UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

"Trabajo de grado previo a la obtención del Título de Ingeniero. En Sistemas y Computación"

TRABAJO DE GRADUACION

INVESTIGAR Y DESARROLLAR UNA GUÍA METODOLÓGICA DE LOS MECANISMOS DE TRANSICIÓN Y COEXISTENCIA IPV4-IPV6 EN EL ÁREA DE SISTEMAS DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO

Autores:

Ramírez Mosquera Danilo Enrique

Hidalgo Pazmiño José de Jesús

Director:

Ing. Javier Haro

Riobamba – Ecuador

AÑO 2010

CALIFICACIÓN

Los miembros del tribunal, luego de haber receptado la defensa de trabajo escrito, hemos determinado la siguiente calificación.

Para constancia de lo expuesto firman:

INTEGRANTES	**CALIFICACIÓN**	**FIRMA**
Ing. Jorge Delgado **Presidente**	_____	_____
Ing. Javier Haro **Director - Coautor**	_____	_____
Ing. Daniel Santillán **Miembro del tribunal**	_____	_____

DERECHO DE AUTOR

Nosotros, Danilo Enrique Ramírez Mosquera, José de Jesús Hidalgo Pazmiño, somos responsables de las ideas, doctrinas, resultados y propuestas expuestas en el presente trabajo de investigación, y los derechos de autoría pertenece a la UNIVERSIDAD NACIONAL DE CHIMBORAZO.

DEDICATORIA

El presente proyecto está dedicado a mis padres José y Adelita, hermanos: Taty, Moni, Xime, a mi esposa Paulina y sobre todo a mí querida hija Génesis las que con su apoyo y esfuerzo me ayudaron a que pudiera concluir satisfactoriamente mi carrera universitaria, ya que día a día me motivaron y apoyaron para que continúe y así alcanzar mi sueño de graduarme.

José de Jesús Hidalgo Pazmiño.

El presente proyecto está dedicado a las personas que con su apoyo y esfuerzo me ayudaron a que pudiera concluir satisfactoriamente mi carrera universitaria, como son: mis padres, hermanas. Que día a día me motivaron y apoyaron para que continúe y alcance mis sueños.

Danilo Enrique Ramírez Mosquera,

.

AGRADECIMIENTO

Al concluir este trabajo de investigación agradecemos a todas aquellas personas que día a día nos apoyan para que culminemos satisfactoriamente el presente proyecto: al Ing. Javier Hago, Ing. Jorge Delgado, Ing. Daniel Santillán, a nuestros padres, hermanos y familia ya que fueron nuestro apoyo en todo el transcurso de nuestra vida estudiantil.

Un agradecimiento muy sincero a la Universidad Nacional de Chimborazo y profesores, quienes con sus conocimientos impartidos en las aulas de clases ayudaron a que desarrollemos nuestro intelecto.

José Hidalgo, Danilo Ramírez

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO

FTP.- File Transfer Protocol (Protocolo de Transferencia de Archivos)

SMT.- Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correo)

POP3.- Post Office Protocol (Protocolo de la oficina de correo)

IPv4.- es la versión 4 del Protocolo IP (Internet Protocol)

IPv6.- es la versión 6 del protocolo IP (Internet Protocol)

TIC.- Las tecnologías de la información y comunicaciones

VoIP.- Voz sobre Protocolo de Internet

ISO/OSI.- Open System Interconnection (El modelo de referencia de Interconexión de Sistemas Abiertos)

TCP.- Transmission Control Protocol (Protocolo de Control de Transmisión)

IANA.- Internet Assigned Numbers Authority, que integran AFRINIC, APNIC, ARIN, LACNIC, RIPENCC

RIR.- Regional Internet Registry (Registro Regional de Internet)

ISP.-Internet Service Provider (proveedores de servicios de internet)

ARP.- Address Resolution Protocol (Protocolo de resolución de direcciones).

LSA.- Light Summary Algorithm (Algoritmo Ligero de Resumen es un algoritmo de reducción criptográfico de 64 bits).

P2P.- Es una red peer-to-peer o red de pares, es una red de computadoras en la que todos o algunos aspectos de ésta funcionan sin clientes niservidores fijos.

LSDB.- database link state (base de datos del estado del enlace)

Host.- Comnputadoras

Subnet.- Subred

DSTM.- Dual Stack Transition Mechanism (Mecanismo de transición de Doble pila)

AIIH.- Asignación de direcciones de IPv4 a IPv6 para host

DTI.- Interfaz Dinámica de Tunel de direcciones de IPv4 a IPv6

TB.- Tunnel Broker

TS.- Tunnel Servers (Túnel de servidor)

DNS.- Domain Name System (sistema de nombre de dominio)

DHCP Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de host)

AAA.- Authentication, Authorization and Accounting (Autenticación, Autorización y Contabilización)

PTR.- Network termination point (Punto de terminación de red)

RFC.- Request for Comments (Petición de Comentarios)

IOS.- Internetwork Operating System, (Sistema Operativo de Interconexión de Redes)

IGMP.- Internet Group management protocol (Protocolo de grupo de manejo de Internet)

MLD.- Multicast Listener Discovery (Descubrimiento de escucha de multidifusión).

ICMP.- Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet)

ICMPv6.- Internet Control Message Protocol versión 6 (Protocolo de Mensajes de Control de Internet versión 6)

RESUMEN

El protocolo de Internet versión 4 (IPv4) ha sido el principal protagonista del desarrollo y expansión de Internet en las últimas décadas. El servicio de Internet con el modelo cliente-servidor se basa en un equipo central de la administración de la red al cual acceden varios clientes, donde el servicio de email o correo electrónico es uno de los más utilizados. Generalmente se usan los protocolos SMTP para enviar los mensajes de correo, y POP3 o IMAP4 para obtener los mensajes. Además cada día es más común la necesidad de enviar o transmitir audio y video por medio de Internet y/o Intranets. La transmisión multimedia se basa en el modelo también se basa en el cliente-servidor.

Por los problemas que presentan IPv4 como son: la saturación del espacio de direcciones, menos direcciones disponibles, obstaculiza el uso de Internet a nuevos usuarios y Disminución de ancho de banda. Por lo cual se ha desarrollado el protocolo de Internet versión 6 (IPv6), que corrige dichos problemas y permite crear la base para el desarrollo de Internet durante las próximas décadas.

