la obtención del mismo y estarán disponibles para la realización de pruebas.

2) Existen diferentes proveedores en el mercado, sin embargo la compañía Cisco System es líder en el mercado de equipos de enrutamiento y conmutación (Routing & Switching), por lo cual es de los fabricantes que mas ha desarrollado aplicaciones e implementado protocolos que soporten Ipv6.

3) Provee una interfaz de comandos no muy amigable a simple vista; pero es fácil de comprender y sencilla de utilizar.

4.2 RESTRICCIONES PARA IMPLEMENTAR CONECTIVIDAD BÁSICA

- Cisco IOS 12.0(21)ST da soporte a la conmutación dCEF y Cisco IOS 12.2(13)T da soporte para CEF y dCEF para Ipv6.

- Los paquetes Ipv6 son transparentes a los switches LAN de capa 2, ya que estos no examinan la información de capa 3 antes de enviar las tramas Ipv6.

- En cualquier Cisco IOS con soporte Ipv6 las direcciones globales múltiples Ipv6 (múltiple Ipv6 global address) y las direcciones locales de sitio (site-local) con el mismo prefijo pueden ser configuradas en una interfaz. Sin embargo, múltiples direcciones de enlace-local (link-local) no son soportadas en una interfaz.

- La serie 12.0 de Cisco IOS provee soporte Ipv6 para los routers de la serie Cisco 12000 y 10700.

4.3 CONECTIVIDAD BASICA EN IPV6.

4.3.1 Habilitando el Protocolo Ipv6 en una PC.

4.3.1.1 Plataformas Windows.

En general, las plataformas de Microsoft disponen de buen soporte para Ipv6. A partir de su versión de sistema operativo "Windows XP", el protocolo viene preinstalado y su configuración es muy sencilla.

Windows XP y Windows 2003 Server.

En Windows XP y Windows 2003 Server, Ipv6 ya esta instalado, pero es preciso habilitarlo. Para ello es necesario ejecutar, con privilegios de administrador, los siguientes pasos.

1) Menú de Inicio.
2) Ejecutar.
3) CMD
4) Enter

Prompt>netsh interface ipv6 install (Windows 2003 Server)
Prompt>ipv6 install (Windows XP)

Aparecerá un mensaje indicando que se ha configurado correctamente.

También se puede utilizar la interfaz grafica con los siguientes pasos.

1) Menú de Inicio.
2) Panel de Control.
3) Conexiones de Red (Doble Clic).
4) Conexión de Área local (Clic derecho).
5) Propiedades.
6) Instalar.
7) Protocolo.
8) Microsoft TCP/IP Version6.
9) Aceptar (Enter)

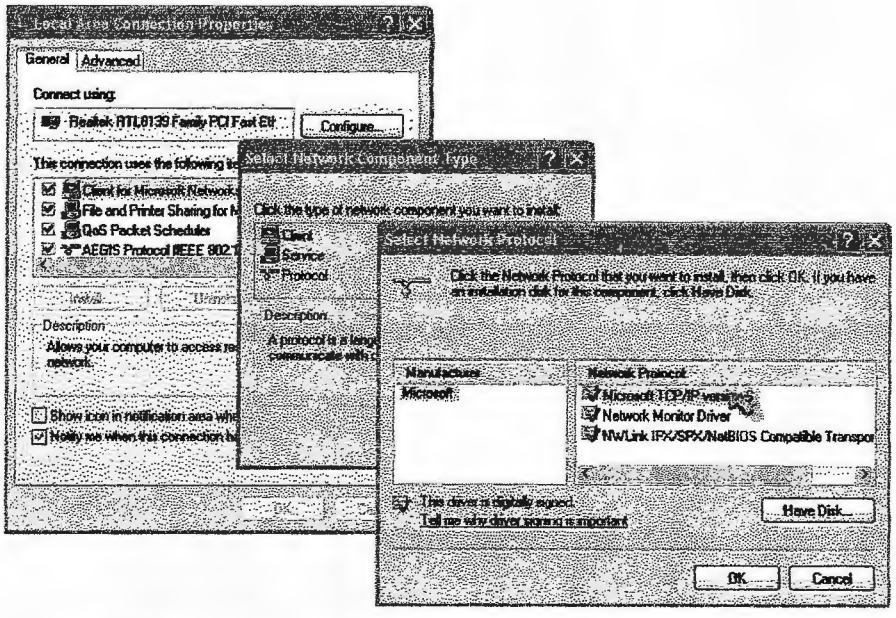


Figura 4.1. Habilitando Ipv6 sobre Windows XP y 2003 Server.

Para comprobar que el protocolo haya sido correctamente instalado se debe ejecutar en el prompt:

Prompt>netsh interface ipv6 show address (Windows 2003 Server)

Prompt>ipv6 if (Windows XP)

Se mostrara la configuración y las direcciones Ipv6 adquiridas (autoconfiguradas) para cada interfaz de red existente.

Windows 2000 con Service Pack1, Service Pack2, Service Pack3 y Service Pack4.

En el caso que se desee utilizar este sistema para navegar por sitios Web ipv6, es preciso utilizar el Internet Explorer versión 5 o posterior (u otros navegadores que soporten Ipv6)
Para habilitar Ipv6 en Windows 2000 se debe instalar un archivo que posee las características de Ipv6, esta instalación es valida en cualquier versión comercial de Windows 2000 , siempre que tenga instalado Service Pack1.
Se debe ejecutar el fichero tpipv6-001295.exe desde:
http://msdn.microsoft.com/downloads/sdks/platform/tpipv6/download.asp.
Una vez se tiene el archivo se debe descomprimir y ejecutar el programa setup.exe para instalar Ipv6, probablemente se tenga que reiniciar el ordenador. A continuación se realizan los siguientes pasos.

1) Menú de Inicio.
2) Panel de Control.
3) Conexiones de Red (Doble Clic).
4) Conexión de Área local (Clic derecho).
5) Propiedades.
6) Instalar.
7) Protocolo
8) Microsoft TCP/IP Version6.
9) Aceptar (Enter)

Para comprobar que el protocolo haya sido correctamente instalado se debe ejecutar en el prompt:
Prompt>ipv6 if
Se mostrara la configuración y las direcciones IPv6 adquiridas (autoconfiguradas) para cada interfaz de red existente.

Para Service Pack2 se debe descargar el fichero tpipv6-001205-SP2-IE6.zip desde:
http://www.ipng.nl/ tpipv6-001205-SP2-IE6.zip
Para Service Pack3 y 4 se debe descargar el fichero tpipv6-001205-SP3-IE6.zip desde:
http://www.ipng.nl/ tpipv6-001205-SP3-IE6.zip

4.3.1.2- Plataformas Linux

En Linux Ipv6 se implementa como un modulo de kernel. Así, las distribuciones con kernel 2.2.x y 2.4.x ya vienen con este soporte y normalmente el modulo Ipv6 ya esta instalado. De todas formas, habrá que asegurarse que el modulo se carga al arrancar.

Para comprobar que el kernel soporta Ipv6, habrá que comprobar que existe la siguiente entrada:
/proa/net/if_inet6
Si no existe, se puede intentar cargar el modulo Ipv6 con:
#> modprobe ipv6

Si se ha cargado correctamente debe existir la entrada mencionada anteriormente.
Nota: Descargar el modulo puede, a veces, provocar la caída del sistema. Aunque en versiones actuales de los módulos (kernel 2.4.19 adelante) el soporte es muy estable.

Para que cargue de forma automática el modulo Ipv6 cuando se demande, se añade al fichero /etc/modules.conf la siguiente línea:

Alias net-pf-10 ipv6
Alias sit0 ipv6
Alias sit1 ipv6
Alias tun6to4 ipv6

Para deshabilitar la carga automática se debe utilizar el comando: alias net-pf-10 off

Las direcciones Ipv6 sobre una interfase se pueden configurar por medio del comando ip o ifconfig, de la siguiente manera:
#> /sbin/ip -6 addr show dev <interface>
#> /sbin/ifconfig <interface>

Donde las interfaces pueden ser de tipo loopback, Ethernet, etc. Por ejemplo:
#> /sbin/ip -6 addr show dev eth0
#> /sbin/ifconfig eth0

También se puede eliminar direcciones Ipv6 con el uso de los comandos ip o ifconfig:
#> /sbin/ip -6 addr del <ipv6address>/<prefixleghnt> dev <interface>
#> /sbin/ifconfig <interface> inet6 del <ipv6address>/<prefixlenght>
Donde las interfaces pueden ser de tipo loopback, Ethernet, etc.

4.3.2 Protocolo Dual Stack Ipv4-Ipv6.

La técnica del Protocolo Dual Stack Ipv4-Ipv6 se creo para el proceso de transición a Ipv6. Esta habilita una a una las actualizaciones de las aplicaciones corriendo en los nodos para que puedan hacer uso del stack del protocolo Ipv6. Las aplicaciones que no son actualizadas pueden coexistir con las aplicaciones actualizadas en el mismo nodo. Las aplicaciones nuevas y actualizadas simplemente hacen uso del Protocolo Doble Pila Ipv4-Ipv6. Ver la figura 4.2.

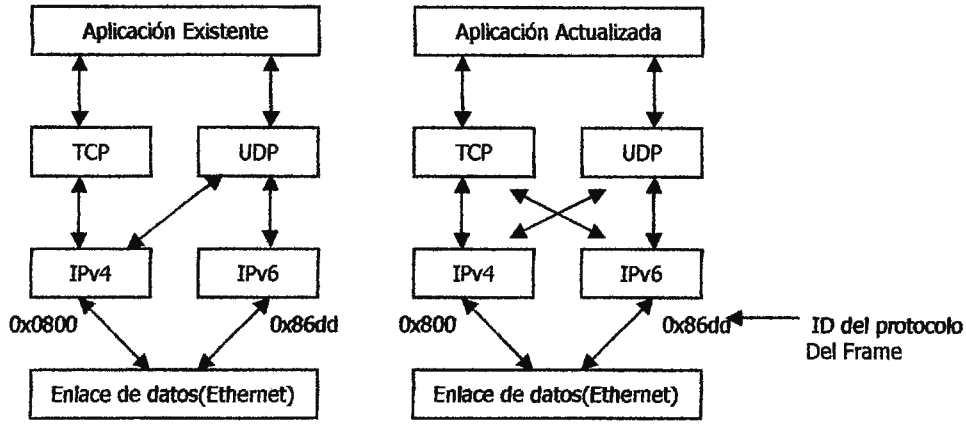


Figura 4.2 Protocolo Doble Pila (Dual Snack) Ipv4-Ipv6.

Una nueva interfaz de programación de aplicación (API), ha sido definida para soportar direcciones Ipv4 e Ipv6 y solicitudes DNS. Una aplicación puede ser actualizada a la nueva API y permanecer con el uso del stack del protocolo Ipv4. El software IOS Cisco soporta la técnica del Protocolo Dual Stack Ipv4-Ipv6. Cuando una interfaz esta configurada con ambas direcciones Ipv4 e Ipv6, esta enviara trafico de ambos protocolos.

En la figura 4.3, una aplicación que soporta el protocolo doble pila Ipv4-Ipv6 solicita todas las direcciones disponibles para un nombre de host www.a.com desde un servidor DNS. El servidor DNS responde con todas las direcciones disponibles (ya sea direcciones Ipv4 o Ipv6) para www.a.com. La aplicación escoge una dirección, por lo general la dirección Ipv6 es la elegida por defecto y conecta el nodo origen al nodo destino utilizando la pila del protocolo Ipv6.

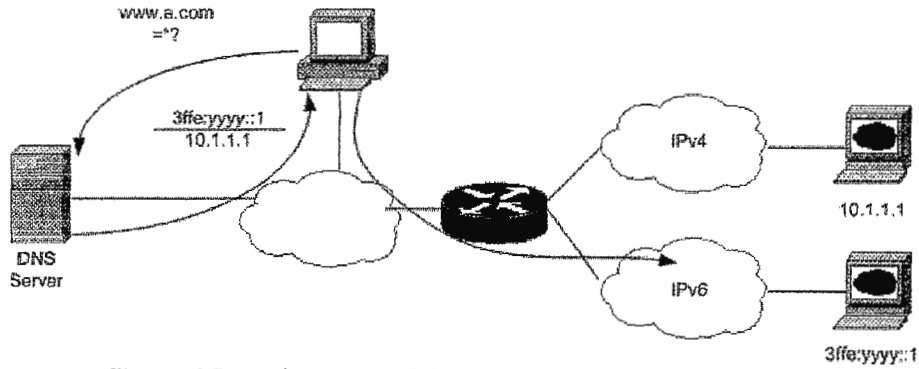


Figura 4.3 Aplicaciones del Protocolo Dual Stack Ipv4-Ipv6.

Cuando una interfaz en un dispositivo de red de Cisco es configurada con ambas direcciones Ipv4 e Ipv6, dicha interfaz envía tráfico de paquetes Ipv4 e Ipv6, además puede enviar y recibir datos desde redes Ipv6 e Ipv4.

Para configurar una interfaz de un dispositivo de red Cisco de tal manera que soporte la pila de protocolos Ipv4 e Ipv6 se debe utilizar la siguiente configuración desde el modo de configuración global.

Pasos de Configuración:

1. enable
2. configure terminal
3. ipv6 unicast-routing
4. interface *type number*
5. ip address *ip-address mask* [**secondary**]
6. ipv6 address *ipv6-prefix/ prefix-length* [**eui-64**]

A continuación se presenta un resumen de los comandos que se utilizan para la configuración del stack de protocolos Ipv4 e Ipv6:

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.

3	**ipv6 unicast-routing** **Ejemplo:** Router(config)# ipv6 unicast-routing	Habilita el envío de datagramas unicast Ipv6
4	**Interface** type number **Ejemplo:** Router(config)# interface Ethernet 0	Especifica el número, el tipo de interfase y entra al modo de configuración de interfase.
5	**ip address** ip-address mask [**secondary**] **Ejemplo:** Router(config-if)# ip address 192.168.99.1 255.255.255.0	Especifica la dirección Ipv4 primaria y secundaria para una interfaz.
6	**ipv6 address** ipv6-prefix/ prefix-length [**eui-64**] **Ejemplo:** Router(config-if)# ipv6 address 2001:0DB8:c18:1::3/64	Especifica la red Ipv6 asignada a la interfaz y habilita el procesamiento Ipv6 sobre la interfaz.

Tabla 4.3 Configuracion del Protocolo Dual Snack.

4.3.2.1 Ejemplo de Configuración:

El siguiente ejemplo habilita el envío de datagramas unicast ipv6 globalmente sobre el router y configura la interfaz ethernet 0 con una dirección Ipv4 y una dirección Ipv6.

```
Ipv6 unicast-routing

interface Ethernet0
ip address 192.168.99.1 255.255.255.0
ipv6 address 2001:0DB8:c18:1::3/64
```

4.3.3 Prefijos Generales Ipv6.

Los 64 bits de la parte alta de una dirección Ipv6 están compuestos de un prefijo de enrutamiento global y un identificador de subred. Un prefijo general utiliza 48 bits y a partir de este se pueden definir prefijos específicos que posean un mayor numero de bits (64 bits) ; pero cuando el prefijo general sea modificado, todos los prefijos específicos creados a partir de este serán modificados también. Esta función simplifica grandemente la renumeración de redes y permite la definición automática de prefijos.

Por ejemplo un prefijo general debe poseer 48 bits de longitud y los prefijos especificos generados a partir de este deben ser de 64 bits de longitud. En el siguiente ejemplo los primeros 48 bits de todos los prefijos específicos son idénticos y los últimos 16 bits son diferentes.

Prefijo General: 2001:0DB8:2222::/48

- Prefijo Especifico: 2001:0DB8:2222:0000::/64
- Prefijo Especifico: 2001:0DB8:2222:0001::/64
- Prefijo Especifico: 2001:0DB8:2222:4321::/64
- Prefijo Especifico: 2001:0DB8:2222:7744::/64

Los Prefijos Generales pueden ser definidos e diferentes formas:

- Manualmente.
- Basados en una interfaz 6to4.
- Dinámicamente, por medio de un prefijo recibido a través de un DHCP para un cliente de delegación de prefijo Ipv6.

4.3.3.1 Definiendo Prefijos Generales Manualmente.

Los siguientes pasos describen como se define un prefijo general manualmente:

1. enable
2. configure terminal

3. ipv6 general-prefix *prefix-name* [*ipv6-prefix/prefix-length*] [**6to4** *interface-type interface-number*]

A continuación se presentan detalladamente los pasos necesarios para la configuración de un Prefijo General manualmente:

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado
2	**configure terminal** **Ejemplo:** Router# configure terminal	Entra al modo de configuración global.
3	**ipv6 general-prefix** prefix-name { ipv6-prefix/ prefix-length | **6to4** interface-type interface-number} **Ejemplo:** Router(config)# ipv6 general-prefix my-prefix 2001:DB8:2222::/48	Define un prefijo general para una dirección Ipv6. Cuando se define un prefijo General manualmente se deben especificar los argumentos *ipv6-prefix* y */prefix-length.*

Tabla 4.4 Definiendo Prefijos Generales Manualmente.

4.3.3.2 Definiendo Prefijos Generales Basados en una Interfase 6to4.

Los siguientes pasos describen como se define un prefijo general basado en una interfaz 6to4:

1. enable

2. configure terminal

3. ipv6 general-prefix *prefix-name* [*ipv6-prefix/prefix-length*] [**6to4** *interface-type interface-number*]

A continuación se presentan detalladamente los pasos necesarios para la configuración de un Prefijo General basado una interfaz 6to4:

PASO	COMANDO	PROPOSITO
1	**Enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado
2	**configure terminal** **Ejemplo:** Router# configure terminal	Entra al modo de configuración global.
3	**ipv6 general-prefix** prefix-name { ipv6-prefix/ prefix-length | **6to4** interface-type interface-number} **Ejemplo:** Router(config)# ipv6 general-prefix my-prefix 6to4 ethernet0	Define un prefijo general para una dirección Ipv6. Cuando se define un Prefijo General basado en una interfaz 6to4 se debe especificar la etiqueta 6to4 y los argumentos *interface-type interface-number.* Cuando la interfase es utilizada para un túnel 6to4 el prefijo general será de la forma 2002:a.b.c.d::/48, donde a.b.c.d es la dirección Ipv4 de la interfase en referencia.

Tabla 4.5 Definiendo Prefijos Generales con Interfase 6to4.

4.3.3.3 Definiendo Prefijos Generales con DHCP para un Cliente de Delegación de Prefijo Ipv6.

Los siguientes pasos describen como se define un prefijo general con DHCP para un Cliente de Delegación de Prefijo Ipv6.

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 dhcp client pd** *prefix-name* [**rapid-commit**]

A continuación se presentan detalladamente los pasos necesarios para la configuración del Prefijo General:

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado

2	**configure terminal** **Ejemplo:** Router# configure terminal	Entra al modo de configuración global.
3	**interface** type number **Ejemplo:** Router(config)# interface Ethernet 0/0	Especifica el tipo de interfaz, el número y ubica el router en el modo de configuración de interfaz.
4	**ipv6 dhcp client pd** prefix-name [**rapid-commit**] **Ejemplo:** Router(config-if)# ipv6 dhcp client pd dhcp-prefix.	Habilita el DHCP para los procesos de cliente Ipv6 y habilita una solicitud para una delegación de prefijo a través una interfaz específica. El prefijo delegado se almacena en el argumento prefix-name del prefijo general.

Tabla 4.6 Definiendo Prefijos Generales con DHCP.

4.3.3.4 Usando Prefijos Generales.

Los siguientes pasos describen como usar un prefijo general:

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address** *prefix-name ipv6-prefix/ prefix-length*

A continuación se presentan detalladamente los pasos necesarios para el uso de Prefijos Generales.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado
2	**configure terminal** **Ejemplo:** Router# configure terminal	Entra al modo de configuración global.
3	**interface** type number **Ejemplo:** Router(config)# interface □erminal 0/0	Especifica el tipo de interfaz, el número y ubica el router en el modo de configuración de interfaz.

4	**ipv6 address** prefix-name ipv6-prefix/ prefix-length **Ejemplo:** Router(config-if) ipv6 address my-prefix 0:0:0:7272::/64	Configura un nombre de prefijo Ipv6 para una dirección Ipv6 y habilita el procesamiento Ipv6 en la interfaz.

Tabla 4.7 Usando Prefijos Generales

4.3.4 DNS para Ipv6.

Ipv6 introduce nuevos tipos de registro DNS en los procesos de búsqueda, ya sea para traducciones de nombre a dirección o de dirección a nombre. Los nuevos tipos de registros DNS soportan direcciones Ipv6 y se muestran en la Tabla 4.8.

REGISTRO	DESCRIPCION	FORMATO
AAAA	Mapea un nombre de host a una dirección Ipv6. Este es equivalente al registro A utilizado en Ipv4. El soporte para el registro AAAA o A ya sea en transporte Ipv6 o Ipv4 respectivamente es soportado por la versión IOS 12.2(8)T o superior.	www.abc.test AAAA FFE:YYYY:C18:1::2
PTR	Mapea una dirección Ipv6 a un nombre de Host. Este es equivalente al registro PTR en Ipv4	2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0.y.y.y.y.e.f.f.3.ip6.int PTR www.abc.test

Tabla 4.8 Nuevos Registros DNS para Ipv6.

4.3.4.1 Mapeando Nombres de Host a Direcciones Ipv6.

Un servidor de nombres puede mantener una base de datos que contiene los mapeos realizados de nombres a direcciones. Cada nombre de host puede mapear una o varias direcciones Ipv4, Ipv6 o ambos tipos.

Para poder utilizar este tipo de servicio se debe especificar un nombre de servidor y habilitar el Servidor de Nombres de Dominio (DNS).
El software de Cisco IOS mantiene una memoria caché que contiene los mapeos de los nombres a direcciones que se utilizan cuando se realiza una conexión Telnet, un comando Ping, operaciones de

soporte Telnet, y otros comandos de ejecución. Además acelera el proceso de conversión de nombres a direcciones.

Así como en Ipv4, Ipv6 utiliza un esquema de nombramiento que permite a un dispositivo de red ser identificado por su posición dentro de un espacio de nombres jerárquico proveído por los dominios. Los nombres de dominio se unen a través de puntos (.), los cuales se utilizan como caracteres de delimitación. Por ejemplo, Cisco es una Organización comercial que esta identificada por un nombre de dominio (com), así que su nombre de dominio es cisco.com. Un dispositivo especifico en este dominio, el FTP Server por ejemplo, es identificado *por ftp.cisco.com.*

A continuación se presenta un resumen de los comandos que se utilizan para la configuración de nombres de host son:

1. enable

2. configure terminal

3. ipv6 host *name* [*porf*] *ipv6-address1* [*ipv6-address2...ipv6-address4*]

4. ip domain-name *name* o **ip domain-list** *name*

5. ip name-server *server-address1* [*server-address2...server-address6*]

6. ip domain-lookup

Los comandos que se utilizan para la configuración de nombres de host se pueden observar en forma detallada en la siguiente tabla.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**ipv6 host** name [port] ipv6-address1 [ipv6-address2...ipv6-address4] **Ejemplo:** Router(config)# ipv6 host cisco-sj 2001:0DB8:20:1::12	Define un mapeo estático de nombre de host a dirección Ipv6 Típicamente, es mas fácil de referirse a dispositivos de red a través de nombres simbólicos que a través de direcciones ip. (Los servicios como Telnet pueden utilizar hostnames o direcciones). La asignación manual de nombres de host a direcciones es muy útil cuando el mapeo dinámico no es disponible.

4	**ip domain-name** name o **ip domain-list** name **Ejemplo:** Router(config)# ip domain-name fifa.com or **Ejemplo:** Router(config)# ip domain-list fifa1.com	(Opcional). Define un nombre de dominio por defecto que el software Cisco IOS utilizara para completar los nombres de host no clasificados. O (Opcional). Define una lista de nombres de dominio por defecto para completar los nombres de host no clasificados. Cualquier host que no contenga un nombre de dominio completo tendrá el nombre de dominio por defecto previamente especificado.
5	**ip name-server** server-address1 [server-address2...server-address6] **Ejemplo:** Router(config)# ip name-server 2001:0DB8::250:8bff:fee8:f800 2001:0DB8:0:f004::1	Especifica uno o más host que pueden funcionar como servidores de nombres para proveer información de nombres por DNS.
6	**ip domain-lookup** **Ejemplo:** Router(config)# ip domain-lookup	Habilita la traducción DNS-based

Tabla 4.9 Mapeando nombres de Host a Direcciones.

4.3.4.2 Ejemplo de configuración.

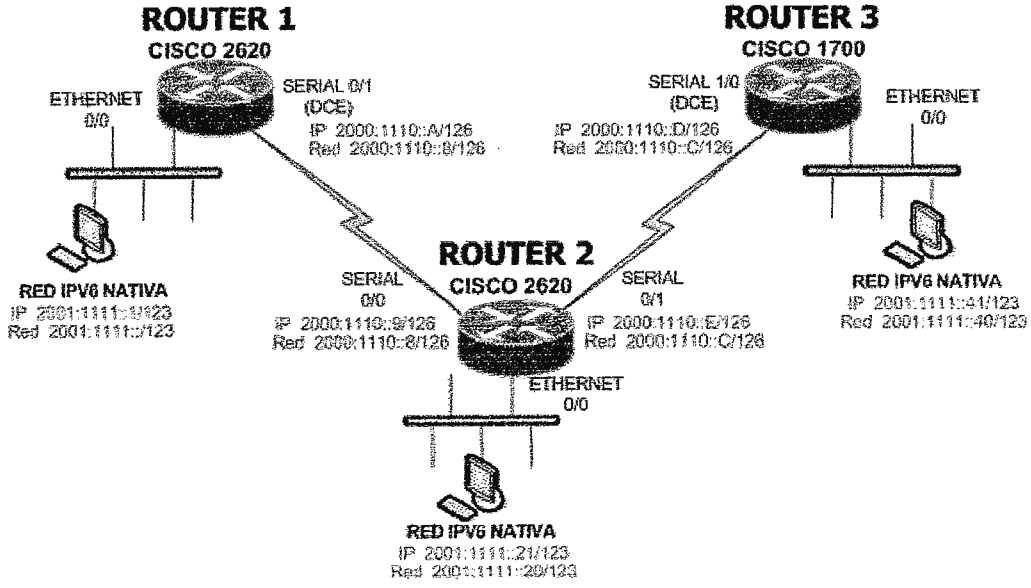


Figura 4.4 Esquema para mapeos de Nombres a Direcciones.

El diagrama anterior se muestra una Red Nativa Ipv6 compuesta por tres enrutadores, los cuales se encuentran conectados a través de sus seriales, cada una de ellas configurada con una dirección Ipv6 así:

- Router 1: Interfase Serial 0/1, con dirección Ipv6 2000:1110::A/126.
- Router 2: Interfase Serial 0/0, con dirección Ipv6 2000:1110::9/126 y
  Interfase Serial 0/1, con dirección Ipv6 2000:1110::E/126.
- Router 3: Interfase Serial 1/0, con dirección Ipv6 2000:1110::D/126.

Cada nodo posee una Red de Área Local (LAN), identificada por intereses FastEthernet, cada una configurada con una dirección Ipv6 perteneciente a una red especifica. Así:

- Router 1: Interfase FastEthernet 0/0, con direccion Ipv6 2001:1111::1/123.
- Router 2: Interfase FastEthernet 0/0, con direccion Ipv6 2001:1111::21/123.
- Router 3: Interfase FastEthernet 0/0, con direccion Ipv6 2001:1111::41/123.

Para facilitar la administración de los nodos, estas direcciones ya sea de interfases Seriales o Ethernet pueden ser mapeadas a Nombres de Host, de esta manera no se necesita conocer toda la dirección Ipv6 para poder acceder al nodo o probar su disponibilidad.

Lo primero que se debe hacer es configurar las direcciones Ipv6 de cada interfase en cada uno de loas enrutadores, como se muestra a continuación:

```
Router1(config)#
interface Serial0/1
description conexion a Router2
no ip address
ipv6 address 2000:1110::A/126
clockrate 1000000
```

Para realizar el mapeo entre direcciones Ipv6 y nombres de host se deben configurar dichos mapeos en cada enrutador con el comando **ipv6 host.** En el siguiente ejemplo se establece el nombre del

dominio y los host 2001:0DB8::250:8bff:fee8:f800 y 2001:0DB8:0:f004::1 como servidores de nombres de dominio y se rehabilita el servicio DNS.

```
Router1(config)#
ipv6 host router1 2000:1110::A
ipv6 host router2a 2000:1110::9
ipv6 host router2b 2000:1110::E
ipv6 host router3 2000:1110::D
ip domain-name prueba.com
ip name-server 2001:0DB8::250:8bff:fee8:f800 2001:0DB8:0:f004::1
ip domain-lookup
```

De esta manera será mas fácil hacer una prueba ping sobre cualquiera de las interfaces seriales de los enrutadores. Así como se muestra a continuación:

```
Router2#ping 2000:1110::a
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2000:1110::A, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
```

Así también se podrá acceder a cualquier nodo a través de un comando telnet, en este ejemplo se tiene acceso al Router 2.

```
Router1#telnet 2000:1110::9
Trying 2000:1110::9 ... Open
User Access Verification
Password:
Router2>ena
```

4.3.5 DHCP para la delegación de Prefijos Ipv6.

DHCP para Ipv6 puede ser utilizado para proveer información con estado o sin estado.

- **Con Estado:** La asignación de direcciones es administrada y los clientes deben obtener información de configuración no disponible a través del DHCP, como por ejemplo la dirección Ipv6, el servidor DNS, el Nombre de Dominio, etc.

- **Sin Estado:** Los parámetros de configuración no requieren de un servidor para mantener cualquier estado dinámico con clientes individuales, como una dirección de servidor DNS o búsquedas de domino.

La implementación de DHCP para Ipv6 sobre Cisco IOS Release 12.3(4)T soporta solamente asignación de direcciones sin estado.

Además, DHCP para Ipv6 también habilita la delegación de prefijos, a través de la cual un ISP (Internet Service Provider) puede automatizar el proceso de asignación de prefijos a un cliente para usarlo dentro de su propia red. La delegación de prefijos ocurre entre un dispositivo proveedor fronterizo o PE (Provider Edge) que comúnmente es un router y un equipo de cliente o CPE (Customer Premises Equipment), utilizando el DHCP para la delegación de prefijos Ipv6. Una vez el ISP ha delegado prefijos al cliente, este puede asignar prefijos a los enlaces en su propia red.

4.3.5.1 Configuración Ipv6 con Estado.

DHCP Con Estado en función de Cliente.

La función de DHCP como un cliente Ipv6 puede ser habilitada sobre una interfaz individual que soporte Ipv6.
DHCP como un cliente Ipv6 puede solicitar una delegación de prefijos Ipv6. Los prefijos adquiridos desde un router delegador están almacenados dentro de un conjunto de prefijos generales Ipv6 previamente definidos.

DHCP para un cliente Ipv6 construye una lista de servidores potenciales enviando un mensaje de solicitud y recolectando los mensajes de respuesta proporcionados por los servidores. Si el cliente necesita adquirir prefijos de los servidores, sólo se consideran los servidores que han anunciado prefijos.

Una Asociación de Identidad para la Delegación de Prefijo (IAPD) es una colección de prefijos asignados a un router solicitante. Un router solicitante puede tener más de un IAPD; por ejemplo, uno para cada uno de sus interfaces.

A continucacion se muestran los pasos para configurar DHCP con estado en funcion de Cliente sobre una interfase y habilitar la Delegacion de Prefijo sobre la misma.

1. enable
2. configure terminal
3. interface *type number*
4. ipv6 dhcp client pd *prefix-name* [**rapid-commit**]

En la siguiente tabla se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado
2	**configure terminal** **Ejemplo:** Router# configure terminal	Entra al modo de configuración global.
3	**interface** interface-type interface-number **Ejemplo:** Router(config)# interface serial 3	Especifica el tipo de interfaz, el número y ubica el router en el modo de configuración de interfaz.
4	**ipv6 dhcp client pd** prefix-name [**rapid-commit**] **Ejemplo:** Router(config-if)# ipv6 dhcp client pd dhcp-prefix	Habilita el DCHP para el Proceso de Cliente Ipv6 y habilita una solicitud para la delegacion de prefijos a traves de una interfase especifica

Tabla 4.10 Configurando DHCP con Estado como Cliente Ipv6.

DHCP con Estado en Funcion de Servidor.

La función de DHCP como un cliente Ipv6 puede ser habilitada sobre una interfaz individual que soporte Ipv6.

El Servidor DHCP se utiliza para proveer algunos parámetros de configuración importantes para el cliente, por ejemplo: la direccion Ip, el Servidor de Nombres de Dominio, el Dominio, etc. Estos

parámetros de configuración para los clientes son independientemente configurados dentro de conjuntos conocidos como "pools", los cuales se almacenan en la NVRAM.

El Servidor DHCP mantine una tabla de asiganciones en memoria, para determinar los parámetros de configuración asignados a los clientes, tales como prefijos entre el servidor y sus clientes.

Los pasos para la configuración del DHCP con estado en funcion de Servidor para Ipv6 son:

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **domain-name** *domain*
5. **dns-server** *ipv6-address*
6. **prefix-delegation** *ipv6-prefix/ prefix-length client-DUID* [**iaid** *iaid*] [**lifetime**]
7. **prefix-delegation pool** *poolname* [**lifetime**]
8. **exit**
9. **interface** *type number*
10. **ipv6 dhcp server** *poolname* [**rapid-commit**] [**preference** *value*] [**allow-hint**]

A continuación se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPÓSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado
2	**configure terminal** **Ejemplo:** Router# configure terminal	Entra al modo de configuración global.
3	**ipv6 dhcp pool** poolname **Ejemplo:** Router(config)# ipv6 dhcp pool dhcp-pool	Entra el DHCP al modo de configuración de intervalo (pool) Ipv6

4	**domain-name** domain **Ejemplo:** Router(config-dhcp)# domain-name domain1.com	Especifica el Nombre de Dominio disponible en el DHCP para los clientes Ipv6.
5	**dns-server** ipv6-address **Ejemplo:** Router(config-dhcp) dns-server 2001:0DB8:3000:3000::42	Especifica el servidor DNS (Domain Name Server) disponible en el DHCP para los clientes Ipv6.
6	**prefix-delegation** ipv6-prefix/ prefix-length client-DUID [**iaid** iaid] [**lifetime**] **Ejemplo:** Router(config-dhcp)# prefix-delegation 2001:0DB8:1263::/48 0005000400F1A4D070D03	Especifica un prefijo numerico manualmente configurado para ser delegado a un cliente específico IAPD del cliente.
7	**prefix-delegation pool** poolname [**lifetime**] **Ejemplo:** Router(config-dhcp)# prefix-delegation pool prefix-pool lifetime 1800 600	Especifica el nombre a un conjunto de prefijos Ipv6, los cuales son delegados a clientes DHCP.
8	**exit** **Ejemplo:** Router(config-if)# exit	Sale del modo de configuración de DHCP y regresa al modo de configuración global del router.
9	**interface** interface-type interface-number **Ejemplo:** Router(config)# interface serial 3	Especifica el tipo de interfaz, el número y ubica el router en el modo de configuración de interfaz.
10	**ipv6 dhcp server** poolname [**rapid-commit**] [**preference** value] [**allow-hint**] **Ejemplo:** Router(config-if)# ipv6 dhcp server dhcp-pool	Habilita el DHCP para Ipv6 sobre un ainterface.

Tabla 4.11 Configurando DHCP con Estado como Servidor Ipv6.

4.3.5.2 Configuración de Ipv6 Sin Estado.

Todas las interfaces sobre nodos Ipv6 deben poseer una dirección de enlace local, la cual es configurada automáticamente desde el identificador por una interfaz y el prefijo de enlace local FE80::/10. Una dirección de enlace local habilita un nodo para comunicarse con otros nodos sobre el enlace y puede ser utilizada para configurar el nodo.

Los nodos se pueden conectar a una red y automáticamente generar una dirección de sitio local o global, sin la necesidad de configurarlas manualmente o de la ayuda de un servidor, como el servidor DHCP. Con Ipv6, un router sobre el enlace, anuncia prefijos de sitio local o global a través de mensajes específicos y puede funcionar como router por defecto para el enlace. Los mensajes de aviso del router son enviados periódicamente y en respuesta a los mensajes de solicitud, los cuales son enviados por las terminales al inicializar el sistema. Ver la figura 4.5.

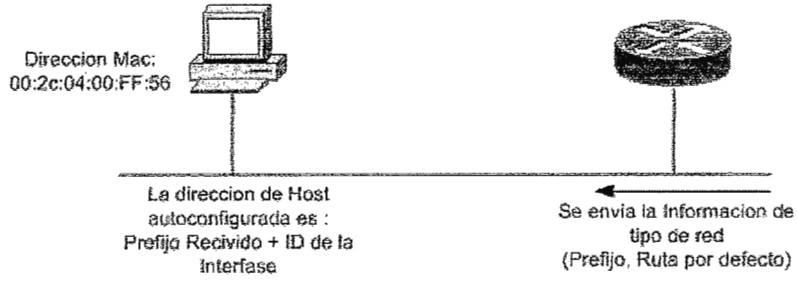


Figura 4.5 Auto configuración Ipv6 sin estado.

Un nodo sobre el enlace puede configurar automáticamente direcciones Ipv6 globales y de sitio local añadiendo su identificador de interfaz de 64 bits a los prefijos de 64 bits incluidos en los mensajes de aviso de los routers. La dirección Ipv6 resultante (128 bits) configurada por el nodo es entonces comparada con un detector de direcciones duplicadas para determinar que sea única en el enlace. Si los prefijos anunciados en los mensajes de aviso de los routers son globalmente únicos, se garantiza que las direcciones Ipv6 configuradas por los nodos serán globalmente únicas. Los mensajes de solicitud de router poseen un valor de 133 en el campo de Tipo del encabezado de paquete ICMP y son enviados por los host cuando se inicializa el sistema, de esta manera los host se pueden configurar inmediatamente sin la necesidad de esperar el siguiente mensaje de aviso del router.

Configurando DHCP Sin Estado como un Servidor Ipv6.

Los siguientes pasos describen como configurar el Protocolo de Configuración Dinamica de Host (DHCP) sin estado. El servidor no mantiene ningún estado relacionado con los clientes; por ejemplo,

no se asocia ningún conjunto de prefijos (prefix pool), ni registros de asignación. Por lo tanto esta función se conoce como DHCP sin estado para Ipv6.

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **dns-server** *ipv6-address*
5. **domain-name** *domain*
6. **exit**
7. **interface** *type number*
8. **ipv6 dhcp server** *poolname* [**rapid-commit**] [**preference** *value*] [**allow-hint**]
9. **ipv6 nd other-config-flag**

A continuación se presentan detalladamente los pasos necesarios para la configuración de DHCP sin estado.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado
2	**configure terminal** **Ejemplo:** Router# configure terminal	Entra al modo de configuración global.
3	**ipv6 dhcp pool** poolname **Ejemplo:** Router(config)# ipv6 dhcp pool dhcp-pool	Entra al modo de configuración del conjunto (pool) Ipv6 para DHCP.
4	**dns-server** ipv6-address **Ejemplo:** Router(config-dhcp) dns-server 2001:0DB8:3000:3000::42	Especifica el servidor DNS (Domain Name Server) disponible en el DHCP para los clientes Ipv6.
5	**domain-name** domain **Ejemplo:** Router(config-dhcp)# domain-name domain1.com	Especifica el Nombre de Dominio disponible en el DHCP para los clientes Ipv6.

6	**exit** **Ejemplo:** Router(config-if)# exit	Sale del modo de configuración de intervalo Ipv6 en el DHCP y regresa al modo de configuración global del router.
7	**interface** interface-type interface-number **Ejemplo:** Router(config)# interface serial 3	Especifica un número, tipo de interfaz y ubica el router en el modo de configuración de interfase.
8	**ipv6 dhcp server** poolname [**rapid-commit**] [**preference** value] [**allow-hint**] **Ejemplo:** Router(config-if)# ipv6 dhcp server dhcp-pool	Habilita del DHCP para Ipv6 sobre una Interfaz.
9	**ipv6 nd other-config-flag** **Example:** Router(config-if)# ipv6 nd other-config-flag	Establece la bandera "Other stateful configuration" en los mensajes de aviso del router Ipv6.

Tabla 4.12 Configurando DHCP Sin Estado como un Servidor Ipv6.

Configurando DHCP Sin Estado como un Cliente Ipv6.

Los siguientes pasos describen como configurar DHCP Sin Estado como un Cliente Ipv6:

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address autoconfig**

A continuación se presentan detalladamente los pasos para configurar DHCP Sin Estado como un Cliente Ipv6:

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado
2	**configure terminal** **Ejemplo:** Router# configure terminal	Entra al modo de configuración global.

3	**interface** interface-type interface-number **Ejemplo:** Router(config)# interface serial 3	Especifica el tipo de interfaz, el número y ubica el router en el modo de configuración de interfaz.
4	**ipv6 address autoconfig** **Ejemplo:** Router(config-if)# **ipv6 address autoconfig**	Habilita la Auto configuración automática de direcciones Ipv6 utilizando la auto configuración sin estado sobre una interface y habilita el procesamiento Ipv6 sobre la Interfaz.

Tabla 4.13 Configurando DHCP Sin Estado como un Cliente Ipv6

4.3.6 Cef y dCef para Ipv6

El Reenvío de Paquetes para Ipv6 (CEFv6) es una tecnología avanzada de conmutación ip de capa 3 que se utiliza para el reenvío de paquetes Ipv6. CEF distribuido para Ipv6 (dCEF) realiza las mismas funciones que CEF pero para plataformas de arquitectura distribuida como por ejemplo los Routers Cisco de la serie 12000 y la serie 7500. CEFv6 y dCEFv6 funcionan y proveen los mismos beneficios que CEFv4 y dCEFv4. Las entradas de red que son agregadas, eliminadas o modificadas en la Base de Información de Enrutamiento (RIB), según lo dictado por el protocolo de enrutamiento en uso, son reflejadas en las Bases de Información de Envío (FIBs) y las tablas de adyacencias Ipv6 mantienen las direcciones de siguiente salto de capa 2 para todas las entradas en cada FIB.

En la versión de Cisco IOS Release 12.0(21)ST, dCEFv6 incluye soporte Ipv6 para prefijos y direcciones. En la versión de Cisco IOS Release 12.0(22)S o posteriores y en la Cisco IOS Release 12.2(13)T o posteriores, dCEFv6 y CEFv6 tienen la capacidad de incluir soporte de FIBs para direcciones globales, enlace local y sitio local, en forma separada.

Cada interfase de un router Ipv6 tiene una asociación con una FIB global, FIB de enlace local y una FIB de sitio local (varias interfaces del router pueden tener una asociación con la misma FIB). Todas las interfaces del router que se encuentren en un mismo enlace Ipv6 comparten una misma FIB de enlace local. Los paquetes Ipv6 que poseen una dirección global como destino son procesados por el FIB global Ipv6 y los paquetes que poseen una dirección de sitio local como destino son procesados por el FIB de sitio local Ipv6.

4.3.6.1 Reenvío Unicast de Trayectoria Reversa (URPF)

El Unicast RPF es utilizado para solucionar problemas causados por direcciones de origen Ipv6 mal formadas (spoofing) que pasan a través de un router Ipv6. Estas direcciones de origen malformadas

pueden indicar ataques de denegación de servicio (DoS) basados en un spoofing a una dirección Ipv6 de origen.
Cuando RPF es habilitado en una interfase, el router examina todos los paquetes recibidos sobre la interfase y verifica que la dirección de origen aparezca en la tabla de enrutamiento y concuerde con la interfase en la cual fue recibido.

Si el Unicast RPF no encuentra ninguna ruta de origen del paquete (Reverse Path), este puede botar o reenviar el paquete dependiendo también de la existencia de alguna lista de acceso especificada; este tipo de trafico también se toma en cuenta en las estadísticas de trafico ip para Unicast RPF.

4.3.6.2 Configurando CEF y dCEF para Ipv6.

Para el envío de trafico CEF y dCEF se debe configurar sobre el router el envío de datagramas unicast en el modo de configuración global utilizando el comando de configuración **ipv6 unicast-routing,** además se debe configurar una dirección ipv6 a la interfaz utilizando el comando **ipv6 address.**

Se debe habilitar CEFv4 globalmente en el router utilizando el comando **ip cef** , antes de habilitar CEFv6 globalmente en el router, de igual manera se debe habilitar dCEFv4 globalmente utilizando el comando **ip cef distributed** antes de habilitar dCEFv6 globalmente en el router.
CEFv6 y dCEFv6 soportan los siguientes tipos de interfaces y encapsulaciones:

- ATM PVC y ATM LANE
- Cisco HDLC (Control de Enlace de Datos de Alto Nivel).
- Ethernet, Fast Ethernet, y Gigabit Ethernet
- FDDI
- Frame Relay PVC
- PPP sobre Packet-Over-SONET,interfaces ISDN, y serial (sincronas y asincronas).

CEFv6 y dCEFv6 no soportan los siguientes tipos de interfaces y encapsulaciones:

- HP 100VG-AnyLAN
- Switched Multimegabit Data Service (SMDS)
- Token Ring
- X.25

Pasos para configurar CEFv6 y dCEFv6.

1. enable

2. configure terminal

3. ipv6 cef

or

ipv6 cef distributed

4. ipv6 cef accounting [non-recursive | per-prefix | prefix-length]

A continuación se presenta un resumen de los comandos que se utilizan para la configuración de CEFv6 y dCEFv6.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**ipv6 cef** o **ipv6 cef distributed** **Ejemplo:** Router(config)# ipv6 cef o **Ejemplo:** Router(config)# ipv6 cef distributed	Habilita CEFv6 globalmente en el router. o Habilita dCEFv6 globalmente en el router.
4	**ipv6 cef accounting [non-recursive | per-prefix | prefix-length]** **Ejemplo:** Router(config)# ipv6 cef accounting	Habilita el conteo de redes para CEFv6 y dCEFv6 globalmente en el router. El conteo de redes para CEFv6 y dCEFv6 te permite una mejor comprensión el comportamiento del trafico CEFv6 dentro de la red, recopilando estadísticas del trafico CEFv6 y dCEFv6. Por ejemplo, te permite recolectar el número de paquetes y bytes enviados hacia un destino o el número de paquetes enviados a través de un destino. El comando opcional **per-prefix**

		habilita la recolección del numero de paquetes y bytes reenviados a un prefijo Ipv6. El comando opcional **prefix-length** habilita la recolección del numero de paquetes y bytes a una longitud de prefijo Ipv6.