En la actualidad, el soporte IPv6 que ofrecen los fabricantes de equipos y programas computacionales ha alcanzado un desarrollo que permite la implementación de redes IPv6 nativas. Ya no es necesario depender de herramientas de traducción y/o túneles para poder desarrollar redes IPv6 que implementen el mismo tipo de servicios otorgados en redes IPv4.

El trabajo presenta el desarrollo e implementación de una guía metodológica de los métodos de transición y coexistencia de IPv4-IPv6 en el área de sistemas de la facultad de Ingeniería de la UNACH.

SUMMARY

The Internet Protocol version 4 (IPv4) has been the main agent of development and expansion of Internet in recent decades. Internet service with client-server model is based on a central computer network administration which multiple clients access, where the email service or email is one of the most used. Are generally used to send SMTP mail messages, and POP3 or IMAP4 to obtain messages. In addition, each day is more common the need to post or transmit audio and video over the Internet and / or Intranets. Multimedia transmission is based on the model is also based on the client-server.

For the problems presented by IPv4 are: address space saturation, fewer addresses available, are impeding the use of the Internet to new users and decreased bandwidth. Therefore it has developed the Internet Protocol version 6 (IPv6), which corrects these problems and to create the basis for the development of the Internet over the coming decades.

Currently, IPv6 support offered by manufacturers of computer hardware and software has reached a development that allows native IPv6 network deployment. It is no longer necessary to rely on translation tools and / or tunnels to develop IPv6 networks that implement the same type of services provided in IPv4 networks.

The paper presents the development and implementation of a methodological guide to the methods of transition and coexistence of IPv4-IPv6 in the area of power systems Engineering UNACH.

CAPÍTULO I

1. MARCO REFERENCIAL

1.1. Introducción

Las tecnologías de la información y comunicaciones (TIC) se han convertido en parte fundamental de nuestras vidas. Durante la última década, se han desarrollado innumerables tecnologías y servicios que han cambiado la forma en cómo nos comunicamos y relacionamos con personas. Poco a poco observamos como los medios tradicionales de comunicación, televisión, telefonía y mensajería, entre otros, convergen hacia una única red de comunicaciones, la Internet

Esta tendencia mundial ha conducido a un crecimiento explosivo en el número de usuarios de Internet. Junto a esto, Internet ha evolucionado desde ser una simple red que conecta computadores a una plataforma que entrega diversos tipos de servicios. Esta evolución ha dejado en descubierto las limitantes del protocolo IPv4, base de esta gran red. IPv4 fue desarrollado en la década de los 70 como una forma de interconectar un reducido número de redes y jamás se pensó en que tendría que ser la base de una red de millones de usuarios. Su reducido número de direcciones disponibles junto a problemas de arquitectura, han restringido y limitado el desarrollo de nuevas aplicaciones y tecnologías en Internet.

Por lo cual hemos visto la necesidad que la UNACH en un futuro no muy lejano se verá obligado a adaptarse a la nueva tendencia de IPV6 debido a que IPV4 tiene problemas como son de agotamiento de direccionamiento, problemas de arquitectura dado el fuerte crecimiento que ha experimentado el internet en los últimos nueve años. Por lo que se hace necesaria la implementación de IPV6 en la infraestructura de la UNACH, debido a motivadores comerciales ya que puede generar un ahorro en los costos de adquisición de nuevos equipos y además realizar una migración con antelación es más económico que una migración tardía.

El Protocolo de Internet IPv6 introduce modificaciones fundamentales. No sólo la longitud de la dirección IP ha sido extendida a 128 bits; también ha sido modificado el formato de la cabecera IP y el modo en que se procesa la información que en ella se alberga. Pasar de IPv4 a IPv6 no es sencillo y los mecanismos que permiten la coexistencia y la transición entre las dos versiones han de estar estandarizadas.

Antes de hablar de una migración de IPV4 A IPV6 tenemos que tener claro cómo funciona su direccionamiento, sus características, encabezado, la forma en que se transportan los paquetes, además de los protocolos de enrutamiento que más convenga para nuestra infraestructura y necesidades. En este caso nos enfocaremos en dos protocolos de enrutamiento: Ripng, Ospf, y por otro lado Enrutamiento Estático, ya que nos servirán para la utilización del mecanismo de coexistencia como es el 6to4 y del tunnel bróker.

Un punto muy importante en tener en cuenta es el análisis comparativo de IPV4 con respecto a IPV6 y los mecanismos de transición y coexistencia donde se analiza sus características, diferencias y equivalentes que posee cada una de estas, equipos a utilizar con sus respectivos Sistemas Operativos que soporta dicha infraestructura.

El principal objetivo de este investigación es diseñar e implementar una red ipv6 para la aplicación de una guía metodológica de los mecanismos de transición y coexistencia ipv4-ipv6, en el área de sistemas de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo El trabajo y los resultados aquí expuestos constituyen el primer paso para una futura migración a IPv6 de todos los servicios ofrecidos por la red institucional de la UNACH.

1.2 Planteamiento y formulación del problema

EI protocolo IPv4 comienza a dar señales de debilidad. Después de 20 años, la versión 4 del protocolo de Internet (IP) ya no puede seguir brindando respuestas adecuadas, sobretodo en cuanto al paulatino agotamiento de las direcciones IP disponibles, un proceso que culminará en unos pocos años, al ritmo actual de crecimiento de Internet. Ante el enorme aumento de usuarios de Internet, que hoy tienen exigencias distintas a las de hace unos años.

Las pocas direcciones IPV4 que posee la UNACH se han venido saturando debido al crecimiento institucional con servicios como son: de SICOA, Sistema de Bibliotecas virtuales, Aulas virtuales, videoconferencia, cantidad de computadoras con acceso a internet, los mismos que conllevan limitaciones como:

1. Inminente saturación del espacio de direcciones
2. Menos direcciones disponibles
3. Limita el crecimiento de Internet
4. Obstaculiza el uso de Internet a nuevos usuarios
5. Disminución de ancho de banda.

En la Facultad de Ingeniería se realiza el estudio de nuevas alternativas para el mejoramiento de IPv4. Y esa mejora se llama IPv6 (Internet Protocol versión 6) con las siguientes características de mejoramiento con respecto a la anterior:

1. Capacidades expandidas de direccionamiento IP: Para nuevos dispositivos, como teléfonos celulares, PDAs, dispositivos de consumo, etc.
2. Seguridad y privacidad mejorada
3. Mayor velocidad para servicios de VoIP, multimedia, teleconferencias.
4. Autoconfiguración y reconfiguración “sin servidor” (“plug-and-play”)
5. Mecanismos de transición gradual de IPv4 - IPv6
6. Incorporación de encriptado y autenticación en la capa IP
7. Formato de la cabecera simplificado e identificación de flujos

1.3 La necesidad de IPv6

1.3.1 Problemas existentes en IPv4

El protocolo de Internet (IP) es un protocolo no orientado a la conexión usado para trasmitir información a través de una red de paquetes conmutados. Se ubica en la capa 3 del modelo ISO/OSI y su función es entregar paquetes desde un nodo de origen a uno de destino, basado en la dirección escrita en cada paquete.

El protocolo de Internet versión 4 (IPv4) es la cuarta iteración del protocolo IP y la primera versión en ser utilizada en ambientes de producción. Es el protocolo dominante en Internet, utilizado para conectar redes de forma interna y hacia el exterior. Dentro de sus principales características se encuentran:

Enrutamiento y direccionamiento: Provee una dirección única a cada dispositivo de una red de paquetes. IPv4 fue especialmente diseñado para facilitar el enrutamiento de información (paquetes) a través de redes de diversa complejidad.

Encapsulación: El protocolo IPv4 nace como una división del antiguo protocolo TCP ("Transmission Control Protocol"). Se ubica en la capa 3 del modelo ISO/OSI y puede funcionar sobre diversos protocolos de nivel inferior.

Mejor esfuerzo: El protocolo IP provee un servicio de transmisión de paquetes no fiable (o de mejor esfuerzo). No se asegura que los paquetes enviados lleguen correctamente al destino.

La versión de IPv4 usada actualmente en Internet no ha cambiado sustancialmente desde su publicación inicial en 1981. IPv4 ha demostrado ser un protocolo robusto, fácil de implementar y con la capacidad de operar sobre diversos protocolos de capa 2. Si bien fue diseñado inicialmente para interconectar unos pocos computadores en redes simples, ha sido capaz de soportar el explosivo crecimiento de internet.

Sin embargo en el último tiempo, se han hecho notar diversos problemas existentes en

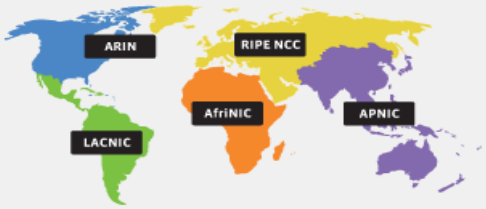
IPv4, asociados al crecimiento de Internet y a la aparición de nuevas tecnologías y servicios que requieren conectividad IP.

1.3.1.1 Agotamiento direcciones IP

Una dirección IPv4 tiene un tamaño de 32 [bit], los que permiten un máximo teórico de 2^{32} (4.294.967.296) direcciones a asignar. En los inicios de Internet, se utilizaron métodos de distribución poco eficientes, como la asignación por clases, mediante los cuales se asignaron grandes bloques de direcciones a organizaciones que solo requerían unas pocas. Esto ha generado que actualmente muchas organizaciones posean un gran número de direcciones que no se encuentran utilizadas.

Los primeros reportes de alerta sobre el inminente agotamiento de direcciones IP se dieron a conocer alrededor de 1990. Diversas soluciones y protocolos han permitido extender la vida útil de IPv4, tales como la traducción de direcciones de red (NAT), el enrutamiento sin clases entre dominios (CIDR) y el uso de asignaciones temporales de direcciones con servicios tales como DHCP, RADIUS/PPP, y SERVIDOR PROXY.

Actualmente, se ha establecido una política jerarquizada para la asignación de direcciones IPv4, en donde el IANA (“Internet Assigned Numbers Authority”) tiene a su cargo el manejo de los bloques de direcciones IPv4 que se encuentran libres. Junto al IANA, se encuentran los registros regionales de Internet (AFRINIC, APNIC, ARIN, LACNIC y RIPENCC) quienes reciben bloques de direcciones delegados por el IANA y los distribuyen entre los proveedores de servicios (ISP) de la región del mundo que administran.



Registro	Área cubierta
AfriNIC	Región de África
APNIC	Asia y el Pacífico
ARIN	Región Norte de América
LACNIC	América Latina y algunas islas del Caribe
RIPE NCC	Europa, el Medio Oriente y Asia Central

Figura 1 Delegados de la IANA a nivel mundial

El IANA asigna bloques de prefijo /8, (equivalentes a 1/256 del total de direcciones) a los registros regionales. Dado que el rango de direcciones comprendido entre 224.X.X.X y 239.X.X.X se encuentra reservado para tráfico "multicast", y el rango entre 240.X.X.X y 254.X.X.X se encuentra reservado para trabajos experimentales, el espacio real de direcciones disponibles para ser asignadas es de 223 bloques /8, los cuales representan 16.777.214 direcciones cada uno. En la Figura 2 se observa la distribución actual de bloques /8.