Tabla 4.14 Configurando CEF y dCEF para Ipv6.

4.3.6.3 Ejemplo de Configuración.

En el siguiente ejemplo, CEFv6 y el conteo de red para CEFv6 ha sido habilitado globalmente en un router dentro de una arquitectura no distribuida, donde CEFv6 ha sido habilitado sobre la interfase Ethernet 0. El ejemplo también muestra que ha sido habilitado el reenvío de datagramas unicast por medio del comando **ipv6 unicast-routing** en el modo de configuración global.
Una dirección Ipv6 también ha sido configurada sobre la interfase Ethernet 0 y al mismo tiempo se ha configurado CEFv4 por medio del comando **ip cef** en el modo de configuración global.

```
ip cef
ipv6 unicast-routing
ipv6 cef
ipv6 cef accounting prefix-length
interface Ethernet0
ip address 10.4.9.11 255.0.0.0
media-type 10BaseT
ipv6 address 2001:0DB8:C18:1::/64 eui-64
```

En el siguiente ejemplo, dCEFv6 y el conteo de red para dCEFv6 ha sido habilitado globalmente en un router dentro de una arquitectura distribuida. También ha sido habilitado el reenvío de datagramas unicast por medio del comando **ipv6 unicast-routing** en el modo de configuración global y el dCEFv4 ha sido configurado por medio del comando **ip dcef** en el modo de configuración global.

```
ip cef distributed
ipv6 unicast-routing
ipv6 cef distributed
```

ipv6 cef accounting prefix-length

4.3.7 Configurando Unicast RPF.

Para usar Unicast RPF, se debe habilitar CEF o dCEF previamente en el router; pero no es necesario configurar una interface de entrada para el CEF. Mientras CEF se encuentre habilitado en el router las interfaces individuales pueden ser configuradas con otro tipo de conmutación.

El Unicast RPF no debe ser aplicado a los routers internos de una red. Las interfaces internas tienen mayor probabilidad de poseer un enrutamiento asimétrico, esto significa que existen diferentes rutas para el origen de un paquete. El Unicast RPF debe ser aplicado solamente donde exista una simetría natural o configurada.
Por ejemplo los routers fronterizos en una red de un Proveedor de Servicios de Internet (ISP) tienen mayor probabilidad de poseer un enrutamiento simétrico, que los routers que se encuentran en el núcleo (core) de la red del ISP. Los routers que se encuentran en núcleo no garantizan que la mejor ruta de reenvío hacia fuera del router será la ruta seleccionada para que los paquetes retornen al router. Por eso se recomienda aplicar el Unicast RPF sobre un enrutamiento simétrico y no sobre un enrutamiento asimétrico.

Pasos para configurar Unicast RPF.

1. enable
2. configure terminal
3. interface *interface-type interface-number*
4. ipv6 verify unicast source reachable-via {**rx** | **any**} [**allow-default**] [**allow-self-ping**] [*list*]

A continuación se presenta un resumen de los comandos que se utilizan para la configuración del Unicasst RPF.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.

3	**interface** interface-type interface-number **Ejemplo:** Router(config)# interface atm 0	Especifica el número, el tipo de interface y entra al modo de configuración de interface.
4	**ipv6 verify unicast source reachable-via** {**rx** | **any**} [**allow-default**] [**allow-self-ping**] [list] **Ejemplo:** Router(config-if)# ipv6 verify unicast source reachable-via any	Verifica la ruta de origen que existe en la tabla FIB y habilita el Unicast RPF.

Tabla 4.15 Configurando Unicast RPF.

4.3.8 Agregación de Prefijos Ipv6.

La naturaleza de agregación del espacio de direcciones Ipv6 permite realizar un direccionamiento jerárquico Ipv6. Por ejemplo una empresa puede subdividir un solo prefijo Ipv6 proveído por un ISP en múltiples prefijos para ser utilizados dentro de su propia red interna. Inversamente, un Proveedor de Servicios puede agregar todos los prefijos de sus clientes en un solo prefijo corto que el ISP puede anunciar al Internet Ipv6. (Ver la figura 4.6).

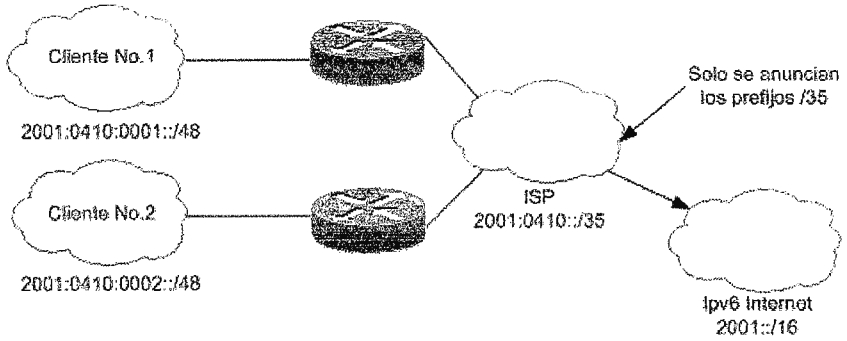


Figura 4.6 Esquema de Agregación de Prefijos Ipv6.

4.3.9 Sitio multihoming Ipv6.

Muchos prefijos pueden ser asignados a redes y usuarios. Al tener múltiples prefijos Ipv6 asignados a una red se hace más fácil que la red se pueda conectar a múltiples ISPs sin permitir el rompimiento de la tabla de enrutamiento global. Ver Figura 4.7.

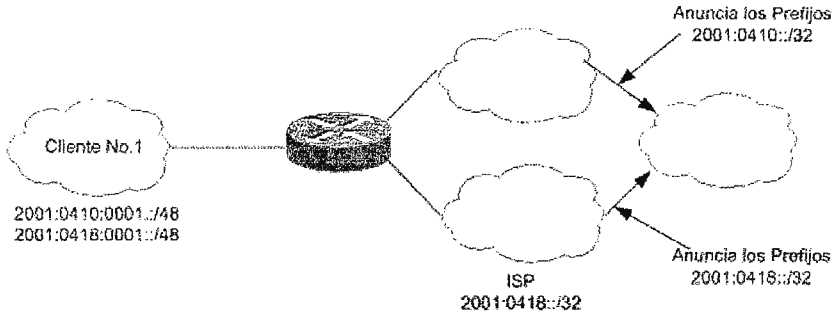


Figura 4.7 Esquema Multihoming Ipv6.

4.3.10 Movilidad Ipv6.

Se entiende por movilidad a la capacidad para que un nodo de la red mantenga la misma dirección IP a pesar de que este se desplace físicamente a otra área. Es decir que sin importar su ubicación, este pueda seguir siendo accesible a través de la misma dirección IP.

Sin esta capacidad, los paquetes destinados a un nodo móvil no estarán posibilitados para llegar al destino mientras el nodo móvil se encuentre alejado de su enlace principal (home link).

Un nodo móvil bien podría seguir manteniendo la comunicación al ir cambiando su dirección IP cada vez que salta de proveedor a proveedor, pero esto trae aparejado el problema de ir perdiendo la conexión en las capas de transporte y superiores.

Por eso es que resulta necesario el estudio y desarrollo de protocolos que permitan movilidad a lo largo de varios tipos de redes, en distintas áreas geográficas.

El soporte de movilidad es una característica muy tomada en cuenta en la implementación de IPv6, ya que se espera que una gran parte de la población requiera de servicios de movilidad durante el periodo de vida de IPv6.

La definición del protocolo que permite movilidad en IPv6 esta representada principalmente en RFC3775 (Soporte Movil para Ipv6) , además de una gran variedad de escritos que aun no han sido aprobados por la IETF.

4.3.10.1 Funcionamiento General

Un nodo móvil siempre pretenderá ser accesible desde su dirección principal, sin importar si este se encuentra físicamente conectado al su vinculo principal o ya sea que se encuentre geográficamente alejado. La dirección principal o "home address" según lo expresado en la [RFC3775] es la dirección IP que le corresponde al nodo en el ámbito de su vinculo principal. Mientras el nodo se encuentra en su vínculo principal, los paquetes destinados a esa dirección principal, son enrutados utilizando los mecanismos estándares de ruteo de Internet.

Cuando el nodo se encuentra físicamente conectado a otro vínculo, aun es accesible, por lo que se denomina un mantenimiento de direccion (care-of-address de la [RFC3775]) . La cual es una dirección IP asociada al nodo móvil que contiene el prefijo de subred del vínculo externo.
Un nodo móvil puede llegado el caso ser accedido por mas de una care-of-address. El nodo móvil puede obtener la dirección en el vínculo externo mediante los mecanismos habituales de IPv6.

El proceso de asociación entre una dirección de tipo mantenida (care of address) de un nodo móvil y su dirección principal se conoce como arrendamiento (binding). Cuando el nodo móvil se encuentra alejado, este registra su dirección de tipo care-of -address en el router de su vinculo principal (home-agent según [RFC3775]).
Cualquier otro nodo que desee comunicarse con el nodo móvil tiene dos maneras para establecer un vínculo con el nodo móvil. La primera conocida la cual se menciona en la [RFC3775] como túnel bidireccional la cual no requiere soporte de Movilidad IPv6 por parte del nodo que desee comunicarse (nodo correspondiente según la [RFC3775]). Los paquetes enviados por el nodo correspondiente son enviados al router en el vínculo principal del nodo móvil.
Y es este router (home-agent según [RFC3775]) quien a su vez lo envía al nodo móvil, ya que es el único que conoce su dirección en el vínculo externo. Para este túnel se utiliza encapsulacion de IPv6

El segundo modo mencionado en [RFC3775] se conoce como ruteo optimizado. Para este caso se necesita que el nodo móvil registre su binding actual al correspondent node.
De esta manera los paquetes con destino al nodo móvil son enrutados de manera directa a la dirección de tipo mantenida (care-of –address) del nodo móvil. Cada vez que el correspondent node necesita

enviar un paquete al nodo móvil, este primero verifica por una entrada conteniendo la dirección principal del nodo móvil en sus cached bindings , si encuentra una de estas entradas entonces mediante una cabecera especial IPv6 enrutara de manera directa hacia el nodo móvil a través de la dirección tipo mantenida.

4.3.10.2 Algunas diferencias respecto a la Movilidad en IPv4.

- La implementación de movilidad sobre IPv4 comparte muchas de las características que su contraparte en IPv6. Sin embargo debido a las características esenciales de la implementación de IPv6, es que la movilidad sobre IPv6 ofrecen una serie de ventajas.

- No hay necesidad de routers especiales. La implementación de movilidad en IPv6 funciona en cualquier lugar físico sin la necesidad de características especiales en el router local.

- El soporte de optimización en el ruteo es intrínseco a la implementación de IPv6, no así en IPv4 que requiere una serie de parches externos.

- La implementación de Movilidad sobre IPv6 esta totalmente desacoplada de la capa de enlace, usando el Protocolo de Descubrimiento de Vecinos. Lo cual le otorga mayor robustez al protocolo.

4.3.11 ICMP para Ipv6.

El protocolo de Mensajes de Control de Internet (Internet Control Message Protocol), descrito originalmente en el documento RFC792 para Ipv4, ha sido actualizado para permitir su uso bajo Ipv6.
El protocolo resultante de dicha modificación es el ICMPv6, y se le ha asignado un valor, para el campo de siguiente cabecera igual a 58. ICMPv6 es parte integral de Ipv6 y debe ser totalmente incorporado a cualquier implementación de nodo Ipv6.
ICMPv6 es empleado por Ipv6 para reportar errores que se encuentran durante el procesamiento de los paquetes, así como para la realización de otras funciones relativas a la capa "Internet", como diagnósticos (ping).

El formato genérico de los mensajes ICMPv6 es el siguiente:

8 bits	16 bits	32 bits
Tipo	Código	Checksum
Cuerpo del Mensaje		

Figura 4.6 Formato de Mensajes Ipv6

El campo tipo, indica el tipo del mensaje, y su valor determina el formato del resto de la cabecera.
El campo código, depende del tipo de mensaje, y se emplea para crear un nivel adicional de jerarquía para la clasificación del mensaje.

El checksum o código de redundancia nos permite detectar errores en el mensaje ICMPv6.
Los mensajes ICMPv6 se agrupan en dos tipos o clases: mensajes de error y mensajes informativos.
Los mensajes de error tienen cero en el bit de mayor peso del campo tipo, por los que sus valores se sitúan entre 0 y 127.
Los valores de los mensajes informativos oscilan entre 128 y 255.
Los mensajes definidos por la especificación básica son los siguientes:

MENSAJES DE ERROR ICMPV6		
Tipo	**Descripción y Códigos**	
1	Destino no Alcanzable (Destination Unreachable)	
	Código	Descripción
	0	Sin ruta hacia el destino.
	1	Comunicación prohibida administrativamente.
	2	Sin Asignar.
	3	Dirección no alcanzable
	4	Puerto no Alcanzable
2	Paquete demasiado grande. (Packet too big)	
3	Tiempo Excedido (time Exceeded)	
	Código	Descripción
	0	Limite de saltos excedido.
	1	Tiempo de defragmentacion excedido.
4	Problema de Parámetros(Parameter Problems)	
	Código	Descripción
	0	Campo erróneo en cabecera.
	1	Tipo de "cabecera siguiente" desconocida.
	2	Opción Ipv6 desconocida
MENSAJES INFORMATIVOS ICMPV6		
Tipo	Descripción	
128	Solicitud de Eco (Echo Request)	
129	Respuesta de Eco (Echo Reply)	

Tabla 4.16 Mensajes de Error de Ipv6.

Se esta trabajando en nuevos tipos de mensajes, siendo el mas interesante de ellos el definido en un borrador de IETF (draft-ietf-ipngwg-icmp-name-lookups-05.txt), que permitirá solicitar a un nodo información completa como su "nombre de dominio completamente calificado" (Fully- Qualyfied-Domain-Name).

Por razones de seguridad, las cabeceras ICMPv6 pueden ser autenticadas y encriptadas, usando la cabecera correspondiente. El uso de este mecanismo permite , además, la prevención de ataques ICMP, como el conocido "Negación de Servicio". (DoS o Denial of Service Attack)

4.3.12 Descubrimiento de Vecindario en Ipv6 (Neighbor Discovery)

En Ipv6, el protocolo equivalente, en cierto modo, a ARP en Ipv4, es el denominado Descubrimiento de Vecindario. Sin embargo, incorpora también la funcionalidad de otros protocolos Ipv4, (Descubrimiento ICMP del Router) y Redirector ICMP .

Consiste en el mecanismo por el cual un nodo se incorpora a una red, descubre la presencia de otros, en su mismo enlace, para determinar sus direcciones en la capa de enlace, para localizar los routers, y para mantener la información de conectividad acerca de las rutas a los vecinos activos.

El protocolo de descubrimiento de vecinos también se emplea para mantener limpias las memorias cache donde se almacena la información relativa al contexto de la red a la que esta conectado un nodo (host o router), y por tanto para detectar cualquier cambio en la misma. Cuando un router o una ruta hacia el, falla, el host buscara alternativas funcionales.
ND emplea los mensajes de ICMPv6 , incluso a través de mecanismos de multicast, en la capa de enlace, para algunos de sus servicios.
El protocolo ND es bastante complejo y sofisticado, ya que es la base para permitir el mecanismo de auto configuración en Ipv6.
Define, entre otros, mecanismos para: descubrir routers, prefijos y parámetros, auto configuración de direcciones, resolución de direcciones, determinación del siguiente salto, detección de nodos no alcanzables, detección de direcciones duplicadas o cambios, redirección, balanceo de carga entrante, direcciones anycast, y anunciación de proxies.

ND define cinco tipos de paquetes ICMPv6:

- Solicitud de Router (Router Solicitation): Generado por una interfaz cuando es activada, para pedir a los routers que se anuncien inmediatamente.

Tipo en paquete ICMPv6=133.

- Anunciación de Router (Router Advertisement): Generado por los routers periódicamente (entre cada 4 y 1800 segundos) o como consecuencia de una solicitud de router, a través de multicast, para informar de su presencia así como otros parámetros de enlace y de Internet, como prefijos (uno o varios), tiempos de vida, configuración de direcciones, limite de salto sugerido, etc. Es fundamental para permitir la renumeración. Tipo en paquete ICMPv6=134.

- Solicitud de Vecino (Neighbor Solicitation): Generado por los nodos para determinar la dirección en la capa de enlace de sus vecinos, o para verificar que el no vecino sigue activo (es alcanzable), así como para detectar las direcciones duplicadas. Tipo en paquete ICMPv6 = 135.

- Anunciación de Vecino (Neighbor Advertisement): Generado por los nodos como respuesta a la solicitud de vecino, o bien para indicar cambios de direcciones en la capa de enlace. Tipo en paquete ICMPv6 = 136.

- Redirección (Redirect): Generado por los routers para informar a los host de un salto mejor para llegar a un determinado destino. Equivalente, en parte al redirector ICMPv6. Tipo en paquete ICMPv6 = 137.

El protocolo ND, frente a los mecanismos existentes en Ipv4, reporta numerosas ventajas:

- El descubrimiento de routers es parte de la base del protocolo, no es preciso recurrir a los protocolos de enrutamiento.
- La anunciación de router incluye las direcciones de la capa de enlace, no es necesario ningún intercambio adicional de paquetes para su resolución.
- La anunciación de router incluye los prefijos para enlace, por lo que no hay necesidad de un mecanismo adicional para configurar la mascara de red.
- La anunciación de router permite la auto configuración de direcciones.

- Los routers pueden anunciar el MTU (Tamaño Máximo de Unidad de Transmisión) a los host del mismo enlace.
- Las redirecciones contienen la dirección de la capa de enlace del nuevo salto, lo que evita la necesidad de una resolución de dirección adicional.}
- Se pueden asignar múltiples prefijos al mismo enlace y por defecto los host aprenden todos los prefijos por la anunciación del router. Sin, embargo los routers pueden ser configurados para omitir parte o todos los prefijos en la anunciación, de forma que los host consideren que los destinos están fuera del enlace; de esta forma enviaran el trafico a los routers, quien a su vez lo redireccionara según corresponda.
- A diferencia de Ipv4, en Ipv6 el receptor de una redirección asume que el siguiente salto esta en el mismo enlace. Se prevé una gran utilidad en el sentido de no ser deseable o posible que los nodos conozcan todos los prefijos de los destinos o del mismo enlace (enlaces sin multidifusion y medio compartido).

La detección de vecinos no alcanzables es parte de la base de mejoras para la robustez en la entrega de paquetes frente a fallos en routers, particiones de enlaces, nodos que cambian sus direcciones, nodos móviles, etc.

4.3.13 Frame Relay y ATM sobre Ipv6.

Para implementar Frame Relay o ATM se deben mapear direcciones Ipv6 en Circuitos Virtuales Permanentes (PVC's) a través de los cuales viajan los paquetes hacia un nodo destino.

Las redes Frame Relay y ATM utilizan mapeos dinámicos de direcciones y Circuitos Virtuales Permanentes para alcanzar otros nodos. Al asignar una dirección Ipv6 a una interfase por medio del comando **ipv6 address** se define la dirección de la misma y la red a la cual será conectada.
Cuando la interfase posee solamente un PVC, esta posee una conexión punto a punto y se esta realizando un mapeo implícito entre todas las direcciones pertenecientes a dicha red y el PVC utilizado para alcanzar dichas direcciones.

Cuando la interfase posee varios PVC's, esta posee una conexión punto a multipunto y se deben utilizar los comandos **protocol ipv6 ATM VC** (para las redes ATM) o **frame-relay map ipv6** (para las redes Frame Relay) en el modo de configuración de interfase para realizar un mapeo explicito entre las direcciones Ipv6 de los nodos remotos y los PVC´s utilizados para alcanzar dichas direcciones.

El Protocolo de Resolución de Direcciones Inverso (Inverse ARP) es utilizado en Ipv4 para mapear dinámicamente la dirección de la capa de red de un nodo inicial, hacia un nodo final, para un mismo PVC. En Ipv6, el Protocolo de Resolución de Direcciones Inverso es utilizado para mapear dinámicamente la dirección Ipv6 global de un nodo hacia el nodo final del PVC.

Pasos para configurar ATM y Frame Relay.

1. enable
2. configure terminal
3. interface *interface-type interface-number*
4. pvc [*name*] *vpi/vc*
5. protocol ipv6 *ipv6-address* [[**no**] **broadcast**]]
6. exit

7. ipv6 address *ipv6-address* {*/ prefix-length* | **link-local**}
8. exit
9. interface *interface-type interface-number*
10. frame-relay map ipv6 *ipv6-address dlci* [**broadcast**] [**cisco**] [**ietf**] [**payload-compression**]
11. ipv6 address *ipv6-address* {*/ prefix-length* | **link-local**}

A continuación se presenta un resumen de los comandos que se utilizan para la configuración de ATM y Frame Relay.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**interface** interface-type interface-number **Ejemplo:** Router(config)# interface atm 0	Especifica el número, el tipo de interface y entra al modo de configuración de interface.

4	**pvc** [name] vpi/vci **Ejemplo:** Router(config-if)# pvc 1/32	Especifica un nombre para el PVC ATM y entra al modo de configuración del PVC ATM.
5	**protocol ipv6** ipv6-address [[**no**] **broadcast**] **Ejemplo:** Router(config-if-atm-vc)# protocol ipv6 2001:0DB8:2222:1003::45	Mapea la dirección Ipv6 del nodo remoto hacia el PVC utilizado para llegar a esa dirección.
6	**exit** **Ejemplo:** Router(config-if-atm-vc)# exit	Sale del modo de configuración del PVC ATM y entra al modo de configuración de interfase del router.
7	**ipv6 address** ipv6-address {**/** prefix-length | **link-local**} **Ejemplo:** Router(config-if)# ipv6 address 2001:0DB8:2222:1003::72/64	Especifica una dirección de red Ipv6 asignada a la interfase y habilita el procesamiento Ipv6 en la interfase.
8	**exit** **Ejemplo:** Router(config-if)# exit	Sale del modo de configuración de interfase y retorna al modo de configuración global del router.
9	**interface** interface-type interface-number **Ejemplo:** Router(config)# interface serial 3	Especifica un número y tipo de interfase y entra al modo de configuración de interfase.
10	**frame-relay map ipv6** ipv6-address dlci [**broadcast**] [**cisco**] [**ietf**] [**payload-compression**] **Ejemplo:** Router(config-if)# frame-relay map ipv6 FE80::E0:F727:E400:A 17 broadcast	Mapea una dirección Ipv6 de un nodo remoto al identificador de enlace de conexión (DLCI) del PVC usado para alcanzar las direcciones.
11	**ipv6 address** ipv6-address {**/** prefix-length | **link-local**} **Ejemplo:** Router(config-if)# ipv6 address 2001:0DB8:2222:1044::46/64	Especifica una red Ipv6 asignada a la interfase y habilita el procesamiento Ipv6 sobre la interfase.

Tabla 4.17 Configuracion de aTM y Frame Relay sobre Ipv6.

4.3.13.1 Ejemplos de Configuración.

- **Configuración de PVC ATM sobre una interfase Punto a Punto.**

En el siguiente ejemplo, dos nodos llamados Router1 y Router2 se encuentran conectados por un solo PVC. La subinterfase Punto a Punto ATM0 .132 es utilizada en ambos nodos para terminar el PVC. Por lo tanto, el mapeo entre las direcciones Ipv6 de ambos nodos y el PVC es implícito y no se requiere ningún mapeo adicional.

Configuracion de Router 1

```
interface ATM0
no ip address


interface ATM0.132 point-to-point
pvc 1/32
encapsulation aal5snap

ipv6 address 2001:0DB8:2222:1003::72/64
```

Configuracion de Router 2

```
 interface ATM0
no ip address

interface ATM0.132 point-to-point
pvc 1/32
encapsulation aal5snap

ipv6 address 2001:0DB8:2222:1003::45/64
```

- **Configuración de PVC ATM sobre una interfase Punto a Multipunto.**

En el siguiente ejemplo se utilizan los dos nodos referidos en el ejemplo anterior conectados al mismo PVC. La interfase ATM0 es Punto a Multipunto y es utilizada en ambos nodos para terminar el PVC, por lo tanto se requieren mapeos explícitos entre las direcciones Ipv6 globales y de enlace local sobre la interfase ATM0 y el PVC.

Configuración del Router 1

interface ATM0
no ip address
pvc 1/32
protocol ipv6 2001:0DB8:2222:1003::45
protocol ipv6 FE80::60:2FA4:8291:2 broadcast
encapsulation aal5snap

ipv6 address 2001:0DB8:2222:1003::72/64

Configuracion del Router 2

interface ATM0
no ip address
pvc 1/32

protocol ipv6 FE80::60:3E47:AC8:C broadcast
protocol ipv6 2001:0DB8:2222:1003::72
encapsulation aal5snap
!
ipv6 address 2001:0DB8:2222:1003::45/64

- **Configuración de PVC Frame Relay sobre una interfase Punto a Punto.**

En el siguiente ejemplo se ha creado una malla completa entre tres nodos llamados RouterA, RouterB y RouterC. Cada nodo esta configurado con dos PVC´s, los cuales proveen una conexión individual a cada uno de los dos nodos restantes. Cada pvc esta configurado en una diferente subinterfases Punto

a Punto, las cuales crean tres redes diferentes que son la 2001:0DB8:2222:1017:/64, 2001:0DB8:2222:1018::/64, y 2001:0DB8:2222:1019::/64.

Por lo tanto, los mapeos entre las direcciones Ipv6 de cada nodo y los DLCI (17,18, y 19) de los PVC utilizados, son implícitos.

Configuracion del Router A

```
interface Serial3
encapsulation frame-relay

interface Serial3.17 point-to-point
description to Router B
ipv6 address 2001:0DB8:2222:1017::46/64
frame-relay interface-dlci 17

interface Serial3.19 point-to-point
description to Router C
ipv6 address 2001:0DB8:2222:1019::46/64
frame-relay interface-dlci 19
```

Configuracion del Router B

```
interface Serial5
encapsulation frame-relay

interface Serial5.17 point-to-point
description to Router A
ipv6 address 2001:0DB8:2222:1017::73/64
frame-relay interface-dlci 17

interface Serial5.18 point-to-point
description to Router C
ipv6 address 2001:0DB8:2222:1018::73/64
frame-relay interface-dlci 18
```

Configuracion del Router C

interface Serial0
encapsulation frame-relay

interface Serial0.18 point-to-point
description to Router B
ipv6 address 2001:0DB8:2222:1018::72/64
frame-relay interface-dlci 18

interface Serial0.19 point-to-point
description to Router A
ipv6 address 2001:0DB8:2222:1019::72/64
frame-relay interface-dlci 19

- **Configuración de PVC Frame Relay sobre una interfase Punto a Multipunto.**

En el siguiente ejemplo se ha creado una malla completa entre tres nodos llamados RouterA, RouterB y RouterC. Cada nodo esta configurado con dos PVC´s, los cuales proveen una conexión individual a

cada uno de los dos nodos restantes. La diferencia es que los dos PVC son configurados en una misma interfase (serial 3, serial 5, y serial 10, respectivamente); las cuales hacen a cada interfase, una interfase Punto a Multipunto.
Por lo tanto, se requieren mapeos explícitos de las direcciones Ipv6 globales y de enlace local de las interfaces que se encuentran en cada nodo, con el DLCI (17,18 y 19) del PVC usado para alcanzar las interfaces.

Configuracion del Router A

interface Serial3
encapsulation frame-relay
ipv6 address 2001:0DB8:2222:1044::46/64
frame-relay map ipv6 FE80::E0:F727:E400:A 17 broadcast
frame-relay map ipv6 FE80::60:3E47:AC8:8 19 broadcast
frame-relay map ipv6 2001:0DB8:2222:1044::72 19

frame-relay map ipv6 2001:0DB8:2222:1044::73 17

Configuracion del Router B

interface Serial5

encapsulation frame-relay

ipv6 address 2001:0DB8:2222:1044::73/64

frame-relay map ipv6 FE80::60:3E59:DA78:C 17 broadcast

frame-relay map ipv6 FE80::60:3E47:AC8:8 18 broadcast

frame-relay map ipv6 2001:0DB8:2222:1044::46 17

frame-relay map ipv6 2001:0DB8:2222:1044::72 18

Configuracion del Router C

interface Serial10

encapsulation frame-relay

ipv6 address 2001:0DB8:2222:1044::72/64

frame-relay map ipv6 FE80::60:3E59:DA78:C 19 broadcast

frame-relay map ipv6 FE80::E0:F727:E400:A 18 broadcast

frame-relay map ipv6 2001:0DB8:2222:1044::46 19

frame-relay map ipv6 2001:0DB8:2222:1044::73 18

4.3.14 Enrutamiento Estático en Ipv6.

El enrutamiento estático se utiliza para que una red específica en un nodo pueda alcanzar a otra red diferente en otro nodo, sin necesidad de utilizar protocolos de enrutamiento. Esto se realiza por medio del comando **ipv6 route.**

Los pasos para configurar una ruta estatica hacia una red diferente se muestran a continuación.

1. **enable**
2. **configure terminal**

3. **ipv6 route 2000:1110::C/126 Serial 0/1**

A continucacion se presentan estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**ipv6 route** *ipv6 network address/ipv6 prefix interface_output*	Crea una ruta estatica hacia una red diferente a traves de una interfase de salida correspondiente al nodo actual.

4.3.14.1 Ejemplo de Configuración.

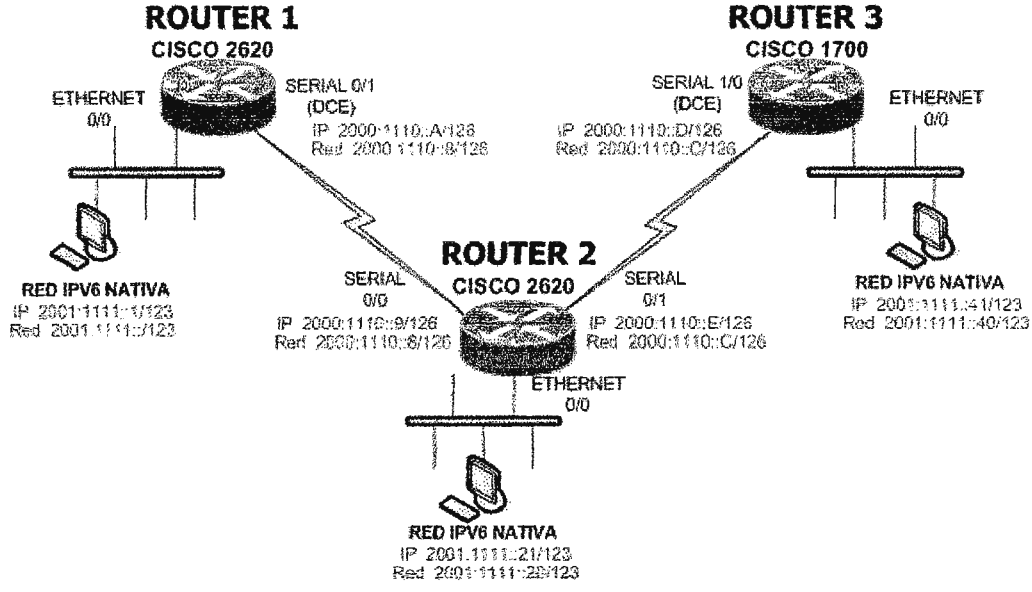


Figura 4.8. Esquema de Conexión para Enrutamiento Estatico en Ipv6.

El diagrama anterior muestra una Red Nativa Ipv6 compuesta por tres enrutadores, los cuales se encuentran conectados a través de sus seriales, cada una de ellas configurada con una dirección Ipv6 así:

- Router 1: Interfase Serial 0/1, con dirección Ipv6 2000:1110::A/126.
- Router 2: Interfase Serial 0/0, con dirección Ipv6 2000:1110::9/126 y
  Interfase Serial 0/1, con dirección Ipv6 2000:1110::E/126.
- Router 3: Interfase Serial 1/0, con dirección Ipv6 2000:1110::D/126.

Cada nodo posee una Red de Área Local (LAN), identificada por intereses FastEthernet, cada una configurada con una dirección Ipv6 perteneciente a una red especifica. Así:

- Router 1: Interfase FastEthernet 0/0, con direccion Ipv6 2001:1111::1/123.
- Router 2: Interfase FastEthernet 0/0, con direccion Ipv6 2001:1111::21/123.
- Router 3: Interfase FastEthernet 0/0, con direccion Ipv6 2001:1111::41/123.

Para que los tres nodos se puedan accesar unos con otros es necesaria la configuracion de rutas estaticas entre los mismos o de un protocolo de enrutamiento especifico.
A continuación se muestra la configuración necesaria en cada uno de los enrutadores para que se establezca un enrutamiento estatico.

Para Router1:
ipv6 route 2000:1110::C/126 Serial0/1
ipv6 route 2001:1111::40/123 Serial0/1

Para Router2:
ipv6 route 2001:1111::/123 Serial0/0
ipv6 route 2001:1111::40/123 Serial0/1

Para Router3:
ipv6 route 2000:1110::8/126 Serial1/0
ipv6 route 2001:1111::/123 2000:1110::9

Despues de haber configurado las rutas estaticas se puede comprobar su operación en cada enrutador a traves del comando show ipv6 route. A continuación se utiliza este comando para el Router2 asi como se muestra a continuación:

```
Router2#sh ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2000:1110::8/126 [0/0]
     via ::, Serial0/0
L   2000:1110::9/128 [0/0]
     via ::, Serial0/0
C   2000:1110::C/126 [0/0]
     via ::, Serial0/1

L   2000:1110::E/128 [0/0]
     via ::, Serial0/1
S   2001:1111::/123 [1/0]
     via ::, Serial0/0
S   2001:1111::40/123 [1/0]
     via ::, Serial0/1
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

Las rutas identificadas por la letra S son las aprendidas por el enrutamiento estatico. Ademas se puede utilizar el comando **traceroute** para observar el camino que toma el paquete mientras llega a su destino. Para este ejemplo se realiza un **traceroute** desde el Router3 hasta el Router1.

```
Router3#traceroute 2001:1111::1

Type escape sequence to abort.
```

Tracing the route to 2001:1111::1

1 router2b (2000:1110::E) 4 msec 0 msec 4 msec
2 router1 (2000:1110::A) 4 msec 4 msec 4 msec

4.3.15 Verificando Conectividad Basica en Ipv6.

- **Show Ipv6 Interfaces.**

Sintaxis:
show ipv6 interface [**brief**] [[interface-type
interface-number] [**prefix**]]

Ejemplo:
Router# show ipv6 interface ethernet 0

En el siguiente ejemplo se muestra como el comando **sh ipv6 interfaces** es utilizado para verificar que las direcciones Ipv6 están configuradas correctamente en la interfase Ethernet 0. También se puede verificar información acerca del estado de los Mensajes de Redirección de Vecinos (Ipv6 Neighbors Redirect Messages) ICMPv6, utilizados para proveer información del siguiente salto para una ruta hacia un destino. Además de los mensajes de descubrimiento de vecinos y de la configuración sin estado.

Salida en Pantalla:
Router# **show ipv6 interface ethernet 0**
Ethernet0 is up, line protocol is up
IPv6 is stalled, link-local address is FE80::1
Global unicast address(es):
2000::1, subnet is 2000::/64
3000::1, subnet is 3000::/64
Joined group address(es):
FF02::1
FF02::2
FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled

ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.

- **Show Ipv6 Neighbors.**

Sintaxis:

show ipv6 neighbors [interface-type interface-number | ipv6-address]

Ejemplo:

Router# show ipv6 neighbors ethernet 2

En el siguiente ejemplo el comando **show ipv6 neighbors** es utilizado para desplegar en pantalla información del caché de descubrimiento de vecinos. El signo (-) en el campo de edad de la salida en pantalla, indica que es una entrada estática. A continuación se muestra la información del caché de descubrimiento de vecinos para la interfase Ethernet 2.

Salida en pantalla:

Router# **show ipv6 neighbors ethernet 2**

IPv6 Address	Age	Link-layer Addr	State	Interface
2000:YYYY:0:4::2	0	0003.a0d6.141e	REACH	Ethernet2
FE80::XXXX:A0FF:FED6:141E	0	0003.a0d6.141e	REACH	Ethernet2
3001:YYYY:1::45a	-	0002.7d1a.9472	REACH	Ethernet2

- **Show Ipv6 Route.**

Sintaxis:

show ipv6 route [ipv6-address |
ipv6-prefix/ prefix-length | protocol]

Ejemplo:

Router# show ipv6 route

Este comando muestra el contenido de la tabla de enrutamiento para una dirección Ipv6 específica. El siguiente ejemplo muestra la salida del comando show ipv6 route para un prefijo de dirección Ipv6 igual a **2001:200::/35**.

Salida en Pantalla:

Router# **show ipv6 route 2001:200::/35**

IPv6 Routing Table - 261 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea

B 2001:200::/35 [20/3]
via FE80::60:5C59:9E00:16, Tunnel1

- **Show Ipv6 Traffic.**

Sintaxis:
show ipv6 traffic

Ejemplo:
Router# show ipv6 traffic

Este comando muestra estadísticas acerca del trafico Ipv6. En el siguiente ejemplo se utiliza el comando para desplegar información sobre los contadores de límites de tasa de ICMP.

Salida en Pantalla:

Router# **show ipv6 traffic**
ICMP statistics:
Rcvd: 188 input, 0 checksum errors, 0 too short
0 unknown info type, 0 unknown error type
unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port

parameter: 0 error, 0 header, 0 option

0 hopcount expired, 0 reassembly timeout,0 too big

0 echo request, 0 echo reply

0 group query, 0 group report, 0 group reduce

1 router solicit, 175 router advert, 0 redirects

0 neighbor solicit, 12 neighbor advert

Sent: 7376 output, 56 rate-limited

unreach: 0 routing, 15 admin, 0 neighbor, 0 address, 0 port

parameter: 0 error, 0 header, 0 option

0 hopcount expired, 0 reassembly timeout,0 too big

15 echo request, 0 echo reply

0 group query, 0 group report, 0 group reduce

0 router solicit, 7326 router advert, 0 redirects

2 neighbor solicit, 22 neighbor advert

- **Show Frame Relay Map.**

Sintaxis:

show frame-relay map

Ejemplo:

Router# show frame-relay map

En el siguiente ejemplo, el comando **show frame-relay map** es utilizado para verificar que la dirección Ipv6 de un nodo remoto esta mapeada a un DLCI de un PVC utilizado para alcanzarla.
El siguiente ejemplo muestra que las direcciones Ipv6 de enlace local y global (FE80::E0:F727:E400:A y 2001:0DB8:2222:1044::73; FE80::60:3E47:AC8:8 y 2001.0DB8:2222:1044::72) de dos nodos remotos, están explícitamente mapeadas a las DLCI 17 y 19 respectivamente. Estas DLCI terminan en la interfase serial 3 de este nodo. Por lo tanto, la interfase serial 3 es un nodo Puno a Multipunto.

Salida en Pantalla:

Router# **show frame-relay map**

Serial3 (up): ipv6 FE80::E0:F727:E400:A dlci 17(0x11,0x410), static,

broadcast, CISCO, status defined, active
Serial3 (up): ipv6 2001:0DB8:2222:1044::72 dlci 19(0x13,0x430), static,

CISCO, status defined, active
Serial3 (up): ipv6 2001:0DB8:2222:1044::73 dlci 17(0x11,0x410), static,
CISCO, status defined, active
Serial3 (up): ipv6 FE80::60:3E47:AC8:8 dlci 19(0x13,0x430), static,
broadcast, CISCO, status defined, active

- **Show ATM Map.**

Sintaxis:
show atm map

Ejemplo:
Router# show atm map

Este comando muestra una lista de todos los mapas estáticos creados hacia hosts remotos sobre una red ATM. En el siguiente ejemplo este comando es utilizado para verificar que las dirección Ipv6 de un nodo remoto se encuentra mapeada al PVC utilizado para alcanzar dicha dirección Este ejemplo muestra que las direcciones Ipv6 de enlace local (FE80::60:3E47:AC8:C) y global (2001:0DB8:2222:1003::72) de un nodo remoto están explícitamente mapeadas a un PVC 1/32 de la interfaz ATM0.

Salida en Pantalla:

Router# **show atm map**

Map list ATM0pvc1 : PERMANENT
ipv6 FE80::60:3E47:AC8:C maps to VC 1, VPI 1, VCI 32, ATM0
, broadcast
ipv6 2001:0DB8:2222:1003::72 maps to VC 1, VPI 1, VCI 32, ATM0

- **Show Ip DHCP Binding.**

Sintaxis:

show ipv6 dhcp binding [ipv6-address]

Ejemplo:

Router# show ipv6 dhcp binding

Este comando muestra automáticamente los clientes enlazados con DHCP (Protocolo de Configuración Dinamica de Host). El siguiente ejemplo muestra información sobre dos clientes, incluyendo sus DUIDs, IAPDs, prefijos y tiempos de vida validos.

Salida en Pantalla:

Router# **show ipv6 dhcp binding**

Client: FE80::202:FCFF:FEA5:DC39 (Ethernet2/1)
DUID: 000300010002FCA5DC1C
IA PD: IA ID 0x00040001, T1 0, T2 0
Prefix: 3FFE:C00:C18:11::/68
preferred lifetime 180, valid lifetime 12345
expires at Nov 08 2002 02:24 PM (12320 seconds)
Client: FE80::202:FCFF:FEA5:C039 (Ethernet2/1)
DUID: 000300010002FCA5C01C
IA PD: IA ID 0x00040001, T1 0, T2 0
Prefix: 3FFE:C00:C18:1::/72
preferred lifetime 240, valid lifetime 54321
expires at Nov 09 2002 02:02 AM (54246 seconds)
Prefix: 3FFE:C00:C18:2::/72
preferred lifetime 300, valid lifetime 54333
expires at Nov 09 2002 02:03 AM (54258 seconds)
Prefix: 3FFE:C00:C18:3::/72
preferred lifetime 280, valid lifetime 51111

- **Show Ipv6 DHCP Interface.**

Sintaxis

show ipv6 dhcp interface [interface-type
interface-number]

Ejemplo:

Router# show ipv6 dhcp interface

Este comando muestra información de DHCP para una interfase Ipv6. En el primer ejemplo el comando es usado en un router que tienen una interfase actuando como servidor DHCP para Ipv6. En el segundo ejemplo el comando es utilizado sobre un router que tiene una interfase actuando como un cliente DHCP.

Salida en Pantalla.

Router1# **show ipv6 dhcp interface**

Ethernet2/1 is in server mode
  Using pool: svr-p1
  Preference value: 20
  Rapid-Commit is disabled

Router2# **show ipv6 dhcp interface**
  Ethernet2/1 is in client mode
  State is OPEN (1)
  List of known servers:
    Address: FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
        Preference: 20
        IA PD: IA ID 0x00040001, T1 120, T2 192
        Prefix: 3FFE:C00:C18:1::/72
        preferred lifetime 240, valid lifetime 54321
        expires at Nov 08 2002 09:10 AM (54319 seconds)
        Prefix: 3FFE:C00:C18:2::/72
        preferred lifetime 300, valid lifetime 54333

expires at Nov 08 2002 09:11 AM (54331 seconds)
Prefix: 3FFE:C00:C18:3::/72
preferred lifetime 280, valid lifetime 51111
expires at Nov 08 2002 08:17 AM (51109 seconds)
DNS server: 1001::1
DNS server: 1001::2
Domain name: domain1.net
Domain name: domain2.net
Domain name: domain3.net
Prefix name is cli-p1
Rapid-Commit is enabled

- **Show Running-Config.**

En el siguiente ejemplo, el comando **show running-config** es utilizado para verificar que el procesamiento de paquetes Ipv6 es habilitado globalmente en el router y sobre las interfaces aplicables, además de la configuración de una dirección Ipv6 sobre una interfase.

Router# **show running-config**
Building configuration...
Current configuration : 22324 bytes
!
! Last configuration change at 14:59:38 PST Tue Jan 16 2001
! NVRAM config last updated at 04:25:39 PST Tue Jan 16 2001 by bird
!
hostname Router
!
ipv6 unicast-routing
!
interface Ethernet0
no ip route-cache
no ip mroute-cache
no keepalive

media-type 10BaseT
ipv6 address 2001:0DB8:0:1::/64 eui-64

En el siguiente ejemplo, el comando **show running-config** es utilizado para verificar que CEFv6 y el conteo de redes CEFv6 se encuentra habilitado en una plataforma de una arquitectura no distribuida y que CEFv6 ha sido habilitado en una interfase Ipv6.

Router# **show running-config**
Building configuration...
Current configuration : 22324 bytes
!
! Last configuration change at 14:59:38 PST Tue Jan 16 2001
! NVRAM config last updated at 04:25:39 PST Tue Jan 16 2001 by bird
!
hostname Router
!
ip cef
ipv6 unicast-routing
ipv6 cef
ipv6 cef accounting prefix-length
!
!
interface Ethernet0
ip address 10.4.9.11 255.0.0.0
media-type 10BaseT
ipv6 address 2001:0DB8:C18:1::/64 eui-64

En el siguiente ejemplo, el comando **show running-config** es utilizado para verificar que dCEFv6 y el conteo de redes dCEFv6 se encuentra habilitado en una plataforma de una arquitectura distribuida, por ejemplo los routers Cisco de la serie 7500.
DCEFv6 se encuentra habilitado por defecto en los routers Cisco de la serie 12000 y se encuentra deshabilitado por defecto en los routers Cisco de la serie 7500.

Router# **show running-config**

Building configuration...

Current configuration : 22324 bytes

!

! Last configuration change at 14:59:38 PST Tue Jan 16 2001

! NVRAM config last updated at 04:25:39 PST Tue Jan 16 2001 by bird

!

hostname Router

!

ip cef distributed

ipv6 unicast-routing

ipv6 cef distributed

ipv6 cef accounting prefix-length

En el siguiente ejemplo, el comando **show running-config** es utilizado para verificar mapeos estáticos de nombre a dirección, nombres de dominio, servidores DNS habilitados.

Router# **show running-config**

Building configuration...

!

ipv6 host cisco-sj 2001:0DB8:20:1::12

!

ip domain-name cisco.com

ip domain-lookup

ip name-server 2002:C01F:768::1

4.4 PROTOCOLOS DE ENRUTAMIENTO INTERIOR PARA IPV6.

4.4.1 RIP Para Ipv6.

4.4.1.1 Prerrequisitos.

- Se debe estar familiarizado con el manejo de direcciones Ipv6 y con el protocolo Ipv4.
- Los requerimientos del IOS se describen en la siguiente tabla.

Característica	Mínimo Cisco IOS Requerido
RIP para Ipv6	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
Predistribución de Ruta	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T

Tabla 4.18 Requerimientod de IOS para RIP Ipv6.

Las funciones que ofrece RIPv6 poseen los mismos beneficios que ofrece para Ipv4. Cada proceso de RIP en Ipv6 posee una tabla de enrutamiento local, que se encuentra referida a una base de datos de información de enrutamiento (RIB). La RIB contiene una tabla que posee los mejores costos de las rutas Ipv6 aprendidas por RIP. Si RIP Ipv6 aprende la misma ruta de dos vecinos diferentes, pero con costos diferentes, este almacenara en su tabla solamente la de menor costo en la RIB local.

4.4.1.2 Implementando RIP Para Ipv6.

Para configurar un protocolo de enrutamiento en Ipv6, se debe crear un proceso de enrutamiento, habilitar el proceso de enrutamiento sobre las interfaces, y elegir un protocolo de enrutamiento para la red.

Habilitando RIP para IPV6.

Para habilitar RIP Ipv6 debemos crear primeramente un proceso de enrutamiento RIP Ipv6 y especificarlo en la interface.

Antes de habilitar RIP Ipv6, se debe habilitar el protocolo Ipv6 globalmente en el router utilizando el comando **ipv6 unicast-routing** y habilitar Ipv6 en cualquier interfase a la cual se le habilitara RIP.

A continuación se describen los pasos necesarios para habilitar RIP en una interfase.

Pasos para habilitar RIP en una Interfase

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 rip** *name* **enable**

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**interface** interface-type interface-number **Ejemplo:** Router(config)# interface Ethernet 0/0	Especifica el número, el tipo de interface y entra al modo de configuración de interface.
4	**ipv6 rip** name **enable** **Ejemplo:** Router(config-if)# ipv6 rip process1 enable	Habilita el proceso de enrutamiento RIP Ipv6 sobre una interfase.

Tabla 4.19 Habilitando RIP en una Interfase.

Modificando Características de RIP Ipv6.

En los siguientes pasos se describe la forma de configurar el número máximo de rutas de igual costo que RIP Ipv6 puede soportar, ajustar los temporizadores de RIP Ipv6 y originar una ruta Ipv6 por defecto.

1. **enable**
2. **configure terminal**
3. **ipv6 router rip** *name*
4. **maximum-paths** *number-paths*
5. **exit**
6. **interface** *type number*
7. **ipv6 rip** *name* **default-information** {**only** | **originate**}

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**ipv6 router rip** name **Ejemplo:** Router(config)# ipv6 router rip procesorip	Configura un proceso de enrutamiento RIP Ipv6 y entra al modo de configuración del router para dicho proceso. El argumento *name* se utiliza para especificar el nombre del proceso de enrutamiento.
4	**maximum-paths** number-paths **Ejemplo:** Router(config-router)# maximum-paths 2	Define el número de rutas de igual costo que Ipv6 puede soportar. El argumento number-paths puede ser un entero de 1 a 64, por defecto para RIP son cuatro rutas.
5	**exit** **Ejemplo:** Router(config-if)# exit	Sale del modo de configuración de interfase y entra al modo de configuración global.
6	**interface** type number **Ejemplo:**	Especifica el tipo y numero de la interfase y entra al modo de configuración de interfase.

	Router(config)# interface Ethernet 0/0	
7	**ipv6 rip** name **default-information {only | originate}** **Ejemplo:** Router(config-if)# ipv6 rip procesorip default-information originate	Origina una ruta Ipv6 por defecto (::/0) dentro de las actualizaciones del proceso de enrutamiento RIP Ipv6 enviadas desde una interfase especificada. Utilizando la palabra *only* se origina la ruta por defecto (::/0); pero se suprimen todas las otras rutas en las actualizaciones enviadas por esta interfase Utilizando la palabra *originate* se origina la ruta por defecto (::/0); En adicion a todas las otras rutas en las actualizaciones enviadas por esa interfase.

Tabla 4.20 Modificando Características de RIP Ipv6.

Redistribuyendo Rutas en un Proceso de Enrutamiento RIP Ipv6.

RIP soporta el uso de mapas de ruta para seleccionar rutas para redistribución. Las rutas pueden ser especificadas por prefijo, usando una lista de prefijos de mapa de ruta, o por etiqueta, utilizando la función de mapa de ruta (match tag).

La máxima métrica que RIP puede soportar es 16, tomando en cuenta que esta métrica denota una ruta inalcanzable. Por lo tanto, si se están redistribuyendo rutas con métricas mayores o iguales que 16, el protocolo RIP las anunciara inalcanzables por defecto. Estas rutas no serán utilizadas por los routers vecinos. El usuario debe configurar una métrica de redistribución menor a 15 para estas rutas. Si no se especifica una métrica. Para encontrar la métrica actual de ruta utilice el comando **show ipv6 route.**

Para la redistribución de rutas etiquetadas dentro de un proceso de enrutamiento RIP Ipv6 se deben seguir los siguientes pasos.

1. enable
2. configure terminal

3. interface *type number*

4. ipv6 rip *word* **enable**

5. redistribute *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [**metric** *metric-value*] [**metric-type**

{**internal** | **external**}] [**route-map** *map-name*]

En la siguiente tabla se presentan estos pasos de manera detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado
2	**configure terminal** **Ejemplo:** Router# configure terminal	Entra al modo de configuración global.
3	**interface** type number **Ejemplo:** Router(config)# interface ethernet 0/0	Especifica el tipo de interfaz, el número y ubica el router en el modo de configuración de interfaz.
4	**ipv6 rip** word **enable** **Ejemplo:** Router(config-if)# ipv6 rip procesorip enable	Habilita el proceso de enrutamiento RIP Ipv6 en una interfase.
5	**redistribute** protocol [process-id] {**level-1** | **level-1-2** | **level-2**} [**metric** metric-value] [**metric-type** {**internal** | **external**}] [**route-map** map-name] **Ejemplo:** Router(config-router)# redistribute bgp 65001 route-map bgp-to-rip	Redistribuye las rutas especificadas en el proceso de enrutamiento RIP Ipv6. El *argumento* de protocolo puede ser cualquiera de los siguientes: bgp, connected, isis, rip, or static. Al digitar rip y un argumento de *process-ip* se especifica un proceso de enrutamiento RIP Ipv6. Note: La palabra connected se refiere a rutas que se establecen automáticamente al asignar una dirección Ipv6 a una interfase.

Tabla 4.21 Redistribuyendo Rutas en un Proceso de Enrutamiento RIP Ipv6.

Configurando Etiquetas para rutas RIP.

Al crear una distribución de ruta podemos asociar una etiqueta numérica a dicha ruta. La etiqueta se anuncia con la ruta con la ayuda de RIP y ambas son agregadas en la tabla de enrutamiento del router vecino.

Si se redistribuye una ruta etiquetada (por ejemplo, una ruta existente en la tabla de enrutamiento Ipv6 que ya posee una etiqueta) en RIP, entonces RIP la anunciara automáticamente. Si se utiliza un mapa de ruta de redistribución para especificar una etiqueta. Entonces RIP utilizara la etiqueta del mapa de ruta en preferencia a la etiqueta de la tabla de enrutamiento.

Para establecer etiquetas de ruta utilizando un mapa de ruta se deben seguir los siguientes pasos de configuración.

1. enable
2. configure terminal
3. route-map *map-tag* [**permit** | **deny**] [*sequence-number*]
4. match ipv6 address {**prefix-list** *prefix-list-name* | *access-list-name*}
5. set tag *value*

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado
2	**configure terminal** **Ejemplo:** Router# configure terminal	Entra al modo de configuración global.
3	**route-map** map-tag [**permit** | **deny**] [sequence-number] **Ejemplo:** Router(config)# route-map bgp-to-rip permit 10	Define un mapa de ruta y entra al modo de configuración de mapa de ruta Este paso se utiliza con un comando **match**.
4	**match ipv6 address** {**prefix-list** prefix-list-name | access-list-name} **Ejemplo:** Router(config-route-map)# match ipv6 address prefix-list bgp-to-rip-flt	Especifica una lista de prefijos Ipv6 para ser combinada.

5	**set tag** value **Ejemplo:** Router(config-route-map)# set tag 4	Establece un valor de etiqueta para asociarla con las rutas distribuidas.

4.22 Configurando Etiquetas para rutas RIP.

4.4.1.3 Ejemplo de configuración para RIP Ipv6.

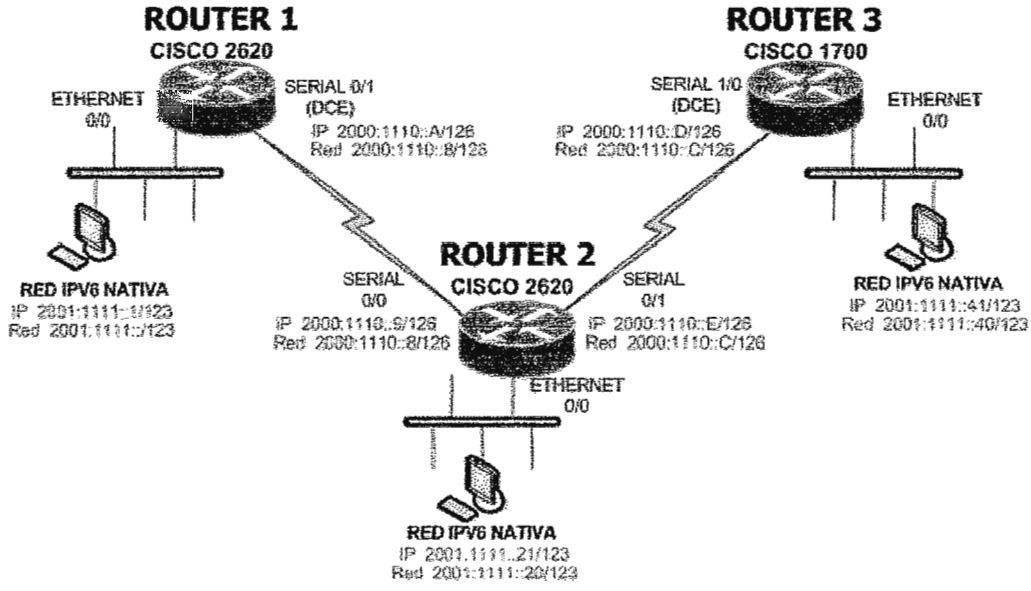


Figura 4.9. Esquema para Conectividad RIP Ipv6.

El diagrama anterior muestra una Red Nativa Ipv6 compuesta por tres enrutadores, los cuales se encuentran conectados a través de sus seriales, cada una de ellas configurada con una dirección Ipv6 así:

- Router 1: Interfase Serial 0/1, con dirección Ipv6 2000:1110::A/126.

- Router 2: Interfase Serial 0/0, con dirección Ipv6 2000:1110::9/126 y
  Interfase Serial 0/1, con dirección Ipv6 2000:1110::E/126.
- Router 3: Interfase Serial 1/0, con dirección Ipv6 2000:1110::D/126.

Cada nodo posee una Red de Área Local (LAN), identificada por intereses FastEthernet, cada una configurada con una dirección Ipv6 perteneciente a una red especifica. Así:

- Router 1: Interfase FastEthernet 0/0, con direccion Ipv6 2001:1111::1/123.
- Router 2: Interfase FastEthernet 0/0, con direccion Ipv6 2001:1111::21/123.
- Router 3: Interfase FastEthernet 0/0, con direccion Ipv6 2001:1111::41/123.

Para configurar RIP es necesario crear un proceso de enrutamiento RIP para los enrutadores en el modo de configuración global, el cual debe ser el mismo para todos los nodos sobre los cuales queremos que exista el enrutamiento. Una vez creado y nombrado un proceso de enrutamiento, este se debe habilitar en cada una de las interfases de los enrutadores.

A continuación se presenta el ejemplo de configuración de RIP para el Router2 del esquema anterior. Esta configuración es similar para los Router 1 y 3.