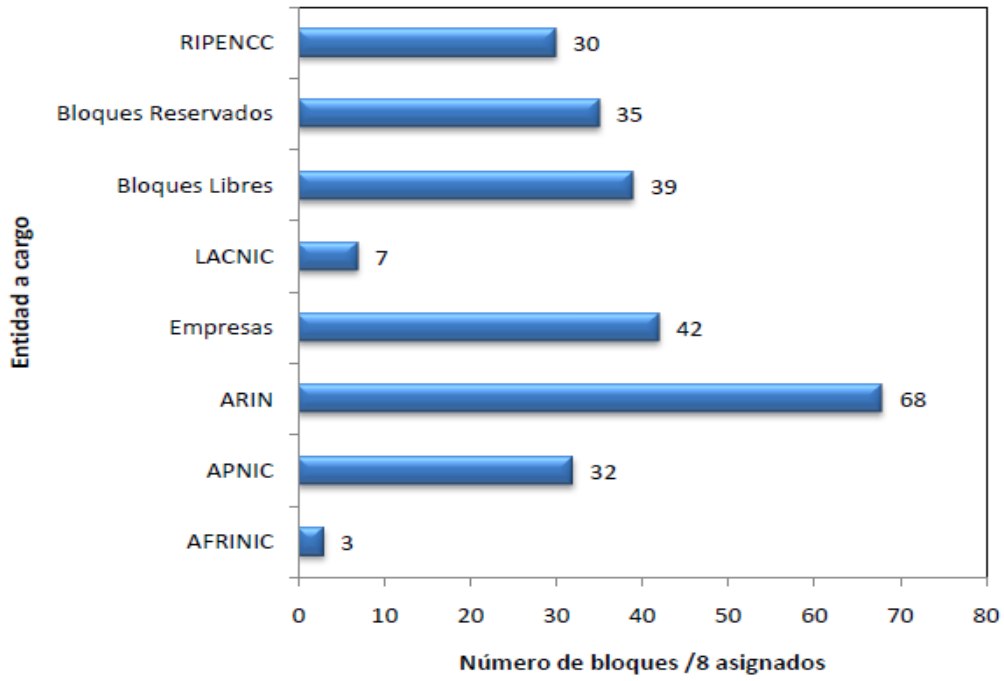


Figura 2. Distribución actual de bloques /8 asignados

En la Figura 2 se observa que la mayor parte de los bloques se encuentra asignado al registro regional ARIN, que distribuye direcciones a Canada, EE.UU. e islas del Noratlántico. Se puede apreciar que una parte importante de los bloques /8 se encuentran asignados directamente a empresas y organizaciones, quienes recibieron dichos bloques como producto de las políticas de asignación anteriores a 1993. Dentro de los grupos reservados, se encuentran los bloques asignados a direcciones IP privadas, tráfico "multicast" y otros usos aun no definidos. Los 39 bloques libres son manejados directamente por el IANA, quien los delega a cada registro regional de acuerdo a sus requerimientos.

Es complicado estimar la fecha exacta en que se agotarán todas las direcciones IPv4 disponibles, ya que diversos factores pueden adelantar o retrasar dicha fecha. Dentro de esos factores se encuentran posibles cambios en la política de asignación, recuperación de bloques no utilizados o incluso la venta de direcciones IP entre privados. Pero a partir de la información publicada por el IANA y los registros regionales, entrega una fecha estimada de agotamiento de direcciones IPv4.

En la figura 3 hace una comparación global del número de direcciones IPv4 asignadas hasta la fecha para cada Registro de Internet Regional (RIR).

Se consideran también en esa grafica las direcciones "legadas", o sea, aquellas asignadas por el Registro Central antes de la creación de los RIRs. La cantidad de direcciones IPv4 asignadas se representa en número de "/8". Siendo que cada bloque de prefijo /8 contiene 16777216 direcciones IPv4.

La ultima barra indica el total de /8 asignados a los 5 RIRs.

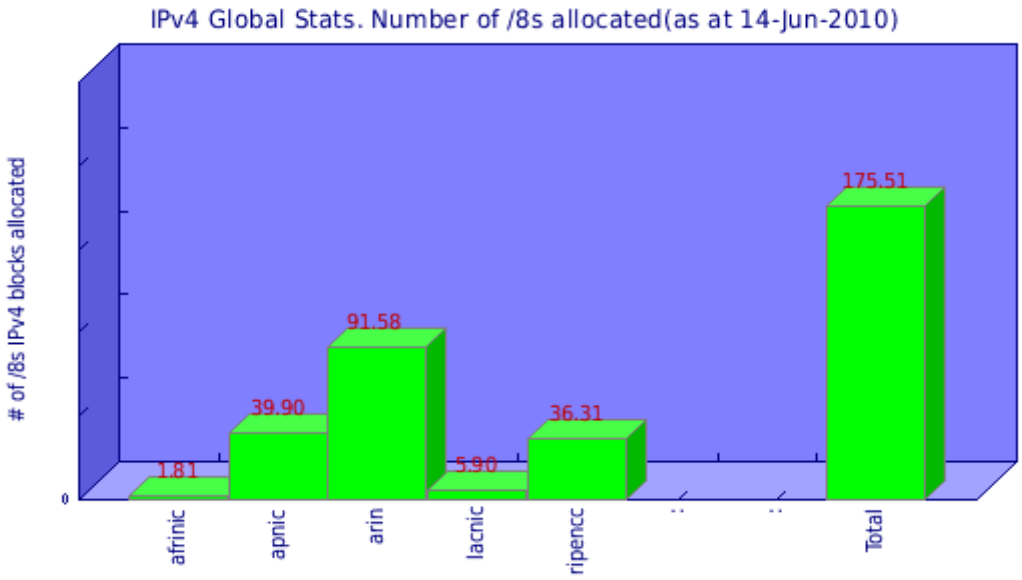


Figura 3. IPv4 global Stats.

En la Figura 4 se presenta una proyección del agotamiento de bloques /8. Este análisis modela el comportamiento de cada registro regional, considerando su demanda histórica de bloques de direcciones IP. En la figura se observan tres curvas, una asociada a los bloques asignados a registros regionales (“Assigned”), otra que

representa aquellos bloques asignados que son anunciados efectivamente hacia internet (“Advertised”) y una que señal aquellos bloques asignados que no son anunciados (“Unadvertised”).

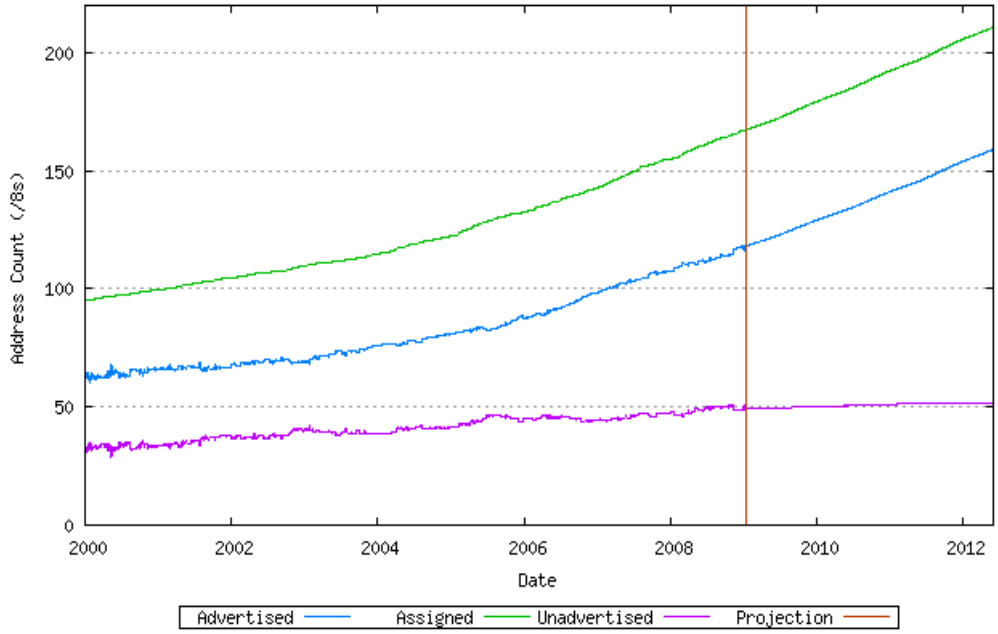


Figura 4. Proyección del agotamiento de bloques /8. Fuente: “IPv4 Address Report”.