```
Router2(config)#
ipv6 router rip procesorip
 maximum-paths 2

interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:1111::1/123
 ipv6 rip procesorip enable

interface Serial0/0
 no ip address
 shutdown
 no fair-queue

interface Serial0/1
 description conexion a router2
 no ip address
 ipv6 address 2000:1110::A/126
 ipv6 rip procesorip enable
```

clockrate 1000000

4.4.1.4 Verificando Conectividad RIP.

Los siguientes pasos se utilizan para desplegar información sobre la configuración de RIP Ipv6.

1. **show ipv6 rip** [*name*] [**database** | **next-hops**]
2. **show ipv6 route** [*ipv6-address* | *ipv6-prefix*/ *prefix-length* | *protocol*]
3. **enable**
4. **debug ipv6 rip** [*interface-type interface-number*]

PASO	COMANDO	PROPOSITO
1	**show ipv6 rip** [name] [**database** | **next-hops**] **Ejemplo:** Router> show ipv6 rip procesorip database	Muestra información acerca del proceso de enrutamiento Ipv6 actual. En este ejemplo, la información de la base de datos de procesamiento RIP Ipv6 es desplegada para el proceso de enrutamiento actual.
2	**show ipv6 route** [ipv6-address | ipv6-prefix/ prefix-length | protocol] **Ejemplo:** Router> show ipv6 route rip	Muestra el contenido actual de la tabla de enrutamiento Ipv6 actual. En este ejemplo, solamente se muestran rutas RIP Ipv6.
3	**enable** **Ejemplo:** Router> enable	Entra al modo privilegiado de configuración del router.
4	**debug ipv6 rip** [interface-type interface-number] **Ejemplo:** Router# debug ipv6 rip	Muestra mensajes de depuración para transacciones de enrutamiento de RIP Ipv6.

Tabla 4.23 Verificando Conectividad RIP

- **Salida en Pantalla para el comando Show Ipv6 RIP.**

En el siguiente ejemplo se muestra información acerca de todo el procesamiento RIP Ipv6 actual.

```
Router1#sh ipv6 rip
RIP process "procesorip", port 521, multicast-group FF02::9, pid 134
    Administrative distance is 120. Maximum paths is 2
    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 363, trigger updates 11
  Interfaces:
    Serial0/1
    FastEthernet0/0
  Redistribution:
    None
```

El siguiente ejemplo muestra información acerca del procesamiento RIP Ipv6 de una base de datos específica, utilizando el argumento *name* y la palabra **database** al final de la sentencia. En este caso se muestra el proceso RIP Ipv6 llamado procesorip, la información de los temporizadores y métrica.

```
Router1#sh ipv6 rip procesorip database
RIP process "procesorip", local RIB
 2000:1110::8/126, metric 2
    Serial0/1/FE80::212:80FF:FE51:6F60, expires in 163 secs
 2000:1110::C/126, metric 2, installed
    Serial0/1/FE80::212:80FF:FE51:6F60, expires in 163 secs
 2001:1111::40/123, metric 3, installed
    Serial0/1/FE80::212:80FF:FE51:6F60, expires in 163 secs
```

El siguiente ejemplo muestra información acerca de un proceso RIP Ipv6 especifico utilizando el comando **show ipv6 rip** con el argumento *name* y el comando **next-hops**.

```
Router1#sh ipv6 rip procesorip next-hops
 RIP process "procesorip", Next Hops
  FE80::212:80FF:FE51:6F60/Serial0/1 [3 paths]
```

- **Salida en Pantalla para el comando Show Ipv6 Route.**

La métrica actual de la ruta puede ser encontrada a través del comando show ipv6 route. En el siguiente ejemplo se muestra información en pantalla de todas las rutas RIP Ipv6 utilizando el comando **show ipv6 route rip.**

Router1#**sh ipv6 route rip**
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
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 2000:1110::C/126 [120/2]
via FE80::212:80FF:FE51:6F60, Serial0/1
R 2001:1111::40/123 [120/3]
via FE80::212:80FF:FE51:6F60, Serial0/1

- **Salida en Pantalla del comando Debug Ipv6 RIP.**

En el siguiente ejemplo se muestran mensajes de depuración para transacciones de rutas RIP Ipv6.

Router# **debug ipv6 rip**

RIPng: Sending multicast update on Serial0/1 for procesorip
src=FE80::212:FF:FE38:1C40
dst=FF02::9 (Serial0/1)
sport=521, dport=521, length=52
command=2, version=1, mbz=0, #rte=2
tag=0, metric=1, prefix=2000:1110::8/126
tag=0, metric=1, prefix=2001:1111::/123
RIPng: Sending multicast update on FastEthernet0/0 for procesorip
src=FE80::212:FF:FE38:1C40
dst=FF02::9 (FastEthernet0/0)
sport=521, dport=521, length=92

command=2, version=1, mbz=0, #rte=4
tag=0, metric=1, prefix=2000:1110::8/126
tag=0, metric=2, prefix=2000:1110::C/126
tag=0, metric=1, prefix=2001:1111::/123
tag=0, metric=3, prefix=2001:1111::40/123

4.4.2 OSPF Para IPv6.

4.4.2.1 Prerrequisitos para Implementar OSPF para Ipv6.

Antes de implementar el protocolo de enrutamiento OSPF (Primero la Ruta Libre mas Corta) RFC2740, se debe hacer los siguiente:

- Planear la distribución y aplicación de OSPF sobre nuestra red. Por ejemplo, se debe decidir cual será el número de áreas requerido.
- Habilitar el enrutamiento unicast Ipv6.
- Habilitar Ipv6 sobre la interfase.
- Habilitar CEFv4 globalmente en el router utilizando el comando **ip cef** en el modo de configuración global.
- Habilitar CEFv6 globalmente en el router utilizando el comando **ipv6 cef** en el modo de configuración global.

La siguiente tabla muestra las últimas versiones de Sistema Operativo Cisco IOS que soportan las características de OSPF.

CARACTERISTICA	CISCO IOS REQUERIDO
Expansion de OSPF versión 3 sobre OSPF versión 2.	12.2(15)T, 12.0(24)S, 12.2(18)S, 12.3, 12.3(2)T
Tipos de LSA en OSPF para Ipv6.	12.2(15)T, 12.0(24)S, 12.2(18)S, 12.3, 12.3(2)T
Interfases NBMA en OSPF para Ipv6	12.2(15)T, 12.0(24)S, 12.2(18)S, 12.3, 12.3(2)T
Force SPF en OSPF para Ipv6	12.2(15)T, 12.0(24)S, 12.2(18)S, 12.3, 12.3(2)T
Balance de Carga en OSP para Ipv6	12.2(15)T, 12.0(24)S, 12.2(18)S, 12.3, 12.3(2)T
Direcciones sobre una interfase en OSPF para Ipv6	12.2(15)T, 12.0(24)S, 12.2(18)S, 12.3, 12.3(2)T
OSPF para soporte de autenticación Ipv6 con IPsec	12.3(4)T

Tabla 4.24 Cisco IOS para OSPF

4.4.2.2 Funcionamiento de OSPF.

OSPF es un protocolo de enrutamiento IP. Este es un protocolo de estado de enlace y no de vector distancia. Tomando en cuenta un enlace que pertenece a una interfase de un dispositivo de red; un protocolo de estado de enlace toma sus decisiones de enrutamiento de acuerdo al estado de los enlaces que conectan a un dispositivo origen y un destino. El estado de un enlace es la descripción de la interfase y su relación con los dispositivos de red vecinos.

La información de la interfase incluye el prefijo Ipv6 de la interfase, la mascara de red, el tipo de red a la que esta conectada, los routers conectados a la red, etc. Esta información es propagada a través de varios tipos de anuncios de estado de enlace (LSAs).

Una colección de datos LSAs de un router es almacenada en una base de datos de estado de enlace. El contenido de la base de datos. La diferencia entre la base de datos y la tabla de enrutamiento, es que la base de datos una colección completa de datos en bruto; la tabla de enrutamiento contiene una lista de las rutas más cortas hacia los destinos, conocidas a través de puertos específicos de la interfase de un router.

Tipos de LSAs.

La siguiente lista describe los diferentes tipos de LSA, donde cada una de ellas tiene un propósito diferente.

- **LSAs de Enrutamiento (Tipo 1)**

Describen el estado de enlace y los costos de los enlaces de un router para un área específica. Estas LSAs son inundadas dentro de una sola área. Estas también indican si un router es un Router de Borde de Área (ABR) o un Router de Limite de Sistema Autónomo (ASBR) y si este es un dispositivo final o un enlace virtual. En OSPF para Ipv6, estas LSAs no poseen información de dirección y son independientes del protocolo de red. La información de interfase de un router es expandida a través de múltiples LSAs y los receptores deben concatenar todas las LSAs recibidas cuando esta corriendo el algoritmo SPF.

- **LSAs de Red (Tipo 2)**

Describen el estado de enlace y la información de costo para todos los routers que forman parte de la red. Solamente un router designado puede generar una LSA de Red; las cuales no poseen información de dirección y son independientes del protocolo de red.

- **LSAs de Prefijos de Área Interna para ABRs (Tipo3)**

Anuncian redes internas a routers en otras áreas y representan a una sola red o a una conjunto de redes sumarizadas dentro de un solo anuncio. En OSPF para Ipv6 las direcciones para estas LSAs son representadas por un prefijo y la longitud del prefijo, en lugar de una dirección y su mascara de subred. Una ruta por defecto es representada por una longitud de prefijo igual a cero.

- **LSAs de Routers de Área Interna para ASBRs (Tipo 4)**

Anuncia la ubicación de un ASBR. Los routers que están tratando de alcanzar una red externa utilizan estos anuncios para determinar la mejor ruta para el siguiente salto.

- **LSAs de Sistema Autónomo Externo (Tipo 5)**

Redistribuyen rutas a otros sistemas autónomos, usualmente de un protocolo de enrutamiento diferente hacia OSPF. En OSPF para Ipv6 las direcciones para estas LSAs son representadas por un

prefijo y la longitud del prefijo, en lugar de una dirección y su mascara de subred. Una ruta por defecto es representada por una longitud de prefijo igual a cero.

- **LSAs de Enlace (Tipo 8)**

Provee la dirección de enlace local de un router a los otros routers agregados al enlace y les informa sobre una lista de prefijos Ipv6 para ser asociados con el enlace y permite que el router establezca una colección de bits de opción para ser asociados con la LSA de red que será originada por el enlace.

- **LSAs para Prefijos de Área Interna (Tipo 9)**

Un router puede originar muchas de estas LSAs para cada router o red en transito, cada una con un identificador de estado de enlace único. Este identificador define para cada LSA la asociación que tenga con una LSA de Enrutamiento o LSA de Red y contiene los prefijos para la red stub o redes en transito.

NBMA en OSPF para Ipv6.

En una red NBMA, el router designado (DR) o el router designado de respaldo (BDR) son encargados de la inundación LSA. Sobre una red punto a punto, la inundación sale solamente de una interfase hacia un solo vecino.
Los routers que comparten un segmento común (enlace de capa 2 entre dos interfases) comparten los vecinos sobre este segmento. OSPF utiliza el protocolo Hola (Hello) , enviando periódicamente este tipo de paquetes a cada interfase.

En las redes punto a punto y redes punto a multipunto, el software inunda con actualizaciones de enrutamiento a los routers inmediatos.
Solamente en los segmentos broadcast o NBMA, OSPF minimiza la cantidad de información que se intercambia en un segmento por medio de la elección de un Router Designado (DR) y un Router Designado de Respaldo (BDR), de esta manera los routers sobre el segmento tendrán un punto central de contacto para el intercambio de información. En lugar de que los routers intercambien actualizaciones de enrutamiento con cada uno de los routers del segmento, los routers del segmento intercambiaran información con el DR o el BDR, los cuales distribuirán esta información a los otros routers.

OSPF determina las prioridades de los routers sobre el segmento, para determinar cuales routers serán el DR y el BDR. El router con la prioridad más alta es seleccionado como DR. Un router con una prioridad igual a cero no puede ser elegido como DR o BDR.
Cuando se utiliza NBMA en OSPF para Ipv6 , no es posible detectar vecinos automáticamente, por lo tanto los vecinos deben ser configurados manualmente en el modo de configuración del router.

Algoritmo SPF en OSPF para Ipv6.

Cuando la palabra **process** se utiliza con el comando **clear Ipv6 ospf,** la base de datos OSPF se vacía y se vuelve a calcular, entonces comienza a realizarse el algoritmo de Primero la Ruta Mas Corta (SPF). Cuando la palabra **force-spf** se utiliza con el comando **clear ipv6 ospf**, la base de datos no se vacía antes de que se realice el algoritmo SPF.

Balance de Carga en OSPF para Ipv6.

Cuando un router aprende múltiples rutas para una red especifica a través de múltiples procesos de enrutamiento (o protocolos de enrutamiento), este captura la ruta que posee la menor distancia administrativa dentro de la tabla de enrutamiento. En algunos casos el router debe seleccionar una ruta de muchas que han sido aprendidas a través del mismo proceso de enrutamiento y que poseen la misma distancia administrativa. En este caso el router elige la ruta con el menor costo o métrica hacia el destino. Cada proceso de enrutamiento calcula un costo de manera distinta y en algunas ocasiones el costo necesita ser manipulado para lograr balancear la carga.

OSPF realiza el balance de carga automáticamente de la siguiente manera. Si OSPF encuentra una manera de alcanzar un destino a través de más de una interfase y cada ruta posee el mismo costo, este captura cada ruta en la tabla de enrutamiento. Para restringir el numero de rutas que van hacia un mismo destino se utiliza el comando **maximum-paths.** Por defecto el mayor número de rutas es 16; pero puede ser configurada de 1 a 64 rutas.

Soporte para la Autenticación Ipv6 con Ipsec.

Para asegurar que los paquetes Ipv6 para OSPF no sean alterados y reenviados al router, causando que el router se comporte de una manera no deseada para sus administradores. OSPF para Ipv6 utiliza el Protocolo de Seguridad Ip (IP Secutrity o Ipsec) para que los paquetes Ipv6 puedan ser autenticados en OSPF.
OSPF para Ipv6 requiere el uso de IPsec para habilitar la autenticación, ya que este provee imágenes encriptadas para que se utilicen en el proceso de autenticación.
Los campos de autenticación ha sido removidos del encabezado OSPF y cuando OSPF corre sobre Ipv6, OSPF asegura la integridad, autenticación y confiabilidad en el intercambio de enrutamiento, utilizando el Encabezado de Autenticación del protocolo Ipv6 y el Encapsulamiento de Carga (ESP).

Para configurar IPsec el usuario debe configurar una política de seguridad, la cual es una combinación de un índice de política de seguridad y una clave (la clave crea y valida el valor del Message Diggest 5 [MD5]). Ipsec para OSPF puede ser configurado sobre una interfase o sobre un área específica. Para mayor seguridad el usuario debe configurar una política diferente en cada interfase donde se configure IPsec. Si IPsec se configura para un área, la política es aplicada en todas las interfases que pertenecen a dicha área, excepto para aquellas que tengan IPsec directamente configurado. Una vez IPsec es configurado en OSPF para Ipv6, este es invisible para el usuario.

Cada interfase posee un identificador de estado con respecto a la autenticación, conocido como socket seguro (secure socket); el cual puede tener cualquiera de los siguientes valores:

- NULO (NULL): No crea un socket seguro para la interfase si la autenticación es configurada para el área.

- DESACTIVADO (DOWN): La autenticación ha sido configurada para la interfase (o el área que contiene la interfase), pero OSPF no ha recibido mensajes CRyPTO_SS_SOCKET_UP desde IPsec.

- ACTIVADO (UP): OSPF ha recibido un mensaje CRyPTO_SS_SOCKET_UP desde IPsec.

- ACERCANDO (CLOSING): El socket seguro para la interfase se ha cerrado y probablemente se esta abriendo uno nuevo para dicha interfase, para el caso, el socket actual hace una

transición al estado DOWN. De otra manera la interfase cambiara a no configurada (UNCONFIGURED).

- NO CONFIGURADO (UNCONFIGURED): La autenticación no esta configurada en la interfase.

OSPF no enviara o recibirá paquetes mientras se encuentre en el estado DOWN.

4.4.2.3 Implementando OSPF para Ipv6.

Habilitando OSPF en una interfase Ipv6.

Los siguientes pasos describen la forma de habilitar OSPF para el enrutamiento Ipv6 y configurarlo sobre cada interfase. Por defecto, el enrutamiento OSPF para Ipv6 se encuentra deshabilitado y mucho menos se encuentra configurado para las interfases.

1. enable
2. configure terminal
3. interface *type number*
4. ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

A continuación se presentan los pasos para habilitar OSPF, de forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**interface** interface-type interface-number **Ejemplo:** Router(config)# interface ethernet 0/0	Especifica el número, el tipo de interface y entra al modo de configuración de interface.

4	**ipv6 ospf** process-id **area** area-id [**instance** instance-id] **Ejemplo:** Router(config-if)# ipv6 ospf 1 area 0	Habilita OSPF para Ipv6 sobre una interfase.

Tabla 4.25 Habilitando OSPF en una Interfase.

Definiendo un área OSPF para Ipv6.

El costo sumarizado de un conjunto de rutas, será el costo mayor de las rutas que están siendo sumarizadas; por ejemplo, si las siguientes rutas son sumariadas:

OI 2003:0:0:7::/64 [110/20]
via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
OI 2003:0:0:8::/64 [110/100]
via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
OI 2003:0:0:9::/64 [110/20]
via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0

la ruta sumarizada resultante seria la siguiente:

OI 2003::/48 [110/100]
via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0

Para establecer un área OSPF es necesario sumarizar las rutas pertenecientes a dicha área. Para lograr esto se deben seguir los siguientes pasos.

1. enable
2. configure terminal
3. ipv6 router ospf *process-id*
4. area *area-id* **range** {*ipv6-prefix / prefix-length*} [**advertise** | **not-advertise**] [**cost** *cost*]

A continuación se presentan los pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**ipv6 router ospf** process-id **Ejempo:** Router(config)# ipv6 router ospf 1	Habilita el modo de configuración de OSPF en el router.
4	**area** area-id **range** { ipv6-prefix/ prefix-length} [**advertise** | **not-advertise**] [**cost** cost] **Ejemplo:** Router(config-rtr)# area 1 range 2001::/48	Sumariza las rutas en una sola área.

Tabla 4.26 Definiendo un área OSPF para Ipv6.

Configurando IPsec en OSPF para Ipv6.

Una vez se ha configurado OSPF y se ha definido el uso de autenticación, se debe determinar la política de seguridad que será aplicada en cada una de las rutas dentro del grupo. La política de seguridad consiste en la combinación de una clave y un SPI, que deben ser definidos previamente.

La autenticación puede ser configurada en una interfase o sobre un área OSPF especifica. Cuando se define un área, esta busca las interfases que se encuentran dentro de la misma y aplica la autenticación a todas ellas. Para mayor seguridad utilice una autenticación diferente para cada interfase.

Autenticación sobre una Interfase.

Antes de configurar IPsec sobre una interfase, se debe habilitar OSPF previamente sobre dicha interfase.

Los siguientes pasos muestran como configurar IPsec sobre una interfase.

1. enable

2. configure terminal

3. interface *type number*

4. ipv6 ospf authentication ipsec spi *spi* **md5** [*key-encryption-type*] *key* / **null**

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**interface** interface-type interface-number **Ejemplo:** Router(config)# interface ethernet 0/0	Especifica el número, el tipo de interface y entra al modo de configuración de interface.
4	**ipv6 ospf authentication ipsec spi** spi **md5** [key-encryption-type] key | **null** **Ejemplo:** Router(config-if)# ipv6 ospf authentication ipsec spi 500 md5 1234567890abcdef1234567890abcdef	Especifica el tipo de autenticación para una interfase.

Tabla 4.27 Autenticación sobre una Interfase.

Autenticación sobre un área OSPF.

Los siguientes pasos se utilizan para configurar la autenticación Ipsec sobre un área OSPF.

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **area** *area-id* **authentication ipsec spi** *spi* **md5** [*key-encryption-type*] *key*

A continuación se presentan los pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	ipv6 router ospf process-id **Ejemplo:** Router(config)# ipv6 router ospf 1	Habilita OSPF en el modo de configuración del router.
4	**area** area-id **authentication ipsec spi** spi **md5** [key-encryption-type] key **Ejemplo:** Router(config-rtr)# area 1 authentication ipsec spi 678 md5 1234567890ABCDEF1234567890ABCDEF	Habilita la autenticación para un área específica.

Tabla 4.28 Autenticación sobre un área OSPF.

Configurando interfaces NBMA.

OSPF para Ipv6 puede ser personalizado en una red para utilizar interfases NBMA, ya que este no tiene la capacidad de detectar vecinos automáticamente sobre interfase NBMA. Sobre una interfase NBMA se deben configurar los vecinos manualmente utilizando el modo de configuración de interfase.

Antes de configurar interfaces NBMA se deben realizar las siguientes tareas:

- Configurar la red para que sea una red NBMA.
- Identificar cada vecino.

Los siguientes pasos se utilizan para configurar una interfase como NBMA.

1. enable
2. configure terminal
3. interface *type number*
4. frame-relay map ipv6 *ipv6-address dlci* **[broadcast] [cisco] [ietf] [payload-compression** {**packet-by-packet | frf9 stac** [*hardware-options*] | **data-stream stac** [*hardware-options*]}]
5. ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

A continuación se presentan los pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**interface** type number **Ejemplo:** Router(config)# interface serial 0	Especifica el numero, el tipo de interfase y entra al modo de configuración de interfase

4	**frame-relay map ipv6** ipv6-address dlci [**broadcast**] [**cisco**] [**ietf**] [**payload-compression** {**packet-by-packet** | **frf9 stac** [hardware-options] | **data-stream stac** [hardware-options]}] **Ejemplo:** Router(config-if)# frame-relay map ipv6 FE80::A8BB:CCFF:FE00:C01 120	Define un mapeo entre una dirección Ipv6 destino y el identificador de conexión del enlace de datos (DLCI) utilizado para conectarse a ese destino. Para este ejemplo, el enlace NBMA es un Frame Relay.
5	**ipv6 ospf neighbor** ipv6-address [**priority** number] [**poll-interval** seconds] [**cost** number] [**database-filter all out**] **Ejemplo:** Router(config-if) ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01	Configura un router vecino OSPF.

Tabla 4.29 Configurando interfaces NBMA.

Forzando un Calculo SPF.

Los siguientes pasos se utilizan para iniciar el algoritmo SPF sin limpiar la base de datos OSPF.

1. enable

2. clear ipv6 ospf [*process-id*] {**process** | **force-spf** | **redistribution** | **counters** [**neighbor** [*neighbor-interface*]]}

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**clear ipv6 ospf** [process-id] {**process** | **force-spf** | **redistribution** | **counters** [**neighbor** [neighbor-interface]]} **Ejemplo:** Router# clear ipv6 ospf 1 force-spf	Limpia el estado de OSPF basado en el ID del proceso de enrutamiento.

Tabla 4.30 Forzando un Calculo SPF.

4.4.2.4 Ejemplos de Configuración de OSPF en Ipv6.

- **Configuración de un Proceso de Enrutamiento OSPF y Habilitacion de Interfases.**

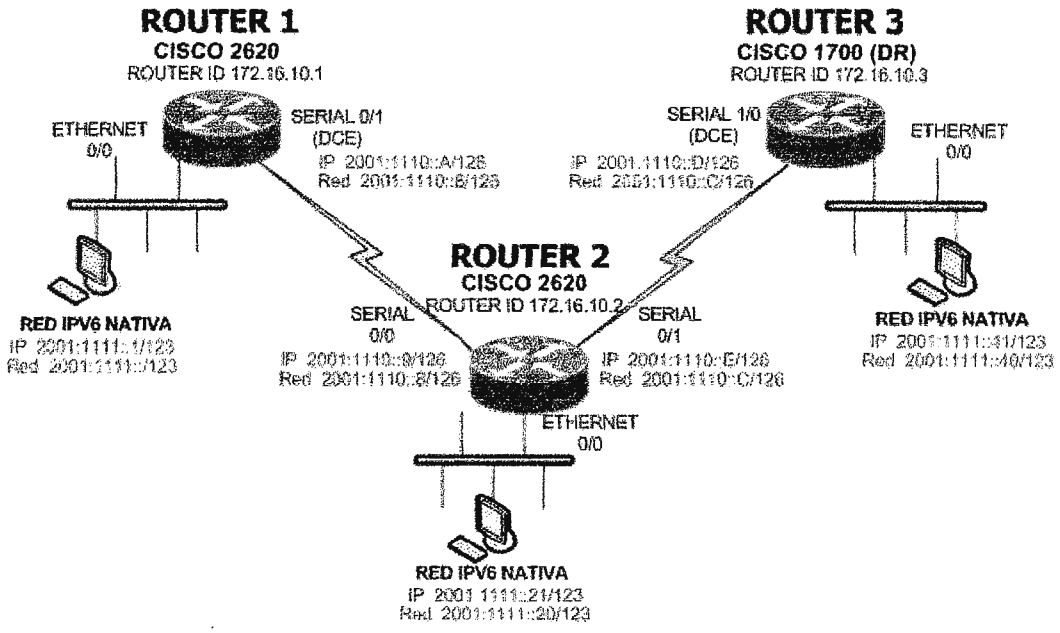


Figura 4.10 Diagrama para la Configuración de OSPF para Ipv6.

El diagrama anterior muestra una Red Nativa Ipv6 compuesta por tres enrutadores, los cuales se encuentran conectados a través de sus seriales, cada una de ellas configurada con una dirección Ipv6 así:

- Router 1: Interfase Serial 0/1, con dirección Ipv6 2001:1110::A/126.
- Router 2: Interfase Serial 0/0, con dirección Ipv6 2001:1110::9/126 e
  Interfase Serial 0/1, con dirección Ipv6 2001:1110::E/126.
- Router 3: Interfase Serial 1/0, con dirección Ipv6 2001:1110::D/126.

Cada nodo posee una Red de Área Local (LAN), identificada por intereses FastEthernet, cada una configurada con una dirección Ipv6 perteneciente a una red especifica. Así:

- Router 1: Interfase FastEthernet 0/0, con direccion Ipv6 2001:1111::1/123.

- Router 2: Interfase FastEthernet 0/0, con direccion Ipv6 2001:1111::21/123.
- Router 3: Interfase FastEthernet 0/0, con direccion Ipv6 2001:1111::41/123.

Cada enrutador posee un identificador único (Router ID), el cual es utilizado para decisiones de enrutamiento propias de protocolo, estos identificadores poseen la sintaxis de una dirección Ipv4 y se han definido los siguientes:

- Router1: 172.16.10.1
- Router2: 172.16.10.2
- Router3: 172.16.10.3

Para configurar el enrutamiento OSPF primeramente se debe crear un Proceso de enrutamiento OSPF en el modo de configuración global del router, el cual puede ser un número entre 1 y 65535.

Además se debe configurar un identificador para el enrutador (Router ID) y se define un área específica para dicho proceso de enrutamiento con un rango de direcciones Ipv6 que sumarice el rango que poseen las interfases del enrutador actual. Así como se muestra a continuación:

```
Router1(config)#
ipv6 router ospf 1
 router-id 172.16.10.1
 log-adjacency-changes
 area 0 range 2001::/16
```

Después de haber configurado el proceso de enrutamiento en el modo de configuración global del enrutador, se debe habilitar dicho proceso y el área especifica en cada una de las interfases del enrutador, así como se muestra a continuación:

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:1111::1/123
 ipv6 ospf 1 area 0
```

```
interface Serial0/1
 description conexion a router2
 no ip address
 ipv6 address 2001:1110::A/126
 ipv6 ospf 1 area 0
 clockrate 1000000
```

- **Ejemplo de Configuracion de Autenticación sobre una Interfase.**

El siguiente ejemplo define la autenticación sobre la interfase ethertnet 0/0.

```
interface Ethernet0/0
  ipv6 enable
  ipv6 ospf 1 area 0
  ipv6 ospf authentication ipsec spi 500 md5 1234567890ABCDEF1234567890ABCDEF
interface Ethernet0/0
  ipv6 enable
  ipv6 ospf authentication null
  ipv6 ospf 1 area 0
```

- **Ejemplo de Configuracion de Autenticación sobre una Interfase.**

El siguiente ejemplo define la autenticación OSPF sobre un área 0.

```
ipv6 router ospf 1
  router-id 172.16.10.1
  area 0 authentication ipsec spi 1000 md5 1234567890ABCDEF1234567890ABCDEF
```

- **Ejemplo de Configuracion de Interfases NBMA.**

El siguiente ejemplo configura un router vecino OSPF con la dirección Ipv6 FE80::A8BB:CCFF:FE00:C01.

```
interface serial 0
  ipv6 enable
  ipv6 ospf 1 area 0
  encapsulation frame-relay
  frame-relay map ipv6 FE80::A8BB:CCFF:FE00:C01 120
  ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01\
```

- **Ejemplo de Configuración de SPF.**

El siguiente ejemplo dispara el algoritmo SPF.

```
clear ipv6 ospf force-spf
```

4.4.2.5 Verificando la Operación de OSPF para Ipv6.

Los siguientes comandos se utilizan para verificar la configuración y operación de OSPF para Ipv6.

1. **enable**
2. **show ipv6 ospf** [*process-id*] [*area-id*] **interface** [*interface-type interface-number*]
3. **show ipv6 ospf** [*process-id*] [*area-id*]
4. **show crypto ipsec policy** [**name** *policy-name*]
5. **show crypto ipsec sa ipv6** [*interface-type interface-number*] [**detailed**]

A continuación se presentan estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**show ipv6 ospf** [process-id] [area-id] **interface** [interface-type interface-number] **Ejemplo:** Router# **show ipv6 ospf interface**	Muestra información de una interfase OSPF

3	**show ipv6 ospf** [process-id] [area-id] **Ejemplo:** Router# **show ipv6 ospf**	Muestra información general acerca de los procesos de enrutamiento de OSPF.
4	**show ipv6 route ospf** **Ejemplo:** Router# **show ipv6 route ospf**	Muestra las rutas OSPF aprendidas por el router.
5	**show ipv6 ospf traffic** **Ejemplo:** Router# **show ipv6 ospf traffic**	Muestra el trafico OSPF de salida y de entrada en el enrutador.
6	**show crypto ipsec policy** [**name** policy-name] **Ejemplo:** Router# show crypto ipsec policy	Muestra los parámetros para cada política IPsec.
7	**show crypto ipsec sa ipv6** [interface-type interface-number] [**detailed**] **Ejemplo:** Router# show crypto ipsec sa ipv6	Muestra las opciones utilizadas por las asociaciones de seguridad actuales.

Tabla 4.31 Verificando la Operación de OSPF para Ipv6.

- **Salida en Pantalla del comando Show Ipv6 OSPF Interface.**

El siguiente es un ejemplo de salida en pantalla para el comando **show ipv6 ospf interface:**

Router# **show ipv6 ospf interface**

Serial0/1 is up, line protocol is up
Link Local Address FE80::212:FF:FE38:1C40, Interface ID 5
Area 0, Process ID 1, Instance ID 0, Router ID 172.16.10.1
Network Type POINT_TO_POINT, Cost: 64
Transmit Delay is 1 sec, State POINT_TO_POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
Index 1/2/2, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 2
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 172.16.10.2
Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
Link Local Address FE80::212:FF:FE38:1C40, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 172.16.10.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 172.16.10.1, local address FE80::212:FF:FE38:1C40
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:00
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

- **Salida en Pantalla para el commando Show ipv6 ospf.**

Este es un ejemplo de salida en pantalla del commando **show ipv6 ospf:**

Router# **show ipv6 ospf**

Routing Process "ospfv3 1" with ID 172.16.10.1
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs

Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Area BACKBONE(0)

Number of interfaces in this area is 2

SPF algorithm executed 6 times

Area ranges are

2001::/16 Passive Advertise

Number of LSA 9. Checksum Sum 0x0444D8

Number of DCbitless LSA 0

Number of indication LSA 0

Number of DoNotAge LSA 0

Flood list length 0

- **Salida de Pantalla para el commando sh ipv6 route ospf.**

Router1#**sh ipv6 route ospf**

IPv6 Routing Table - 8 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

O 2001:1110::C/126 [110/128]

via FE80::212:80FF:FE51:6F60, Serial0/1

O 2001:1111::40/123 [110/129]

via FE80::212:80FF:FE51:6F60, Serial0/1

- **Salida en Pantalla del comando Show ipv6 ospf traffic.**

Router1#**sh ipv6 ospf traffic**

OSPFv3 statistics:

Rcvd: 398 total, 0 checksum errors

360 hello, 3 database desc, 1 link state req

11 link state updates, 4 link state acks

0 link state updates ignored

Sent: 0 total

- **Salida en Pantalla para el commando Show crypto ipsec policy.**

A continuación se muestra un ejemplo de salida de pantalla para el comando **show crypto ipsec policy**:

Router# **show crypto ipsec policy**

Crypto IPsec client security policy data

Policy name: OSPFv3-1-1000

Policy refcount: 1

Inbound AH SPI: 1000 (0x3E8)

Outbound AH SPI: 1000 (0x3E8)

Inbound AH Key: 1234567890ABCDEF1234567890ABCDEF

Outbound AH Key: 1234567890ABCDEF1234567890ABCDEF

Transform set: ah-md5-hmac

- **Salida de Pantalla del comando Show crypto ipsec sa ipv6.**

A continuación se muestra un ejemplo de salida de pantalla para el comando **show crypto ipsec sa ipv6**:

Router# **show crypto ipsec sa ipv6**

IPv6 IPsec SA info for interface Ethernet0/0

protected policy name:OSPFv3-1-1000

IPsec created ACL name:Ethernet0/0-ipsecv6-ACL

local ident (addr/prefixlen/proto/port):(FE80::/10/89/0)

remote ident (addr/prefixlen/proto/port):(::/0/89/0)

current_peer:::

PERMIT, flags={origin_is_acl,}

#pkts encaps:21, #pkts encrypt:0, #pkts digest:21

#pkts decaps:20, #pkts decrypt:0, #pkts verify:20

```
#pkts compressed:0, #pkts decompressed:0
#pkts not compressed:0, #pkts compr. failed:0
#pkts not decompressed:0, #pkts decompress failed:0
#send errors 0, #recv errors 0

local crypto endpt. ::, remote crypto endpt. ::
path mtu 1500, media mtu 1500
current outbound spi:0x3E8(1000)

inbound ESP SAs:

inbound AH SAs:
spi:0x3E8(1000)
transform:ah-md5-hmac ,
in use settings ={Transport, }
slot:0, conn_id:2000, flow_id:1, crypto map:N/R
no sa timing (manual-keyed)
 replay detection support:N

inbound PCP SAs:
outbound ESP SAs:
outbound AH SAs:
spi:0x3E8(1000)
transform:ah-md5-hmac ,
in use settings ={Transport, }
   slot:0, conn_id:2001, flow_id:2, crypto map:N/R
   no sa timing (manual-keyed)
   replay detection support:N

outbound PCP SAs:
```

4.4.3 IS-IS Para Ipv6.

System Sistema Intermedio Integrado hacia Sistema Integrado (IS-IS) es u protocolo de enrutamiento interior (IGP) que anuncia información de estado de enlace hacia afuera de la red para crear una fotografía de la topología de la red. IS-IS es un Sistema de Interconexión Abierto (OSI) y un protocolo de enrutamiento jerárquico que designa un Sistema Intermedio como un dispositivo de Nivel 1 o Nivel 2.