En base a estas proyecciones, se estima que en Marzo del 2011 se agotará el total de los bloques /8 libres manejados por el IANA. A partir de dicho momento, los registros regionales no tendrán la posibilidad de solicitar bloques de direcciones adicionales, sólo podrán administrar las direcciones que ya tienen asignadas. La segunda fecha a considerar es cuando los registros agoten su reserva de direcciones y ya no puedan solicitar un bloque adicional al IANA. Se ha estimado que ello ocurra en Mayo del 2012, un año después del agotamiento de los bloques disponibles.

Todos estos cálculos y estimaciones están realizados en base al crecimiento histórico que ha tenido la demanda de direcciones IP a nivel mundial. Sin embargo, se espera que en los próximos años, la demanda por direcciones IP sea aún mayor debido a diversos factores tales como:

- Grandes poblaciones en China, India, Indonesia y África aun no están conectadas.
- El número de individuos conectados a Internet crece en 77 millones por año.

- Dispositivos electrónicos de todo tipo están paulatinamente conectándose a Internet.
- De todas formas, es posible advertir que en estos días ya estamos en presencia de problemas relacionados con la baja disponibilidad de direcciones IP:
- Las organizaciones normalmente obtienen pocas direcciones IP para toda su red, limitando las posibilidades de implementar servidores y aplicaciones.
- Algunos proveedores de servicios (ISP) están asignando direcciones IP privadas a sus subscriptores, lo que significa que el suscriptor no puede ser contactado directamente desde internet.
- Gran parte de las compañías de telefonía celular no proveen de direcciones públicas a los usuarios de servicios 3G.
- Muchas aplicaciones disminuyen su rendimiento al no disponer de conectividad punto a punto auténtica.

1.3.1.2 Problemas de arquitectura

Dado el fuerte crecimiento que ha experimentado Internet en los últimos años, ha sido necesario introducir modificaciones y protocolos complementarios a IPv4, con el fin de poder satisfacer la creciente demanda. Estos cambios han causado que las redes IP estén perdiendo paulatinamente el principio de conectividad punto a punto bajo el cual se diseño IPv4. Dicho principio estable lo siguiente:

- Ciertas funciones solo pueden ser realizadas por los nodos finales. El estado de una comunicación punto a punto debe ser mantenida únicamente por los nodos finales y no por la red. La función de la red es enrutar paquetes de forma eficaz y transparente.

- Los protocolos de transporte están designados para proveer las funciones deseadas sobre una red que no ofrece garantías (mejor esfuerzo).

- Paquetes deben viajar sin modificación a través de la red.

- Las direcciones IP son usadas como identificadores únicos para nodos finales. Una de las medidas introducidas para frenar el agotamiento de direcciones IPv4 es el protocolo de traducción de direcciones de red (NAT). NAT es un protocolo que permite convertir en tiempo real las direcciones utilizadas en los paquetes transportados en un a red. El uso de NAT permite que un grupo de dispositivos configurados con direcciones IPv4 privadas compartan un reducido grupo de direcciones IPv4 públicas, permitiendo el acceso hacia Internet.

  Si bien el uso de NAT ha permitido la expansión actual de Internet, su uso introduce una serie de problemas y desventajas, asociados a la pérdida del principio de conectividad punto a punto.

Dentro de las desventajas del uso de NAT podemos encontrar:

- Complejidad: NAT representa un nivel de complejidad adicional al momento de configurar y manejar una red. Se deben crear grupos de dispositivos y/o redes que comparten un número limitado de direcciones IPv4 públicas.

- Compatibilidad con ciertas aplicaciones: Muchas aplicaciones no funcionan correctamente cuando se ejecutan desde dispositivos que están en una red donde se realiza NAT. Los desarrolladores han tenido que inventar nuevos mecanismos para poder funcionar correctamente en dichas redes.

- Problemas con protocolos de Seguridad: Protocolos de seguridad tales como IPSec están designados para detectar modificaciones en las cabeceras de los paquetes, que es precisamente lo que hace NAT al traducir direcciones. El uso de NAT dificulta la implementación de este tipo de protocolos.

- Reducción de rendimiento: Por cada paquete que atraviesa una red donde opera NAT, se deben realizar una serie de operaciones adicionales. Dichas operaciones introducen mas carga a la CPU del dispositivo que realiza la traducción, disminuyendo su rendimiento.

- Manejo de estados TCP: El dispositivo que realiza NAT debe manejar y mantener correctamente los estados de cada conexión TCP entre equipos de la red interna y externa.

- A pesar de todas sus desventajas, NAT permitió posponer en varios años el agotamiento de direcciones IPv4. Sin embargo, en la actualidad se ha llegado a un punto en donde el uso de NAT no es suficiente para la creciente demanda de direcciones IPv4. Esto ha motivado la evaluación de otras alternativas, tales como IPv6.

1.4 Motivadores del cambio a IPv6

El cambio desde IPv4 a IPv6 se suele comparar con la crisis que se vivió a fines de los 90 ante la llegada de año 2000 y sus consecuencias en los sistemas informáticos. Sin embargo, en el caso de IPv6 no existe una fecha límite o "flag day" en que se puedan deshabilitar todas las redes IPv4 y actualizarlas a IPv6. El proceso de migración debe realizarse en forma progresiva, se prevé que IPv4 siga en funcionamiento durante la próxima década.

El mayor problema que enfrenta IPv6 es que desde el punto de vista de las empresas y organizaciones, su implementación se ve como un gasto poco justificado. En la actualidad, el tráfico IPv6 representa menos de un 1% del tráfico total de Internet, y la mayoría corresponde a Universidades e instituciones que trabajan en el tema.

Sin embargo, existen una serie de motivadores para la implementación a IPv6, los que se pueden agrupar en las siguientes categorías.

1.4.1 Motivadores Comerciales

- La implementación de IPv6 es un movimiento estratégico. Su implementación en las redes de una empresa permite estar preparados para futuras necesidades de los clientes, generando una ventaja comparativa respecto del a competencia.
- Puede generar un ahorro en los costos de adquisición de nuevos equipos.
- Diversos fabricantes buscan impulsar la implementación de IPv6, ofreciendo descuentos a empresas e instituciones en la compra de nuevos equipos habilitados para IPv6.
- Un plan de migración a IPv6 realizado con antelación es más económico que una migración tardía.
- IPv6 abre las puertas a nuevos productos y servicios a ser ofrecidos por empresas TIC. Sus nuevas características, entre las que destaca el amplio rango de direcciones disponibles, permite generar nuevos proyectos que no podrían ser llevados a cabos en IPv4.

1.4.2 Motivadores Políticos

- En Estados Unidos, la implementación de IPv6 es un mandato gubernamental, en el que se obligó a todas las agencias a implementar IPv6 en sus redes centrales antes de Junio del 2008. El caso más destacado es el del Departamento de defensa (DOD), el cual realizo un amplio y publicitado plan de integración.
- Los gobiernos de Japón, China y Corea han establecido la implementación de IPv6 como prioritaria, otorgando un gran apoyo a todas las iniciativas en esta línea.
- Las olimpiadas de Beijing 2008 fueron un ejemplo de dichas políticas, toda su infraestructura de telecomunicaciones fue implementada mayoritariamente en IPv6.

1.4.3 Motivadores Técnicos

- Casi la totalidad de los equipos de red, sistemas operativos y dispositivos móviles en venta actualmente proveen soporte para IPv6.
- El soporte IPv6 que proveen equipos de red como "switches," routers" y "firewalls" ha alcanzado un grado de madurez que ya permite implementar redes que funcionan únicamente con IPv6 sin mayores contratiempos.
- Algunos ISP ya proveen conectividad IPv6 a usuarios finales.
- IPv6 facilita la implementación de mecanismos de seguridad y de control de tráfico en redes IP.

En el caso particular de las instituciones de educación superior, como la Universidad Técnica Federico Santa María, la implementación de IPv6 en sus redes permite además el desarrollo de trabajos de investigación y colaboración en torno a IPv6 y/o a otras tecnologías.

Es por esto que en la actualidad la IANA ha asignado un cierto número de direcciones de IPv6 a las diferentes Registro de Internet Regional RIR la cuales podemos ver en la siguiente grafica

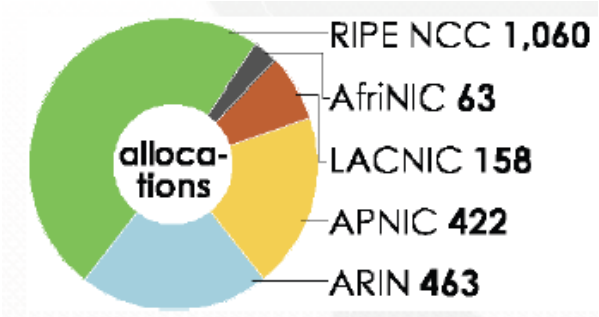


Figura 5 Direcciones IPV6 asignadas por la RIR

1.5 Justificación

El crecimiento de los servicios que presta la UNACH tanto para estudiantes, docentes y personal administrativo, como son los de SICOA, Bibliotecas virtuales, videoconferencia, internet, etc, ha provocado la saturación de la red presentado problemas como saturación del ancho de banda, congestión tráfico red.

Por lo tanto es necesario que se establezcan normativas que permitan una transición entre ipV4 a ipV6, basada en una proyección de los futuros requerimientos institucionales.

1.6 Objetivos generales y específicos

1.6.1 General

Investigar y desarrollar una Guía Metodológica de los Mecanismos De Transición Y Coexistencia Ipv4-Ipv6 En el área de Sistemas De La Facultad De Ingeniería De La Universidad Nacional De Chimborazo

1.6.2 Específicos:

- Estudiar y analizar los mecanismos existentes de transición de ipv4-ipv6 mediante la instalación de una red local y analizar sus ventajas y desventajas que ofrecen cada uno de ellos.
- Comprobar la validez de los procesos de transición y coexistencia de ipv4-ipv6 sobre las plataformas operativas Linux y Windows server
- Desarrollar una guía metodológica con los mecanismos de transición coexistencia ipv4-ipv6 utilizados durante las pruebas.

1.7 Hipótesis

La implementación de mecanismo túnel 6to4 de transición y coexistencia de IPv4 a IPv6, permitirá optimizar la comunicación, y direccionamiento en la infraestructura de las redes del área de sistemas de la Facultad de Ingeniería.

VARIABLE	TIPO	DEFINICION
MECANISMO DE TRANSICIÓN	INDEPENDIENTE	Conjunto de métodos que ayudan a minimizar problemas suscitados en una coexistencia y migración razonable de IPv4 a IPv6.
COEXISTENCIA DE LOS PROTOCOLOS DE INTERNET ENTRE VERSIÓN IV Y VI	DEPENDIENTE	Capacidad de los dispositivos de red para establecer comunicación entre el protocolo IP en sus dos versiones garantizando compatibilidad y confiabilidad. En un ambiente transparente para el usuario

CAPITULO II

2. MARCO TEORICO DE LOS MECANISMOS DE TRANSICIÓN Y COEXISTENCIA DE IPV4-IPV6

2.1 Introducción al protocolo IPv6

El protocolo Internet versión 6 (IPv6) es una nueva versión de IP (Internet Protocol), diseñada para reemplazar a la versión 4 (IPv4), actualmente en uso dominante.

Diseñado por Steve Deering de Xerox PARC y Craig Mudge, IPv6 está destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados. Pero el nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionará a futuras celdas telefónicas y dispositivos móviles sus direcciones propias y permanentes. Se calcula que, actualmente, las dos terceras partes de las direcciones que ofrece IPv4 ya están asignadas.

El protocolo IPv6 comenzó a desarrollarse en el año 1990, tras la primera voz de alerta sobre el posible agotamiento de direcciones IP. Se creó un grupo de trabajo al interior de la IETF, quienes presentaron sus primeras recomendaciones sobre el nuevo protocolo que debería reemplazar a IPv4. En el mismo año se publicó oficialmente la primera versión del protocolo IPv6.