IS-IS integrado utiliza un solo algoritmo de enrutamiento para el soporte de varias familias de direcciones como Ipv6, Ipv4 y OSI.

4.4.3.1 Prerrequisitos para Implementar IS-IS.

- Estar familiarizado con la configuración de Ipv4.
- Estar familiarizado con la configuración de Ipv6.

La siguiente tabla muestra las últimas versiones de Sistema Operativo Cisco IOS que soportan las características de IS-IS.

CARACTERISTICA	CISCO IOS REQUERIDO
Configuraciones Basicas de IS-IS	12.2(8)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
Soporte de Multitopologia IS-IS	12.2(15)T, 12.2(18)S, 12.0(26)S, 12.3, 12.3(2)T
Base de Información de Enrutamiento Local para IS-IS (RIB)	12.3(4)T, 12.2(25)S
Configurando IS-IS para Ipv6	12.2(8)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
Personalizando IS-IS para Ipv6	12.2(8)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
Redistribuyendo rutas Ipv6 en un proceso de enrutamiento.	12.2(8)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
Redistribuyendo rutas Ipv6 entre niveles IS-IS	12.2(8)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3,

	12.3(2)T
Deshabilitando el protocolo de soporte Ipv6.	12.2(8)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T

Tabla 4.32 Sistema Operativo Cisco IOS que soportan las características de IS-IS.

Un solo algoritmo de Primero la Ruta mas Corta (SPF) por nivel, es utilizado para computar las direcciones Ipv4, Ipv6 u OSI. El uso de un solo SPF significa que el protocolo de enrutamiento IS-IS debe estar configurado para Ipv4 e Ipv6 y deben compartir una misma topología de red. Para utilizar IS-IS para el enrutamiento Ipv4 e Ipv6, cada interfase debe ser configurada con IS-IS para Ipv4 y con IS_IS para Ipv6.

Todos los routers dentro de un área IS-IS (enrutamiento de nivel 1) o dominio (enrutamiento de nivel 2) deben también soportar las mismas familias de direcciones establecidas; ya sea Ipv4, Ipv6 o ambas.

4.4.3.2 Funcionamiento de IS-IS para Ipv6.

IS-IS para Ipv6 funciona de la misma manera y provee los mismos beneficios que en Ipv4. Las mejorías que provee Ipv6 para IS-IS, es que le permite anunciar los prefijos Ipv6 adicionalmente a las rutas Ipv4 e Ipv6.

La interfase de línea de comandos IS-IS para Ipv6 pose extensiones que permiten la configuración de parámetros específicos de Ipv6.

IS-IS para Ipv6 extiende el número de familias de direcciones soportadas agregando la familia de direcciones Ipv6 en adición a la Ipv4 y a la OSI. Además, IS-IS para Ipv6 provee soporte para modos de topologías únicas y múltiples.

Topología Única IS-IS para Ipv6.

Permite que IS-IS para Ipv6 pueda ser configurado en interfases junto a otros protocolos de red, por ejemplo Ipv4 o CLNS (Servicios de Red sin Conexión). Todas las interfases deben ser configuradas exactamente con las mismas familias de direcciones. Adicionalmente todos los routers que pertenezcan

a la misma área IS-IS o dominio deben soportar exactamente las mismas familias de direcciones de capa de red en todas las interfases.

Cuando una topología única esta siendo utilizada, se debe utilizar un estilo nuevo o antiguo de TLVs. De cualquier manera, los TLVs utilizados para anunciar la alcanzabilidad de prefijos ipv6 usan métricas extendidas. Los routers cisco no permiten que la métrica se establezca con un valor suprior a 63 si la configuración no se ha establecido para el uso exclusivo de TLVs de nuevo estilo, en Ipv4. En el modo de topología única para Ipv6, la métrica configurada siempre es la misma para Ipv4 e Ipv6.

Multitopologia IS-IS para Ipv6.

Permite a IS-IS mantener un conjunto de topologías independientes dentro de una sola área o dominio. En este modo, desaparece la restricción en la que todas las interfases a las cuales se les ha configurado IS-IS deban soportar las mismas familias de direcciones. También desaparece la restricción en la cual todos los routers que pertenecen a una misma área IS-IS o dominio deben soportar las mismas familias de direcciones de capa de red. Para cada topología configurada debe existir un SPF, de este modo es suficiente que la conectividad exista entre un conjunto de routers dentro del área o dominio para que una familia de direcciones dada sea ruteable.

Se puede utilizar el comando **isis ipv6 metric** para configurar diferentes métricas sobre una interfase para Ipv6 o Ipv4.
Cuando se utilice Multitopologia para Ipv6, utilice el comando **metric-style wide** para configurar IS-IS para utilizar un nuevo estilo de TLVs, ya que estas son utilizadas para anunciar información de Ipv6 por medio de paquetes de estado de enlace (LSPs) que están definidos para utilizarse en métricas extendidas.

Transición de una Topología Única a una Multitopologia para Ipv6.
Todos los routers en un área o dominio deben poseer el mismo tipo de soporte Ipv6, ya sea para Topología Única o para Multitopologia. Un router que operando sobre un modo de multiptopologia no reconocerá la disponibilidad de un router sobre un modo de topología única para el soporte del trafico Ipv6, lo cual ocasionara agujeros sobre la topología Ipv6.
Para la transición de una topología única a una multitopologia más flexible, existe un modo de transición a multitopologia proveído para el usuario.

El modo de transición a multitopologia permite a una red operando en una topología única IS-IS para Ipv6, continuar trabajando mientras se actualizan los routers para incluir un soporte para multitopologia IS-IS para Ipv6. Mientras se encuentra en modo de transición, ambos tipos de TLV's

(para Topología Unica y Multitopologia) son enviadas por medio de LSPs para todas las direcciones Ipv6 configuradas, pero el router continua trabajando en modo de topología única. Después, todos los routers del área o dominio estarán actualizados para soportar multitopologia Ipv6 y estar operando en el modo de transición. El modo de transición puede ser removido de la configuración.
Una vez que todos los routers que se encuentren en la misma área o dominio estén operando en el modo de multitopologia Ipv6, las restricciones topológicas del modo de topología única ya no tendrán efecto.

Base de Información de Enrutamiento Local (RIB) para IS-IS Ipv6.

Un router que esta corriendo IS-IS para Ipv6 mantiene una RIB local la cual almacena todas las rutas de destino aprendidas a través de los routers vecinos. Al final de cada SPF, IS-IS intenta instalar la mejor de las rutas (la de menor costo) para un destino presente en la RIB local dentro de la tabla de enrutamiento Ipv6.

4.5.3.3 Implementando IS-IS para Ipv6.

Cuando se configura un protocolo de enrutamiento en Ipv6 se debe crear un proceso de enrutamiento, habilitar un proceso de enrutamiento sobre las interfases y personalizar el protocolo de enrutamiento para la red en particular.

Configurando una Topología Unica en IS-IS para Ipv6.

Para configurar IS-IS se deben realizar dos actividades. La primera actividad es crear un proceso de enrutamiento IS-IS que es creado utilizando los comandos del protocolo IS-IS. La segunda actividad es configurar la operación del protocolo IS-IS sobre una interfase.
Antes de configurar el router con el protocolo de enrutamiento IS-IS para Ipv6, se debe habilitar globalmente en el router el uso del protocolo Ipv6 por medio del comando ipv6 unicast-routing.
Los siguientes pasos se utilizan para configurar IS-IS con soporte para topología única.

1. **enable**
2. **configure terminal**
3. **router isis** *area-name*
4. **net** *network-entity-title*
5. **exit**
6. **interface** *type number*
7. **ipv6 address** *ipv6-prefix/ prefix-length* [**eui-64**]
8. **ipv6 router isis** *area-name*

A continuación se presentan estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**router isis** area-name **Ejemplo:** Router(config)# router isis area2	Habilita IS-IS para un proceso de enrutamiento específico y entra en el modo de configuración del router.
4	**net** network-entity-title **Ejemplo:** Router(config-router)# net 49.0001.0000.0000.000c.00	Configura un titulo de entidad de red IS-IS (NET) para el proceso de enrutamiento. El argumento del titulo de identidad de red define las direcciones del área IS-IS y el ID del sistema del router.
5	**exit** **Ejemplo:** Router(config-router)# exit	Sale del modo de configuración del router y entra al modo de configuración global
6	**interface** type number **Ejemplo:** Router(config)# interface serial 0	Especifica el numero, el tipo de interfase y entra al modo de configuración de interfase
7	**ipv6 address** ipv6-prefix/ prefix-length [**eui-64**]	Especifica la red Ipv6 asignada a la interfase y habilita el procesamiento

	Ejemplo: Router(config-if)# ipv6 address 2001:0DB8::3/64	Ipv6 en la interfase.
8	**ipv6 router isis** area-name **Ejemplo:** Router(config-if)# ipv6 router isis area2	Habilita el proceso de enrutamiento IS-IS Ipv6 especificado sobre la interfase.

Tabla 4.33 Configurando una Topología Unica en IS-IS para Ipv6.

Implementando Multitopologia en IS-IS para Ipv6.

Cuando se configura multitopologia en OSPF para Ipv6, el comando **transition** permite a un usuario que esta trabajando sobre una Topología Única, continuar trabajando mientras se esta actualizando hacia una Multitopolgia IS-IS.

Después de que cada router se haya configurado con la palabra **transition**, el usuario puede removerla posteriormente de cada router. Cuando no esta habilitado el modo de transición, la conectividad Ipv6 entre los routers que están operando en el modo de Topología Única y los routers que están operando en el modo de Multitopologia no puede ser posible.

El comando opcional **isis ipv6 metric** permite diferenciar entre costos de enlace para Ipv6 y trafico Ipv4, cuando se esta operando en el modo multitopologia.

Los siguientes pasos se utilizan para configurar IS-IS con soporte para multitopologia.

1. enable
2. configure terminal
3. router isis *area-name*
4. metric-style wide [**transition**] [**level-1** | **level-2** | **level-1-2**]
5. address-family ipv6 [**unicast** | **multicast**]
6. multi-topology [**transition**]

A continuación se presentan estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:**	Habilita el modo EXEC privilegiado.

	Router> enable	
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**router isis** area-name **Ejemplo:** Router(config)# router isis area2	Habilita IS-IS para el proceso de enrutamiento IS-IS específico y entra en el modo de configuración del router.
4	**metric-style wide** [**transition**] [**level-1** | **level-2** | **level-1-2**] **Example:** Router(config-router)# metric-style wide level-1	Configura un router corriendo el protocolo IS-IS para que pueda generar y aceptar solo TLVs de nuevo estilo.
5	**address-family ipv6** [**unicast** | **multicast**] **Ejemplo:** Router(config-router)# address-family ipv6	Especifica la familia de direcciones Ipv6 y entra al modo e configuración de familias de direcciones. La palabra **unicast** especifica la familia de direcciones tipo unicast para Ipv6. El modo unicast es el configurado por defecto.
6	**multi-topology** [**transition**] **Ejemplo:** Router(config-router-af)# multi-topology	Habilita multitopologia IS-IS para Ipv6. La palabra opcional **transition** permite al usuario de IS-IS Ipv6 continuar con el modo de topología única mientras se actualiza el modo de multitopologia.

4.34 Implementando Multitopologia en IS-IS para Ipv6.

Personalizando IS-IS para Ipv6.

Algunas formas de personalizar IS-IS para Ipv6 son:

- Configurar el mayor número de rutas con igual costo que pueda soportar IS-IS para Ipv6.
- Configurar prefijos sumarizados para IS-IS Ipv6.
- Configurar una instancia IS-IS para anunciar la ruta Ipv6 por defecto (::/0).
- Configurar el periodo de asentamiento entre los cálculos de rutas parciales (PRCs).

Se puede personalizar la multitopologia IS-IS Ipv6 para una red, pero no es necesario hacerlo. Las opciones por defecto para esta característica están establecidas para adaptarse a los requerimientos de muchos clientes y características.

Los siguientes pasos se utilizan para personalizar IS-IS para Ipv6.

1. enable
2. configure terminal
3. router isis *area-name*
4. address-family ipv6 [**unicast** | **multicast**]
5. default-information originate [**route-map** *map-name*]
6. distance *value*
7. maximum-paths *number-paths*
8. summary-prefix *ipv6-prefix*/ *prefix-length* [**level-1** | **level-1-2** | **level-2**]
9. prc-interval *seconds* [*initial-wait*] [*secondary-wait*]
10. spf-interval [**level-1** | **level-2**] *seconds* [*initial-wait*] [*secondary-wait*]
11. exit
12. interface *type number*
13. isis ipv6 metric *metric-value* [**level-1** | **level-2** | **level-1-2**]

A continuación se presentan estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**router isis** area-name **Ejemplo:** Router(config)# router isis area2	Habilita IS-IS para el proceso de enrutamiento específico y entra al modo de configuración del router.
4	**address-family ipv6** [**unicast** | **multicast**] **Ejemplo:**	Especifica la familia de direcciones Ipv6 y entra al modo e configuración de familias de direcciones.

	Router(config-router)# address-family ipv6	La palabra **unicast** especifica la familia de direcciones tipo unicast para Ipv6. El modo unicast es el configurado por defecto.
5	**default-information originate** [**route-map** map-name] **Ejemplo:** Router(config-router-af)# default-information originate	Establece una ruta por defecto Ipv6 dentro de un dominio de enrutamiento IS-IS. La palabra route-map y el argumento map-name especifica las condiciones bajo las cuales la ruta por defecto Ipv6 es anunciada.
6	**distance** value **Ejemplo:** Router(config-router-af)# distance 90	Define la distancia administrativa para las rutas IS-IS en la tabla de enrutamiento Ipv6. El argumento value es un entero de 10 a 254 (los valores de 0 a 9 están reservados para uso interno)
7	**maximum-paths** number-paths **Ejemplo:** Router(config-router-af)# maximum-paths 3	Define el número máximo de rutas de igual costo que IS-IS Ipv6 puede soportar. Este comando también da soporte al protocolo BGP (Border Gateway Protocol) y RIP (Routing Information Protocol). El argumento number-paths es un entero de 1 a 64. Por defecto en BGP es una ruta; y para IS-IS y RIP son 16 rutas.
8	**summary-prefix** ipv6-prefix/ prefix-length [**level-1** | **level-1-2** | **level-2**] **Ejemplo:** Router(config-router-af)# summary-prefix 2001:0DB8::/24	Permite a los routers de Nivel 1-2 sumarizar los prefijos de Nivel 1 al Nivel 2. El argumento *ipv6-prefix* en el comando **summary-prefix** debe ser una dirección formada por valores hexadecimales de 16 bits separados por dos puntos. El argumento *prefix-length* es un valor decimal que indica cuantos de los bits de la parte alta de la dirección forman parte del prefijo. (Porción de red de la dirección).
9	**prc-interval** seconds [initial-wait] [secondary-wait] **Ejemplo:** Router(config-router-af)# prc-	Configura el periodo de asentamiento entre PRCs para la multitopologia IS-IS para Ipv6.

	interval 20	
10	**spf-interval** [**level-1** | **level-2**] seconds [initial-wait] [secondary-wait] **Ejemplo:** Router(config-router-af)# spf-interval 30	Configura la frecuencia con la que el Software Cisco IOS realiza el calculo SPF para una multitopologia IS-IS para Ipv6.
11	**exit** **Ejemplo:** Router(config-router-af)# exit	Sale del modo de configuración de familias de direcciones y regresa al modo de configuración del router.
12	**interface** type number **Ejemplo:** Router(config-router)# interface Ethernet 0/0/1	Especifica el tipo y numero de la interfase y entra al modo de configuración de interfase.
13	**isis ipv6 metric** metric-value [**level-1** | **level-2** | **level-1-2**] **Ejemplo:** Router(config-if)# isis ipv6 metric 20	Configura el valor de la métrica Ipv6 para una multitopologia IS-IS.

Tabla 4.35 Personalizando IS-IS para Ipv6.

Redistribuyendo rutas en un Proceso de Enrutamiento IS-IS Ipv6.

Los siguientes pasos se utilizan para redistribuir rutas Ipv6 entre protocolos.

1. enable

2. configure terminal

3. router isis *area-name*

4. address-family ipv6 [**unicast** | **multicast**]

5. redistribute *protocol* [*process-id*] [**level-1** | **level-1-2** | **level-2**] [**metric** *metric-value*] [**metric-type**

{**internal** | **external**}] [**route-map** *map-name*]

A continuación se presentan estos pasos de forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**show ipv6 ospf** [process-id] [area-id] **interface** [interface-type interface-number] **Ejemplo:** Router# **show ipv6 ospf interface**	Muestra información de una interfase OSPF
3	**router isis** area-name **Ejemplo:** Router(config)# router isis area2	Habilita IS-IS para el proceso de enrutamiento específico y entra al modo de configuración del router.
4	**address-family ipv6** [**unicast** | **multicast**] **Ejemplo:** Router(config-router)# address-family ipv6	Especifica la familia de direcciones Ipv6 y entra al modo e configuración de familias de direcciones. La palabra **unicast** especifica la familia de direcciones tipo unicast para Ipv6. El modo unicast es el configurado por defecto.
5	**redistribute** protocol [process-id] [**level-1** | **level-1-2** | **level-2**] [**metric** metric-value] [**metric-type** {**internal** | **external**}] [**route-map** map-name] **Ejemplo:** Router(config-router-af)# redistribute bgp 64500 metric 100 route-map isismap	Redistribuye rutas de un protocolo especificado dentro de un proceso de enrutamiento IS-IS. El argumento protocolo puede ser : **bgp, connected, isis, rip** o **static.**

Tabla 4.36 Redistribuyendo rutas en un Proceso de Enrutamiento IS-IS Ipv6.

Redistribuyendo rutas IS-IS Ipv6 entre niveles IS-IS.

Los siguientes pasos se utilizan para redistribuir rutas Ipv6 aprendidas en un nivel IS-IS hacia otro nivel.

1. enable

2. configure terminal

3. router isis *area-name*

4. address-family ipv6 [**unicast** | **multicast**]

5. redistribute *protocol* [**level-1** [**into level-2**] | **level-1-2** | **level-2** [**into level-1**]]

A continuación se presentan estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**show ipv6 ospf** [process-id] [area-id] **interface** [interface-type interface-number] **Ejemplo:** Router# **show ipv6 ospf interface**	Muestra información de una interfase OSPF
3	**router isis** area-name **Ejemplo:** Router(config)# router isis area2	Habilita IS-IS para el proceso de enrutamiento específico y entra al modo de configuración del router.
4	**address-family ipv6** [**unicast**	**multicast**] **Ejemplo:** Router(config-router)# address-family ipv6	Especifica la familia de direcciones Ipv6 y entra al modo e configuración de familias de direcciones. La palabra **unicast** especifica la familia de direcciones tipo unicast para Ipv6. El modo unicast es el configurado por defecto.
5	**redistribute** protocol [**level-1** [**into level-2**] | **level-1-2**	**level-2** [**into level-1**]] **Ejemplo:**	Redistribuye rutas Ipv6 de un nivel IS-IS hacia otro nivel. Por defecto, las rutas aprendidas por el nivel 1 son redistribuidas por el nivel 2.

	Router(config-router-af)# redistribute isis level-1 into level-2	

4.37 Redistribuyendo rutas IS-IS Ipv6 entre niveles IS-IS.

Deshabilitando el Chequeo de Consistencia del Protocolo Ipv6.

Para una Topología Única en IS-IS para Ipv6, los routers deben ser configurados para correr el mismo conjunto de familias de direcciones. IS-IS realiza los chequeos de consistencia sobre los paquetes "hello"; pero rechaza los paquetes "hello" que no pertenecen al mismo conjunto de familias de direcciones. Por ejemplo, un router que esta corriendo IS-IS para Ipv4 e Ipv6 no establecerá una adyacencia con un router que este corriendo IS-IS solamente para Ipv4 o para Ipv6. Para permitir que una adyacencia sea establecida sobre routers que tengan diferentes conjuntos de familias de direcciones, se debe deshabilitar el comando **adjacency-check** en la familia de direcciones Ipv6. Este comando esta designado para utilizarse solamente en ocasiones especiales.

Deshabilitar el comando **adjacency-checks** puede causar efectos adversos sobre la configuración de la red. Se debe digitar el comando **no adjacency-checks** solamente cuando se esta corriendo IS-IS Ipv4 en todos los routers y se quiere agregar IS-IS Ipv6 a la red; pero se necesita mantener todas las adyacencias durante la transición. Cuando la configuración de IS-IS Ipv6 es completada se debe remover el comando **no adjacency-checks** de la configuración.
Los siguientes pasos se utilizan para deshabilitar el chequeo de consistencia Ipv6 en IS-IS.

1. enable
2. configure terminal
3. router isis *area-name*
4. address-family ipv6 [**unicast** | **multicast**]
5. no adjacency-check

A continuación se presentan estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**router isis** area-name **Ejemplo:** Router(config)# router isis area2	Habilita IS-IS para un proceso de enrutamiento IS-IS específico y entra al modo de configuración del router.
4	**address-family ipv6** [**unicast** | **multicast**] **Ejemplo:** Router(config-router)# address-family ipv6	Especifica la familia de direcciones Ipv6 y entra al modo e configuración de familias de direcciones. La palabra **unicast** especifica la familia de direcciones tipo unicast para Ipv6. El modo unicast es el configurado por defecto.
5	**no adjacency-check** **Ejemplo:** Router(config-router-af)# no adjacency-check	Deshabilita el chequeo de consistencia de protocolo Ipv6 realizado sobre los paquetes "hello", permitiendo al protocolo Ipv6 ser introducido dentro de una redIpv4 sin afectar las adyacencias existentes. El comando adjacency-check es habilitado por defecto.

Tabla 4.38 Deshabilitando el Chequeo de Consistencia del Protocolo Ipv6.

Deshabilitando los Chequeos de Consistencia de Subred Ipv4.

El software Cisco IOS realiza chequeos sobre los paquetes "hello" para asegurar que la dirección Ipv4 esta presente y tiene una subred consistente con el vecino de donde proviene el paquete. Para deshabilitar este chequeo se debe utilizar el comando **no adjacency-check** en el modo de configuración del router. Sin embargo, si se configura una multitopologia IS-IS, este chequeo se deshabilita por defecto, ya que la multitopologia requiere que los routers formen adyacencias sin importar que los routers sobre la LAN soporten o no un protocolo común.

Los siguientes pasos se utilizan para deshabilitar los chequeos de consistencia de red para Ipv4.

1. enable

2. configure terminal

3. router isis *area-name*

4. no adjacency-check

A continuación se presentan los pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**router isis** area-name **Ejemplo:** Router(config)# router isis area2	Habilita IS-IS para un proceso de enrutamiento IS-IS específico y entra al modo de configuración del router.
4	**no adjacency-check** **Ejemplo:** Router(config-router-af)# no adjacency-check	Deshabilita el chequeo de consistencia de protocolo Ipv6 realizado sobre los paquetes "hello", permitiendo al protocolo Ipv6 ser introducido dentro de una red Ipv4 sin afectar las adyacencias existentes. El comando adjacency-check es habilitado por defecto.

Tabla 4.39 Deshabilitando los Chequeos de Consistencia de Subred Ipv4.

4.4.3.5 Verificando la Configuración y Operación de IS-IS.

Para verificar la configuración de IS-IS se pueden utilizar los siguientes pasos:

1. enable

2. show ipv6 protocols [**summary**]

3. show isis [*area-tag*] [**ipv6** | *] **topology**

4. show clns [*area-tag*] **neighbors** [*interface-type interface-number*] [**area**] [**detail**]

5. show clns *area-name* **is-neighbors** [*type number*] [**detail**]

6. show isis [*area-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**]

7. show isis ipv6 rib [*ipv6-prefix*]

A continuación se muestra los pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**show ipv6 protocols** [**summary**] **Ejemplo:** Router# show ipv6 protocols	Despliega los parámetros y los estados actuales del proceso de enrutamiento Ipv6 activo.
3	**show isis** [area-tag] [**ipv6** | *] **topology** **Ejemplo:** Router# show isis topology	Despliega una lista de todos los routers conectados corriendo IS-IS en todas las áreas.
4	**show clns** [area-tag] **neighbors** [interface-type interface-number] [**area**] [**detail**] **Ejemplo:** Router# show clns neighbors detail	Despliega los vecinos, End System (ES), Intermediate System (IS) y Miltitopologia (M-ISIS)
5	**show clns** area-name **is-neighbors** [type number] [**detail**] **Ejemplo:** Router# show clns is-neighbors detail	Despliega información de adyacencia IS-IS para vecinos IS-IS. Utilice la palabra *detail* para desplegar la dirección de enlace local de los vecinos Ipv6.
6	**show isis** [area-tag] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**] **Ejemplo:** Router# show isis database detail	Despliega la base de datos de estados de enlace. En este ejemplo, el contenido de cada LSP es desplegado utilizando la palabra detail.
7	**show isis ipv6 rib** [ipv6-prefix] **Ejemplo:** Router# show isis ipv6 rib	Muestra la RIB local Ipv6.

Tabla 4.40 Verificando la Configuración y Operación de IS-IS.

- **Salida en Pantalla del Comando Show Ip Protocol.**

En el siguiente ejemplo, muestra información acerca de los parámetros y el estado actual de los procesos de enrutamiento Ipv6 activos utilizando el comando **show ipv6 protocol.**

Router# **show ipv6 protocols**
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "isis"
  Interfaces:
Ethernet0/0/3
Ethernet0/0/1
Serial1/0/1
Loopback1 (Passive)
Loopback2 (Passive)
Loopback3 (Passive)
Loopback4 (Passive)
Loopback5 (Passive)
  Redistribution:
    Redistributing protocol static at level 1
  Address Summarization:
L2: 33::/16 advertised with metric 0
L2: 44::/16 advertised with metric 20
L2: 66::/16 advertised with metric 10
L2: 77::/16 advertised with metric 10

- **Salida de pantalla para el comando Show isis Topology.**

El siguiente ejemplo, muestra información acerca de todos los routers conectados que se encuentran corriendo IS-IS.

Router# **show isis topology**

IS-IS paths to level-1 routers

System Id	Metric	Next-Hop	Interface	SNPA
0000.0000.000C				
0000.0000.000D	20	0000.0000.00AA	Se1/0/1	*HDLC*
0000.0000.000F	10	0000.0000.000F	Et0/0/1	0050.e2e5.d01d
0000.0000.00AA	10	0000.0000.00AA	Se1/0/1	*HDLC*

IS-IS paths to level-2 routers

System Id	Metric	Next-Hop	Interface	SNPA
0000.0000.000A	10	0000.0000.000A	Et0/0/3	0010.f68d.f063
0000.0000.000B	20	0000.0000.000A	Et0/0/3	0010.f68d.f063
0000.0000.000C	--			
0000.0000.000D	30	0000.0000.000A	Et0/0/3	0010.f68d.f063
0000.0000.000E	30	0000.0000.000A	Et0/0/3	0010.f68d.f063

- **Salida del comando Show clns neighbors.**

En el siguiente ejemplo se muestra información de los vecinos End System (Sistema Final) e Intermediate System (Sistema Intermedio), por medio del comando **show clns neighbors**, junto a la palabra **deatil.**

Router# **show clns neighbors detail**

System Id	Interface	SNPA	State	Holdtime	Type	Protocol
0000.0000.0007	Et3/3	aa00.0400.6408	UP	26	L1	IS-IS
Area Address(es): 20						
IP Address(es): 172.16.0.42*						
Uptime: 00:21:49						
0000.0C00.0C35	Et3/2	0000.0c00.0c36	Up	91	L1	IS-IS
Area Address(es): 20						
IP Address(es): 192.168.0.42*						
Uptime: 00:21:52						
0800.2B16.24EA	Et3/3	aa00.0400.2d05	Up	27	L1	M-ISIS

Area Address(es): 20
IP Address(es): 192.168.0.42*
IPv6 Address(es): FE80::2B0:8EFF:FE31:EC57
Uptime: 00:00:27
0800.2B14.060E Et3/2 aa00.0400.9205 Up 8 L1 IS-IS
Area Address(es): 20
IP Address(es): 192.168.0.30*
Uptime: 00:21:52

- **Salida en Pantalla para el comando Show clns is-neighbors.**

El siguiente ejemplo, muestra información para confirmar que el router local ha formado todas las adyacencias IS-IS necesarias con otros vecinos IS-IS, por medio del comando **show clns is-neighbors**. Para mostrar la dirección de enlace local de los vecinos, se debe especificar la palabra **detail**.

Router# **show clns is-neighbors detail**

System Id Interface State Type Priority Circuit Id Format
0000.0000.00AA Se1/0/1 Up L1 0 00 Phase V
Area Address(es): 49.0001
IPv6 Address(es): FE80::YYYY:D37C:C854:5
Uptime: 17:21:38
0000.0000.000F Et0/0/1 Up L1 64 0000.0000.000C.02 Phase V
Area Address(es): 49.0001
IPv6 Address(es): FE80::XXXX:E2FF:FEE5:D01D
Uptime: 17:21:41
0000.0000.000A Et0/0/3 Up L2 64 0000.0000.000C.01 Phase V
Area Address(es): 49.000b
IPv6 Address(es): FE80::ZZZZ:F6FF:FE8D:F063
Uptime: 17:22:06

- **Salida en Pantalla para el comando Show isis database.**

El siguiente ejemplo muestra información acerca de los LSPs recibidos desde otros routers y el prefijo Ipv6 que están anunciando, por medio del comando **show isis database** y utilizando la palabra detail en el comando.

Router# **show isis database detail**

IS-IS Level-1 Link State Database

LSPID	LSP Seq Num	LSP Checksum	LSP Holdtime	ATT/P/OL
0000.0C00.0C35.00-00	0x0000000C	0x5696	325	0/0/0

Area Address: 47.0004.004D.0001

Area Address: 39.0001

Metric: 10 IS 0000.0C00.62E6.03

Metric: 0 ES 0000.0C00.0C35

0000.0C00.40AF.00-00*	0x00000009	0x8452	608	1/0/0

Area Address: 47.0004.004D.0001

Topology: IPv4 (0x0) IPv6 (0x2)

NLPID: 0xCC 0x8E

IP Address: 172.16.21.49

Metric: 10 IS 0800.2B16.24EA.01

Metric: 10 IS 0000.0C00.62E6.03

Metric: 0 ES 0000.0C00.40AF

IPv6 Address: 2001:0DB8::/32

Metric: 10 IPv6 (MT-IPv6) 2001:0DB8::/64

Metric: 5 IS-Extended cisco.03

Metric: 10 IS-Extended cisco1.03

Metric: 10 IS (MT-IPv6) cisco.03

IS-IS Level-2 Link State Database:

LSPID	LSP Seq Num	LSP Checksum	LSP Holdtime	ATT/P/OL
0000.0000.000A.00-00	0x00000059	0x378A	949	0/0/0

Area Address: 49.000b

NLPID: 0x8E

IPv6 Address: 2001:0DB8:1:1:1:1:1:1

Metric: 10 IPv6 2001:2:YYYY::/64

Metric: 10 IPv6 3001:3:YYYY::/64
Metric: 10 IPv6 3001:2:YYYY::/64
Metric: 10 IS-Extended 0000.0000.000A.01
Metric: 10 IS-Extended 0000.0000.000B.00
Metric: 10 IS-Extended 0000.0000.000C.01
Metric: 0 IPv6 11:1:YYYY:1:1:1:1:1/128
Metric: 0 IPv6 11:2:YYYY:1:1:1:1:1/128
Metric: 0 IPv6 11:3:YYYY:1:1:1:1:1/128
Metric: 0 IPv6 11:4:YYYY:1:1:1:1:1/128
Metric: 0 IPv6 11:5:YYYY:1:1:1:1:1/128
0000.0000.000A.01-00 0x00000050 0xB0AF 491 0/0/0
Metric: 0 IS-Extended 0000.0000.000A.00
Metric: 0 IS-Extended 0000.0000.000B.00

- **Salida en pantalla del comando show isis Ipv6 RIB.**

El siguiente ejemplo muestra la salida del comando **show isis ipv6 rib.** El asterisco (*) indica los prefijos que han sido instalados en la RIB Ipv6 como rutas IS-IS. Después de cada prefijo se encuentran una lista de todas las rutas en orden de preferencia, las rutas más óptimas al principio y las menos óptimas al final.

Router# **show isis ipv6 rib**

IS-IS IPv6 process "", local RIB
88:1::/64
via FE80::210:7BFF:FEC2:ACC9/Ethernet2/0, type L2 metric 20 LSP [3/7]
via FE80::210:7BFF:FEC2:ACCC/Ethernet2/1, type L2 metric 20 LSP [3/7]
* 1357:1::/64
via FE80::202:7DFF:FE1A:9471/Ethernet2/1, type L2 metric 10 LSP [4/9]
* 2001:45A::/64
via FE80::210:7BFF:FEC2:ACC9/Ethernet2/0, type L1 metric 20 LSP [C/6]
via FE80::210:7BFF:FEC2:ACCC/Ethernet2/1, type L1 metric 20 LSP [C/6]
via FE80::210:7BFF:FEC2:ACC9/Ethernet2/0, type L2 metric 20 LSP [3/7]
via FE80::210:7BFF:FEC2:ACCC/Ethernet2/1, type L2 metric 20 LSP [3/7]

4.4.3.5 Ejemplos de Configuración para IS-IS Ipv6.

- **Ejemplo de configuración de una Topología Unica IS-IS.**

El siguiente Ejemplo habilita el modo de Topología Única, crea un proceso de enrutamiento IS-IS, define la red, configura una dirección ipv6 sobre la interfase y configura la interfase para correr Ipv6 IS-IS.

```
 ipv6 unicast-routing
!
router isis
  net 49.0001.0000.0000.000c.00
  exit
interface Ethernet0/0/1
  ipv6 address 2001:0DB8::3/64
  ipv6 router isis area2
```

- **Ejemplo para Personalizar IS-IS para Ipv6.**

El siguiente ejemplo anuncia la ruta Ipv6 por defecto (::/0) junto con las otras rutas por medio de actualizaciones enviadas por la interfase Ethernet 0/0/1, este ejemplo también establece una distancia administrativa igual a 90 para IS-IS Ipv6, define el máximo numero de rutas de igual costo que IS-IS Ipv6 puede soportar y configura un prefijo sumarizado de 2001:0DB8::/24 para IS-IS Ipv6.

```
router isis

address-family ipv6
default-information originate
distance 90
maximum-paths 3
summary-prefix 2001:0DB8::/24
exit
```

- **Ejemplo de Predistribución de rutas dentro de un proceso de enrutamiento IS-IS Ipv6.**

En el siguiente ejemplo se redistribuyen rutas BGP Ipv6 dentro de un proceso de enrutamiento de nivel 2 IS-IS para Ipv6.

```
router isis
 address-family ipv6
 redistribute bgp 64500 metric 100 route-map isismap
 exit
```

- **Ejemplo para deshabilitar los chequeos de consistencia del Protocolo Ipv6.**

El siguiente ejemplo deshabilita el comando **adjacency-check** para permitir a un administrador de red configurar IS-IS Ipv6 sobre un router, sin afectar las adyacencias existentes.

```
router isis
address-family ipv6
no adjacency-check
exit
```

- **Ejemplo de Configuración de Multitopologia IS-IS para Ipv6.**

El siguiente ejemplo configura multitopologia IS-IS para Ipv6, después de haber configurado IS-IS para Ipv6.

```
router isis
metric-style wide
address-family ipv6
multi-topology
exit
```

- **Ejemplo de configuración de la métrica de Ipv6 para una Multitopologia.**

```
interface Ethernet 0/0/1
 isis ipv6 metric 20
```

4.5 PROTOCOLOS DE ENRUTAMIENTO EXTERIOR PARA IPV6.

4.5.1 Multiprotocolo BGP para Ipv6.

El Protocolo de Enrutamiento de Borde (BGP) es un Protocolo de Enrutamiento Exterior (EGP) utilizado para conectar dominios de enrutamiento diferentes y que contienen diferentes políticas de enrutamiento (Sistemas Autónomos). Conectar a un proveedor de servicios para acceder a Internet es un uso común del protocolo BGP. BGP puede ser utilizado dentro de un Sistema Autónomo y esta variación se conoce como BGP interno (iBGP). El multiprotocolo BGP es una mejora de BGP que lleva información de enrutamiento para múltiples familias de direcciones del protocolo de capa de red, por ejemplo, la familia de direcciones Ipv6 y rutas multicast Ip. Todos los comandos de BGP y capacidades de políticas de enrutamiento pueden ser utilizadas con el protocolo BGP.

4.5.1.1 Prerrequisitos.

- Estar familiarizado con el Protocolo Ipv6 y con su direccionamiento
- Estar familiarizado con el Protocolo Ipv4 y con su direccionamiento.

Cisco IOS Software da soporte al desarrollo de Ipv6 de acuerdo a la siguiente tabla:

Característica	Mínimo Cisco IOS Requerido
Extensiones del Multiprotocolo BGP para Ipv6.	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3,12.3(2)T
Configurar un proceso de enrutamiento BGP y el ID del router BGP.	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3,12.3(2)T
Configurar un vecino en BGP.	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3,12.3(2)T

Aparejar Dirección de enlace local del Multiprotocolo BGP	12.2(4)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3,12.3(2)T
Configurar un grupo de Vecinos en el Multiprotocolo BGP Ipv6.	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3,12.3(2)T
Anunciando Rutas dentro del Multiprotocolo BGP.	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3,12.3(2)T
Configurar mapas de ruta para los prefijos del Multiprotocolo BGP.	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3,12.3(2)T
Redistribuyendo Prefijos dentro del Multiprotocolo BGP.	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3,12.3(2)T
Soporte para familias de direcciones multicast	12.0(26)S, 12.2(25)S
Multiruta 6PE	12.2(25)S

Tabla 4.41 Cisco IOS con Soporte para BGP

Implementando Multiprotocolo BGP para Ipv6.

Para configurar extensiones sobre el Multiprotocolo BGP, se necesitan entender los siguientes conceptos:

- Extensiones del Multiprotocolo BGP para Ipv6.
- Multiprotocolo BGP para las Familias de Direcciones Multicast Ipv6.

Extensiones del Multiprotocolo BGP para Ipv6.

El Multiprotocolo BGP es el EGP soportado por Ipv6. Las extensiones del Multiprotocolo BGP soportan las mismas características y funcionalidades que el BGP Ipv4. Las mejoras que da Ipv6 al Multiprotocolo BGP incluye el soporte para una familia de direcciones Ipv6, provee información de alcanzabilidad de la capa de red (NLRI) y los atributos que usan las direcciones Ipv6 para el siguiente salto (la siguiente router en la ruta hacia el destino).

Multiprotocolo BGP para las Familias de Direcciones Multicast Ipv6.

Esta característica provee extensiones Multicast BGP para Ipv6 y soporta las mismas características y funcionalidades que BGP para Ipv4.

Multicast BGP es una mejora de BGP que permite el desarrollo de un dominio interno multicast Ipv6. El Multiprotocolo BGP lleva información de ruta de múltiples familias de direcciones del protocolo de capa de red. Los usuarios deben utilizar el Multiprotocolo BGP para multicast Ipv6 cuando se utiliza un multicast Ipv6 con BGP, porque las rutas unicast BGP aprendidas no serán utilizadas por el multicast BGP.

La funcionalidad de multicast BGP es proveída a través de un contexto separado de familias de direcciones. Un identificador subsiguiente de la familia de direcciones (SAFI) provee información acerca de la alcanzabilidad de la capa de red, la cual es llevada en el atributo. El modo Unicast del Multiprotocolo BGP utiliza mensajes SAFI 1 y el Multicast BGP utiliza mensajes SAFI 2.

Los mensajes SAFI 1 indican que las rutas pueden ser utilizadas solamente para Unicast Ip y no para Multicast Ip.

Una tabla de enrutamiento BGP separada, es mantenida para configurar políticas y topologías incongruentes, utilizando la busqueda multicast RPF, que es muy similar al Unicast IP lookup.

4.5.1.2 Implementando Multiprotocolo BGP sobre Ipv6.

Cuando se configure el Multiprotocolo BGP sobre Ipv6, se debe crear primeramente un proceso de enrutamiento BGP, configurar relaciones con vecinos y personalizar BGP para una red en particular.

Configurando un Proceso de Enrutamiento BGP para Ipv6 y un BGP Router ID.

Antes de configurar el router para correr BGP sobre Ipv6, se debe habilitar el enrutamiento Ipv6 globalmente en el router, utilizando el comando **ipv6 unicast-routing** en el modo de configuración global.

BGP utiliza un Router ID (Identificador del router) para identificar a otros vecinos BGP. El Router ID es un valor de 32 bits que frecuentemente es representado por una dirección Ipv4. Por defecto, el software Cisco IOS establece como router ID a la dirección Ipv4 de la interfase loopback del router. Si una interfase loopback no se encuentra configurada en el router, entonces se elige la dirección Ipv4 más alta configurada sobre las interfases del router para representar el Router ID.

Cuando se configura BGP sobre un router que esta habilitado solamente para Ipv6, el router no posee una dirección Ipv4, por lo tanto el Router ID se debe configurar manualmente sobre el router. El Router ID debe ser único para los vecinos BGP del router.

Los siguientes pasos muestran como configurar un proceso de enrutamiento BGP y un Router ID

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **no bgp default ipv4-unicast**
5. **bgp router-id** *ip-address*

A continuación se presentan estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**router bgp** autonomous-system-number **Ejemplo:** Router(config)# router bgp 65000	Configura un Proceso de Enrutamiento BGP y entra al modo de configuración del router de acuerdo al proceso de enrutamiento especificado.
4	**no bgp default ipv4-unicast** **Ejemplo:** Router(config-router)# no bgp default ipv4-unicast	Deshabilita las familias de direcciones Unicast Ipv4 para el proceso de enrutamiento BGP especificado en el paso anterior.
5	**bgp router-id** ip-address **Ejemplo:** Router(config-router)# bgp router-id 172.16.10.1	Configura un router ID de 32 bits como identificador del router local corriendo BGP. Al utilizar el comando **bgp router-id** se resetean todas las sesiones activas con los vecinos.

Tabla 4.42 Implementando BGP para Ipv6.

Configurando un Vecino en BGP para Ipv6.

Por defecto, los vecinos que están definidos utilizando el comando **neighbor remote-as** en el modo de configuración del router, intercambian solamente prefijos de direcciones Ipv4. Para que exista un intercambio de prefijos de direcciones de otros tipos, como los prefijos Ipv6, los vecinos deben activar el comando **neighbor activate** en el modo de configuración de familias de direcciones para los otros tipos de prefijos.

Los siguientes pasos se utilizan para configurar un vecino BGP para Ipv6.

1. enable
2. configure terminal
3. router bgp *autonomous-system-number*
4. neighbor *ipv6-address* **remote-as** *autonomous-system-number*
5. address-family ipv6 [unicast | multicast]
6. neighbor *ipv6-address* **activate**

A continuación se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**router bgp** autonomous-system-number **Ejemplo:** Router(config)# router bgp 65000	Configura un Proceso de Enrutamiento BGP y entra al modo de configuración del router de acuerdo al proceso de enrutamiento especificado.
4	**neighbor** ipv6-address **remote-as** autonomous-system-number **Ejemplo:** Router(config-router)# neighbor 2001:1110::9 remote-as 64450	Agrega la dirección Ipv6 del vecino en el sistema autónomo especificado, a la tabla de vecinos de BGP Ipv6 en el router local.

5	**address-family ipv6** [**unicast** | **multicast**] **Ejemplo:** Router(config-router)# address-family ipv6	Especifica la Familia de Direcciones Ipv6 y entra al modo de configuración de la misma. La palabra Unicast especifica la familia de direcciones unicast Ipv6. Esta opción viene por defecto. La palabra multicast especifica los prefijos de direcciones multicast Ipv6.
6	**neighbor** ipv6-address **activate** **Ejemplo:** Router(config-router-af)# neighbor 2001:1110::9 activate	Habilita el intercambio de prefijos Ipv6 con el vecino.

Tabal 4.43 Configurando un Vecino en BGP para Ipv6.

Configurando un vecino BGP utilizando una dirección de Enlace Local.

Para configurar un vecino BGP utilizando una dirección de enlace local, se requiere que la interfase del vecino sea identificada con el comando **update-source** y que un mapa de ruta sea configurado para establecer un salto siguiente.

Por defecto, los vecinos que están definidos utilizando el comando **neighbor remote-as** en el modo de configuración del router, intercambian solamente prefijos de direcciones Ipv4. Para que exista un intercambio de prefijos de direcciones de otros tipos, como los prefijos Ipv6, los vecinos deben activar el comando **neighbor activate** en el modo de configuración de familias de direcciones para los otros tipos de prefijos.

Por defecto, los mapas de ruta que se crean en la configuración de un router a través del comando **neighbor route-map** son aplicados sobre prefijos de direcciones Ipv4. Los mapas de ruta para otras familias de direcciones deben ser aplicados en el modo de configuración de familia de direcciones utilizando el comando **neighbor route-map** y especificando el tipo de familia de direcciones. Al configurar mapas de ruta separados para cada familia de direcciones, se simplifica la administración y las diferentes políticas para cada familia de direcciones.

Los siguientes pasos se utilizan para configurar un vecino utilizando una dirección de enlace local.

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ipv6-address* **remote-as** *autonomous-system-number*
5. **neighbor** *ipv6-address* **update-source** *interface-type*
6. **address-family ipv6** [**unicast** | **multicast**]
7. **neighbor** *ipv6-address* **activate**
8. **neighbor** *ipv6-address* **route-map** *map-name* {**in** | **out**}
9. **exit**
10. Repeat Step 9.
11. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
12. **match ipv6 address prefix-list** *prefix-list-name*
13. **set ipv6 next-hop** *ipv6-address* [*link-local-address*]

A continuación se presentan estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**router bgp** autonomous-system-number **Ejemplo:** Router(config)# router bgp 65000	Configura un Proceso de Enrutamiento BGP y entra al modo de configuración del router de acuerdo al proceso de enrutamiento especificado.
4	**neighbor** ipv6-address **remote-as** autonomous-system-number **Ejemplo:** Router(config-router)# neighbor 2001:0DB8:0:CC00::1 remote-as 64600	Agrega la dirección Ipv6 del vecino en el sistema autónomo especificado, a la tabla de vecinos de BGP Ipv6 en el router local.