En líneas generales, el protocolo IPv6 es considerado una evolución más que una revolución respecto al protocolo IPv4. Se han mantenido los conceptos principales del protocolo, removiendo aquellas características de IPv4 que son poco utilizadas en la práctica. Se han añadido nuevas características que buscan solucionar los problemas existentes en el protocolo IPv4, discutidos en el capítulo 2.

2.2 Características del protocolo IPv6

Dentro de las principales características de IPv6 se encuentran:

- Mayor número de direcciones: El tamaño de una dirección aumenta desde 32 a 128[bit] lo que se traduce en alrededor de $3{,}4 \cdot 10^{38}$ direcciones disponibles. Esto permite asegurar que cada dispositivo conectado a una red pueda contar con una dirección IP pública.

- Direccionamiento jerárquico: Las direcciones IPv6 globales están diseñadas para crear una infraestructura eficiente, jerárquica y resumida de enrutamiento basada en la existencia de diversos niveles de ISP. Esto permite contar con tablas de enrutamiento más pequeñas y manejables.

- Nuevo formato de cabecera: Aún cuando el tamaño de la cabecera en IPv6 es mayor que en IPv4, el formato de ella se ha simplificado. Se han eliminado campos que en la práctica eran poco usados, de forma de hacer más eficiente el manejo de los paquetes. Con la incorporación de cabeceras adicionales, IPv6 permite futuras expansiones.

- Autoconfiguración: IPv6 incorpora un mecanismo de auto configuración de direcciones, "stateless address configuration", mediante el cual los nodos son capaces de auto asignarse una dirección IPv6 sin intervención del usuario.

- Nuevo protocolo para interactuar con vecinos: El protocolo de descubrimiento de vecinos, reemplaza a los protocolos ARP y "Router Discovery" de IPV4. Una de sus mayores ventajas es que elimina la necesidad de los mensajes del tipo "broadcast".

2.3 Formato de una dirección IPv6

Las direcciones IPv6 están compuestas con 8 campos de 16 [bit] de largo, separados por dos puntos ":". Cada campo está representado por 4 caracteres hexadecimales (0-f). Un ejemplo de dirección IPv6 válida es:

2001:0000:1234:0000:0000:C1C0:ABCD:0876.

Con el fin de simplificar la escritura y memorización de direcciones, se pueden aplicar las siguientes reglas a las direcciones IPv6.

a) No se hace distinción entre mayúsculas y minúsculas. "ABC9" es equivalente a "abC9" .

b) Los ceros al inicio de un campo son opcionales. "00c1" es equivalente a"c1".

c) Una sucesión de campos con ceros puede ser reemplazados por "::".

"1234:0000:0000:abc9" es igual a „1234::abc9"[2].

Tomando la dirección de ejemplo: 2001:0000:1234:0000:0000:C1C0:ABCD:0876

Mediante la regla se puede escribir como: 2001:0000:1234:0000:0000:**c**1**c**0:**abcd**:0876

La dirección se puede escribir de forma resumida utilizando la regla b):
2001:**0**:1234:**0**:**0**:c1c0:abcd:**876**

Aplicando la regla c) se puede resumir aún más a: 2001:0:1234**::**c1c0:abcd:876

Tal como en el caso de IPv4, para señalar las secciones de la dirección que identifican a la red y al dispositivo, se utiliza el formato CIDR en la forma <dirección>/<prefijo>. (Dirección IPv6**:** Es una dirección IPv6 en alguna de las notaciones ya descritas prefijo o prefix**:** Es un valor decimal que especifica cuantos, de los bits más significativos, son considerados prefijo.) Por ejemplo, una dirección en la forma 3ffe:b00:c18:1::1/64 señala que los primeros 64 [bit] identifican a la red (3ffe:b00:c18:1) y los restantes 64[bit] identifican al dispositivo de dicha red (::1).

2.4 Direccionamiento IPv6

En IPv6 se han definido los siguientes tipos de direcciones:

- **Unicast:** Identifican a un nodo único y particular.
- **Multicast:** Identifican a un grupo de nodos. El trafico enviado a una dirección multicast es reenviado a todos los nodos pertenecientes al grupo
- **Anycast**: Identifica a un grupo de nodos. El tráfico enviado a una dirección anycast es enviado al nodo más cercano al emisor.
- **Dirección de Loopback (::1):** Ésta, sirve para enviar paquete de IPv6 de un nodo a si mismo

Se han eliminado las direcciones del tipo "broadcast", reemplazando su uso con direcciones "multicast" que identifican a determinados grupos de dispositivos en una red.

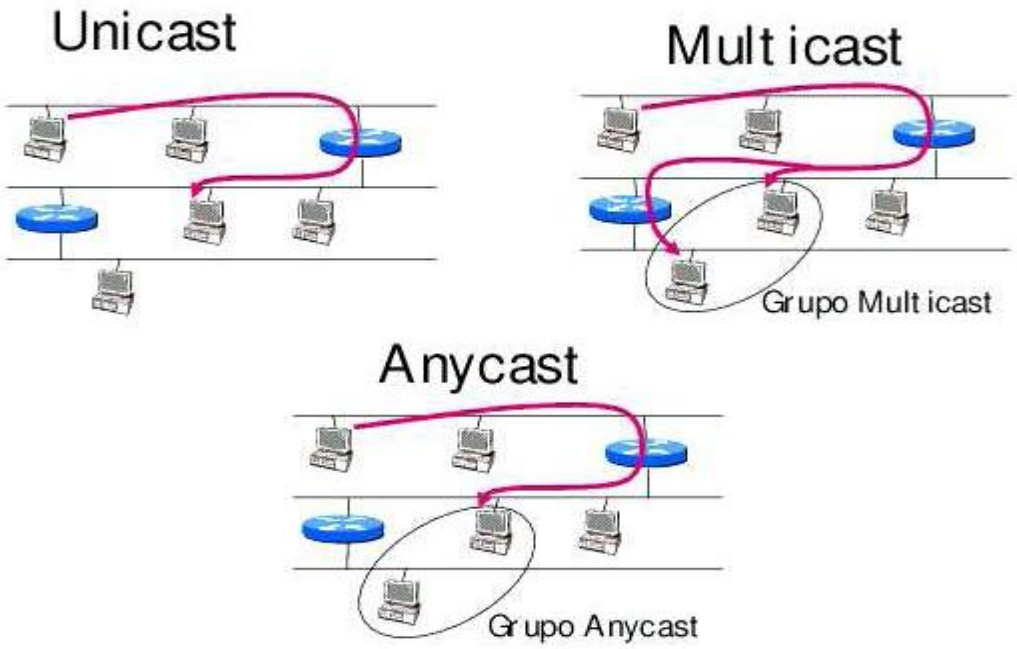


Figura 6 Tipos de direcciones IPv6

2.4.1 Unicast

Las direcciones "unicast" cumplen la función de individualizar a cada nodo conectado a una red. Esto permite otorgar conectividad punto a punto entre los nodos pertenecientes

a ella.