5	**neighbor** ipv6-address **update-source** interface-type interface-number **Ejemplo:** Router(config-router)# neighbor FE80::XXXX:BFF:FE0E:A471 update-source fastethernet0	Especifica la dirección de enlace local con la cual se establecerá el vecino. Si existen múltiples conexiones y no se especifica la interfase del vecino utilizando los argumentos *interface type* e *nterface number* en el comando **neighbor update source.**
6	**address-family ipv6** [**unicast** | **multicast**] **Ejemplo:** Router(config-router)# address-family ipv6	Especifica la Familia de Direcciones Ipv6 y entra al modo de configuración de la misma. La palabra Unicast especifica la familia de direcciones unicast Ipv6. Esta opción viene por defecto. La palabra multicast especifica los prefijos de direcciones multicast Ipv6.
7	**neighbor** ipv6-address **activate** **Ejemplo:** Router(config-router-af)# neighbor 2001:0DB8:0:CC00::1 activate	Habilita el intercambio de prefijos Ipv6 con el vecino.
8	**neighbor** ipv6-address **route-map** map-name {**in** | **out**} **Ejemplo:** Router(config-router-af)# neighbor FE80::XXXX:BFF:FE0E:A471 route-map nh6 out	Aplica a un mapa de ruta, rutas de entrada o de salida.
9	**exit** **Ejemplo:** Router(config-router-af)# exit	Sale del modo de configuración de familias de direcciones y regresa al modo de configuración del router.
10	Repeat Step 9. **Ejemplo:** Router(config-router)# exit	Sale del modo de configuración del router y regresa al modo de configuración global.
11	**route-map** map-name [**permit** | **deny**] [sequence-number] **Ejemplo:** Router(config)# route-map nh6 permit 10	Define un mapa de ruta y entra al modo de configuración de mapa de ruta.

12	**match ipv6 address prefix-list** prefix-list-name **Ejemplo:** Router(config-route-map)# match ipv6 address prefix-list cisco	Distribuye cualquier ruta que tenga una dirección Ipv6 de destino dentro de un rango permitido por una lista de prefijos y crea políticas de enrutamiento en los paquetes.
13	**set ipv6 next-hop** ipv6-address [link-local-address] **Ejemplo:** Router(config-route-map)# set ipv6 next-hop 2001:0DB8::1	Establece la dirección de enlace local del vecino, como siguiente salto. El argumento *ipv6-address* especifica la dirección Ipv6 global del siguiente salto. Este no necesita ser un router adyacente. El argumento *link-locla-address* especifica la dirección Ipv6 de enlace local del siguiente salto. Este necesita ser un router adyacente.

Tabla 4.44 Configurando un Vecino BGP utilizando una dirección de Enlace Local.

Configurando un Grupo de Vecinos BGP.

Por defecto, los vecinos que están definidos utilizando el comando **neighbor remote-as** en el modo de configuración del router, intercambian solamente prefijos de direcciones Ipv4. Para que exista un intercambio de prefijos de direcciones de otros tipos, como los prefijos Ipv6, los vecinos deben activar el comando **neighbor activate** en el modo de configuración de familias de direcciones.

Por defecto, los grupos de vecinos que están definidos en el modo de configuración del router utilizando el comando **neighbor peer-group** intercambian solamente prefijos de direcciones unicast Ipv4. Para intercambiar otros tipos de prefijos de direcciones como los de Ipv6, se deben activar los grupos de vecinos para Ipv6 utilizando el comando **neighbor activate** en el modo de configuración de familias de direcciones.

Los miembros de un grupo de vecinos conocen la configuración de los prefijos de direcciones de los miembros del grupo.

Los vecinos activos Ipv4 no pueden existir en el mismo grupo de vecinos activos para Ipv6. Se deben crear grupos separados de vecinos Ipv4 e ipv6.

Los siguientes pasos se utilizan para configurar un grupo de vecinos BGP.

1. enable

2. configure terminal

3. router bgp *autonomous-system-number*

4. **neighbor** *peer-group-name* **peer-group**
5. **neighbor** *ipv6-address* **remote-as** *autonomous-system-number*
6. **address-family ipv6** [**unicast** | **multicast**]
7. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
8. **neighbor** *ipv6-address* **peer-group** *peer-group-name*
9. **exit**

A continuación se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**router bgp** autonomous-system-number **Ejemplo:** Router(config)# router bgp 65000	Configura un Proceso de Enrutamiento BGP y entra al modo de configuración del router de acuerdo al proceso de enrutamiento especificado.
4	**neighbor** peer-group-name **peer-group** **Ejemplo:** Router(config-router)# neighbor group1 peer-group	Crea un grupo de vecinos BGP
5	**neighbor** ipv6-address **remote-as** autonomous-system-number **Ejemplo:** Router(config-router)# neighbor 2001:0DB8:0:CC00::1 remote-as 64600	Agrega la dirección Ipv6 del vecino en el sistema autónomo especificado, a la tabla de vecinos de BGP Ipv6 en el router local.
6	**address-family ipv6** [**unicast** | **multicast**] **Ejemplo:** Router(config-router)# address-family ipv6	Especifica la Familia de Direcciones Ipv6 y entra al modo de configuración de la misma. La palabra Unicast especifica la familia de direcciones unicast Ipv6. Esta opción viene por defecto. La palabra multicast especifica los prefijos de direcciones multicast Ipv6.

7	**neighbor** { ip-address | peer-group-name | ipv6-address} **activate** **Ejemplo:** Router(config-router-af)# neighbor 2001:0DB8:0:CC00::1 activate	Habilita al vecino y al router local para intercambiar prefijos del tipo de familia especificada. Para permitir pasos de configuración extra para cada vecino utilice el comando **neighbor activate** junto con el argumento *peer-group-name*.
8	**neighbor** ipv6-address **peer-group** peer-group-name **Ejemplo:** Router(config-router-af)# neighbor 2001:0DB8:0:CC00::1 peer-group group1	Asigna la dirección Ipv6 de un vecino BGP a un Grupo de Vecinos
9	**exit** **Ejemplo:** Router(config-router-af)# exit	Sale del modo de configuración de familias de direcciones y regresa al modo de configuración del router.

Tabla 4.45 Configurando un Grupo de Vecinos BGP.

Anunciando Rutas Ipv6 dentro de un protocolo BGP.

Por defecto, las redes que se han definido en el modo de configuración del router usando el comando **network**, se encuentran dentro de una base de datos unicast Ipv4. Para introducir una red en otra base de datos, como una base de datos BGP Ipv6, se debe definir una red con el comando **network** en el modo de configuración de familias de direcciones para la otra base de datos.

Los siguientes pasos se utilizan para anunciar rutas Ipv6 dentro del protocolo BGP.

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv6** [**unicast** | **multicast**]
5. **network** *ipv6-address/ prefix-length*
6. **exit**

A continuación se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**router bgp** autonomous-system-number **Ejemplo:** Router(config)# router bgp 65000	Configura un Proceso de Enrutamiento BGP y entra al modo de configuración del router de acuerdo al proceso de enrutamiento especificado.
4	**address-family ipv6 [unicast | multicast]** **Ejemplo:** Router(config-router)# address-family ipv6	Especifica la Familia de Direcciones Ipv6 y entra al modo de configuración de la misma. La palabra **Unicast** especifica la familia de direcciones unicast Ipv6. Esta opción viene por defecto. La palabra **multicast** especifica los prefijos de direcciones multicast Ipv6.
5	**network** ipv6-address/ prefix-length **Ejemplo:** Router(config-router-af)# network 2001:0DB8::/24	Introduce un prefijo específico dentro de la base de datos BGP Ipv6. Específicamente el prefijo es introducido dentro de la base de datos para la familia de direcciones especificada en el paso anterior
6	**exit** **Ejemplo:** Router(config-router-af)# exit	Sale del modo de configuración de familia de direcciones y regresa al modo de configuración del router.

Tabla 4.46 Anunciando Rutas Ipv6 dentro de un protocolo BGP.

Configurando un Mapa de Ruta para los prefijos BGP Ipv6.

Por defecto, los vecinos que están definidos utilizando el comando **neighbor remote-as** en el modo de configuración del router, intercambian solamente prefijos de direcciones Ipv4. Para que exista un intercambio de prefijos de direcciones de otros tipos, como los prefijos Ipv6, los vecinos deben activar el comando **neighbor activate** en el modo de configuración de familias de direcciones para los otros tipos de prefijos.

Por defecto, los mapas de ruta que se crean en la configuración de un router a través del comando **neighbor route-map** son aplicados sobre prefijos de direcciones Ipv4. Los mapas de ruta para otras familias de direcciones deben ser aplicados en el modo de configuración de familia de direcciones utilizando el comando **neighbor route-map** y especificando el tipo de familia de direcciones. Al configurar mapas de ruta separados para cada familia de direcciones, se simplifica la administración y las diferentes políticas para cada familia de direcciones.
Los siguientes pasos se utilizan para configurar un mapa de ruta para los prefijos BGP Ipv6.

1. enable
2. configure terminal
3. router bgp *autonomous-system-number*
4. **neighbor** *ipv6-address* **remote-as** *autonomous-system-number*
5. address-family ipv6 [unicast | multicast]
6. neighbor *ipv6-address* **activate**
7. neighbor *ipv6-address* **route-map** *map-name* **{in | out}**
8. exit
9. Repeat Step 8.
10. route-map *map-name* **[permit | deny]** [*sequence-number*]
11. match ipv6 address prefix-list *prefix-list-name*

A continuación se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.

2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**router bgp** autonomous-system-number **Ejemplo:** Router(config)# router bgp 65000	Configura un Proceso de Enrutamiento BGP y entra al modo de configuración del router de acuerdo al proceso de enrutamiento especificado.
4	**neighbor** ipv6-address **remote-as** autonomous-system-number **Ejemplo:** Router(config-router)# neighbor 2001:0DB8:0:CC00::1 remote-as 64600	Agrega la dirección Ipv6 del vecino en el sistema autónomo especificado, a la tabla de vecinos de BGP Ipv6 en el router local.
5	**address-family ipv6** [**unicast** | **multicast**] **Ejemplo:** Router(config-router)# address-family ipv6	Especifica la Familia de Direcciones Ipv6 y entra al modo de configuración de la misma. La palabra Unicast especifica la familia de direcciones unicast Ipv6. Esta opción viene por defecto. La palabra multicast especifica los prefijos de direcciones multicast Ipv6.
6	**neighbor** ipv6-address **activate** **Ejemplo:** Router(config-router-af)# neighbor 2001:0DB8:0:CC00::1 activate	Habilita el intercambio de prefijos Ipv6 con el vecino.
7	**neighbor** ipv6-address **route-map** map-name {**in** | **out**} **Example:** Router(config-router-af)#neighbor 2001:0DB8:0:cc00::1 route-map rtp in	Aplica un mapa de ruta para rutas de entrada o de salida. Los cambios en el mapa de ruta no tendrán efecto para los vecinos existentes hasta que se de un reset en los routers. Utilizando el comando **clear bgp ipv6** se realiza un reset por software.
8	**exit** **Ejemplo:** Router(config-router-af)# exit	Sale del modo de configuración de familia de direcciones y regresa al modo de configuración del router.

9	**exit** **Ejemplo:** Router(config-router-af)# exit	Sale del modo de configuración del router y entra al modo de configuración global.
10	**route-map** map-name [**permit** | **deny**] [sequence-number] **Ejemplo:** Router(config)# route-map rtp permit 10	Define un mapa de ruta y entra al modo de configuración de mapa de ruta.
11	**match ipv6 address prefix-list** prefix-list-name **Ejemplo:** Router(config-route-map)# match ipv6 address prefix-list cisco	Distribuye cualquier ruta que tenga una dirección Ipv6 de destino dentro de un rango permitido por una lista de prefijos y crea políticas de enrutamiento en los paquetes.

Tabla 4.47 Configurando un Mapa de Ruta para los prefijos BGP Ipv6.

Redistribuyendo Prefijos dentro de BGP Ipv6.

La redistribución es un proceso que introduce prefijos de un protocolo de enrutamiento dentro de otro protocolo de enrutamiento. Específicamente, los prefijos que se redistribuyen dentro de BGP Ipv6 utilizando el comando **redistribute,** son introducidos dentro de una base de datos unicast Ipv6.

1. enable
2. configure terminal
3. router bgp *autonomous-system-number*
4. address-family ipv6 [**unicast** | **multicast**]
5. redistribute *protocol* [*process-id*] [**level-1** | **level-1-2** | **level-2**] [**metric** *metric-value*] [**metric-type**
{**internal** | **external**}] [**route-map** *map-name*]
6. exit

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**router bgp** autonomous-system-number **Ejemplo:** Router(config)# router bgp 65000	Configura un Proceso de Enrutamiento BGP y entra al modo de configuración del router de acuerdo al proceso de enrutamiento especificado.
4	**address-family ipv6** [**unicast** | **multicast**] **Ejemplo:** Router(config-router)# address-family ipv6	Especifica la Familia de Direcciones Ipv6 y entra al modo de configuración de la misma. La palabra **Unicast** especifica la familia de direcciones unicast Ipv6. Esta opción viene por defecto. La palabra **multicast** especifica los prefijos de direcciones multicast Ipv6.
5	**redistribute** protocol [process-id] [**level-1** | **level-1-2** | **level-2**] [**metric** metric-value] [**metric-type** {**internal** | **external**}] [**route-map** map-name] **Ejemplo:** Router(config-router-af)# redistribute rip	Especifica el protocolo de enrutamiento desde el cual se redistribuirá dentro de BGP Ipv6. El argumento protocol puede ser uno de los siguientes: **bgp, connected, isis, rip** o **static.**
6	**exit** **Ejemplo:** Router(config-router-af)# exit	Sale del modo de configuración de familia de direcciones y regresa al modo de configuración del router.

Tabla 4.48 Redistribuyendo Prefijos dentro de BGP Ipv6.

Anunciando Rutas Ipv4 entre Vecinos BGP Ipv6.

Si una red Ipv6 esta conectando dos redes Ipv4 separadas, es posible utilizar Ipv6 para anunciar las rutas Ipv4. Se debe configurar a los vecinos utilizando direcciones Ipv6 dentro una familia de direcciones Ipv4. Se establece el salto siguiente por medio de una ruta estática o con un mapa de ruta, porque usualmente el salto siguiente anunciado es inalcanzable. Este modelo también se puede utilizar anunciar rutas Ipv6 entre dos vecinos Ipv4.

Los siguientes pasos se utilizan para anunciar rutas Ipv4 entre vecinos BGP Ipv6.

1. enable

2. configure terminal

3. router bgp *autonomous-system-number*

4. neighbor *peer-group-name* **peer-group**

5. neighbor *peer-group-name* **remote-as** *autonomous-system-number*

6. address-family ipv4

7. neighbor *ipv6-address* **peer-group** *peer-group-name*

8. neighbor *peer-group-name* **route-map** *map-name* {**in** | **out**}

9. exit

10. Repeat Step 11.

11. route-map *map-name* [**permit** | **deny**] [*sequence-number*]

12. set ip next-hop *ipv4-address* [**peer-address**]

A continuación se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**router bgp** autonomous-system-number **Ejemplo:** Router(config)# router bgp 65000	Configura un Proceso de Enrutamiento BGP y entra al modo de configuración del router de acuerdo al proceso de enrutamiento especificado.

4	**neighbor** peer-group-name **peer-group** **Ejemplo:** Router(config-router)# neighbor 6peers peer-group	Crea un grupo de vecinos BGP
5	**neighbor** peer-group-name **remote-as** autonomous-system-number **Ejemplo:** Router(config-router)# neighbor 6peers remote-as 65002	Agrega la dirección Ipv6 del vecino en el sistema autónomo especificado, a la tabla de vecinos de BGP Ipv6 en el router local.
6	**address-family ipv4** **Ejemplo:** Router(config-router)# address-family ipv4	Especifica la Familia de Direcciones Ipv4 y entra al modo de configuración de la misma.
7	**neighbor** ipv6-address **peer-group** peer-group-name **Ejemplo:** Router(config-router-af)# neighbor 2000:yyyy::2 peer-group 6peers	Asigna las direcciones Ipv6 de un vecino BGP a un grupo de vecinos (peer-group).
8	**neighbor** peer-group-name **route-map** map-name {**in** | **out**} **Ejemplo:** Router(config-router-af)# neighbor 6peers route-map rmap out	Aplica un mapa de ruta para rutas de entrada o de salida.
9	**exit** **Ejemplo:** Router(config-router-af)# exit	Sale del modo de configuración de familias de direcciones y regresa al modo de configuración del router.
10	Repetir paso 9. **Ejemplo:** Router(config-router)# exit	Sale del modo de configuración del router y entra al modo de configuración global.
11	**route-map** map-name [**permit** | **deny**]	Define u n mapa de ruta y entra al modo de configuración de mapa de

	[sequence-number] **Ejemplo:** Router(config)# route-map rmap permit 10	ruta.
12	**set ip next-hop** ipv4-address [**peer-address**] **Ejemplo:** Router(config-route-map)# set ip next-hop 10.21.8.10	Establece la dirección del vecino del siguiente salto.

4.49 Anunciando Rutas Ipv4 entre Vecinos BGP Ipv6.

Asignando una Distancia Administrativa BGP.

Los siguientes pasos muestran como especificar una distancia administrativa para rutas BGP Multicast.

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address family ipv6** [**unicast** | **multicast**}
5. **distance bgp** *external-distance internal-distance local-dista*

A continuación se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**router bgp** autonomous-system-number **Ejemplo:** Router(config)# router bgp 100	Configura un Proceso de Enrutamiento BGP y entra al modo de configuración del router de acuerdo al proceso de enrutamiento especificado.

4	**address-family ipv6** [**unicast** | **multicast**] **Ejemplo:** Router(config-router)# address-family ipv6 multicast	Especifica la Familia de Direcciones Ipv6 y entra al modo de configuración de la misma. La palabra Unicast especifica la familia de direcciones unicast Ipv6. Esta opción viene por defecto. La palabra multicast especifica los prefijos de direcciones multicast Ipv6.
5	**distance bgp** external-distance internal-distance local-distance **Ejemplo:** Router(config-router)# distance bgp 20 20 200	Asigna una distancia administrativa BGP

Tabla 4.50 Asignando una Distancia Administrativa BGP.

Reiniciando Sesiones BGP.

Los siguientes pasos se utilizan para reiniciar sesiones BGP.

1. enable

2. clear bgp ipv6 {**unicast** | **multicast**} {* | *autonomous-system-number* / *ip-address* | *ipv6-address* | *peer-group-name*} [**soft**] [**in** | **out**]

A continuación se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**clear bgp ipv6** {**unicast** | **multicast**} {* | autonomous-system-number | ip-address | ipv6-address | peer-group-name} [**soft**] [**in** | **out**] **Ejemplo:** Router# clear bgp ipv6 unicast peer-group marketing soft out	Reinicia las sesiones BGP.

Tabla 4.51 Reiniciando Sesiones BGP.

Eliminar Vecinos BGP Externos.

Los siguientes pasos se utilizan para eliminar vecinos BGP externos y miembros de un grupo de vecinos BGP Ipv6.

1. enable
2. clear bgp ipv6 {**unicast** | **multicast**} **external** [**soft**] [**in** | **out**]
3. clear bgp ipv6 {**unicast** | **multicast**} **peer-group** [*name*]

A continuación se muestran estos pasos de forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**clear bgp ipv6** {**unicast** | **multicast**} **external** [**soft**] [**in** | **out**] **Example:** Router# clear bgp ipv6 unicast external soft in	Elimina las relaciones con los vecinos BGP Ipv6 externos.
3	**clear bgp ipv6** {**unicast** | **multicast**} **peer-group** [name] **Example:** Router# clear bgp ipv6 unicast peer-group	Elimina todos los miembros de un grupo de vecinos BGP Ipv6.

Tabla 4.52 Eliminar Vecinos BGP Externos.

4.5.1.3 Ejemplos de Configuración BGP.

- **Configuración de Vecinos BGP.**

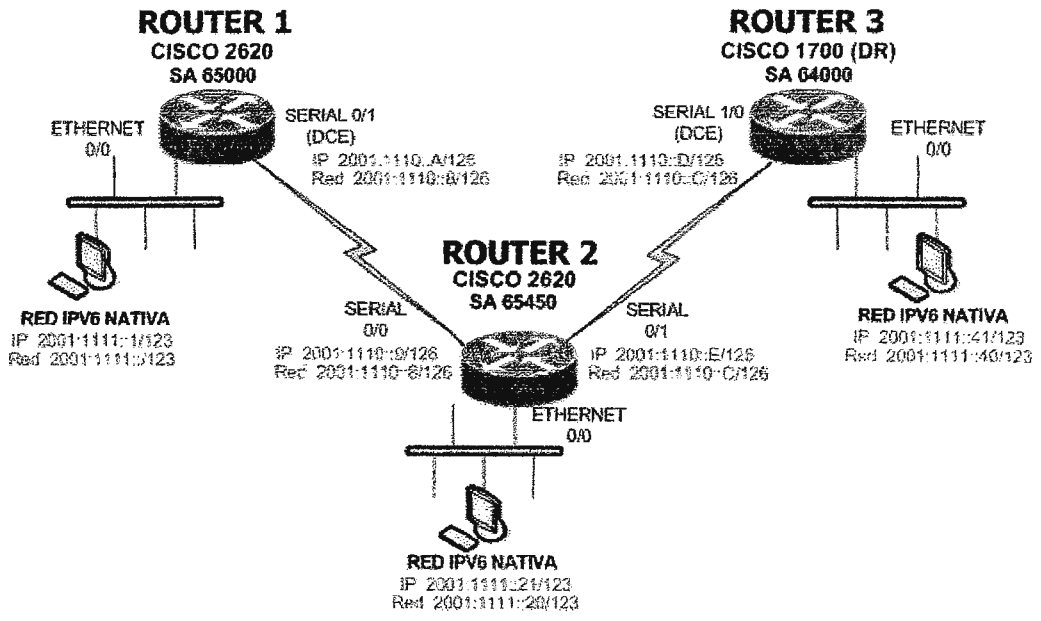


Figura 4.11 . Esquema para la Configuración de BGP en Ipv6.

El diagrama anterior muestra una Red Nativa Ipv6 compuesta por tres enrutadores, los cuales se encuentran conectados a través de sus seriales, cada una de ellas configurada con una dirección Ipv6 así:

- Router 1: Interfase Serial 0/1, con dirección Ipv6 2001:1110::A/126.
- Router 2: Interfase Serial 0/0, con dirección Ipv6 2001:1110::9/126 e Interfase Serial 0/1, con dirección Ipv6 2001:1110::E/126.
- Router 3: Interfase Serial 1/0, con dirección Ipv6 2001:1110::D/126.

Cada nodo posee una Red de Área Local (LAN), identificada por intereses FastEthernet, cada una configurada con una dirección Ipv6 perteneciente a una red especifica. Así:

- Router 1: Interfase FastEthernet 0/0, con direccion Ipv6 2001:1111::1/123.
- Router 2: Interfase FastEthernet 0/0, con direccion Ipv6 2001:1111::21/123.
- Router 3: Interfase FastEthernet 0/0, con direccion Ipv6 2001:1111::41/123.

Cada enrutador posee un Numero de Sistema Autónomo (ASN) distinto el cual identifica a la red de cada nodo independiente, el cual puede ser un numero de 1 a 65535. Los ASNs para los enrutadores en este ejemplo son:

- Router1: 65000
- Router2: 65450
- Router3: 64000

Para configurar vecinos BGP se debe crear primeramente un sistema autónomo para cada enrutador en el modo de configuración global del router, dentro de la configuración del sistema autónomo se debe especificar un identificador al router y el vecino con el cual se quiere establecer una relación, especificando la dirección ipv6 del mismo y el numero de su sistema autónomo.
Posteriormente se habilita la familia de direcciones ipv6 con el comando **address-family ipv6,** entonces se activa la conexión con el vecino y especificamos el prefijo que deseamos compartir.
A continuación se muestra la configuración de BGP para cada enrutador.

Router1(config)#

```
interface Serial0/1
 description conexion a router2
 no ip address
 ipv6 address 2000:1110::A/126
 ipv6 address 2001:1110::A/126
 clockrate 1000000

router bgp 65000
 bgp router-id 172.16.10.1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 2001:1110::9 remote-as 65450

 address-family ipv6
 neighbor 2001:1110::9 activate
 neighbor 2001:1110::9 soft-reconfiguration inbound
 network 2001:1111::/123
 exit-address-family
```

```
Router2(config)#

interface Serial0/0
 description conexion con Router1
 no ip address
 ipv6 address 2001:1110::9/126

interface Serial0/1
 description conexion con Router1
 no ip address
 ipv6 address 2001:1110::E/126

router bgp 65450
 bgp router-id 172.16.10.2
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 2001:1110::A remote-as 65000
 neighbor 2001:1110::D remote-as 64000

 address-family ipv6
 neighbor 2001:1110::A activate
 neighbor 2001:1110::D activate
 network 2001:3333::/123
 exit-address-family

interface Loopback10
 no ip address
 ipv6 address 2001:3333::1/123

Router3(config)#

interface Loopback10
 no ip address
 ipv6 address 2001:4444::1/123
```

```
router bgp 64000
 no synchronization
 bgp router-id 172.16.10.3
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 2001:1110::E remote-as 65450
 no auto-summary

 address-family ipv6
 neighbor 2001:1110::E activate
 network 2001:4444::/123
 exit-address-family
```

- **Ejemplo de configuración de un vecino BGP utilizando una dirección de enlace local.**

El siguiente ejemplo configura a un vecino BGP con la dirección FE80::XXXX:BFF:FE0E:A471 sobre la Interfase Fast Ethernet 0 y establece el mapa de ruta llamado nh6 para incluir la dirección global de salto siguiente de la interfase Fast Ethernet 0 en las actualizaciones de BGP. La dirección de enlace local del salto siguiente puede ser establecida por el mapa de ruta nh6 o desde la interfase especificada con el comando **neighbor update-source**.

```
router bgp 65000
  neighbor FE80::XXXX:BFF:FE0E:A471 remote-as 64600
  neighbor FE80::XXXX:BFF:FE0E:A471 update-source fastethernet 0

address-family ipv6
  neighbor FE80::XXXX:BFF:FE0E:A471 activate
  neighbor FE80::XXXX:BFF:FE0E:A471 route-map nh6 out

route-map nh6 permit 10
  match ipv6 address prefix-list cisco
  set ipv6 next-hop 2001:5y6::1

ipv6 prefix-list cisco permit 2Fy2::/48 le 128
```

ipv6 prefix-list cisco deny ::/0

- **Ejemplo de Configuración de un grupo de vecinos BGP.**

En el siguiente ejemplo se configura un grupo de vecinos con el nombre "group1".

```
router bgp 65000
no bgp default ipv4-unicast
neighbor group1 peer-group
neighbor 2001:0DB8:0:CC00::1 remote-as 64600

address-family ipv6 unicast
  neighbor group1 activate
  neighbor 2001:0DB8:0:CC00::1 peer-group group1
```

- **Ejemplo de Anunciación de rutas dentro del protocolo BGP.**

El siguiente ejemplo introduce la red 2001:0DB8::/24 dentro de la base de datos unicast Ipv6 del router local.

```
router bgp 65000

  no bgp default ipv4-unicast
address-family ipv6 unicast
  network 2001:0DB8::/24
```

- **Ejemplo de configuración de un mapa de ruta para prefijos BGP.**

El siguiente ejemplo configura el mapa de ruta llamado rtp para permitir rutas unicast Ipv6 desde la red 2001:0DB8::/4, si estas se encuentran en las listas de prefijo llamada cisco.

```
router bgp 64900
no bgp default ipv4-unicast
neighbor 2001:0DB8:0:CC00::1 remote-as 64700
```

```
address-family ipv6 unicast
  neighbor 2001:0DB8:0:CC00::1 activate
  neighbor 2001:0DB8:0:CC00::1 route-map rtp in

ipv6 prefix-list cisco seq 10 permit 2001:0DB8::/24

route-map rtp permit 10
  match ipv6 address prefix-list cisco
```

- **Ejemplo de Rredistribución de Prefijos dentro de BGP.**

El siguiente ejemplo redistribuye rutas RIP dentro de una base de datos Ipv6 del router local.

```
router bgp 64900
no bgp default ipv4-unicast
address-family ipv6 unicast
  redistribute rip
```

- **Ejemplo de Anunciación de rutas Ipv4 entre vecinos Ipv6.**

El siguiente ejemplo, anuncia rutas Ipv4 entre vecinos Ipv6, cuando la red Ipv6 esta conectando dos redes Ipv4 por separado. La relación entre vecinos es configurada utilizando direcciones Ipv6 dentro del modo de configuración de familia de direcciones Ipv4. El mapa de ruta llamado rmap establece el salto siguiente.

```
router bgp 65000
!
neighbor 6peers peer-group
neighbor 2000:yyyy::2 remote-as 65002
address-family ipv4
neighbor 6peers activate
neighbor 6peers soft-reconfiguration inbound
neighbor 2000:yyyy::2 peer-group 6peers
```

```
neighbor 2000:yyyy::2 route-map rmap in
!
route-map rmap permit 10
  set ip next-hop 10.21.8.10
```

4.5.1.4 Verificando la Configuración de BGP.

Los siguientes pasos se utilizan para mostrar información sobre la configuración del Protocolo BGP.

1. show bgp neighbor

2. show bgp ipv6 summary

3. show ipv6 route bgp

4. debug bgp ipv6 {**unicast** | **multicast**} **dampening** [*access-list-name*] [**prefix-list** *prefix-list-name*]

5. debug bgp ipv6 {**unicast** | **multicast**} **updates** [*ipv6-address*] [**prefix-list** *prefix-list-name*] [**in** |**out**]

A continuación se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**show bgp neighbors** **Ejemplo:** Router> show bgp neighbors	Muestra los vecinos configurados desde un nodo BGP.
2	**show bgp ipv6 summary** **Ejemplo:** Router> show bgp ipv6 summary	Muestra un resumen de las conexiones BGP existentes y caracteristicas como el nuemro de sistema autono, el router ID, etc.
3	**show ipv6 route bgp** **Ejemplo:** Router> show ipv6 route bgp	Muestra las rutas BGP aprendidas dentro de la tabla de enrutamiento.
4	**debug bgp ipv6** {**unicast** | **multicast**} **dampening** [access-list-name] [**prefix-list** prefix-list-name] **Ejemplo:** Router# debug bgp ipv6 unicast dampening	Muestra mensajes de depuración para paquetes "dampening" BGP Ipv6.

5	**debug bgp ipv6** {**unicast** | **multicast**} **updates** [ipv6-address] [**prefix-list** prefix-list-name] [**in** | **out**] **Ejemplo:** Router# debug bgp ipv6 unicast updates	Muestra información de depuración de los paquetes de actualización para BGP. Si se especifica el argumento *ipv6-address*, se muestran los mensajes de depuración para las actualizaciones BGP para el vecino especificado. Se utiliza el argumento **in** para mostrar actualizaciones en banda, y el argumento **out** para mostrar actualizaciones fuera de banda.

Tabla 4.53 Verificando la Configuración de BGP.

- **Salida en Pantalla para el comando Show bgp Neighbors.**

Router1#**sh bgp neighbors**

BGP neighbor is 2001:1110::9, remote AS 65450, external link

BGP version 4, remote router ID 172.16.10.2

BGP state = Established, up for 09:34:24

Last read 00:00:24, hold time is 180, keepalive interval is 60 seconds

Neighbor capabilities:

Route refresh: advertised and received(old & new)

Address family IPv6 Unicast: advertised and received

Message statistics:

InQ depth is 0

OutQ depth is 0

	Sent	Rcvd
Opens:	4	4
Notifications:	0	0
Updates:	7	2
Keepalives:	1588	1588
Route Refresh:	1	0
Total:	1600	1594

Default minimum time between advertisement runs is 30 seconds

- **Salida en Pantalla para el commando Show bgp ipv6 Neighbors.**

Router2#**sh bgp ipv6 summary**
BGP router identifier 172.16.10.2, local AS number 65450
BGP table version is 21, main routing table version 21
2 network entries using 266 bytes of memory
2 path entries using 144 bytes of memory
2 BGP path attribute entries using 120 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 554 total bytes of memory
BGP activity 9/7 prefixes, 11/9 paths, scan interval 60 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
2001:1110::A	4	65000	5513	5509	0	0	0	11:33:54	Active
2001:1110::D	4	64000	1666	1668	21	0	0	1d03h	1

- **Salida en Pantalla del comando Show ipv6 route ospf.**

Router1#**sh ipv6 route bgp**
IPv6 Routing Table - 15 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B 2001:3333::/123 [20/0]
via FE80::212:80FF:FE51:6F60, Serial0/1

- **Salida en Pantalla del Comando Debug BGP Ipv6 Dampening.**

Router# **debug bgp ipv6 unicast dampening**
00:13:28:BGP(1):charge penalty for 2000:y:0:1::/64 path 2 1 with halflife-time 15
reuse/suppress 750/2000

00:13:28:BGP(1):flapped 1 times since 00:00:00. New penalty is 1000
00:13:28:BGP(1):charge penalty for 2000:y:0:1:1::/80 path 2 1 with halflife-time 15
reuse/suppress 750/2000
00:13:28:BGP(1):flapped 1 times since 00:00:00. New penalty is 1000
00:13:28:BGP(1):charge penalty for 2000:y:0:5::/64 path 2 1 with halflife-time 15
reuse/suppress 750/2000
00:13:28:BGP(1):flapped 1 times since 00:00:00. New penalty is 1000
00:16:03:BGP(1):charge penalty for 2000:y:0:1::/64 path 2 1 with halflife-time 15
reuse/suppress 750/2000
00:16:03:BGP(1):flapped 2 times since 00:02:35. New penalty is 1892
00:18:28:BGP(1):suppress 2000:y:0:1:1::/80 path 2 1 for 00:27:30 (penalty 2671)
00:18:28:halflife-time 15, reuse/suppress 750/2000
00:18:28:BGP(1):suppress 2000:y:0:1::/64 path 2 1 for 00:27:20 (penalty 2664)
00:18:28:halflife-time 15, reuse/suppress 750/2000

- **Salida en Pantalla del Comando Debug BGP Ipv6 Updates.**

En el siguiente ejemplo, se muestran los mensajes de depuración de los paquetes de actualización BGP por medio del comando **debug bgp ipv6 unicast updates.**

Router# **debug bgp ipv6 unicast updates**

14:04:17:BGP(1):2000:y:0:2::2 computing updates, afi 1, neighbor version 0, table version
1, starting at ::
14:04:17:BGP(1):2000:y:0:2::2 update run completed, afi 1, ran for 0ms, neighbor version
0, start version 1, throttled to 1
14:04:19:BGP(1):sourced route for 2000:0:0:2::1/64 path #0 changed (weight 32768)
14:04:19:BGP(1):2000:y:0:2::1/64 route sourced locally
14:04:19:BGP(1):2000:y:0:2:1::/80 route sourced locally
14:04:19:BGP(1):2000:y:0:3::2/64 route sourced locally
14:04:19:BGP(1):2000:y:0:4::2/64 route sourced locally
14:04:22:BGP(1):2000:y:0:2::2 computing updates, afi 1, neighbor version 1, table version
6, starting at ::
14:04:22:BGP(1):2000:y:0:2::2 send UPDATE (format) 2000:0:0:2::1/64, next 2000:0:0:2::1,

metric 0, path
14:04:22:BGP(1):2
14:04:22:BGP(1):2000:y:0:2::2 send UPDATE (prepend, chgflags:0x208) 2000:0:0:3::2/64, next 2000:0:0:2::1, metric 0, path
14:04:22:BGP(1):2000:y:0:2::2 send UPDATE (prepend, chgflags:0x208) 2000:0:0:4::2/64, next 2000:0:0:2::1, metric 0, path

4.6 ADMINISTRACION DE APLICACIONES DEL IOS SOBRE IPV6.

4.6.1 Prerrequisitos.

- Estar familiarizado con el protocolo Ipv4.

- El enrutamiento Ipv6 esta deshabilitado por defecto en el Software Cisco IOS. Para habilitar el enrutamiento Ipv6 se debe habilitar primeramente el reenvío de trafico Ipv6 globalmente en el router y entonces se deben anunciar direcciones Ipv6 a interfases individuales en el router.

- Para habilitar el acceso telnet en el router se debe crear una interfase vty en el router y una contraseña.

- Para la administración de Aplicaciones como: Acceso Telnet, Descarga de archivos TFTP, Ping, Traceroute, SSH sobre un transporte Ipv6 y SNMP sobre transporte Ipv6; se debe utilizar un Cisco IOS Software que soporte estas características.

Característica	Mínimo Cisco IOS Requerido
Acceso Telnet Sobre Ipv6	12.0(21)ST, 12.0(22)S, 12.2(2)T, 12.2(14)S
Descarga de Archivos TFTP, Ping, Traceroute, para Ipv6.	12.0(21)ST, 12.0(22)S, 12.2(2)T, 12.2(14)S
SSH sobre un transporte Ipv6	12.0(22)S, 12.2(8)T, 12.2(14)S, 12.3(1)
SNMP sobre un Transporte Ipv6	12.0(27)S

Tabla 4.54 Administracion de Aplicaciones sobre Ipv6.

Accesso Telnet sobre Ipv6.

El cliente y servidor Telnet el software Cisco IOS proporciona soporte a las conexiones Ipv6. Un usuario puede establecer fácilmente una sesión Telnet con el Router utilizando un cliente Telnet Ipv6 o una conexión Telnet puede ser iniciada desde un router. Para habilitar el acceso Telnet se debe configurar previamente una interfase vty y una contraseña en el router Ipv6.

Descarga de Archivos TFTP, Ping y Traceroute para Ipv6.

Ipv6 soporta la descarga y la carga de archivos TFTP utilizando el comando copy. Este comando acepta una dirección destino Ipv6 o un nombre de host como argumento, y guarda la configuración del router sobre un servidor TFTP, así como se muestra a continuación:

Router#copy running-config ftp://[3ffe:xxxx:c18:1:290:27ff:fe3a:9e9a]/running-config

El comando ping acepta una dirección Ipv6 destino o un nombre de host como argumento y envía mensajes de solicitud de respuesta a través del protocolo ICMPv6 (Internet Control Message Protocol version 6). Los mensajes de solicitud de respuesta son reportados sobre la consola. La funcionalidad de ping extendido también es soportada sobre Ipv6.

El comando traceroute acepta una dirección Ipv6 destino o un nombre de host como argumento y genera trafico Ipv6 para reportar cada salto Ipv6 utilizado para alcanzar la dirección destino.

SSH sobre transporte Ipv6.

En el software Cisco IOS Release 12.2(8)T o superiores en esta serie, o la serie 12.0(22)S o superiores, SSH en Ipv6 funciona de la misma forma en que funciona con SSH para Ipv4. Un servidor SSH habilita a un cliente SSH para hacer una conexión segura y encriptada con otro router o cualquier dispositivo

que este corriendo un servidor SSH. La mejoría que presenta Ipv6 para SSH es el soporte para direcciones Ipv6 que habilita un router para aceptar y establecer una conexión segura y encriptada hacia un nodo remoto Ipv6 sobre un transporte Ipv6.

SSH sobre un transporte Ipv6 no tareas de configuración especificas. El comando **ssh** puede ser utilizado para iniciar una sesión encriptada con un dispositivo de red Ipv4 o Ipv6. Después de haber habilitado el servidor SSH utilizando el comando de configuración global **ip ssh**, las conexiones Ipv4 e ipv6 pueden ser realizadas hacia el router local.

SNMP sobre transporte Ipv6.

El Protocolo de Administración de Redes (SNMP) puede ser configurado sobre transporte Ipv6, de modo que un nodo Ipv6 puede realizar consultas SNMP y recibir notificaciones SNMP desde un dispositivo que posea un IOS Ipv6. La información que maneja SNMP es transportada en módulos llamados MIB's (Base de Información de Administración), los cuales poseen información de objetos administrados.

Los siguientes MIB's son soportados por Ipv6:

- CISCO-DATA-COLLECTION-MIB
- ENTITY-MIB
- NOTIFICTAION-LOG-MIB
- SNMP-TARGET-MI

4.6.2 Administrando Aplicaciones del IOS sobre Ipv6.

Habilitando y Estableciendo una Sesión Telnet.

Utilizando cualquier tipo de transporte, ya sea Ipv4 o Ipv6, se puede utilizar Telnet para conectar desde un Host a un Router, desde un Router a un Rouer y desde un Router a un Host.

Los siguientes pasos se utilizan para habilitar y establecer una sesión Telnet.

1. enable
2. configure terminal
3. ipv6 host *name* [*port*] *ipv6-address1* [*ipv6-address2...ipv6-address4*]
4. line [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
5. password *password*
6. login [**local** | **tacacs**]
7. telnet host [*port*] [*keyword*]

A continuación se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.

2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**ipv6 host** name [port] ipv6-address1 [ipv6-address2...ipv6-address4] **Ejemplo:** Router(config)# **ipv6 host Router1 2001:1111::1**	Define un nombre de host a una dirección Ipv6 específica.
4	**line** [**aux** | **console** | **tty** | **vty**] line-number [ending-line-number] **Ejemplo:** Router(config)# **line vty 0 4**	Configura una interface vty.
5	**password** password **Ejemplo:** Router(config)# **password hostword**	Crea una contraseña para habilitar el Telnet.
6	**login** [**local** | **tacacs**] **Ejemplo:** Router(config)# **login**	Habilita el chequeo de contraseña al usuario.
7	**telnet** host [port] [keyword] **Ejemplo:** Router(config)# **telnet Router1** o Router(config)# **telnet 2001:1111::1**	Establece una sesión telnet de un router hacia un host remoto utilizando el nombre de host o la dirección del mismo.

4.55 Habilitando y Estableciendo una Sesión Telnet.

Habilitando SSH sobre un Router Ipv6.

Antes de configurar SSH sobre transporte Ipv6, se debe asegurar que existan las siguientes condiciones.

- El transporte Ipv6 para un servidor SSH y un cliente SSH requiere una imagen del sistema operativo (IOS) que soporte la encriptación Ipsec, por ejemplo, el IOS Release 12.2(8)T,

- Un nombre de host debe ser configurado para el router.

- Una clave criptográfica RSA, la cual habilita automáticamente SSH, es configurada en el Router. La clave RSA viene en parejas: Una clave pública y una privada.

- Un mecanismo de autenticación de usuario para acceso local o remoto, es configurado en el router.

Como restricción se podría mencionar que el único mecanismo de autenticación soportado por SSH sobre un transporte Ipv6, es el uso de nombres de usuario y contraseñas locales. Los mecanismos de autenticación como TACACS+ y RADIUS no son soportados sobre un transporte Ipv6.
Los siguientes pasos se utilizan para habilitar SSH sobre transporte Ipv6.

1. enable

2. configure terminal

3. ip ssh {[**timeout** *seconds*] | [**authentication-retries** *integer*]}

4. exit

5. ssh

A continuación se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**ip ssh {[timeout** seconds] | [**authentication-retries** integer]} **Ejemplo:** Router(config)# **ip ssh timeout 100** **authentication-retries 2**	Configura variables de control SSH sobre el router. • Se puede establecer el tiempo de espera en segundos, no debe exceder 120 segundos. Por defecto son 120 segundos. Esta característica aplica solamente para la fase de negociación SSH. Una vez la sesión inicia se aplican los estándares de tiempo configurados en la línea vty. Por defecto se definen cisco líneas vty (0-4); por lo tanto se pueden realizar cinco sesiones de Terminal. El tiempo de espera de la línea vty por defecto son 10 minutos.

		• Se puede especificar también el número de intentos de autenticación para que no excedan en cinco intentos. Por defecto se permiten tres intentos.
4	**exit** **Ejemplo:** Router(config)# **exit**	Sale del modo de configuración y regresa al modo privilegiado.
5	**ssh** **Ejemplo:** Router# **ssh**	Inicia una sesión encriptada con un dispositivo de red remoto.

4.56 Habilitando SSH sobre un Router Ipv6.

Deshabilitando el Acceso HTTP a un Router Ipv6.

El acceso HTTP sobre Ipv6 es habilitado automáticamente si un servidor HTTP es habilitado y el router posee una dirección Ipv6.

Los siguientes pasos se utilizan para deshabilitar el acceso http a un router Ipv6.

1. enable

2. configure terminal

3. no ip http server

A continuación se presentan estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**no ip http server** **Ejemplo:** Router(config)# **no ip http server**	Deshabilita el acceso HTTP

4.57 Deshabilitando el Acceso HTTP a un Router Ipv6.

Configurando un Servidor de Notificación SNMP.

Se debe utilizar la el comando **SNMP community string** (clave de comunidad) para definir la relación entre el administrador y el agente SNMP. La clave de comunidad actúa como una contraseña para regular el acceso al agente sobre el router. Opcionalmente se pueden especificar una o más de las siguientes características asociadas con la comunidad.

- Una lista de acceso de las direcciones Ip de los administradores SNMP que son permitidos para utilizar la clave de comunidad para obtener acceso al agente.

- Una vista del MIB, la cual define un subconjunto de todos los objetos MIB accesibles de la comunidad dada.

- Permisos de Lectura/Escritura o solamente de Lectura para los objetos MIB accesibles a la comunidad.

Se pueden configurar una o mas claves de comunidad. Para remover una comunidad específica se debe utilizar el comando **no snmp-server community.**

El comando **snmp-server host** especifica cual de los host recibirá notificaciones SNMP, y si se quieren enviar las notificaciones como traps (información) o solicitud de informe.

El comando **snmp-server enable traps** habilita globalmente los mecanismos de producción para los tipos de notificación específicos como: BGP traps, config traps, entity traps y Hot Standby Router Protocol (HSRP) traps.
Los siguientes pasos se utilizan para configurar un servidor de notificación SNMP.

1. **enable**
2. **configure terminal**
3. **snmp-server community string** [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number*]
4. **snmp-server engineID remote** {*ipv4-ip-address* / *ipv6 address*}[**udp-port** *udp-port-number*] [**vrf***vrf-name*] *engineid-string*

5. **snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *read-view*][**write** *write-view*] [**notify** *notify-view*] [**context** *context-name*] [**access** [**ipv6** *named-access-list*]{*acl-number* | *acl-name*}]
6. **snmp-server host** {*hostname* | *ip-address*} [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] [**vrf** *vrf-name*]
7. **snmp-server user** *username group-name* [**remote** *host* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] {*acl-number* | *acl-name*}]
8. **snmp-server enable traps** [*notification-type* [*notification-options*]]

A continuación se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	Router(config)# **snmp-server community** string [**view** view-name] [**ro**	**rw**] [**ipv6** nacl] [access-list-number] **Ejemplo:** Router(config)# **snmp-server community mgr view restricted rw ipv6 mgr2**	Define la clave de acceso a la comunidad.
4	Router(config)# **snmp-server engineID remote** { ipv4-ip-address	ipv6-address}[**udp-port** udp-port-number] [**vrf** vrf-name] engineid-string **Ejemplo:** Router(config)# snmp-server engineID remote 3ffe:b00:c18:1::3/127 remotev6	Especifica el nombre del SNMP remoto.
5	Router(config)# **snmp-server group** group-name	Configura un Nuevo grupo SNMP o una tabla que mapea usuarios SNMP

	{**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** read-view] [**write** write-view] [**notify** notify-view] [**context** context-name] [**access** [**ipv6** named-access-list]{ acl-number | acl-name}] **Ejemplo:** Router(config)# snmp-server group public v2c access ipv6 public2	a vistas SNMP.
6	Router(config)# **snmp-server host** { hostname | ip-address} [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] community-string [**udp-port** port] [notification-type] [**vrf** vrf-name] **Ejemplo:** Router(cofig)# snmp-server host host1.com 2c vrf trap-vrf	Especifica el receptor de una operación de notificación SNMP. Especifica si se desean las notificaciones SNMP enviadas como traps o como informes, la versión del SNMP a utilizar, el nivel de seguridad para las notificaciones y el host receptor de las mismas.
7	Router(config)# **snmp-server user** username group-name [**remote** host [**udp-port** port]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} auth-password]} [**access** [**ipv6** nacl] { acl-number | acl-name}] **Ejemplo:** Router(cofig)# **snmp-server user user1 bldg1** **remote 3ffe:b00:c18:1::3/127** **v2c access ipv6** **public2**	Configura un nuevo usuario a un grupo SNMP existente. Nota: No se puede configurar a un usuario remoto sin antes configurar el EngideID para ese host remoto. Esta es una restricción impuesta en el diseño de estos comandos; si se intenta configurar al usuario antes que al host, se recibirá un mensaje de precaución y el comando no será ejecutado.
8	Router(config)# **snmp-server enable traps** [notification-type [notification-options]] **Ejemplo:**	Habilita el envío de Traps o Informes y especifica el tipo de notificaciones a ser enviadas. Si no se especifica un tipo de notificación, todas las notificaciones

	Router(config)# **snmp-server enable traps bgp**	soportadas serán habilitadas en el router. Para descubrir el tipo de notificaciones disponibles en el router, se debe ejecutar el comando **snmp-server enable traps ?.**

4.58 Configurando un Servidor de Notificación SNMP.

4.6.3 Ejemplos de Configuración para la Administración de Aplicaciones IOS para Ipv6.

- **Ejemplo para Habilitar el Acceso Telnet en un Router Ipv6.**

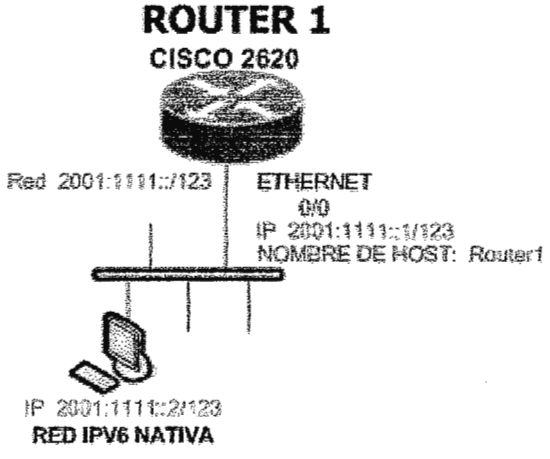


Figura 4.12 Acceso Telnet hacia un Router.

El siguiente ejemplo provee información de cómo habilitar Telnet e iniciar una sesión desde o hacia un Router Ipv6. En el siguiente ejemplo, la dirección Ipv6 esta especificada como 2001:1111::1/123, y el nombre de host esta especificado como Router1. El comando **show host** es el utilizado para verificar esta información.

Router# **configure terminal**
Router(config)# **ipv6 host Router1 2001:1111::1**
Router(config)# **end**

Router# **show host**
Default domain is not set
Name/address lookup uses static mappings

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
Temp - temporary, perm - permanent
NA - Not Applicable None - Not defined

Host	Port	Flags	Age	Type	Address(es)
Router1	None	(perm, OK)	0	IPv6	2001:1111::1

Habilitar el acceso Telnet sobre el Router, crear una interfase vty y una contraseña:

Router(config)# **line vty 0 4**
password **lab**
login

Para utilizar el acceso telnet se debe utilizar una contraseña:

Router# **telnet Router1**
Trying Router1 (2001:1111::1)... Open

User Access Verification
Password:

No es necesario utilizar el comando Telnet , es suficiente especificar solamente la dirección o el nombre del host remoto, como lo muestra el siguiente ejemplo.

Router# **Router1**
or
Router# **2001:1111::1**

Para mostrar los usuarios conectados al Router en el que estamos conectados se utiliza el comando show users.

```
Router# show users
Line       User     Host(s)     Idle        Location
* 0 con 0           idle        00:00:00
130 vty 0          idle        00:00:22    2001:1111::2
```

Note que la dirección mostrada es la dirección Ipv6 del origen de la conexión. Si el nombre de host del origen es conocido, entonces este es mostrado en lugar de la dirección. Así como lo muestra el siguiente ejemplo:

```
Router# show users
Line       User     Host(s)     Idle        Location
* 0 con 0           idle        00:00:00
130 vty 0          idle        00:02:47    Router
```

- **Ejemplo para habilitar el acceso SSH a un Router Ipv6.**

En el siguiente ejemplo se configura un tiempo de espera de 100 segundos para la etapa de negociación de SSH, establece el numero de intentos de autenticación igual a 2, e inicia una sesión encriptada con un dispositivo de red remoto:

```
Router(config)# ip ssh timeout 100 authentication-retries 2
Router(config)# exit
Router# ssh
```

- **Ejemplo para Verificar la Configuración del Servidor SSH.**

El acceso SSH es mas seguro que el acceso telnet. Utilizando un transporte Ipv6 o Ipv4, el acceso SSH puede ocurrir en cualquiera de las siguientes situaciones:

- Hacia un router desde un host.
- Hacia un router desde un router.

La salida del comando **show users** y del comando **show sessions** es la misma que se muestra en los ejemplos de Telnet.

Para verificar que el servidor SSH esta habilitado, y mostrar la versión y datos de configuración de la conexión SSH, utilice el comando **hz. id hz.** El siguiente ejemplo muestra que SSH esta habilitado:

Router# **show ip ssh**

SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3

El siguiente ejemplo muestra que SSH esta deshabilitado:

Router# **show ip ssh**
%SSH has not been enabled

Para verificar el estado de la conexión del servidor SSH, utilice el comando show hz.. El siguiente ejemplo muestra la conexión del servidor hz. sobre el router cuando SSH es habilitado:

Router# **show ssh**

Connection	Version	Encryption	State	Username
0	1.5	3DES	Session	Started	guest

El siguiente ejemplo muestra que el servidor SSH esta deshabilitado:

Router# **show ssh**
%No SSH server connections running.

- **Ejemplo para configurar un Servidor de Notificación SNMP.**

El siguiente ejemplo permite que cualquier SNMP tenga acceso a todos los objetos con permisos de solo lectura utilizando la clave de comunidad igual a "public". El router también enviara traps BGP al host Ipv4 172.16.1.111 y al host Ipv6 3ffe:b00:c18:1::3/127 utilizando SNMPv1 y al host 172.16.1.27 utilizando SNMPv2c. La clave de comunidad es enviada con los traps.

```
Router(config)# snmp-server community public
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host 172.16.1.27 version 2c public
Router(config)# snmp-server host 172.16.1.111 version 1 public
Router(config)# snmp-server host 3ffe:b00:c18:1::3/127 public
```

- **Ejemplo para crear un Servidor de Notificación SNMP.**

El siguiente ejemplo configura el host Ipv6 como servidor de notificación.

```
Router> enable
Router# configure terminal
Router(config)# snmp-server community mgr view restricted rw ipv6 mgr2
Router(config)# snmp-server engineID remote 3ffe:b00:c18:1::3/127 remotev6
Router(config)# snmp-server group public v2c access ipv6 public2
Router(cofig)# snmp-server host host1.com 2c vrf trap-vrf
Router(cofig)# snmp-server user user1 bldg1 remote 3ffe:b00:c18:1::3/127 v2c access ipv6 public2
Router(config)# snmp-server enable traps bgp
Router(config)# exit
```

4.7 CALIDAD DE SERVICIO PARA IPV6 (QoS).

Es una característica de una red de telecomunicaciones que permite garantizar al cliente una calidad pactada por cada servicio contratado.

4.7.1 Prerrequisitos para Implementar Calidad de Servicio para Ipv6.

La siguiente tabla muestra el Sistema Operativo de Cisco requerido para soportar las diferentes caracteristicas de QoS.

Característica	Mínimo Cisco IOS Requerido
Calidad de Servicio para Ipv6	12.2(13)T, 12.3, 12.3(2)T, 12.0(28)S
Línea de Comando Modular para QoS (MQC).	12.2(13)T, 12.3, 12.3(2)T
Manipular el trafico MQC.	12.2(13)T, 12.3, 12.3(2)T, 12.0(28)S1
Establecer Políticas de Trafico MQC	12.2(13)T, 12.3, 12.3(2)T, 12.0(28)S1

Marcar Paquetes MQC	12.2(13)T, 12.3, 12.3(2)T, 12.0(28)S1
Encolamiento	12.2(13)T, 12.3, 12.3(2)T, 12.0(28)S1
MQC WRED	12.2(13)T, 12.3, 12.3(2)T, 12.0(28)S1

Tabla 4.59 cisco IOS requerido para QoS.

4.7.2 Estrategia para Implementar Calidad de Servicio sobre Ipv6.

Las características de Calidad de Servicio que son soportadas por ambientes Ipv6 incluyen la Clasificación de Paquetes, Encolamiento, Prevención de la Congestión (WRED), Marcación de Paquetes y Políticas de Enrutamiento para Paquetes Ipv6. Estas características están disponibles para la conmutación de procesos y para las rustas Ipv6 conmutadas por CEF (Cisco Express Forwarding).
Todas las características de QoS disponibles para ambientes Ipv6 son administradas desde la interfaz de línea de comando (CLI) para QoS, definida en el Sistema Operativo de Cisco; la cual permite crear clases de trafico, políticas de trafico (policy maps) y agregar estas mismas a interfaces especifica de los enrutadores.
Antes de implementar Calidad de Servicio en redes Ipv6, se deben determinar ciertos aspectos importantes, los cuales son:

- Conocer las aplicaciones que necesitan QoS en la red.
- Entender las características de las aplicaciones para así poder tomar decisiones de cual es la característica de QoS apropiada.
- Conocer la topología de la red para así poder conocer como son afectados los tamaños de los encabezados de capa de enlace.
- Crear clases basadas en los criterios que se establecieron para la red. En particular, si en la misma red sé esta llevando trafico Ipv4 e Ipv6, se puede decidir el trato que se le dará a cada tipo de trafico. Si se quiere dar el mismo trato al trafico Ipv4 e Ipv6 se deben utilizar los comandos: **match precedente, match dscp, set precedente** y **set dscp.** Si se quieren tratar por separado, se debe agregar un criterio de comparación como **match protocolo id** o **match protocolo ipv6** dentro de un mapa de clase (class map).
- Crear una política para marcar cada clase.
- Trabar desde las fronteras hacia el núcleo aplicando políticas de QoS.
- Construir las políticas para tratar él trafico.
- Aplicar la Política.

Clasificación de Paquetes en Ipv6.

La clasificación de paquetes esta disponible en los procesos de conmutación y en las rutas de conmutación CEF. La clasificación puede ser basada en una Precedencia Ipv6 (id Precedente), Punto de Control de Servicios Diferenciados (DSCP) y otros valores específicos del protocolo Ipv6 que pueden ser especificados en listas de acceso Ipv6. Una vez se determina que aplicaciones necesitan de QoS, se pueden crear clases basadas en las características de las aplicaciones. Existe una cantidad muy variada de criterios de comparación para clasificar el tráfico y se pueden combinar varios criterios de comparación para aislar y diferenciar el tráfico.
La interfase de comandos para QoS permite realizar comparaciones de precedencia, DSCP y de listas de control de acceso para él trafico Ipv6 e Ipv4.

Políticas y Marcación de Paquetes en redes Ipv6.

Se pueden crear políticas para marcar el tráfico con valores de prioridad apropiados, utilizando precedencia y DSCP. La marcación de paquetes ipv6 permite establecer un valor de precedencia o de DSCP al tráfico para facilitar su administración.
El tráfico es marcado en el momento que entra al router por una interfase específica y esta marca se utiliza para darle un trato específico al tráfico al salir del router. Siempre se debe marcar él trafico lo mas cerca posible del origen.
Para marcar los paquetes se utilizan los comandos **set dscp** y **set precedente**; Los cuales han sido modificados para manipular el tráfico Ipv4 e Ipv6.

Administración de la Congestión para Redes Ipv6.

Una vez el tráfico se encuentra marcado, se pueden utilizar dichas marcas para crear una política y clasificar el tráfico sobre el resto de los segmentos de red. Si se mantienen políticas simples (sin sobrepasar cuatro clases), estas serán fáciles de administrar.

Políticas de Trafico en Ambientes Ipv6.

La administración de la congestión para Ipv6 es similar a esta implementación para paquetes Ipv6 y los comandos que se utilizan para configurar las características de encolamiento (queueing) y manipulación del trafico (traffic shaping) para Ipv6 son los mismos que se utilizan en Ipv4.

4.7.3 Implementando Calidad de Servicio para Ipv6.

Restricciones para Clasificar el Tráfico en redes Ipv6.

Excepto para las modificaciones del comando **match dscp, match precedente** y la adición del comando **match Access-group name** específico para Ipv6, la funcionalidad de todos los comandos **match** es la misma que para Ipv4.
El comando **match access-group** que se utiliza para comparar listas de control de acceso numeradas, no es soportado.
Los comandos **set cos** y **match cos** para interfaces tipo 802.1Q (dot1Q) son soportados solamente para los paquetes conmutados por CEF. Los paquetes de conmutación de procesos, como los generados por el router, no son marcados cuando estas opciones son utilizadas.

Especificando un Criterio de Marcación para los Paquetes Ipv6.

Para marcar los paquetes se utiliza el comando **set precedente,** este valor Serra utilizado posteriormente para comparar los paquetes y clasificar él trafico de la red. Los comandos utilizados para este propósito pueden ser **set precedente** o **set dscp.** Estos comandos han sido modificados para poder marcar trafico Ipv6.

Los siguientes pasos de configuración son utilizados para marcar los paquetes Ipv6.

1. enable
2. configure terminal
3. policy map *policy-map-name*
4. class {*class-name* | **class-default**}
5. set precedente <0-7 [valor de precedencia] >
o
set dscp <0-63 [valor de servicio diferenciado]>

A continuación se presenta una tabla con los pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Acceso al modo de configuración global.
3	**policy map** policy-map-name **Ejemplo:** Router(config)# policy map policy1	Crea una Política de mapa (Policy Map), con un nombre especifico y entra al modo de configuración de la misma.
4	**class** { class-name | **class-default**} **Ejemplo:** Router(config-pmap)# class class-default	Especifica el tratamiento para él trafico de una clase especifica y entra al modo de configuración de la clase para la política de mapa.
5	**set precedente** <0-7 [valor de precedencia] > o **set dscp** <0-63 [valor de servicio diferenciado]> **Ejemplo:** Router(config-pmap-c)# set dscp 7 table-map1 Router(config-pmap-c)# set precedence 5	Establece el valor de precedencia. Entre mas alto sea el valor, más prioritario es el tráfico.

Tabla 4.60 Marcación de Paquetes Ipv6

Para verificar que CEF (Cisco Express Forwarding) se encuentra habilitado en la interfase, se pueden utilizar varios comando de verificación, algunos de estos son: **Show cef interface, show ipv6 cef, show ipv6 interface neighbors** y **show interface statistics**. Para desplegar estadísticas de la conmutación CEF por interfase y por política se utilice el comando **show policy-map interface.**

Criterios de Comparación para Administrar el Flujo de Trafico Ipv6.

Una vez se hayan definido las clases de trafico y las políticas, se puede utilizar el comando **match** para comparar él trafico con las políticas establecidas anteriormente. Se pueden utilizar varios criterios de comparación y dependiendo del tipo de clase se puede especificar si se desean comparar todas las clases o algunas de ellas.

Los siguientes pasos se utilizan para realizar criterios de comparación sobre él trafico ipv6.

1. enable
2. configure terminal
3. class-map {*class-name* | **class-default**}
4. match precedence *precedence-value* [*precedence-value precedence-value*]
o
match access-group name *ipv6-access-group*
o
match [**ip**] **dscp** *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*]

A continuación se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**class-map** { class-name | **class-default**} **Ejemplo:** Router(config-pmap-c)# class cls1	Crea una clase específica y entra al modo de configuración de la clase de mapa (class-map.

4	**match precedence** precedence-value [precedence-value precedence-value] o **match access-group name** ipv6-access-group o **match [ip] dscp** dscp-value [dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value] **Ejemplo:** Router(config-pmap-c)# match precedence 5 Router(config-pmap-c)# match access-group name ipv6acl Router(config-pmap-c)# match ip dscp 15	Compara el valor de precedencia, el cual es aplicado al tráfico Ipv4 e ipv6. Especifica el nombre de una lista de control de acceso Ipv6 contra la cual se van a comparar los paquetes para determinar si pertenece a la clase de trafico. Identifica un valor IP DSCP de comparación específico.

Tabla 4.61 Criterios de Comparación para el Trafico Ipv6

4.7.4 Ejemplo de Configuración.

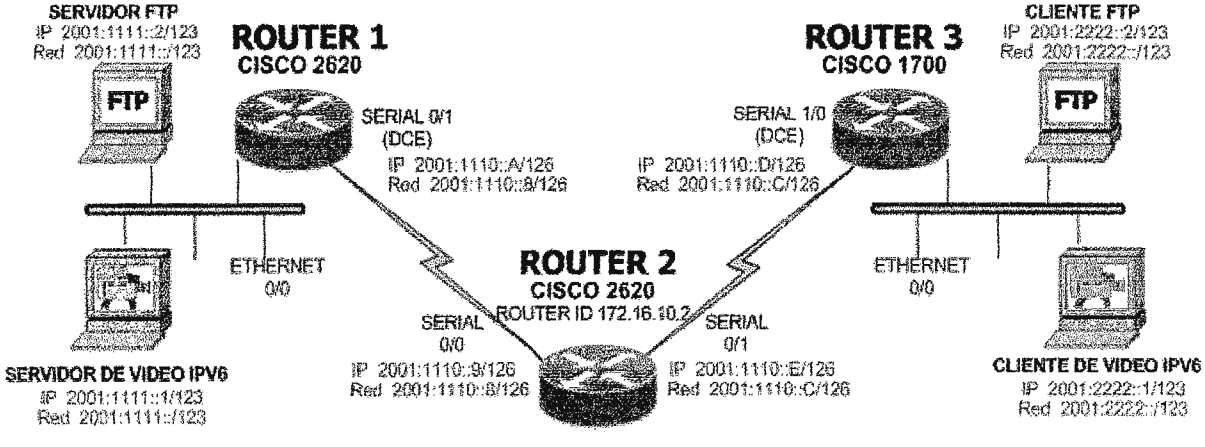


Figura 4.12 Calidad de Servicio sobre Trafico de video.

El diagrama anterior muestra una Red Nativa Ipv6 compuesta por tres enrutadores, los cuales se encuentran conectados a través de sus seriales, cada una de ellas configurada con una dirección Ipv6 así:

- Router 1: Interfase Serial 0/1, con dirección Ipv6 2001:1110::A/126.
- Router 2: Interfase Serial 0/0, con dirección Ipv6 2001:1110::9/126 e
  Interfase Serial 0/1, con dirección Ipv6 2001:1110::E/126.
- Router 3: Interfase Serial 1/0, con dirección Ipv6 2001:1110::D/126.

Cada nodo posee una Red de Área Local (LAN). En la LAN del Router1 se encuentra un servidor de video con dirección Ipv6 2001:1111::1/123 y un Servidor FTP (Protocolo de Transmisión de Archivos) con dirección Ipv6 2001:1111: 2/123, los cuales se encuentran dentro el mismo segmento LAN.

En la LAN del Router3 se encuentran dos host con direcciones 2001:2222::1/123 y 2001:2222::1/123, los cuales son clientes de video y FTP respectivamente.

Se aplicaran configuraciones de calidad de servicio para priorizar el tráfico de video sobre el tráfico de archivos FTP. De esta manera, si en el mismo momento los clientes de video y FTP solicitan la transferencia de paquetes, al trafica de video se le asignara un ancho de banda mucho mayor que al trafico FTP.
Para realizar esta tarea primeramente se necesita marcar el tráfico de video y posteriormente darle un trato específico a este tipo de tráfico. De la siguiente manera:

- En la interface FastEthernet del Router1 se debe aplicar una política para marcar los paquetes que origina el servidor de video.
- En la interface serial 0/1 del Router2 se debe comparar el valor de precedencia (marca que poseen los paquetes), y si cumplen con el valor especifico se establece un ancho de banda del 80% del ancho de banda total del enlace al trafico que posea dicha marca, que en este caso es el de video.

A continuación se presentan los comandos de configuración utilizados en los enrutadores.

ROUTER1

"Se crea la lista de acceso para filtrar él trafico del servidor de video"
ipv6 access-list video
 permit udp host 2001:1111::1 host 2001:2222::1

"Filtra los paquetes Ipv6 que provienen del Servidor de video"
class-map match-all etiqueta
  match protocol ipv6
  match access-group name video
exit

"Establece un valor de precedencia a los paquetes de video"
policy-map etiqueta
  class etiqueta
   set precedente 5
exit

"Aplica la política a la interface FastEthernet como de entrada"
interface fastethernet 0/0
service-policy input etiqueta

ROUTER2

"Compara si los paquetes están marcados con un valor de precedencia igual a 5"
class-map match-all video-class
  match protocol ipv6
  match precedence 5

"Asigna el 80% del ancho de banda del enlace al trafico de video"
policy-map video-policy
  class video-class
   priority percent 80

"Aplica la política a la interface de salida"
interface serial 0/1
service-policy output video-policy

4.8 POLITICAS DE ENRUTAMIENTO EN IPV6 (PBR).

Las políticas de enrutamiento para él trafico Ipv4 e Ipv6 permite al usuario configurar manualmente como serán ruteados los paquetes recibidos. PBR permite a los usuarios identificar los paquetes utilizando ciertos atributos y establecer cual era el siguiente salto o la interface de salida por la cual los paquetes deben ser enviados. PBR también posee la capacidad de marcar los paquetes.

4.8.1 Prerrequisitos para Implementar Políticas de Enrutamiento.

- Estar familiarizado con el direccionamiento Ipv6.
- Estar familiarizado con las diferentes configuraciones de Ipv4.
- La versión del Sistema Operativo del enrutador debe ser igual o superior a la 12.3(7)T para que pueda soportar Políticas de Enrutamiento.

4.8.2 Definición de Políticas de Enrutamiento (PBR).

PBR permite dar sentido al enrutamiento de los paquetes, permitiendo configurar una política definida para el flujo de tráfico. En este sentido, PBR provee mayor control sobre el enrutamiento, complementando los mecanismos existentes que utilizan los protocolos de enrutamiento. PBR permite establecer precedencias Ipv6 y permite establecer una ruta prioritaria para cierto tipo de tráfico aunque posea un alto costo de enlace. PBR puede ser aplicado a paquetes Ipv6 originados en el enrutador o reenviados por el mismo. Para paquetes reenviados, PBR debe ser implementado como una característica en la interfase de entrada.
Se puede establecer PBR como una forma de enlutar los paquetes basados en políticas configuradas. Por ejemplo se pueden implementar políticas de enrutamiento para permitir o denegar rutas basadas en la identidad de un sistema final en particular, un protocolo de aplicación o el tamaño de los paquetes.

PBR permite realizar las siguientes tareas:

- Clasificar el tráfico basado en criterios especificados en lista de control de acceso. De esta manera las listas de acceso establecen el criterio de comparación.
- Establecer los bits de precedencia Ipv6, dando a la red la capacidad de habilitar diferentes clases de servicio.
- Enrutar los paquetes a diferentes tipos de rutas de trafico; esto puede ser necesario para brindar algun tipo de calidad de servicio.

Las políticas pueden ser basadas en direcciones ipv6, números de puertos, protocolos o tamaño de los paquetes. Para una política sencilla se pueden utilizar cualquiera de estos atributos, para una política compleja se pueden utilizar todos los atributos.
PBR permite marcar y clasificar los paquetes en las fronteras de la red. PBR marca un paquete estableciéndole un valor de precedencia, el cual puede ser usado directamente por los enrutadores de la red para aplicar una característica específica de calidad de servicio a los paquetes, la cual mantenga la clasificación de los paquetes en la red.

Forma en que trabaja PBR.

Todos los paquetes que recibe una interfase que tiene habilitado PBR son pasados a través de filtros de paquetes anteriormente especificados, conocidos como mapas de ruta (route maps). Los mapas de ruta utilizados por PBR son los que establecen las políticas, determinando hacia donde se deben enviar los paquetes.

Los mapas de ruta están compuestos por declaraciones, las cuales pueden establecer el permitir o denegar trafico, y son interpretadas en diferentes formas:

- Si el paquete concuerda con todos los criterios de comparación de un mapa de ruta que esta marcado como permitir (permit), entonces el router lo enruta utilizando las declaraciones establecidas; si no, el paquete es enviado normalmente.
- Si el paquete concuerda con cualquiera de los criterios de comparación de un mapa de ruta marcado como denegar (deny), entonces el paquete no se sujeta al PBR y es reenviado normalmente.
- Si el criterio de comparación esta marcado como permitir y los paquetes no concuerdan con cualquiera de los criterios de comparación, el paquete es retornado a través de los canales de envió normales.

Se debe especificar PBR sobre la interfase que recibe el paquete y no en interfase a la cual el paquete es enviado.

Comparación de Paquetes.

PBR para IPv6 compara los paquetes utilizando el comando **match ipv6 address** dentro de un mapa de ruta especificado. Los criterios de comparación también son soportados por las listas de control de acceso (ACL's) en Ipv6. Los atributos que pueden ser tomados como criterios de comparación en los paquetes son:

- Interfase de Entrada del Paquete.
- Dirección Ipv6 de Origen. (Utilizando una lista de prefijos o una ACL)
- Protocolo. (Lista de Acceso Extendida)
- Puerto Origen y Puerto Destino (ACL Extendida).
- Código de Servicios Diferenciados (DSCP) (ACL Extendida).
- Etiqueta de Flujo (ACL Extendida).
- Fragmento (ACL Extendida).

Los paquetes también pueden ser clasificados por el tamaño utilizando la declaración de clasificar por tamaño (match length) en el mapa de ruta PBR.
Si por ejemplo se utiliza un criterio de comparación para el tamaño de los paquetes y una ACL en la misma declaración, el paquete debe sujetarse primero a la ACL. Solamente los paquetes que concuerden con la ACL podrán pasar al criterio de comparación por el tamaño del paquete. Y finalmente, solamente a los paquetes que concuerden con los dos criterios de comparación se les aplicara la política de enrutamiento.

Envío de Paquetes utilizando las sentencia Set.

Él reenvió de paquetes Ipv6 se puede establecer de diferentes formas, de acuerdo a la sentencia "set" que se utilice en el mapa de ruta PBR. Esta sentencia puede ser:

- Siguiente Salto Ipv6: Identifica al siguiente salto al cual el paquete debe ser enviado. El siguiente salto debe estar presente en la Base de Información de Enrutamiento (RIB), y este debe estar directamente conectado. Si el siguiente salto es invalido, la sentencia set es ignorada.

- Interfase de Salida: El paquete es enviado hacia fuera a traves de una interface de salida. Debe existir una dirección de destino del paquete dentro de la RIB Ipv6, y la interfase de salida especificada debe estar en la ruta establecida. Si la interfase es invalida, la sentencia es ignorada.
- Siguiente Salto Ipv6 por defecto: es el siguiente salto al cual el paquete Ipv6 deberia ser enviado. Esta sentencia set es utilizada solamente cuando no existen entradas explicitas para el destino del paquete en la RIB.
- Interfase de salida por defecto: paquete es enviado hacia fuera a traves de una interface específica. Esta sentencia set es utilizada solamente cuando no existen entradas explicitas para el destino del paquete en la RIB.

Se puede establecer varias sentencias set de reenvío de paquetes en los mapas de ruta PBR. Estas sentencias son evaluadas en el orden mostrado.

¿Cuándo se debe utilizar PBR?

Es necesario habilitar PBR cuando se requiere enrutar los paquetes Ipv6 a través de un camino que no es el más corto, ni el que razonablemente seria mas optimo. Por ejemplo, PBR puede ser utilizado para proveer la siguiente funcionalidad:

- Igual Acceso.
- Enrutamiento por sensibilidad de Protocolo.
- Enrutamiento por sensibilidad de Origen.
- Enrutamiento basado en enlaces dedicados.

4.8.3 Implementación de PBR para Ipv6.

Habilitar PBR para IPv6.

Para habilitar PBR para Ipv6, se debe crear un mapa de ruta que especifique el criterio de comparación para los paquetes y decidir la acción a tomar de la política de enrutamiento. Todos los paquetes que llegan a una interface especifica y que cumplen con los criterios de comparación, serán sujetas a PBR.

Los siguientes pasos se utilizan para habilitar PBR sobre una interface.

1. enable

2. configure terminal

3. route-map *map-tag* [**permit** | **deny**] [*sequence-number*]

4. match length *minimum-length maximum-length*

o

match ipv6 address {**prefix-list** *prefix-list-name* | *access-list-name*}

5. set ipv6 precedence *precedence-value*

o

set ipv6 next-hop *ipv6-address* [*ipv6-address...*]

o

set interface *type number* [*...type number*]

o

set ipv6 default next-hop *ipv6-address* [*ipv6-address...*]

o

set default interface *type number* [*...type number*]

6. interface *type number*

7. ipv6 policy route-map *route-map-name*

A continuación se presentan estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Acceso al modo de configuración global.
3	**route-map** map-tag [**permit** | **deny**] [sequence-number] **Ejemplo:** Router(config)# route-map rip-to-ospf permit	Define las condiciones para redistribuir rutas desde un protocolo de enrutamiento a otro, o habilita las políticas de enrutamiento. Entra al modo de configuración del mapa de ruta.
4	Router(config-route-map)# **match length** minimum-length maximum-length	Especifica el criterio de comparación, el cual puede ser por tamaño de paquete o por una lista de acceso especifica. Si no se especifica el comando **match**, el mapa de

	o Router(config-route-map)# **match ipv6 address** {**prefix-list** prefix-list-name | access-list-name} **Ejemplo:** Router(config-route-map)# match length 3 200 o Router(config-route-map)# match ipv6 address marketing	ruta aplica para todos los paquetes.
5	Router(config-route-map)# **set ipv6 precedence** precedence-value o Router(config-route-map)# **set ipv6 next-hop** ipv6-address [ipv6-address...] o Router(config-route-map)# **set interface** type number [...type number] o Router(config-route-map)# **set ipv6 default next-hop** ipv6-address [ipv6-address...] o Router(config-route-map)# **set default interface** type number [...type number] **Ejemplo:** Router(config-route-map)# set ipv6 precedence 1 o	Especifica la acción a tomar por los paquetes que concuerdan con el criterio de comparación. Se puede especificar cualquiera de los siguientes: • Especificar un valor de precedencia. • Especificar el siguiente salto. • Especificar la interfase de salida. • Especificar el siguiente salto por defecto. • Especificar la interfase de salida por defecto.

	Router(config-route-map)# set ipv6 next-hop 2003:1::95 o Router(config-route-map)# set interface ethernet 0 o Router(config-route-map)# set ipv6 default next-hop 2003:1::95 o Router(config-route-map)# set default interface ethernet 0	
6	**interface** type number **Ejemplo:** Router(config)# interface FastEthernet 1/0	Especifica el tipo y numero de la interfase y entra al modo de configuración de la misma.
7	**ipv6 policy route-map** route-map-name **Ejemplo:** Router(config)# ipv6 policy-route-map interactive	Aplica el mapa de ruta a la interfase específica.

Tabla 4.62 Habilitar PBR para IPv6.

Habilitar una PBR Local para Ipv6.

Los paquetes generados por el enrutador normalmente no son tomados en cuenta por las políticas de enrutamiento. Con los siguientes pasos se habilita el PBR local para dichos paquetes, indicando el mapa de ruta que debe ser utilizado por el router.

1. enable

2. configure terminal

3. ipv6 local policy route-map *route-map-name*

A continuación se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.
3	**ipv6 local policy route-map** route-map-name **Ejemplo:** Router(config)# ipv6 local policy route-map pbr-src-90	Configura PBR para Ipv6, para paquetes generados por el router.

Tabla 4.63 Habilitar PBR Local para IPv6.

PBR trabaja de manera mas optima cuando se encuentra habilitado sobre la conmutación CEF, esta característica esta disponible a partir de la versión 12.3(7)T de Cisco IOS y no requiere de algún tipo de configuración especial, ya que se habilita por defecto al habilitar CEF.

Verificar PBR para Ipv6.

Los siguientes pasos se utilizan para desplegar información para verificar la configuración y operación de PBR para Ipv6.

1. enable

2. show ipv6 policy

A continuación se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Accesa al modo de configuración global.

Tabla 4.64 Verificar PBR para IPv6.

Solucionar Problemas de PBR para IPv6.

Las políticas de enrutamiento miran varias partes del paquete y lo enlutan de acuerdo a ciertos atributos definidos en el paquete. Los siguientes pasos se utilizan para determinar la política de enrutamiento que sé esta utilizando y desplegar información de los paquetes que cumplen con el criterio de comparación y si es así la información de ruta resultante.

1. enable
2. debug ipv6 policy [*access-list-name*]
3. show route-map [*map-name*]

A continuación se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**debug ipv6 policy** [access-list-name] **Ejemplo:** Router# debug ipv6 policy	Despliega la actividad de los paquetes de la política de enrutamiento Ipv6.

3	**show route-map** [map-name] **Ejemplo:** Router# show route-map	Despliega todos los mapas de rutas configurados o alguno en particular.

Tabla 4.65 Solucionar Problemas de PBR en Ipv6.

A continuación se muestra un ejemplo de salida en pantalla para el comando **show ipv6 policy**, el cual despliega la PBR configurada.

Router# **show ipv6 policy**

Interface Routemap

Ethernet0/0 src-1

A continuación se muestra un ejemplo de salida en pantalla para el comando **show route-map**, el cual despliega información de mapa de ruta.

Router# **show route-map**

route-map bill, permit, sequence 10

Match clauses:

Set clauses:

Policy routing matches:0 packets, 0 bytes

4.8.4 Ejemplo de Configuración de PBR para Ipv6.

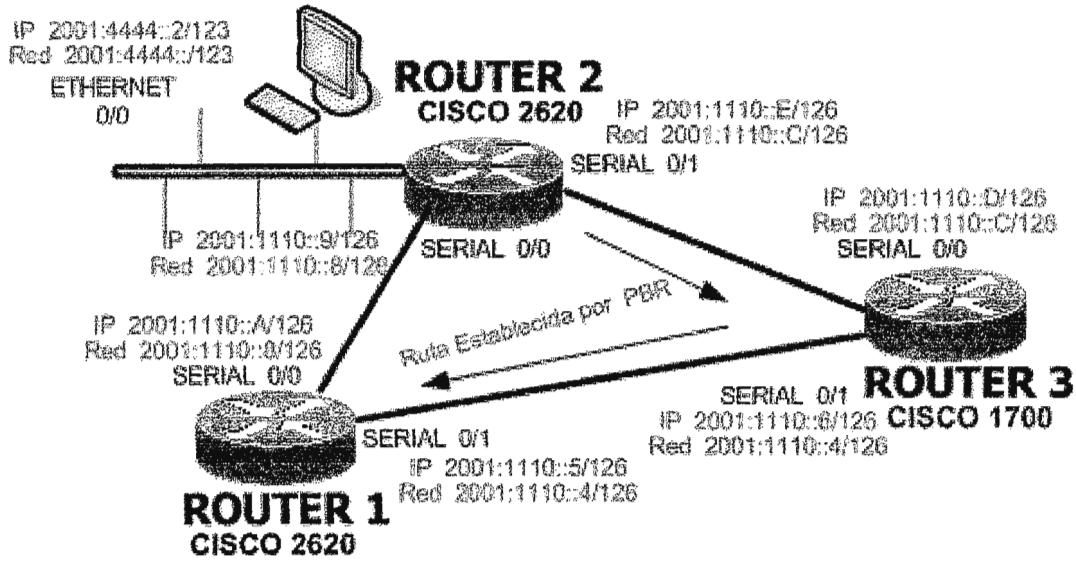


Figura 4.13 PBR sobre Ipv6.

El diagrama anterior muestra una Red Nativa Ipv6 compuesta por tres enrutadores, los cuales se encuentran conectados a través de sus seriales, cada una de ellas configurada con una dirección Ipv6 así:

- Router 1: Interfase Serial 0/0, con dirección Ipv6 2001:1110::A/126.
  Interfase Serial 0/1, con dirección Ipv6 2001:1110::5/126.
- Router 2: Interfase Serial 0/0, con dirección Ipv6 2001:1110::9/126.
  Interfase Serial 0/1, con dirección Ipv6 2001:1110::E/126.
- Router 3: Interfase Serial 0/0, con dirección Ipv6 2001:1110::D/126.
  Interfase Serial 0/1, con dirección Ipv6 2001:1110::6/126.

En la red local del Router2 se tiene un host con una direccion 2001:4444::2/123, el cual se utilizara para realizar la prueba de PBR para Ipv6.

La prueba consiste en enviar paquetes ICMP (Ping) desde el host que se encuentra en la LAN del Router2 hacia el Router1. Por lógica la ruta que debería ser prioritaria para llegar al Router1 es la que se encuentra directamente conectada al Router2 , ya que solo posee un salto de distancia.

Vamos a suponer que el enlace que va del Router1 al Router2 posee 2MB de ancho de banda, y que el enlace que va del Router2 al Router3 y del Router3 al Router1 posee 100MB de ancho de banda.
Se aplicara PBR al Router2 para crear una política de enrutamiento que obligue al trafico proveniente del host 2001:4444::2, poseer como siguiente salto la dirección del Router3, de esta manera los paquetes tomaran el camino que posee un ancho de banda igual a 100MB.

A continuación se muestran los comandos de configuración de PBR en el Router2.

ROUTER2

"Crea la lista de acceso para filtrar él trafico del host en la LAN del Router2"

```
ipv6 access-list acl-host
permit tcp host 2001:4444::2 any
```

"Crea el mapa de ruta pbr-route utilizando como criterio de comparación la ACL anteriormente creada y especificando la dirección de siguiente salto para él trafico que concuerde con la ACL"

```
route-map pbr-route permit 10
match ipv6 address acl-host
set ipv6 next-hop 2001:1110::D
```

"Aplica mapa de ruta en forma local para que se evalúe él trafico originado en el Router2"
interface fastethernet 0/0
ipv6 local policy route-map pbr-route

4.9 SEGURIDAD EN IPV6.

4.9.1 Prerrequisitos para Implementar Seguridad en Ipv6.

- Estar familiarizado con las diferentes configuraciones del protocolo Ipv4.
- Estar familiarizado con el direccionamiento Ipv6.
- Que la versión del Sistema Operativo de Cisco soporte las características de Seguridad en ipv6.

Característica	Mínimo Cisco IOS Requerido
Listas de Control de Acceso Estándar	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T
Listas de Control de Acceso Extendidas	12.0(23)S, 12.2(13)T, 12.2(14)S, 12.3, 12.3(2)T
Firewall de Cisco IOS para Ipv6	12.3(7)T

Tabla 4.66 Cisco IOS Requeridas para PBR en IPv6.

4.9.2 Características de la Seguridad en Ipv6.

Listas de Control de acceso (ACL's) en Ipv6.

Las listas de control de acceso permiten filtrar él trafico en base a direcciones de origen y destino de los paquetes, protocolos o puertos; Ya sea trafico de entrada o de salida en una interfase especifica. Cada lista de acceso posee implícitamente una sentencia de denegar (deny) al final de la misma. Para definir una condición de permitir o denegar en una lista de acceso Ipv6, se debe utilizar el comando **ipv6 access-list** con los comandos **deny** o **permit** en el modo de configuración global del router.

IPSec para Ipv6.

IPSec es un estándar que proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP (TCP y UDP, entre otros).
Entre las ventajas de IPSec destacan que esta apoyado en estándares del IETF y que proporciona un nivel de seguridad común y homogéneo para todas las aplicaciones, además de ser independiente de la tecnología física empleada. IPSec se encuentra incluido por defecto en el protocolo Ipv6.
Entre los benéficos que aporta IPSec, cabe señalar que:

- Posibilita nuevas aplicaciones como el acceso seguro y transparente de un nodo IP remoto.
- Facilita el comercio electrónico de negocio a negocio, al proporcionar una infraestructura segura sobre la que realizar transacciones usando cualquier aplicación.
- Permite construir una red corporativa segura sobre redes públicas, eliminando la gestión y el coste de líneas dedicadas.

IPSec es, en realidad, un conjunto de estándares para integrar en IP funciones de seguridad basadas en criptografía. Proporciona confidencialidad, integridad y autenticidad de data gramas IP, combinando tecnologías de clave publica (RSA), algoritmos de cifrado (DES, 3DES, IDEA, Blowfish), algoritmos de hash (MD5, SHA-1) y certificados digitales X509v3.

IPSec ha sido diseñado de forma modular, de modo que se pueda seleccionar el conjunto de algoritmos deseados sin afectar a otras partes de la implementación. Sin embargo, se han definido ciertos algoritmos estándar que deberían soportar todas las implementaciones para asegurar la interoperabilidad en el mundo global de Internet. Dichos algoritmos de referencia son DES y 3DES, para cifrado, así como MD5 y SHa-1, como funciones de Hash.

Dentro de IPSec se distinguen los siguientes componentes:

- Dos protocolos de seguridad: El Protocolo de Autenticación de Encabezado (AH) y el de Seguridad de Encapsulacion de la Carga IP (ESP) que proporciona mecanismos de seguridad para proteger trafico IP.
- Un protocolo de gestión de claves conocido como Intercambio de Claves de Internet (IKE), que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

El protocolo AH es el procedimiento previsto dentro de IPSec para garantizar la integridad y autenticación de los data gramas IP. Proporciona un medio al receptor de los paquetes IP para autenticar el origen de los datos y para verificar que dichos datos no han sido alterados en transito. Sin

embargo no proporciona ninguna garantía de confidencialidad, es decir, los datos transmitidos pueden ser vistos por terceros.
Tal como indica su nombre, AH es una cabecera de autenticación que se inserta entre la cabecera IPv6 estándar y los datos transportados, que pueden ser un mensaje TCP, UDP o ICMP, o incluso una data grama IP completo. AH es realmente un protocolo IP nuevo, y como tal el IANA le ha asignado el número decimal 51. Esto significa que el campo protocolo de la cabecera IPv6 contiene el valor 51.

El protocolo ESP tiene como objetivo principal el proporcionar confidencialidad, para ello especifica la forma de cifrar los datos que se desean enviar y como este contenido cifrado se incluye en una data grama IP. Adicionalmente, puede ofrecer servicios de integridad y autenticación del origen de los datos incorporando un mecanismo similar al de AH.
Dado que ESP proporciona mas funciones que AH, el formato de la cabecera es más complejo; este formato consta de una cabecera y una cola que rodean los datos transportados, los cuales pueden ser TCP, UDP o ICMP.
El IANA ha asignado al protocolo ESP él numero decimal 50.

Antes de entrar en los detalles del protocolo IKE es necesario explicar los dos modos de funcionamiento que permite IPSec. Tanto ESP como AH proporcionan dos modos de uso:

1) El modo Transporte. En este modo el contenido transportado dentro del data grama AH o ESP son datos de la capa de Transporte (por ejemplo, datos TCP o UDP). Por tanto la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSec.
2) El modo Tunel. En este el contenido de la data grama AH o ESP es una data grama IP completo, incluida la cabecera IP original. Así, se toma un data grama IP al cual se añade inicialmente una cabecera AH o ESP, posteriormente se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes a través de la red. El modo túnel se usa normalmente cuando el destino final de los datos coincide con el dispositivo que realiza las funciones IPSec.

Un concepto esencial en Ipsec es el de la asociación de seguridad (SA): es un canal de comunicación unidireccional que conecta dos nodos, a traves del cual fluyen los datagramas protegidos mediante mecanismos criptograficos acordados previamente. Al identificar únicamente un canal unidireccional, una conexión IPSec se compone de dos SAs, una por cada sentido de la comunicación.

Hasta el momento se ha supuesto que ambos extremos de una asociación de seguridad deban tener conocimiento de las claves, así como del resto de la información que necesitan para enviar y recibir data gramas AH o ESP. Tal como se ha indicado anteriormente, es necesario que ambos nodos estén de acuerdo tanto en los algoritmos criptográficos a emplear como en los parámetros de control. Esta operación puede realizarse mediante una configuración manual, o mediante algún protocolo de control que se encargue de la negociación automática de los parámetros necesarios; a esta operación se le llama negociación de SAs.

El IETF ha definido el protocolo IKE para realizar tanto esta función de gestión automática de claves como el establecimiento de SAs correspondientes. Una característica importante de IKE es que su utilidad no se limita a IPSec, sino que es un protocolo estándar de gestión de claves que podría ser útil en otros protocolos, como, por ejemplo, OSPF o RIPv2.

El objetivo principal de IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPSec.

El Protocolo IPSec es soportado de forma nativa por Ipv6 y se encuentra implementado dentro de la cabecera de los paquetes Ipv6, utilizando el campo de encabezado de extensión, en el cual se encuentra el encabezado de Autenticación (AH) y el Encabezado de Seguridad de Encapsulacion de Carga (ESP), utilizados por IPsec para autenticar y encriptar los paquetes. Hasta la fecha, la configuración del protocolo IPsec para IPv6 sobre los dispositivos de red, no esta disponible públicamente, ya que esta en proceso de desarrollo. Por lo tanto la implementación práctica de IPsec no es contemplada en este documento debido a las razones anteriormente mencionadas. Sin embargo, Ipv6 posee las características necesarias para dar soporte a IPsec de forma nativa.

Firewall de Cisco para IPv6.

El Firewall de Cisco posee funciones avanzadas de filtrado de trafico. El firewall de Cisco para ipv6 posibilita implementarlo dentro redes ipv6 nativas y puede coexistir con el Firewall de Cisco para Ipv4, además es soportado en todos los enrutadores que soporten los dos protocolos (dual snack).

El Firewall de Cisco posee las siguientes características:

- Inspección de Paquetes Fragmentados. El encabezado de fragmento es utilizado para disparar procesamientos de fragmento. El Reensamblador Virtual de Fragmentos (VFR) examina los fragmentos que están fuera de secuencia y les establece en el orden correcto. Examina los fragmentos en busca de ataques de denegación de servicio (DoS).
- Mitigación de ataques DoS.
- Inspección de Paquetes en Túneles.

- Inspección de Paquetes TCP, UDM, ICMPv6 y sesiones FTP.
- Inspección de Paquetes originados en una red Ipv4 y terminados en una red Ipv6, proveyendo servicios de traslación de Ipv4 a Ipv6.
- Interpretación y reconocimiento de muchos encabezados de extensión para Ipv6, incluyendo encabezados de enrutamiento, encabezados de siguiente salto y encabezados de fragmento.
- Mapeo de puerto a Aplicaciones.

Inspección de Paquetes Ipv6.

La inspección se realiza sobre los siguientes campos de encabezado;

- Clase de Trafico.
- Etiqueta de Flujo.
- Tamaño de la carga.
- Siguiente cabecera.
- Limite de Saltos.
- Dirección Origen y Destino.

4.9.3 Implementando Seguridad sobre Ipv6.

Configurar Filtros de Trafico en Ipv6

Para habilitar el filtrado de trafico Ipv6, se deben realizar los siguientes pasos :

- Crear un Lista de Control de Acceso (ACL) Ipv6.
- Configurar la ACl para permitir o bloquear él trafico.
- Aplicar la ACL a una interfase.

En ipv6 las ACL's deben ser definidas con un nombre, ya que Ipv6 no soporta ACL's numeradas. Además una ACL Ipv4 e Ipv6 no pueden compartir el mismo nombre.

Para crear una lista de acceso sobre Ipv6 se utiliza el comando ipv6 **access-list** acompañado de las sentencias **permit** o **deny**, que se utilizan para permitir o bloquear él trafico respectivamente.

Los siguientes pasos se utilizan para crear una lista de acceso Ipv6.

1. enable

2. configure terminal

3. ipv6 access-list *access-list-name*

4. permit {*protocol*} {*source-ipv6-prefix*/ *prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix*/ *prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**reflect** *name* [**timeout** *value*]] [**routing**] [**time-range** *name*] [**sequence** *value*]

o

deny {*protocol*} {*source-ipv6-prefix*/ *prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix*/ *prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**time-range** *name*] [**undetermined-transport**] [**sequence** *value*]

A continuación se presentan estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Entra al modo de configuración global del router.
3	**ipv6 access-list** access-list-name **Ejemplo:** Router(config)# ipv6 access-list outbound	Define una ACL Ipv6 y entra al modo de configuración de la ACL. El argumento *access-list name* especifica el nombre de la lista de acceso, el cual no puede poseer espacios en blanco o empezar con un numeral.
4	**permit** { protocol} { source-ipv6-prefix/ prefix-length | **any** | **host** source-ipv6-address} [operator [port-number]] { destination-ipv6-prefix/ prefix-length | **any** | **host** destination-ipv6-address} [operator [port-number]] [**dscp** value] [**flow-label** value] [**fragments**] [**log**] [**log-input**] [**reflect** name [**timeout** value]] [**routing**] [**time-range** name] [**sequence** value]	Especifica las condiciones de permitir o bloquear par alas ACL's. El argumento protocolo especifica el nombre o él numero de algún protocolo de Internet y puede ser alguna de las siguientes sentencias **ahp**,**esp**, **icmp**, **ipv6**, **pcp**, **sctp**, **tcp**, or **udp**, o un numero de 0 a 255 representando el numero del protocolo. Los argumentos *source-ipv6-prefix*/ *prefix-length* y *destination-ipv6-prefix*/ *prefix-length* especifican la red de origin y a la cual se aplica la ACL Destino.

	o **deny** { protocol} { source-ipv6-prefix/ prefix-length | **any** | **host** source-ipv6-address} [operator [port-number]] { destination-ipv6-prefix/ prefix-length | **any** | **host** destination-ipv6-address} [operator [port-number]] [**dscp** value] [**flow-label** value] [**fragments**] [**log**] [**log-input**] [**routing**] [**time-range** name] [**undetermined transport**] [**sequence** value] **Ejemplo:** Router(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/32 eq telnet any reflect reflectout **Ejemplo:** Router(config-ipv6-acl)# deny tcp host 1::1 any log-input	La sentencia **any** es una abreviación del prefijo: /0. La sentencia **host** *source-ipv6-address* especifica la dirección IPv6 de origen del host sobre el cual se aplica la condición de permitir.

Tabla 4.67 Crear una lista de Acceso en Ipv6.

Aplicar una ACL en una Interfase.

Los siguientes pasos de configuración se utilizan para aplicar una ACL a una interfase.

1. enable

2. configure terminal

3. interface *type number*

4. ipv6 traffic-filter *access-list-name* {**in** | **out**}

A continuacion se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.

2	**configure terminal** **Ejemplo:** Router# configure Terminal	Entra al modo de configuración global del router.
3	**interface** type number **Exempla:** Router(comfit)# interface Ethernet 0	Especifica el tipo de interfase y entra al modo de configuración de la misma.
4	**ipv6 traffic-filter** access-list-name {**in** | **out**} **Ejemplo:** Router(config-if)# ipv6 traffic-filter outbound out	Aplica la lista de acceso Ipv6 a la interfase especificada en el paso anterior. La sentencia **in** filtra trafico de entrada sobre la interfase especificada. La sentencia **out** filtra trafico de salida sobre la interfase especificada.

Tabla 4.68 Aplicar una lista de Acceso a una Interfase.

Controlar el Acceso vty (Telnet).

Los filtros para las conexiones de entrada o salida a un router se realizan en base a una lista de acceso utilizando el comando **ipv6 access-class** en le modo de configuración de línea. El comando **ipv6 access-class** es similar al comando **access-class** utilizado con Ipv4, la única diferencia es que la lista de acceso en Ipv6 debe poseer un nombre. Si la ACL Ipv6 es aplicada como trafico de entrada la dirección de origen de la ACL se compara con la dirección de origen de la conexión entrante y la dirección destino de la ACL se comprara con la dirección de la interfase local del router. Si la ACL es aplicada para trafico de salida, la dirección de origen de la ACL es comparada con la dirección local de la interfase del router y la dirección destino de la ACL se compara con la dirección de origen de la conexión remota. Este control se realiza a través de la creación de un filtro de clase especificado en una ACL Ipv6.

Crear un Filtro de Clase de Acceso Ipv6.

Los siguientes pasos se utilizan para controlar el acceso a la línea vty (Telnet) de un router, creando una lista de acceso Ipv6 para proveer un Filtro de Clase de Acceso.

1. enable

2. configure terminal

3. ipv6 access-list *access-list-name*

4. permit {*protocol*} {*source-ipv6-prefix*/ *prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix*/ *prefix-length* | **any** | **host** *destination-ipv6-address*}

[*operator* [*port-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**reflect** *name* [**timeout** *value*]] [**routing**] [**time-range** *name*] [**sequence** *value*]

o

deny {*protocol*} {*source-ipv6-prefix*/ *prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix*/ *prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**time-range** *name*] [**undetermined-transport**] [**sequence** *value*]

A continuación se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Entra al modo de configuración global del router.
3	**ipv6 access-list** access-list-name **Ejemplo:** Router(config)# ipv6 access-list acceso-telnet	Define una ACL Ipv6 y entra al modo de configuración de la ACL. El argumento *access-list name* especifica el nombre de la lista de acceso, el cual no puede poseer espacios en blanco o empezar con un numeral.
4	**permit** { protocol} { source-ipv6-prefix/ prefix-length | **any** | **host** source-ipv6-address} [operator [port-number]] { destination-ipv6-prefix/ prefix-length | **any** | **host** destination-ipv6-address} [operator [port-number]] [**dscp** value] [**flow-label** value] [**fragments**] [**log**] [**log-input**] [**reflect** name [**timeout** value]] [**routing**] [**time-range** name] [**sequence** value] o **deny** { protocol} { source-ipv6-prefix/ prefix-length | **any** | **host** source-ipv6-address} [operator [port-number]]	Especifica las condiciones de permitir o bloquear par alas ACL's. El argumento protocolo especifica el nombre o el numero de algún protocolo de Internet y puede ser alguna de las siguientes sentencias **ahp**,**esp**, **icmp**, **ipv6**, **pcp**, **sctp**, **tcp**, or **udp**, o un numero de 0 a 255 representando el numero del protocolo. Los argumentos *source-ipv6-prefix*/ *prefix-length* y *destination-ipv6-prefix*/ *prefix-length* especifican la red de origen y a la cual se aplica la ACL Destino. La sentencia **any** es una abreviación del prefijo: /0. La sentencia **host** *source-ipv6-address* especifica la dirección IPv6 de origin del host sobre el cual se aplica la condición de

	{ destination-ipv6-prefix/ prefix-length | **any** | **host** destination-ipv6-address} [operator [port-number]] [**dscp** value] [**flow-label** value] [**fragments**] [**log**] [**log-input**] [**routing**] [**time-range** name] [**undetermined transport**] [**sequence** value] **Ejemplo:** Router(config-ipv6-acl)# permit ipv6 host 2001:0DB8:0:4::32 any eq telnet **Ejemplo:** Router(config-ipv6-acl)# deny ipv6 host 2001:0DB8:0:6::6/32 any	permitir.

Tabla 4.69 Crear un Filtro de Acceso Ipv6.

Aplicar una ACL Ipv6 como Filtro de Acceso Telnet.

Después de haber creado la ACL, esta se debe aplicar a la línea Terminal virtual (vty). Los siguientes pasos se utilizan para aplicar una ACL a la línea vty.

1. enable

2. configure terminal}

3. line [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]

4. ipv6 access-class *ipv6-access-list-name* {**in** | **out**}

A continuación se muestran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Entra al modo de configuración global del router.

3	**line** [**aux** | **console** | **tty** | **vty**] line-number [ending-line-number] **Ejemplo:** Router(config)# line vty 0 4	Identifica un línea específica para configuración y entra al modo de configuración de línea. En este ejemplo la sentencia vty se utiliza para especificar la línea Terminal virtual para el acceso remoto.
4	**ipv6 access-class** ipv6-access-list-name {**in** | **out**} **Ejemplo:** Router(config-line)# ipv6 access-class accesso-telnet in	Filtra las conexiones de entrada y salida del router, basado en una ACL Ipv6. El argumento *ipv6-access-list name* específica el nombre de la lista de acceso.

Tabla 4.70 Aplicar un Filtro de Acceso Ipv6 a la linea vty.

Configuración del Firewall de Cisco para Ipv6.

Los siguientes pasos se utilizan para configurar el Firewall de Cisco IOS, esto se hace a través de inspección de paquetes y lista de control de acceso.

1. enable

2. configure terminal

3. ipv6 unicast-routing

4. ipv6 inspect name *inspection-name protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*]

5. interface *type number*

6. ipv6 address *ipv6-address/prefix*

7. ipv6 enable

8. ipv6 traffic-filter [**inbound** | **outbound**}

9. ipv6 inspect *inspect-name*

10. ipv6 access-list *access-list-name*

11. permit {*protocol*} {*source-ipv6-prefix*/ *prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix*/ *prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**reflect** *name* [**timeout** *value*]] [**routing**] [**time-range** *name*] [**sequence** *value*]

or

deny {*protocol*} {*source-ipv6-prefix*/ *prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix*/ *prefix-length* | **any** | **host** *destination-ipv6-address*}

[*operator* [*port-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**time-range** *name*] [**undetermined-transport**] [**sequence** *value*]

A continuacion se presentan estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado.
2	**configure terminal** **Ejemplo:** Router# configure terminal	Entra al modo de configuración global del router.
3	**ipv6 unicast-routing** **Ejemplo:** Router(config)# ipv6 unicast-routing	Habilita el enrutamiento Unicast Ipv6
4	**ipv6 inspect name** inspection-name protocol [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** seconds] **Ejemplo:** Router(config)# ipv6 inspect name ipv6_test icmp timeout 60	Define un conjunto de reglas de inspección Ipv6 para el Firewall.
5	**interface type number** **Ejemplo:** Router(config)# interface FastEthernet0/0	Especifica la interfase donde ocurrirá la inspección.
6	**ipv6 address ipv6-address/prefix** **Ejemplo:** Router(config-if)# ipv6 address 3FFE:C000:0:7::/64 eui-64	Provee la dirección a la interfase inspeccionada.
7	**ipv6 enable** **Ejemplo:** Router(config-if)# ipv6 enable Enables IPv6 routing. **Note** This step is optional if the IPv6	Este paso es opcional si ya se especifico la dirección Ipv6.

	address is specified in step 6.	
8	**ipv6 traffic-filter** access-list-name {**in** | **out**} **Ejemplo:** Router(config-if)# ipv6 traffic-filter outbound out	Aplica la lista de acceso a la interfase especificada en el paso anterior. La sentencia **in** filtra él trafico Ipv6 de entrada en la interfase. La sentencia **out** filtra el trafico Ipv6 de salida en la interfase.
9	**ipv6 inspect** inspection-name {**in** | **out**} **Ejemplo:** Router(config)#ipv6 inspect ipv6_test in	Aplica el conjunto de reglas de inspección.
10	**ipv6 access-list** acl-name **Ejemplo:** Router(config)# ipv6 access-list outbound	Define una ACL Ipv6 y entra al modo de configuración de lista de acceso. El argumento *access-list name* define el nombre de la ACL Ipv6.
11	**permit** { protocol} { source-ipv6-prefix/ prefix-length | **any** | **host** source-ipv6-address} [operator [port-number]] { destination-ipv6-prefix/ prefix-length | **any** | **host** destination-ipv6-address} [operator [port-number]] [**dscp** value] [**flow-label** value] [**fragments**] [**log**] [**log-input**] [**reflect** name [**timeout** value]] [**routing**] [**time-range** name] [**sequence** value] o **deny** { protocol} { source-ipv6-prefix/ prefix-length | **any** | **host** source-ipv6-address} [operator [port-number]] { destination-ipv6-prefix/ prefix-length | **any** | **host** destination-ipv6-address} [operator [port-number]] [**dscp** value] [**flow-label** value] [**fragments**] [**log**] [**log-input**] [**routing**]	Especifica las condiciones de permitir o bloquear par alas ACL's. El argumento protocolo especifica el nombre o él numero de algún protocolo de Internet y puede ser alguna de las siguientes sentencias **ahp**,**esp**, **icmp**, **ipv6**, **pcp**, **sctp**, **tcp**, or **udp**, o un numero de 0 a 255 representando el numero del protocolo. Los argumentos *source-ipv6-prefix/ prefix-length* y *destination-ipv6-prefix/ prefix-length* especifican la red de origin y a la cual se aplica la ACL Destino. La sentencia **any** es una abreviación del prefijo ::/0. La sentencia **host** *source-ipv6-address* especifica la dirección IPv6 de origin del host sobre el cual se aplica la condición de permitir.

	[**time-range** name] [**undetermined transport**] [**sequence** value] **Ejemplo:** Router(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/32 any reflect reflectout **Ejemplo:** Router(config-ipv6-acl)# deny tcp fec0:0:0:0201::/64 any	

Tabla 4.71 Configuración del Firewall de Cisco para Ipv6

Verificar las configuraciones de Seguridad Ipv6.

Los siguientes comandos son utilizados para verificar la configuración y operación de las opciones de seguridad para Ipv6.

1. **show crypto ipsec policy** [**name** *policy-name*]
2. **show crypto ipsec sa ipv6** [*interface-type interface-number*] [**detailed**]
3. **show ipv6 access-list** [*access-list-name*]
4. **show ipv6 inspect** {**name** *inspection-name* | **config** | **interfaces** | **session** [**detail**] | **all**}
5. **show ipv6 prefix-list** [**detail** | **summary**] [*list-name*]
6. **show ipv6 virtual-reassembly interface** *interface-type*
7. **show logging** [**slot** *slot-number* | **summary**]
8. **show ipv6 port-map** [*application-name* | **port** *port-number*]

A continuación se muestran estos comandos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**show crypto ipsec policy** [**name** policy-name] **Ejemplo:** Router> show crypto ipsec policy	Despliega los parámetros para cada política IPSec
2	**show crypto ipsec sa ipv6** [interface-type interface-number] [**detailed**] **Ejemplo:** Router> show crypto ipsec sa ipv6	Despliega las opciones usadas por las asociaciones de seguridad actuales.
3	**show ipv6 access-list** [access-list-name] **Ejemplo:** Router> show ipv6 access-list	Despliega el contenido de todas las ACL's actuales
4	**show ipv6 inspect** {**name** inspection-name |	Despliega información de una regla de inspección.

	config | interfaces | session [**detail**] | **all**} **Ejemplo:** Router> show ipv6 inspect interfaces	
5	**show ipv6 prefix-list** [**detail** | **summary**] [list-name] **Ejemplo:** Router> show ipv6 prefix-list	Despliega información acerca de una lista de prefijo Ipv6.
6	**show ipv6 virtual-reassembly interface** interface-type **Ejemplo:** Router> show ipv6 virtual-reassembly interface e1/1 Displays configuration and statistical information of VFR.	Despliega la configuración y estadísticas de la información de VRF.
7	**show logging** [**slot** slot-number | **summary**] **Ejemplo:** Router> show logging	Despliega es estado del sistema de logeo (syslog.
8	**show ipv6 port-map** [application-name | **port** port-number] **Ejemplo:** Router> show ipv6 port-map ftp	Verifica la configuración del Mapeo de puertos a Aplicaciones (PAM).

Tabla 4.72 Verificación de Configuraciones de Seguridad

4.9.4 Ejemplos de Configuración para Seguridad en Ipv6.

Control de Acceso a la Línea vty.

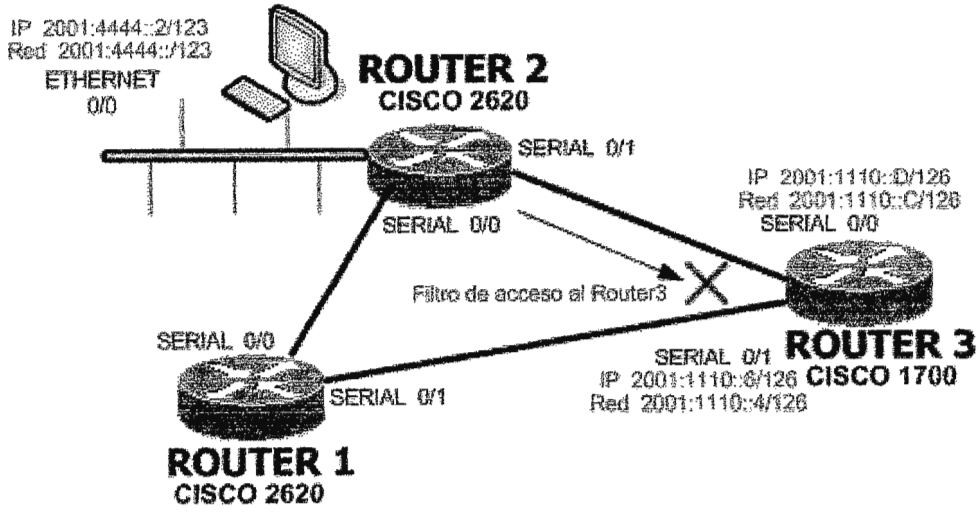


Figura 4.14 Filtro de Acceso a línea vty.

Para lograr filtrar el acceso al Router3 desde el host 2001:4444: 2 o de cualquier otro host de la red, se necesita crear una lista de acceso en la que se definen los host que se desean permitir o bloquear. Posteriormente esta lista de acceso se debe aplicar a la línea de acceso virtual (vty).

ROUTER3

"Se crea la lista de control de Acceso"
ipv6 access-list access-telnet
permit ipv6 host 2001:0DB8:0:4::2/32 any

'Se aplica la lista de acceso a la interfase virtual de acceso"
line vty 0 4
ipv6 access-class Cisco in
exit

Ejemplo de configuración del Firewall de Cisco.

El ejemplo de configuración del Firewall de Cisco utiliza filtros de entrada y de salida para inspeccionar y hacer uso de las listas de acceso para administrar él trafico. A continuación se muestra un ejemplo de configuración del Firewall de Cisco.

```
enable
 configure terminal
  ipv6 unicast-routing
   ipv6 inspect name ipv6_test icmp timeout 60
   ipv6 inspect name ipv6_test tcp timeout 60
   ipv6 inspect name ipv6_test udp timeout 60

interface FastEthernet0/0
  ipv6 address 3FFE:C000:0:7::/64 eui-64
  ipv6 enable
  ipv6 traffic-filter INBOUND out
  ipv6 inspect ipv6_test in

interface FastEthernet0/1
  ipv6 address 3FFE:C000:1:7::/64 eui-64
  ipv6 enable
  ipv6 traffic-filter OUTBOUND in

interfase FastEthernet4/0
  ip address 192.168.17.33 255.255.255.0
  duplex auto
  speed 100

ip default-gateway 192.168.17.8
```

"Lista de acceso que deniega todo él trafico ipv6 , excepto los mensajes ICMP de descubrimiento de vecino"

```
ipv6 access-list INBOUND
  permit icmp any any nd-na
  permit icmp any any nd-ns
deny ipv6 any any log

ipv6 access-list OUTBOUND
  permit icmp any any nd-na
  permit icmp any any nd-ns
  deny ipv6 any any log
```

4.10 TUNELES EN IPV6.

4.10.1 Prerrequisitos para implementar túneles en ipv6.

- Estar familiarizado con el Protocolo Ipv4.
- Poseer una versión del Cisco IOS con soporte para la configuración de Túneles.

Característica	Mínimo Cisco IOS Requerido
Tuneless Automaticos 6to4	12.0(21)ST, 12.0(22)S, 12.2(2)T, 12.2(14)S, 12.3, 12.3(2)T
Túneles compartibles con Ipv4 Automaticos	12.0(21)ST, 12.0(22)S, 12.2(2)T, 12.2(14)S, 12.3, 12.3(2)T
Túneles GRE sobre Ipv6	12.3(7)T
Túneles Ipv4 sobre Ipv6	12.3(7)T
Túneles Ipv6 sobre Ipv4	12.3(7)T
Túneles Manualmente Configurados	12.0(21)ST, 12.0(23)S, 12.2(2)T, or 12.2(14)S, 12.3, 12.3(2)T
Túneles GRE Ipv6 sobre Ipv4	12.0(21)ST, 12.0(22)S, 12.2(2)T, 12.2(14)S, 12.3, 12.3(2)T
Tuneles ISATAP	12.2(14)S, 12.3(2)T
Túneles Ipv6 sobre UTI	12.0(23)S
Soporte CLNS para túneles GRE Ipv4 e Ipv6.	12.3(7)T, 12.2(25)S

Tabla 4.73 Cisco IOS requerido para la implementación de túneles sobre Ipv6.

4.10.2 Uso de Túneles en Ipv6.

Túneles

Consiste en encapsular un paquete IP dentro de otro, estos se utilizan en la actualidad sobretodo para crear redes privadas virtuales. Otra forma de utilizarlos es para enlazar nubes o islas IPv6 en una Internet basada prácticamente en su totalidad en IPv4.
Tenemos dos tipos básicos de túneles: estaticos y dinamicos. El 6bone actual esta formado en su mayoría por túneles estáticos.

Túneles Estáticos o Manualmente Configurados.

Esta es la solución más sencilla y la menos intrusiva si queremos tener acceso tanto a IPv6 como a IPv4. El caso más común seria un host con IPv4 que desee tener acceso a la red IPv6 existente. Para ello debería crear un túnel con un router a través de IPv4 que tenga tanto acceso a IPv6 como a IPv4. Un caso un poco menos común para el usuario es en el que se deseen unir redes IPv6, utilizando para ello la infraestructura IPv4 existente.
Este método se esta utilizando en la actualidad por parte de algunos proveedores de servicios para que cualquiera pueda tener acceso a la red IPv6.
Dentro de esta categoría podemos considerar también la de los servidores de túneles, que en estos momentos son interfaces web que permiten la creación de túneles bajo demanda a cualquier usuario.

Túneles GRE (Encapsulacion Genérica de Enrutamiento.

Esta técnica es utilizada para proveer los servicios necesarios para implementar cualquier estándar de encapsualacion punto a punto. Así como los túneles Ipv6 manualmente configurados, los túneles GRE son enlaces entre dos puntos, con un túnel separado por cada enlace. Los túneles no están sujetos a un determinado protocolo de transporte, pero en este caso llevan trafico Ipv6 como protocolo pasajero, GRE como el proveedor, siendo Ipv4 o Ipv6 el protocolo de transporte.
El principal uso de túneles GRE es para conexiones estables que requieren una comunicación segura entre dos routers fronterizos o entre un router fronterizo y un sistema final, ambos con soporte doble pila (dual snack).
GRE es un campo de protocolo que identifica al protocolo pasajero, el cual puede ser Ipv6 o IS-IS. El campo de protocolo es necesario para diferenciar el tipo de protocolo pasajero que lleva GRE.

Túneles 6to4.

Este mecanismo se puede aplicar para comunicar redes IPv6 aisladas por medio de la red IPv4. El router extremo de la red IPv6 crea un tunel sobre IPv4 para alcanzar la otra red IPv6. Los extremos del túnel son identificados por el prefijo del sitio IPv6. Este prefijo consiste en 16 bits fijos que indican que Sé esta utilizando la técnica 6to4 mas 32 bits que identifican al router externo del sitio.

Un efecto secundario de 6to4 es que deriva automáticamente un prefijo /48 de una dirección IPv4. De esta forma, los sitios pueden empezar a utilizar IPv6 sin solicitar nuevo espacio de direccionamiento a la autoridad competente.

Túneles 6over4.

Puede que no se tenga una red de sitio homogénea en el aspecto de que todos los nodos puedan comunicarse entre sí con la misma versión de protocolo IP.
Con este método se pueden comunicar nodos IPv6 aislados dentro de nuestro sitio con el resto de nodos IPv4. Esta técnica también se emplea en casos en los cuales el router IPv6 no tiene acceso o permiso para transmitir paquetes IPv6 sobre en enlace. Para realizar esta tarea se debe crear un enlace virtual utilizando un grupo multicast IPv4, mapeando las direcciones IPv6 sobre este grupo multicast.

Túnel ISATAP (Protocolo de Direccionamiento de Túnel Automático de Sitio).

Como su nombre indica, este método también esta pensado para la comunicación entre nodos de un mismo sitio. Tiene algunas ventajas respecto a 6over4, como que no necesita multicast IPv4 y que soluciona los problemas que se dan cuando una misma organización no tiene toda su red en un mismo lugar, como la baja escalabilidad en la agregación.

La técnica funciona empotrando la dirección IPv4 del nodo en el identificador EUI-64 de la interfaz. Puesto que este método viene a solucionar los problemas de comunicación dentro de un sitio, las direcciones IPv4 no tienen porque ser globales.
Esto significa que aunque exista NAT, el mecanismo seguirá funcionando correctamente.

4.10.3 Implementación de Túneles Ipv6.

Implementando Túneles Manuales en Ipv6.

Para la implementación de túneles manuales en Ipv6, se debe configurar una dirección Ipv6 en una interfase de túnel, y se deben configurar direcciones Ipv4 como origen y destino en el túnel. El host o el router que se encuentra a cada lado del túnel deben soportar los protocolos Ipv4 e Ipv6.

Los siguientes pasos se utilizan para configurar túneles en forma manual.

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **interface tunnel** *tunnel-number*
4. **ipv6 address** *ipv6-prefix*/ *prefix-length* [**eui-64**]
5. **tunnel source** {*ip-address* | *type number*}
6. **tunnel destination** *ip-address*
7. **túnel mode ipv6ip**

A continuación se presentan estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo privilegiado .
2	**configure terminal** **Ejemplo:** Router# configure terminal	Entra al modo de configuración global del router.
3	**interface tunnel** tunnel-number **Ejemplo:** Router(config)# interface tunnel 0	Especifica una interfase túnel y su numero, entra al modo de configuración del túnel.
4	**ipv6 address** ipv6-prefix/ prefix-length [**eui-64**] **Ejemplo:** Router(config-if)# ipv6 address 3ffe:b00:c18:1::3/127	Especifica una dirección Ipv6 asignada a la interfase y habilita el procesamiento Ipv6 en la interfase.
5	**tunnel source** { ip-address | type number}	Especifica la dirección Ipv4 de origen de la interfase túnel o el nombre de la interfase que utilizara como origen.

	Ejemplo: Router(config-if)# tunnel source ethernet 0	
6	**tunnel destination** ip-address **Ejemplo:** Router(config-if)# tunnel destination 192.168.30.1	Especifica la dirección Ipv4 del destino de la interfase túnel.
7	**tunnel mode ipv6ip** **Ejemplo:** Router(config-if)# tunnel mode ipv6ip	Especifica un túnel manual Ipv6 por medio del comando **túnel mode ipv6ip**, donde el protocolo Ipv6 es el pasajero y el protocolo Ipv4 es el de encapsulacion y transporte.

Tabla 4.74 Configuración de Túnel Manual.

Implementando Túneles GRE en Ipv6.

Cuando se configura un túnel GRE para Ipv6, direcciones IPv6 son asignadas al origen del tunel y al destino del túnel. La interfase túnel puede tener asignada cualquier tipo de dirección, ya sea Ipv4 o Ipv6. El Terminal o el enrutador que se encuentran a cada lado del túnel deben soportar ambos protocolos, Ipv4 e Ipv6.

Los siguientes pasos se utilizan para configurar un túnel GRE para Ipv6.

1. enable
2. configure {**terminal** | **memory** | **network**}
3. interface tunnel *tunnel-number*
4. ipv6 address *ipv6-prefix*/ *prefix-length* [**eui-64**]
5. tunnel source {*ip-address* | *ipv6-address* | *interface-type interface-number*}
6. tunnel destination {*host-name* | *ip-address* | *ipv6-address*}
7. tunnel mode {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ipv6** | **ipip** [**decapsulate-any**] | **iptalk** | **ipv6** | **mpls** | **nos**}

A continuación se encuentran estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo privilegiado.
2	**configure terminal**	Entra al modo de configuración global del

	Ejemplo: Router# configure terminal	router.
3	**interface tunnel** tunnel-number **Ejemplo:** Router(config)# interface tunnel 0	Especifica una interface tunel y su numero, entra al modo de configuración del túnel.
4	**ipv6 address** ipv6-prefix/ prefix-length [**eui-64**] **Ejemplo:** Router(config-if)# ipv6 address 3ffe:b00:c18:1::3/127	Especifica una dirección Ipv6 asignada a la interfase y habilita el procesamiento Ipv6 en la interfase.
5	**tunnel source** { ip-address | type number} **Ejemplo:** Router(config-if)# tunnel source ethernet 0	Especifica la dirección Ipv4 de origen de la interfase túnel o el nombre de la interfase que utilizara como origen.
6	**tunnel destination** ip-address **Ejemplo:** Router(config-if)# tunnel destination 2001:2312::3	Especifica la dirección Ipv4 del destino de la interfase túnel.
7	**túnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ipv6** | **ipip** [**decapsulate-any**] | **iptalk** | **ipv6** | **mpls** | **nos**} **Example:** Router(config-if)# tunnel mode gre ip	Especifica un túnel GRE Ipv6 por medio del comando **túnel mode gre ip**, y establece a GRE como protocolo de encapsulacion del túnel.

Tabla 4.75 Configuración de Túnel GRE.

Implementación e Túneles 6to4.

Cuando se utilizan túneles 6to4, el destino del túnel esta determinado por la dirección Ipv4 del router de borde, la cual es concatenada al prefijo 2002::/16, con el formato 2002:<Dirección Ipv4 del router de borde>::/48. El router de borde de cada lado del túnel 6to4 debe soportar los protocolos Ipv4 e ipv6.

Los siguientes pasos se utilizan para configurar túneles 6to4.

1. enable

2. configure {**terminal** | **memory** | **network**}

3. interface tunnel *tunnel-number*

4. ipv6 address *ipv6-prefix/ prefix-length* [**eui-64**]

5. tunnel source {*ip-address* | *type number*}

6. tunnel mode ipv6ip 6to4

7. exit

8. ipv6 route *ipv6-prefix/ prefix-length* **tunnel** *tunnel-number*

A continuación se presentan estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo privilegiado .
2	**configure terminal** **Ejemplo:** Router# configure terminal	Entra al modo de configuración global del router.
3	**interface tunnel** tunnel-number **Ejemplo:** Router(config)# interface tunnel 0	Especifica una interfase túnel y su numero, entra al modo de configuración del túnel.
4	**ipv6 address** ipv6-prefix/ prefix-length [**eui-64**] **Ejemplo:** Router(config-if)# ipv6 address 2002:c0a8:6301:1::1/64	Especifica la dirección Ipv6 asignada a la interfase y habilita el procesamiento Ipv6 sobre la interfase. Los 32 bits que siguen después del prefijo 2002: /16 corresponden a la dirección Ipv4 asignada al origen del túnel.
5	**tunnel source** { imp-address | type number} **Exempla:** Router(config-if)# tunnel source ethernet 0	Especifica la dirección Ipv4 de origen de la interfase túnel o el nombre de la interfase que utilizara como origen.
6	**tunnel mode ipv6ip 6to4** **Ejemplo:** Router(config-if)# tunnel mode ipv6ip 6to4	Especifica un tunel 6to4.
7	**exit** **Ejemplo:** Router(config-if)# exit	Sale del modo de configuración de la interfase y regresa al modo de configuración global de l router.
8	**ipv6 route** ipv6-prefix/ prefix-length **tunnel** tunnel-number **Ejemplo:** Router(config)# ipv6 route 2002::/16 tunnel 0	Configura una ruta estática para el prefijo 6to4 Ipv6 2002::/16 a través de la interfase túnel.

Tabla 4.76 Configuración de Túnel 6to4.

Implementación de Túneles ISATAP.

Cuando se configura un túnel ISATAP, la dirección de origen del túnel debe apuntar a una interfase con una dirección Ipv4 configurada. La interfase túnel Ipv6 debe ser configurada con una dirección EUI-64 modificada, ya que los últimos 32 bits del identificador de la interfase están formados por la dirección Ipv4 de origen del túnel.

Los siguientes pasos se utilizan para configurar un túnel ISATAP.

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **ipv6 address** *ipv6-prefix/ prefix-length* [**eui-64**]
5. **no ipv6 nd suppress-ra**
6. **tunnel source** {*ip-address* | *type number*}
7. **tunnel mode ipv6ip isatap**

A continuación se presentan estos pasos en forma detallada.

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo privilegiado .
2	**configure terminal** **Ejemplo:** Router# configure terminal	Entra al modo de configuración global del router.
3	**interface tunnel** tunnel-number **Ejemplo:** Router(config)# interface tunnel 1	Especifica una interfase túnel y su número, entra al modo de configuración del túnel.
4	**ipv6 address** ipv6-prefix/ prefix-length [**eui-64**] **Ejemplo:** Router(config-if)# ipv6 address 2001:0DB8:6301::/64 eui-64	Especifica la dirección Ipv6 asignada a la interfase y habilita el procesamiento Ipv6 sobre la interfase.
5	**no ipv6 nd suppress-ra** **Ejemplo:**	Él envió de anuncios Ipv6 del router es deshabilitado por defecto en las interfaces túnel. Este comando rehabilita dicha

	Router(config-if)# no ipv6 nd suppress-ra	acción.
6	**tunnel source** { ip-address | type number} **Ejemplo:** Router(config-if)# tunnel source ethernet 0	Especifica el nombre de la interfase que utilizara como origen.
7	**tunnel mode ipv6ip isatap** **Ejemplo:** Router(config-if)# tunnel mode ipv6ip isatap Specifies an IPv6 overlay tunnel using a ISATAP address.	Especifica un tunel ISATAP.

Tabla 4.77 Configuración de Túnel ISATAP.

Verificación de la Configuración de Túneles.

Los siguientes pasos se utilizan para verificar la configuración de cualquier tipo de túneles.

1. **enable**
2. **show interfaces tunnel** *number* [**accounting**]
3. **ping** [*protocol*] *destination*
4. **show ip route** [*address* [*mask*]]

PASO	COMANDO	PROPOSITO
1	**enable** **Ejemplo:** Router> enable	Habilita el modo privilegiado .
2	**show interfaces tunnel** number [**accounting**] **Ejemplo:** Router# show interfaces tunnel 0	Despliega información de la interfase Túnel. Se debe utilizar el argumento *number* para desplegar infurción de un túnel especifico.
3	**ping** [protocolo] destination **Ejemplo:** Router# ping 10.0.0.1	Diagnostica la conectividad Básica de la red.
4	**show ip route** [address [mask]] **Ejemplo:** Router# show ip route 10.0.0.2	Despliega el estado actual de la tabla de enrutamiento.

Tabla 4.78 Verificando la Configuración de Túneles.

4.10.4 Ejemplo de Configuración de un Túnel.

A continuación se muestra un ejemplo de configuración para un túnel manual, utilizando tres enrutadores, dos de ellos representando los nodos Ipv6 aislados y uno de ellos representando la nube Ipv4.

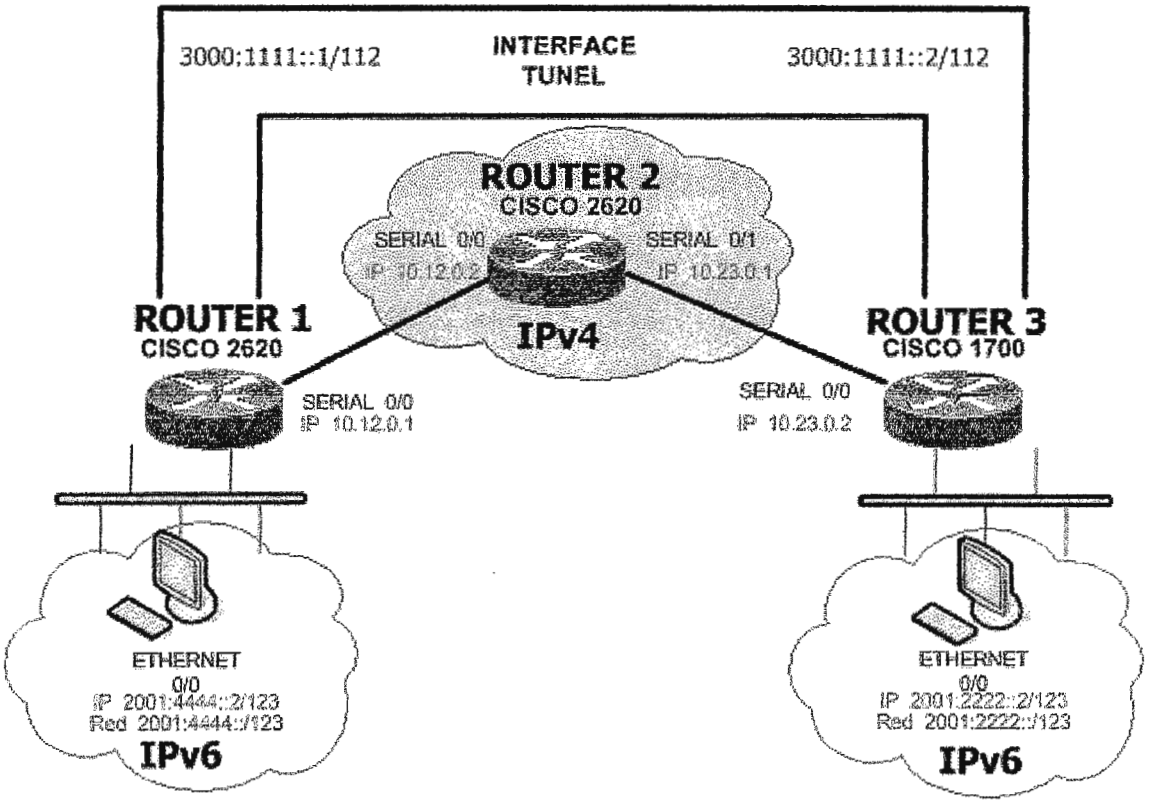


Figura 4.15 Implementación de Túnel Manual sobre Ipv6..

A continuación se muestran los comandos de configuración para cada uno de los enrutadores.

ROUTER1

```
ipv6 unicast-routing

interface Tunnel0
no ip address
ipv6 address 3000:1111::1/112
tunnel source Serial0/0
tunnel destination 10.23.0.2
tunnel mode ipv6ip
```

```
interface Serial0/0
ip address 10.12.0.1 255.255.255.252

interface FastEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address 2000:4444::1/112

router ospf 1
log-adjacency-changes
network 10.23.0.0 0.0.0.255 area 0
```

ROUTER2

```
interface Serial0/0
ip address 10.12.0.2 255.255.255.0
clockrate 64000

interface Serial0/1
ip address 10.23.0.1 255.255.255.0
clockrate 64000

router ospf 1
log-adjacency-changes
network 10.23.0.0 0.0.0.255 area 0
network 10.12.0.0 0.0.0.255 area 0
```

ROUTER3

```
ipv6 unicast-routing

interface Tunnel0
no ip address
ipv6 address 3000:1111::2/112
tunnel source Serial1/5
tunnel destination 10.12.0.1
tunnel mode ipv6ip

interface Serial0/0
ip address 10.23.0.2 255.255.255.252

interface Ethernet0/0
no ip address
half-duplex
ipv6 address 4000:2222::1/112

router ospf 1
log-adjacency-changes
network 10.12.0.0 0.0.0.255 area 0
```

4.11 ESTUDIO PARA LA IMPLEMENTACION DE IPV6 EN LA RED DE LA UNIVERSIDAD DON BOSCO

Los esfuerzos de desarrollo e implementación de productos Ipv6 están disponibles en la comunidad desde hace algunos años. Esta característica contribuye al desarrollo y adopción de esta nueva tecnología. De esta manera redes Ipv6 han nacido en diferentes países del planeta, manteniendo siempre la prestación de los servicios proporcionados por Ipv4 a los usuarios.

Otro factor importante es que los recursos de Internet (como bloques de direcciones Ipv6) ya están disponibles y en ciertos casos ya han sido asignados.

La IANA ha dispuesto a cada uno de los Registros Regionales de Internet (LACNIC, ARIN, RIPE, AFRINIC, APNIC) bloques Ipv6 /29 para su gestión. Todo esto sugiere que la línea de vida de Ipv6 ha superado al menos los pasos básicos de aceptación, que con una debida promoción y publicación, se espera sea adoptado en las próximas décadas.

De acuerdo a lo anterior, ha nacido el interés de realizar un estudio previo, para la implementación del protocolo Ipv6 en la Universidad Don Bosco.

Objetivo.

Implementar una estructura de red Ipv6 paralela, que provea un manejo eficiente de aplicaciones y provea soporte a posibles proyectos a mediano plazo de la red de la Universidad Don Bosco.

Topología de la Red de la UDB

La red de la Universidad Don Bosco presenta una topologia de estrella, la cual se muestra a continuación:

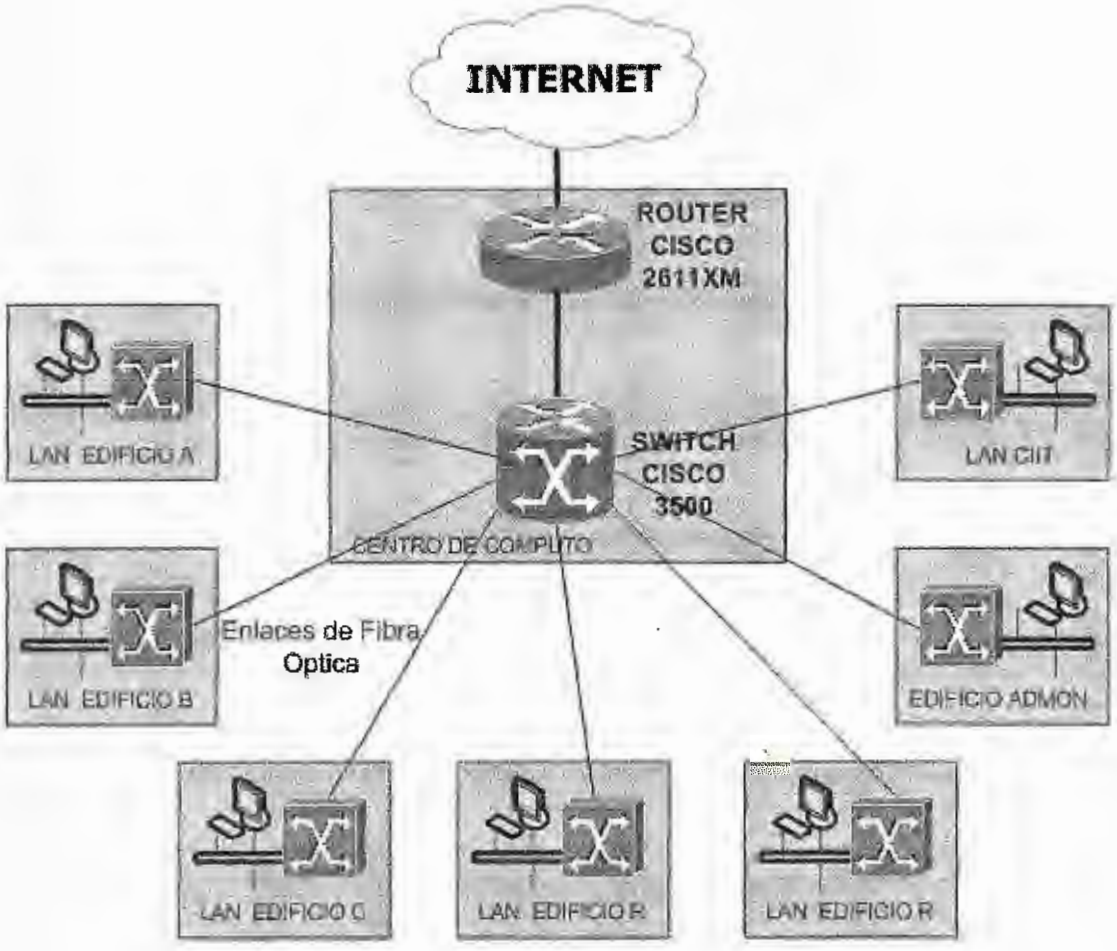
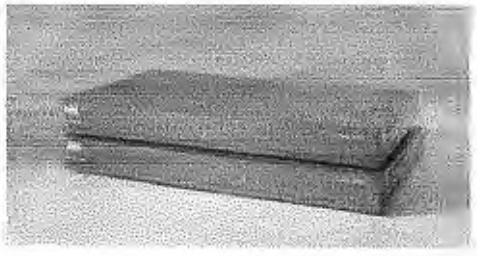


Figura 4.16 Red de Universidad Don Bosco

Por medio del esquema se puede observar que la red de la universidad Don Bosco posee una topología de estrella, en la cual se ocupan dispositivos de capa de enlace (switches) para brindar acceso a la red. Los dispositivos de capa de enlace no verifican los paquetes de capa de red, por ejemplo los de Ipv6. Por lo tanto los dispositivos de capa de enlace son indiferentes al soporte de ipv6.

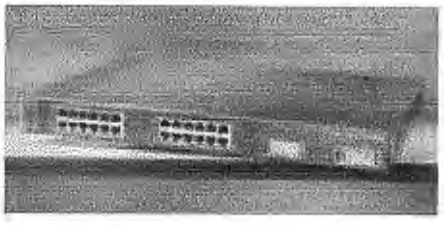
Lo que se debe tomar en cuenta es que el enrutador (dispositivo de capa de red) y las computadoras pertenecientes a las LAN, posean versiones de Sistema Operativo que brinden soporte a Ipv6.

Características del Router Cisco 2611.



- Posee la versión 12.3T del Sistema Operativo de Cisco, la cual provee soporte para Ipv6.
- Posee un Slot de Modulo de Red.
- Posee 2 puertos FastEthernet 10/100BaseT.
- Posee 2 slots para tarjetas WIC. (WAN)
- Posee un Modulo de Integración Avanzada (AIM).

Características del Switch 3550



- Posee 24 puertos Ethernet 10/100 BaseT
- Posee 2 puertos Gigabit Ethernet 10/100/1000
- El switch trabaja en la capa de enlace, por lo tanto no hay ningún problema con respecto al soporte de Ipv6.

Se debe aclarar que esta implementación no busca reemplazar servicios Ipv4 existentes. La adopción exitosa de cualquier nueva tecnología depende de la fácil integración con la infraestructura existente sin interferir significativamente los servicios presentes. Con la implementación se pretende mantener la plataforma dual sobre Ipv4 e Ipv6.

ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACION DE IPV6 .

El presente estudio muestra los diferentes requerimientos necesarios para la implementación del protocolo Ipv6 en la red de la Universidad Don Bosco. Además se presentan los costos financieros que implican la realización de dicho proyecto, para ser analizados con respecto a la disponibilidad de recursos económicos.

Requerimientos Humanos.

Para todas las personas que se encuentren involucradas en la implementación de Ipv6, ya sea internas o externas a la Universidad, será imperativo que tengan un amplio conocimiento de la tecnología de redes.

Si bien Ipv6, es una tecnología relativamente nueva y pudiese no contar del alto conocimiento por parte de la sociedad que eventualmente se integre a esta idea de implementación, esta es un paso de evolución a partir del protocolo Ipv4.

De cualquier forma es necesario fortalecer ciertos conceptos y practicas anunciadas a continuación:

- Conocimiento amplio de tecnologías de redes (Snack de protocolos TCP)
- Conocimientos del Protocolo Ipv6.
- Protocolos de Enrutamiento para Ipv6 (IGP y EGP).
- Funcionalidades y Utilidades relativas a Ipv6 (Multicast, ICMPv6, Seguridad, entre otros)
- Conocimientos de Calidad de servicio (RSVP, MPLS entre Otros).

Para poder transferir estos conocimientos a las personas que localmente implementaran el proyecto, se necesita una capacitación previa en cuanto al uso del protocolo Ipv6. Por lo tanto es necesario que se imparta un curso para las personas involucradas en el mismo.
Los aspectos fundamentales dentro del Curso de Ipv6 son:

- Protocolo IP versión 6.
- Direccionamiento
- Enrutamiento
- Autoconfiguración
- Migración a IPv6.
- Seguridad. ICMP
- Taller de IP versión 6.
- Demostración del funcionamiento del Protocolo IP versión 6.
- Arquitecturas propuestas para mejorar la Calidad de Servicio (QoS) en Internet.
- RSVP/RTP/RTCP y servicios integrados
- Servicios diferenciados
- MPLS
- Ingeniería de tráfico y Encaminamiento basado en restricciones

El contenido de este curso tiene un valor de $100 por participante e incluye material didáctico y una certificación. Este curso es impartido por Ingenieros de la empresa INICTEL en Perú y tiene aproximadamente un tiempo de duración de 3 días.

A continuación se presenta una tabla con los costos necesarios para la capacitación del personal de la Universidad Don Bosco que se encargaría de la implementación del proyecto.

PERSONAL A CAPACITAR	COSTO
Ing. Carlos Bran	$100
Ing. Erick Flores	$100
TOTAL	$200

Tabla 4.79 Costos para Curso de Ipv6.

Tiempo de Implementación.

Tomando en cuenta las actividades a realizar para optimizar la red para el soporte Ipv6, se ha determinado un tiempo estimado de implementación de 2 meses.

El tiempo de implementación, depende también de la disponibilidad para la solicitud de bloques de direcciones IPv6 que deben ser solicitadas al Proveedor de Servicios de Internet Local (ISP). Hasta el momento, ningún ISP en nuestro país tiene asignado un bloque de direcciones Ipv6 por LACNIC; esto obstaculiza la implementación temprana del protocolo en la Universidad Don Bosco.

Requerimientos de Hardware.

Ipv6 ha sido implementado para diferentes dispositivos de red en diferentes casas de hardware muy conocidas. De esta manera se han dispuesto productos al público con soporte para Ipv6 entre los que podemos mencionar:

PROVEEDOR	PRODUCTOS	VERSION DE IOS PARA IPV6
Cisco	Todos	A partir del IOS 12.2(2)T.
Novell	Todos	A partir de Netware6
3Com	Routers NetBuilderII y PhatBuilder S500	Software Version 11.0
Nortel	Todos	A partir de BayRS version 12.0
Hitachi	Familia de Routers GR2000 GB	-
6Wind	Serie 6WIND gate 6200	-

Tabla 4.80 Dispositivos de Red con soporte para Ipv6

Como se ha mencionado anteriormente la Universidad Don Bosco posee el equipo de red necesario con soporte para Ipv6; ya que anteriormente la red de la Universidad poseía un Router Cisco 2550 con un Sistema Operativo que no proveía dicho soporte y actualmente ya se obtuvo un Router Cisco 2620 con la capacidad de dar soporte a Ipv6.

Por la topología de red, que se encuentra basada principalmente en el uso de switches, independientes al protocolo de red que transportan, se puede afirmar que no se necesita comprar otro dispositivo de red adicional y que la red esta lista para soportar Ipv6 en cuanto a equipo se refiere.

Requerimientos de Software.

Para implementar Ipv6 sobre una red existente, solamente se necesita que los dispositivos de red que componen la red tengan soporte para Ipv6, generalmente esta característica esta asociada a la versión del sistema operativo que posean dichos dispositivos, mientras mas reciente es la versión hay mayor probabilidad de que soporte Ipv6.

Los sistemas Operativos de Terminales que actualmente proveen soporte para IPv6 son:

- Windows XP. Requiere que el usuario habilite el servicio. Comandos de configuración y diagnostico en ventana de comandos

- MacOS X. Soporte transparente del usuario y tiene una interfase gráfica para configuración automática o manual.

- Unix.
  Linux: cada distribución provee herramientas para administrar la configuración.
  Solaris: completamente integrado en las últimas 3 versiones.

- Windows 2000 (Servy Pack 4). Este Sistema Operativo no tiene soporte para Ipv6 en forma nativa; pero existe un parche que puede ser instalado para que reconozca el protocolo Ipv6.

Algunas de las Aplicaciones que poseen soporte Ipv6 en ambientes operativos, se muestran en la siguiente tabla.

SERVICIO	ESPECIFICACION	EJEMPLOS SUGERIDOS
DNS	RFC 1886 Y RFC 2874	BIND9
MAIL	RFC 2821	PostFix (Parche), SendMail 8.10.0
HTTP (Web)		Servidores: • Apache 2.0 o mas Reciente • IIS 6.0 o mas reciente. Clientes: • Mozilla 5.0 (Linux) • Internet Explorer 4 (Windows)
FTP	RFC 2428	Servidores: Libra FTP Server. Clientes: • NcFTP. LFTP 2.0.x

Tabla 4.81 Aplicaciones con soporte Ipv6.

Para la actualización de los Sistemas Operativos con soporte para Ipv6, se ha determinado el número de computadoras que forman parte de la red de la Universidad Don Bosco, además de las que requieren dicha actualización. Estos datos se presentan en la tabla 4.82.

NUMERO DE COMPUTADORAS EN LA RED DE LA UDB	
LUGAR	**NUMERO**
LABORATORIO DE CISCO1	19
LABORATORIO DE CISCO2	6
EDIFICIO ELECTRONICA	9
CENTRO DE COMPUTO SALON1	79
CENTRO DE COMPUTO SALON2	30
CENTRO DE COMPUTO SALON3	20

PROFESORES CENTRO DE COMPUTO	10
BIBLIOTECA	5
EDIFICIO B	9
EDIFICIO C	20
EDIFICIO R	12
EDIFICIO DE COMUNICACIONES	7
MATLAB	13
LABORATORIOS DE FISICA	3
TOTAL	242

Tabla 4.82 Cantidad de Computadoras en la red de la UDB.

De acuerdo al estudio realizado en la universidad Don Bosco, los Sistemas Operativos que poseen las computadoras que pertenecen a la red, se muestran en la siguiente tabla.

SISTEMA OPERATIVO	PORCENTAJE	NUMERO DE PC'S
Windows XP	20%	49
Windows 2000	65%	157
Windows 98	13%	31
Linux	2%	5
TOTAL	100%	242

Tabla 4.83 Sistemas Operativos Actuales en las LAN.

Se debe tomar en cuenta que no todas las terminales que forman parte de la red de la Universidad Don Bosco poseen soporte para Ipv6, como se muestra en la tabla 4.79; ya que existe un 78% de las terminales que poseen Sistemas Operativos que no soportan el protocolo Ipv6 (Windows 98 y Windows 2000 profesional).
De esta manera, solamente se debe incurrir en gastos para obtener las licencias de software para las maquinas en que se va actualizar el Sistema Operativo.

El Sistema Operativo a instalar será Windows XP Professional y la licencia de este software según el plan de Volumen Abierto de Microsoft (Instituciones Educativas que compran más de cinco licencias) tiene un precio de 85 dólares por cada computadora a actualizar, precio obtenido desde la página Web de la empresa Microsoft en Internet.

Como podemos observar en la tabla 4.80, un 78% de las computadoras existentes en la red de la UDB no posee soporte para Ipv6 actualmente, este porcentaje corresponde a un número de computadoras igual a 188.

Para ahorrar gastos, las maquinas que poseen el Sistema Operativo de Windows 2000 Profesional que representan un 65 % (157 PC's) pueden ser actualizadas por un parche gratuito en Internet para el soporte Ipv6; el cual puede ser bajado desde el link:
http://msdn.microsoft.com/downloads/sdks/platform/tpipv6.asp

Por lo tanto los gastos de licencias de software que se tendrían para actualizar las PC's que poseen Windows 98 (Correspondientes a un total de 31 computadoras), se muestran a continuación:

LICENCIA	NUMERO	COSTO UNITARIO	TOTAL
Microsoft Windows XP Profesional	31	$85	$2,635

Tabla 4.84 Costos por licencias de Software.

Beneficios y Valor Agregado.

Los beneficios y oportunidades que ofrecerá la implementación de esta nueva tecnología son directamente heredados de las características positivas del protocolo. Sin embargo existen ganancias extrínsecas que forman parte del beneficio organizacional. Un ambiente esperado de la implementación ofrecería condiciones como:

- Dotación de tecnología de punta para la red académica.
- Estimulación de estudios de investigación e implementación de nuevas tecnologías.
- Provisión de plataformas estables donde se logren desempeños óptimos para aplicaciones de tiempo real.
- Sencillez en el manejo de las redes.

Entre algunos proyectos que podrían ser implementados en la Universidad Don Bosco a mediano plazo, se encuentran:

- Acceso a Internet2. Consiste en poseer los requerimientos necesarios para poder integrarse a la red de Internet2, la cual es una red avanzada que posee objetivos educativos y de desarrollo

de nuevas aplicaciones. Además se puede utilizar el protocolo Ipv6 para conectarse a la misma y tener acceso a redes Ipv6 actuales.

- Videoconferencia sobre Ipv6. Proveer una infraestructura multicast y de alto desempeño para lograr reenvió de voz y video en condiciones aceptables, incluyendo las ventajas que provee el protocolo Ipv6. Este proyecto podría ser implementado sobre la red académica y sitios fuera de la misma.

- Telefonía IP. Promover servicios de telefonía IP para las redes internas de la organización, obteniendo una baja en los costos que este servicio aplica.

- WIFI. Desplegar una infraestructura de red inalámbrica dentro del campus de la Universidad.

Los proyectos de telefonía y videoconferencia necesitan plataformas eficientes que logren el reenvío del tráfico de voz y video en tiempo real. Por otro lado, el proyecto WIFI necesita el establecimiento de una red con un soporte eficiente de seguridad ya que en varios casos dichas redes serán dispuestas para uso privado.
Para el desarrollo de estos Proyectos se demandan características de tratamiento especial, para las cuales la condición actual de la red de la UDB no seria la más eficiente. Por lo tanto se ve la necesidad de plantear una infraestructura basada en capa de red robusta y multifuncional que pueda soportar dichas demandas. La solución esta estimada en el despliegue de una plataforma IPv6 donde se pueda tomar provecho de las virtudes que este protocolo puede ofrecer.

Resumen de Costos para la Implementación de Ipv6 en la UDB.

La siguiente tabla muestra el resumen de costos que implica la implementación del Protocolo Ipv6 en la red de la Universidad Don Bosco.

CONCEPTO	COSTO
LICENCIAS DE SOFTWARE	$2,635
CURSO DE IPV6	$200
TOTAL	$2,835

Tabla 4.85 Resumen de Costos del Proyecto.

4.12 IMPACTO EN LA TRANSICION DE IPV4 A IPV6.

El camino de IPv4 a IPv6 no es una simple transición o migración, es un proceso de evolución e integración que requiere de una preparación y de un mejoramiento de las redes. Esto implica entre otras cosas la preparación del personal técnico y de los usuarios, así como la implantación de equipamiento, sistemas operativos y aplicaciones que cumplan las especificaciones IPv6 sin dejar de cumplir las de IPv4.

IPv6 será progresivamente percibido como una prioridad estratégica, más que todo por su influencia como interfaz de valor agregado, que por la arquitectura de su plataforma técnica, con la que se identifica actualmente y ha sido demostrada en este documento.

Algunos impactos que puede causar el protocolo Ipv6 sobre las redes actuales (Ipv4) en forma general, se mencionan a continuación:

- IPv6 puede revitalizar al mundo económico por medio de aplicaciones innovadoras de valor agregado y los nuevos contenidos que surjan en consecuencia.

- IPv6 ofrece redes más seguras y robustas de extremo a extremo que las que ofrece IPv4; ya que el uso del Traductor de Direcciones de Red (NAT) limita esta característica.

- Ipv6 brinda una gran cantidad de direcciones IP disponibles para todos los usos imaginables, suficientes como para ser asignadas a nuevas tecnologías y aplicaciones en todo el mundo como: Computadoras de bolsillo (Pocket PC), Reproductores de música MP3, Televisión sobre Ip (TVoIP), etc. Esto puede contribuir significativamente tanto al desarrollo sostenible como a la reducción de la brecha digital tal como la conocemos hoy en día. Nuevos tipos de brechas pueden ser un tema de discusión el día de mañana. Ipv6 ofrece autonomía infinita de direcciones para todas las personas.

- La nueva característica de autoconfiguración representa una ventaja para el usuario, ya que facilita su conexión en la red, de forma Plug & Play (conectar y operar).

- Es necesario que tanto el administrador de la red, como el usuario final tengan conocimiento del uso del protocolo Ipv6 de lo contrario esto podría causar un impacto negativo en la administración de las aplicaciones.

4.13 SERVIDOR WEB CON SOPORTE PARA IPV6.

Para poder crear un Servidor Web sobre Ipv6 necesitamos un software que funcione como servidor http y que soporte direcciones Ipv6. A continuación se presentan dos soluciones para la instalación de un Servidor Web Ipv6, una para Windows y otra para Linux.

Pasos para Instalar un Web Server para Ipv6 en Windows.

1) Se debe Tener el Programa Foxserv3. (Este programa instala Apache,PHP y MySql de una vez)
(Puedes instalar la versión 1 si lo deseas, en la página web de foxserv)
Este programa puede ser bajado desde este link:
http://easynews.dl.sourceforge.net/sourceforge/foxserv/FoxServ3.1Beta1.exe

2) Se debe ejecutar el programa y seguir los pasos de instalación. Se pedirá un email y un password para registrarte en el Mysql. (Se debe especificar un correo electrónico).

3) Después de haber instalado el Foxserv. Se debe ir a :
-Inicio
-Programas
-FoxServ
- Dar Click en Apache para poner a correr el servidor.
- Se debe hacer lo mismo para el winMySqlAdmin (pone a correr Mysql)

4) Posteriormente se entra a :
-Mi PC
-C:
-Foxserv
-www
- Se borra la pagina index.html por defecto (vacía la carpeta www) y se crea una pagina que se llame index.html y la ubicas dentro de esta carpeta, así se podrá ver la que defina el usuario.

5) Para verificar si tenemos conectividad con nuestra pagina, debos abrir el Internet Explorer y escribir http://localhost para ver la página de inicio. Si después de esto se observa la pagina que se ha creado; significa que ya puede ser accesado el servidor desde otra maquina dentro de la red (La maquina server debe poseer una dirección Publica).

Pasos para Instalar un Servidor Web para Ipv6 en Linux.

1) Se debe bajar el servidor Apache (httpd-2.0.50-i686-pc-linux-gnu.tar.gz)para Linux con soporte ipv6. Desde el link:

http://www.apache.org/dist/httpd/binaries/linux/

2) Para instalar el apache se debe dar doble clic al archivo install-bindist.sh que se encuentra dentro de la carpeta httpd-2.0.x.

3) Después de haber instalado el Apache para Linux se debe buscar el directorio donde se ubicara nuestra página web.

Así:

- Dar doble click en Computer.
- File System.
- Var
- WWW
- html
- Se elimina el contenido de la carpeta html y se ubica el archivo index.html que nosotros deseamos en ese directorio, el cual será nuestra pagina web por defecto.

4) Para verificar si tenemos conectividad con nuestra pagina, debos abrir el Internet Explorer y escribir http://localhost para ver la página de inicio. Si después de esto se observa la pagina que se ha creado; significa que ya puede ser accesado el servidor desde otra maquina dentro de la red (La maquina server debe poseer una dirección Publica).

CONCLUSIONES

- El protocolo Ipv6 se encuentra desarrollado óptimamente para soportar las diferentes configuraciones de protocolos de enrutamiento como: OSPF, RIP, IS-IS. Proporcionando una manera similar y sencilla de configurarlos al igual que el protocolo Ipv4, dentro de la plataforma Cisco; la cual fue la utilizada en esta tesis para la realización de pruebas.

- El espacio de direcciones y el esquema de direccionamiento es la ventaja más representativa que posee el protocolo Ipv6 sobre el protocolo Ipv4. Ya que fue comprobada la amplitud del espacio de direcciones, su nomenclatura y la forma jerárquica en que se pueden utilizar.

- Los desarrolladores de software se han preocupado por crear aplicaciones con soporte para Ipv6 y hasta la fecha, existen muchas aplicaciones que son de gran utilidad para las empresas; como servicios Web, servicios de transferencia de archivos (FTP), servicios de correo electrónico, software de video conferencia, etc.

- Se han comprobado los atributos que provee Ipv6, con respecto a la auto configuración de terminales, el soporte nativo de Ipv6 con Ipsec, el gran espacio de direcciones, calidad de servicio y los métodos de transición entre Ipv6 e Ipv4, como son los túneles y el protocolo Dual Stack.

- Ipv6 es un protocolo funcional que puede ser implementado en cualquier red, siempre y cuando esta cumpla con los requerimientos de hardware y software con soporte para Ipv6. Además, es fundamental la factibilidad económica que se tenga para la optimización de la red y la preparación técnica que posea el usuario para el manejo y conocimiento del protocolo.

- La presencia del protocolo Ipv6 en nuestra región es mínima, ya que nuestro país esta muy limitado en cuanto al estudio y desarrollo de nuevas tecnologías y en las empresas privadas no hay un trato especial para las mismas. Lo contrario sucede en otros países mas desarrollados tecnológicamente donde ya existen redes Ipv6 nativas que dan soporte para aplicaciones de nueva generación.

RECOMENDACIONES

- Para descubrir más aplicaciones y ventajas del protocolo Ipv6 es necesario que se siga experimentando con el mismo en ambientes de prueba. Por lo tanto se recomienda un seguimiento en cuanto al desarrollo del protocolo Ipv6.

- Después del estudio realizado en la Universidad Don Bosco, se determino que esta tiene la capacidad de implementar Ipv6 en su red, para estar preparada para el tratamiento de aplicaciones de nueva generación, para la migración que en algún momento se dará y para la familiarización con el protocolo. Todo esto debe estar sujeto a la capacidad económica que se tenga para el proyecto y a la disponibilidad de recursos humanos, hardware y software.

- Después de haber implementado Ipv6 sobre una red, es necesario capacitar al usuario para el uso del protocolo, en aspectos generales como el establecer una dirección Ipv6 en su maquina, el uso del comando "ping6" y el formato de direcciones. Esto ayudara a solventar y reducir más fácilmente problemas típicos de conectividad en la red.

- El equipo utilizado para la realización de pruebas en este documento posee un soporte óptimo para el desarrollo de aplicaciones con Ipv6; pero no se pretende influir en el usuario para la utilización del mismo, ya que existen otros proveedores que presentan un excelente soporte para Ipv6.

BIBLIOGRAFIA

- IPv6: The New Internet Protocol.
  Christian Huitema.
  Prentice Hall, 1997.

- Implementig IPv6.
  Mark A. Miller.
  IDG Books. (2nd Edition July 1999).

- Internet Working Ipv6 for Cisco Routers.
  Silvano Gai.
  Mc Graw Hill, 1998 (1o.Edition)

- Titorial de Ipv6.
  Jordi Palet Martinez
  Consulintel.

- Internet Protocol, Version 6
  S. Deering and R. Hinden. RFC 2460:
  (IPv6) specification, December 1998.

- Internetworking Ipv6 with Cisco Routers.
  Silvano Gai.
  McGraw-Hill, 1998.

- Understanding Ipv6 addressing.
  Peter H. Salus.
  AP Professional, 1999 (1o. Edition)

ANEXOS

1. Objetivos

Objetivo General

Presentar una solución de acceso exclusivo de Internet2, para clientes del sector Educación en El Salvador.

Objetivos Específicos

- Proveer una solución de acceso a Internet2 exclusivo para clientes del sector Educación que solicitan conexión directa a la red mundial de internet2.
- Determinar los elementos necesarios para la implementación de un sistema de acceso a Internet de esta índole.
- Proveer los costos generales y los elementos críticos para determinar los costos totales para un cliente en particular.

2. Alcance

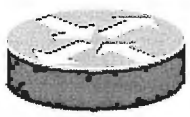
El presente documento muestra una guía para la implementación de una red de acceso a Internet2.

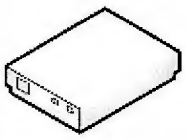
3. Definiciones , acrónimos y símbolos

Ip_wan_backbone(Ip_wan_bb): Se refiere a la dirección IP WAN del backbone, la cual es configurada en la interface serial del Switch de Backbone.
IP_wan_cliente(Ip_wan_cl): Dirección IP WAN del cliente, equivalente a la asignada al backbone menos 1, que se configura en la interface serial del router del cliente.
Wan_ip_mask: Máscara de la subred de WAN, en todos los casos es 255.255.255.252.
Lan_ip_add: Dirección IP asignada al router de cliente en la interface LAN.
Lan_ip_mask: Máscara de la subred asignada a la interface LAN de router de cliente.
Lan_ip_net: dirección de red de la subred asignada a la interface LAN del router de cliente.
VLAN: son redes virtuales de área local, configuradas dentro de los switches, que hacen una agrupamiento lógico para poder compartir pequeños dominios de broadcast.
HDSL: Tecnología DSL de alta tasa de bits que se usa para la transmisión en banda ancha entre la compañía de telefonía y un cliente.


Switch


Red


Router


Modem HDSL

4. Responsabilidades

Ingeniería de Red: Realiza la planeación y diseño de la creación y expansión de la infraestructura de telecomunicaciones para servicios y redes empresariales.

Ingeniería Proyectos de red: Encargado de la ejecución de los proyectos de infraestructura y redes empresariales.

Ingeniería de Clientes: Asigna los recursos de puertos necesarios en el backbone, para el servicio contratado para su instalación.

Network Operations Center: Gestiona el Acceso a las Centrales, Notifica Interrupción a Clientes y áreas involucradas y realiza configuraciones de red.

Soporte Técnico a Ventas: Personaliza las soluciones para cada cliente en particular, tomando como referencia los costos y diseños descritos en el presente documento.

5. Situación Actual

¿Qué es Internet2?

El proyecto Internet2 (I2) es un esfuerzo de colaboración para desarrollar tecnología y aplicaciones avanzadas en la Internet, vitales para las misiones de investigación y educación de las instituciones de educación superiores. Más de 200 universidades estadounidenses, trabajando con la industria y el gobierno, encabezan este proyecto Internet2. Internet2 trabaja para hacer posibles aplicaciones tales como la telemedicina, bibliotecas digitales y laboratorios virtuales que no serían posibles con la tecnología del Internet de hoy. Como proyecto de la Corporación Universitaria para el Desarollo Avanzado de la Internet (UCAID), el proyecto Internet2 no es una simple red aparte, sino que une las aplicaciones de la red y los esfuerzos de desarrollo en ingeniería con redes avanzadas de universidades, regionales y nacionales.

¿Cómo beneficiará la Internet2 a los usuarios de la Internet actuales?

De la misma forma que la Internet de hoy salió de las redes de investigación federales y académicas en la década de 1980, la Internet2 está ayudando a desarrollar y probar nuevas tecnologías, como Ipv6, el multicast y la calidad de servicio (QoS) que hará posible una nueva generación de aplicaciones de Internet. Esto en resumidas cuentas, beneficiará a todos los sectores de la sociedad. Lo sensato de este plan ha sido comprobado por la aparición de la Internet de hoy de entre las redes de investigación académicas y federales de los ochenta. Internet2 repetirá este éxito para el nuevo milenio al conectar la comunidad universitaria con el desarrollo de la red de comunicación electrónica pre-comercial.

RAICES (Red Avanzada de Investigación, Ciencia y Educación Salvadoreña) es una asociación privada sin fines de lucro, constituida en la actualidad por las varias Instituciones Educativas, las que estarían formando parte de la red interna nacional, siendo estas las siguientes:

Universidad Centroamericana José Simeón Cañas (UCA)
Universidad Don Bosco (UDB)
Universidad Tecnológica (UTEC)
Universidad Francisco Gavidia (UFG)

Universidad Dr. José Matías Delgado (UJMD)
Universidad Politécnica (UPES)
Universidad Católica de Occidente (UNICO)
Universidad de El Salvador (UES)
Instituto Tecnológico Centroamericano (ITCA)

RAICES necesita un servicio que le proporcione conectividad entre los miembros de la asociación para poder tener acceso a la red de Internet2.
El Internet Dedicado tradicional se establece por medio del protocolo IPv4, esta fue la primera versión del protocolo que se implemento extensamente, y forma la base de Internet.
IPv4 usa direcciones de 32 bits, limitandola a 4.294.967.296 direcciones únicas, muchas de las cuales están dedicadas a redes locales(LANs). IPv4 en la actualidad presenta algunas limitaciones al funcionamiento de las redes actuales y futuras, tales como:

Escasez de direcciones IP.

- Menos direcciones disponibles.
- Limita el crecimiento de Internet.
- Hoy en día el ruteo es ineficiente.
- Provoca que los usuarios utilicen NAT.

Como una solución a las limitaciones de IPv4, el IETF(Internet Enginnering Task Force), creo el proyecto Ipng(IPv6). Con la nueva versión del protocoló, las direcciones constan de 128 bits. Esto significa, entre otras cosas, que soluciones al agotamiento de direcciones IPv4, como el NAT, no serán necesarias.
Podemos decir que una desventaja de estas nuevas direcciones es su dificultad para recordarlas dado su tamaño. Es de suponer que el servicio DNS tendrá más importancia aún.

Cuando un nodo se conecta a la red, este recibe los datos necesarios para empezar a comunicarse por parte del router: dirección IPv6, mascara de red y rutas. Hay que recordar que este nuevo protocolo trata de simplificar. Con IPv4 tenemos el DHCP (Dynamic Host Configuration Protocol, Protocolo de Configuración Dinámica de Nodo) para conseguir algo equivalente.

Con esta funcionalidad podremos saltar de una red a otra sin apenas percibir ningún cambio. Si bien esto ya era posible con IPv4 de una manera más bien ardua, en IPv6 fue una de los requerimientos del diseño.

La seguridad fue otro de los requerimientos del diseño del nuevo protocolo: todas las aplicaciones se deben beneficiar de las facilidades de autenticación y encriptación de datos de forma transparente. El estándar escogido para esto es el Ipsec.

El encaminamiento bajo IPv6 es bastante similar al de IPv4, es decir, jerárquico y sin clases. Con esto se pretende conseguir que las entradas en las tablas de rutas en los backbones no abunden más de lo necesario. Al mismo tiempo, se consigue simplificar el enrutamiento y se espera que los routers sean más rápidos.

Si bien con IPv4 tenemos unos pocos bits para el control del tipo de servicio, ToS, con IPv6 disponemos de campos más amplios para definir la prioridad y flujo de cada paquete. Según el contenido de este campo, el router deberá darle un trato más o menos especial.

La cabecera de un paquete IPv6 es más sencilla que la del paquete IPv4. La cabecera de un paquete IPv4 es variable, por lo que necesita un campo de tamaño. Sin embargo, para simplificar la vida de los routers, IPv6 utiliza un tamaño de cabecera fijo de 40 bytes, que componen un total de ocho campos:

- Versión (4 bits), sirve para que el router se entere de que es un paquete IPv6.
- Dirección origen y de destino (128 bits cada una), son las direcciones de los nodos IPv6 que realizan la comunicación.
- Clase de tráfico (8 bits), para poder diferenciar entre servicios sensibles a la latencia, como VoIP, de otros que no necesitan prioridad, como tráfico http.
- Etiqueta de flujo (20 bits), permite la diferenciación de flujos de tráfico. Esto tiene importancia a la hora de manejar la calidad de servicio (QoS)
- Siguiente cabecera (8 bits), este campo permite a routers y hosts examinar con más detalle el paquete. A pesar de que el paquete básico IPv6 tiene cabecera de tamaño fijo, el protocolo puede añadir más para utilizar otras características como encriptación y autenticación.

Ventajas del IPv6:

Es más seguro.
Es mejor para las redes inalámbricas.
Ofrece mejor QoS.
Mejor soporte al trafico Multimedia en tiempo real.
Es el único que soporta auto configuración.
Resuelve el escalonamiento en el ruteo.
Proporciona mejor soporte para una rápida renumeración de prefijos.
Aplicaciones Multicast y Anycast.

6. Elementos de la Red de Acceso

La red de acceso a Internet2 para clientes de RAICES, posee la estructura mostrada en la figura 6.1.

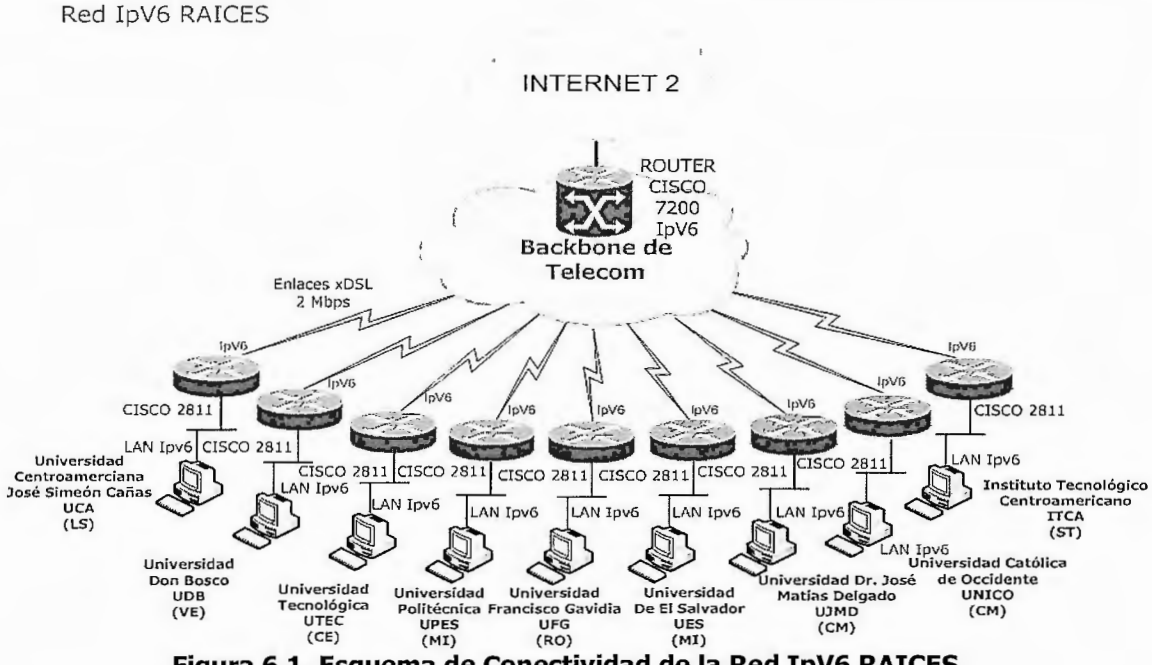


Figura 6.1. Esquema de Conectividad de la Red IpV6 RAICES.

7. Descripción de la Solución

Con la implementación de la solución de acceso a Internet2, se proveerá la alternativa de ofrecer servicios de Internet con anchos de banda de 2 Mbps para las instituciones educativas que se encuentra afiliadas a RAICES.

El servicio de Internet2 sé proveerá a los clientes mediante enlaces HDSL a 2Mbps, instalados entre la central de telecom y el sitio del cliente, conectados por medio de dos modem HDSL y en el sitio del cliente se instalara un router Cisco 2811, cada uno de lo enlaces de 2 Mbps que sean instalados serán transportado integramente por la red TDM la cual se encuentra soportada en la red de transmisión hasta llegar a la central Roma, sitio donde se conectara al nodo de Internet2(router 7200 configurado para este propósito). El enlace será configurado en Ipv6 y transportado en una VRF a través de la red IP/MPLS hacia la red de Internet ALICE.

IMPLEMENTACION DE LA SEGURIDAD EN LA RED IPV6.

La seguridad se implementara en los puntos remotos(Router Cisco 2811), para ello se utilizara Cisco IOS Firewall IpV6, esté coexiste con Cisco IOS Firewall para IpV4, y puede ser implementado en routers dual-stack.

Cisco IOS para IpV6 incluye las siguientes características:

Protección de Paquetes Fragmentados
Mitigacion de ataques DoS (Denial fo services) en Ipv6
Inspección de paquetes en Túneles.
Inspección de paquetes de sesiones TCP, UDP, ICMPv6, y FTP.
Inspección de paquetes originados en una red Ipv4 y terminados en un ambiente Ipv6 proveyendo un servicio de translación Ipv4-Ipv6.
Interpretación y reconocimiento de muchos encabezados de extensión Ipv6, incluyendo encabezados de enrutamiento y encabezados de fragmento.

Nota:

El Router Cisco 2811 cuenta con aplicaciones propias para brindar seguridad a la red:

- *Cisco Router and Security Device Manager. Es una aplicación en ambiente web que se puede acceder remotamente.*
- *Intrusion Prevention System (IPS).*
- *Network Admision Control (NAC).*
-

GESTION DE LA RED IPV6.

Telecom proporcionará a los clientes que lo requieran herramientas de monitoreo, con la cual podrán fácilmente realizar un monitoreo de sus enlaces, esto les permitirá detectar las siguientes anormalidades que presenten sus enlaces digitales de transmisión de datos:

- Detectar el estado de sus equipos.
- Detectar cambios en la topología de red.
- Presentación del estado de los dispositivos por colores de acuerdo a la severidad.
- Visualización de alarmas.
- Administración y Control de Trafico :

- Ancho de Banda Total.
- Ancho de Banda en Uso.
- Ancho de banda Libre.

- Informe de rendimiento del Enlace.

Herramienta de Monitoreo MRTGv6 (Multi Router Traficc Grapher).

Es una aplicación desarrollada por Computer Networks Research Group de la Universidad Roma Tre , la cual puede consultar los routers utilizando SNMP sobre Ipv6. Todas las versiones de MRTG desde la 2.10.0 soportan Ipv6.

Ipv6 se encuentra actualmente deshabilitado por defecto y debe ser habilitado explicitamente. En MRTG esto se logra habilitando la opción global EnableIPv6 en el archivo de configuración. En cfgmaker es habilitado con la opción de comando **enable-ipv6.** La habilitación de Ipv6 no tendrá ningún efecto en configuraciones anteriores del MRTG.

El soporte de Ipv6 requiere de dos librerías que son la Socket6 y la INET6. El Graficador de Tráfico Multi Enrutador (Multi Router Traffic Grapher, MRTG) es una herramienta para monitorear la carga de tráfico en los enlaces de una red. El MRTG genera páginas HTML las cuales contienen gráficos GIF que proveen un representación visual EN VIVO de este tráfico. La herramienta actualmente es utilizada para clientes que poseen servicios de datos IP, FR e ID, los datos son accesados remotamente por los clientes a nivel de la Web por medio de un usuario y password asignado, la información se encuentra alojada en el servidor donde se encuentra instalado el software.

El MRTG está basado en Perl y C y trabaja en estaciones de trabajo UNIX y en Windows NT. El MRTG esta siendo usado exitosamente en muchos sitios alrededor de la red.

Principales Características:

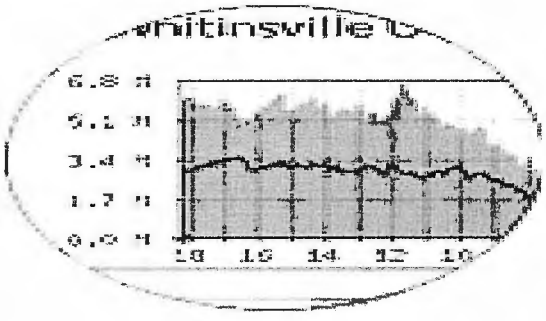
- Portable: El MRTG trabaja sobre la mayoría de las plataformas UNIX y sobre Windows NT.
- Perl: El MRTG esta escrito en Perl y viene con la fuente completa.
- Portable SNMP: El MRTG usa una implementación de SNMP altamente portable escrita completamente en Perl.
- Identificación de Interfaces Confiable: Las interfaces de los enrutadores pueden ser identificadas por su dirección IP, descripción y dirección Ethernet, además del número de interfaz normal.
- Bitácoras (logs) de tamaño constante: Las bitácoras del MRTG NO crecen. Gracias al uso de un algoritmo único de consolidación de datos.
- Configuración Automática: El MRTG viene con un conjunto de herramientas de configuración las cuales hacen la configuración muy simple.
- Gráficos libres de GIF: Los gráficos son generados directamente en formato PNG.
- Personabilidad: La apariencia de las páginas Web producidas por el MRTG son altamente configurables.

El MRTG consiste en un programa en Perl que usa SNMP para leer los contadores de tráfico de sus enrutadores y de un rápido programa en "C" el cual archiva los datos de tráfico y crea hermosas

imágenes que representan el tráfico en la conexión de red monitoreada. Esos gráficos se insertan en páginas Web que pueden ser vistas desde cualquier browser moderno.

Además de una vista diaria detallada, el MRTG crea también representaciones visuales para el tráfico de los últimos siete días, las cuatro últimas semanas y los últimos doce meses. Esto es posible pues el MRTG mantiene un archivo de todos los datos que ha obtenido del enrutador. Este archivo es consolidado automáticamente, así que no crece con el tiempo, pero contiene todos los datos relevantes del tráfico de los últimos dos años. Todo esto se realiza de una manera eficiente. Por lo tanto, usted puede monitorear 200 o más enlaces de red desde cualquier máquina Unix.

El MRTG no está limitado al monitoreo de tráfico, es posible monitorear cualquier variable SNMP que usted elija. Usted puede hasta usar un programa externo para recolectar datos que serán monitoreados por el MRTG. Personas están usando el MRTG para monitorear cosas como Carga del Sistema, Logueo de Sesiones, disponibilidad de módems y más. El MRTG hasta le permite acumular dos a más fuentes de datos en un único gráfico.



La aplicación MRTG integra un módulo de medición de tráfico y una aplicación que grafica estos resultados. Para cada vinculo, los gráficos ofrecen información detallada en base a distintos parámetros temporales.

Los esquemas provistos son los siguientes:

- Gráficos diarios con promedio cada 5 minutos.
- Gráficos semanales con promedio cada 30 minutos.
- Gráficos mensuales con promedio cada 2 horas.
- Gráficos anuales con promedio diario.

En todos los casos, se pueden visualizar en cada gráfico los siguientes datos:

- Máximo tráfico entrante
- Máximo tráfico saliente
- Promedio tráfico entrante
- Promedio tráfico saliente
- Tráfico entrante actual
- Tráfico saliente actual

7.1 Detalle de Equipos y Materiales a Instalar

Los equipos que serán instalados para la implementación de la red de acceso a Internet2 son:

Router de RAICES, Cisco 7026.

Especificaciones de Equipo:

- 7206VXR with NPE-G1 includes 3GigE/FE/E Ports and IP SW.
- Cisco 7200 DC (24V-60V) Power Supply Option
- Cisco 7200 Redundant DC (24V-60V) Power Supply Option
- Cisco 7200 Series IOS SERVICE PROVIDER
- Two 128MB mem modules (256MB total) for NPE-G1 in 7200.
- Cisco 7200 Compact Flash Disk for NPE-G1, 64 MB Option.
- 1000BASE-LX/LH long haul GBIC (singlemode or multimode)
- 8 port multichannel T1/E1 8PRI port adapter.
- E1 Cable BNC 75ohm/Unbal 5m.
- Cisco NPE-G1 Cable Management Bracket.
- Soporte Premium 7x4x24

Caracteristicas Especiales:

- El Router 7206 es un Router de Servicios Universales para Grandes Empresas y Proveedores de Servicios.
- Cisco IOS para soporte de IP/MPLS (QoS, Broadband Agg, Security, Multiservice, MPLS, y mas).
- Alta flexibilidad para interfases modulares (desde DS0 hasta OC12).
- Sopote para mas de 16,000 suscriptores de banda ancha con el procesador NPE-G1.
- Aceleración de Servicios utilizando la tecnología PXF.
- Soporte para multi protocolo.
- Escalabilidad y Flexibilidad, ideal para el desarrollo de la red.
- Soporte para terminacion PPP y L2TP completo.
- Soporte para Fast Ethernet, Giga Ethernet y Packet Over Sonet.

Router del Cliente, Cisco 2811.

Es un Integrated Service Router que esta optimizado para dar servicios de seguridad, envío de datos concurrentes a alta velocidad, voz y video.

Especificaciones del Equipo:

- 4 Slots para Tarjetas de Interfase de alta velocidad HWIC.
- 1 Slot de Compact Flash.
- 2 Puertos USB para dispositivos Cisco futuros aprobados.
- 1 Puerto de Consola.
- 1 Puerto Auxiliar.
- 1 Conector RPS Externo para Fuente Redundante Externa.
- 1 Slot de Modulo de Red NME.

- Fuente AC.
- 2 Puertos Fast Ethernet 10/100 Base T.

Caracteristicas Especiales:

- El Router Cisco 2811 es un Router de Servicios Integrados (Voz, Datos y Video), el cual agrega procesamientos de seguridad, memoria y servicios concurrentes. Puede ser utilizado para Negocios Pequeños, medianos y Proveedores de Servicios.
- Funcionamiento Wire-speed (alta velocidad) para servicios concurrentes como seguridad, voz y video , y servicios avanzados para múltiples T1/E1/xDSL WAN rates.
- Protección de la inversión a través de funcionamiento y modularidad crecientes.
- Soporte para mas de 90 modulos de red y para la mayoria de AIMs, NMs, WICs, VWICs, y VICs existentes.
- Soporte opcional para conmutación de capa 2, con Power over Ethernet (PoE).
- Provee diversos Servicios de Seguridad como:
  - Encriptación On-board
  - Soporte para mas de 1500 VPN túneles con el modulo AIM-EPII-PLUS .
  - Soporte de defensa con Antivirus a través del Network Admission Control (NAC)
  - Soporte para Prevención de Intrusos, así como soporte stateful Cisco IOS Firewall y otras características esenciales de seguridad.
- Cobertura para tecnología LAN inalámbrica, proveyendo capacidades de costo-efectividad, seguridad inalámbrica.
- Provee Servicios Integrados de Voz, telefonía básica, procesamiento de llamadas, mensajerilla y servicios automatizados.

Modem HDSL Central y Cliente.

ASMI-52
2/4-Wire SHDSL Modem