Uno de los nuevos aspectos introducidos en IPv6 es el uso de contextos en las direcciones "unicast". Los contextos definen el dominio de una red, ya sea lógico o físico. El poder reconocer el contexto al que pertenece una determinada dirección permite realizar un manejo óptimo de los recursos de la red, optimizando su desempeño.

En IPv6, las direcciones unicast pueden pertenecer a uno de los tres contextos existentes:

- Local al enlace ("link-local"): Identifica a todos los nodos dentro de un enlace (capa 2).
- Local único ("unique-local"): Identifica a todos los dispositivos dentro de una red interna o sitio, compuesta por varios enlaces o dominios capa 2.

- Global: Identifica a todos los dispositivos ubicables a través de Internet.

Estos contextos presentan una estructura jerárquica, tal como se observa en la Figura 7 El contexto global es el más amplio, englobando al resto.

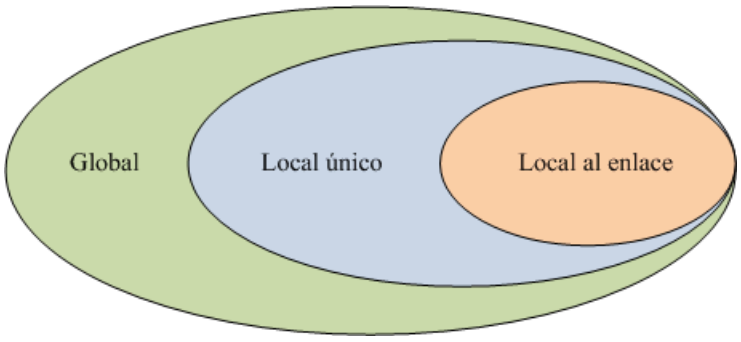


Figura 7 Contextos de direcciones "unicast".

A diferencia de IPv4, en IPv6 una interfaz puede poseer más de una dirección IP. Es así como por ejemplo un nodo puede poseer una dirección local al enlace para comunicarse con los dispositivos locales y una o más direcciones globales para

comunicarse hacia Internet.

2.4.1.1 Direcciones “unicast” locales al enlace

Las direcciones “unicast” locales al enlace son aquellas que permiten la comunicación entre los distintos nodos conectados a un mismo enlace capa 2 del modelo ISO/OSI. Estas direcciones no pueden ser enrutadas y sólo son válidas al interior del enlace.

Cada vez que un nodo IPv6 se conecta a una red, adquiere automáticamente una dirección local al enlace, sin ser necesaria la intervención del usuario o de otros dispositivos.

La estructura de una dirección local al enlace es “fe80:0:0:0:<identificador de interfaz>”“ . El identificador de interfaz se genera automáticamente a partir de su dirección MAC, siguiendo el formato EUI-64. En la Figura 8 se detalla cómo se construye el identificador de interfaz IPv6 a partir de la dirección MAC.

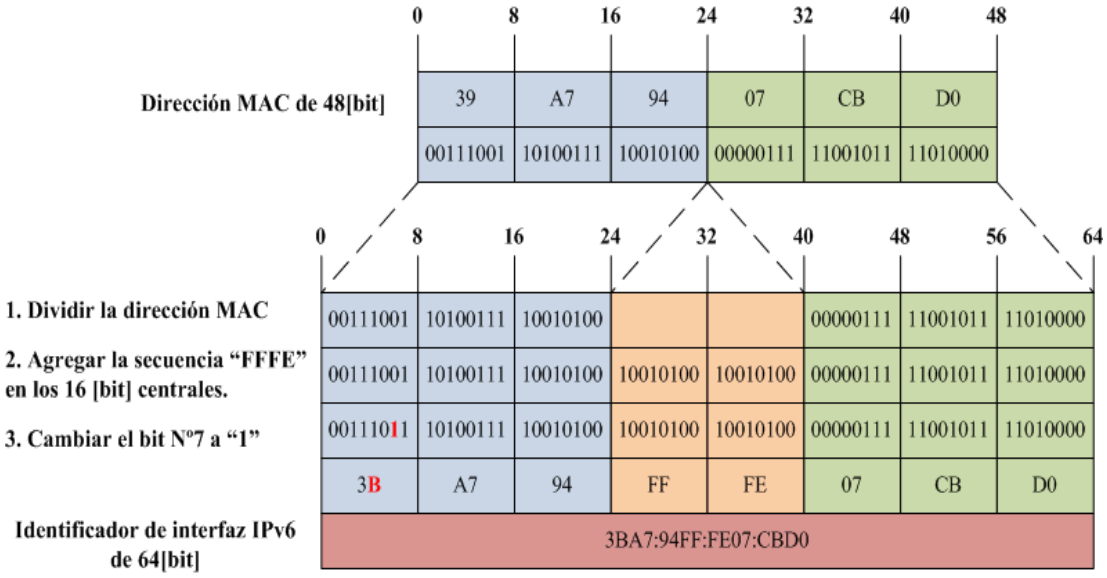


Figura 8 Creación del identificador de interfaz.

Las direcciones locales al enlace permiten proveer de forma rápida y simple conectividad entre los nodos conectados a un mismo enlace. Su principal ventaja es que no dependen de los prefijos IPv6 anunciados en una red, por lo que permiten identificar directamente a los nodos y “routers” presentes en un enlace.

2.4.1.2 Direcciones “unicast” locales únicas

Las direcciones locales únicas son direcciones que permiten la comunicación de nodos al interior de un sitio. Se entiende por sitio a toda red organizacional, de prefijo /48, compuesta por 1 o más subredes.

Son el equivalente a las direcciones privadas en IPv4, cumpliendo la misma función: proveer conectividad entre los nodos de un sitio ó “intranet”. Al igual que las direcciones locales al enlace, no pueden ser enrutadas hacia Internet. Su estructura se detalla en la Figura 9.

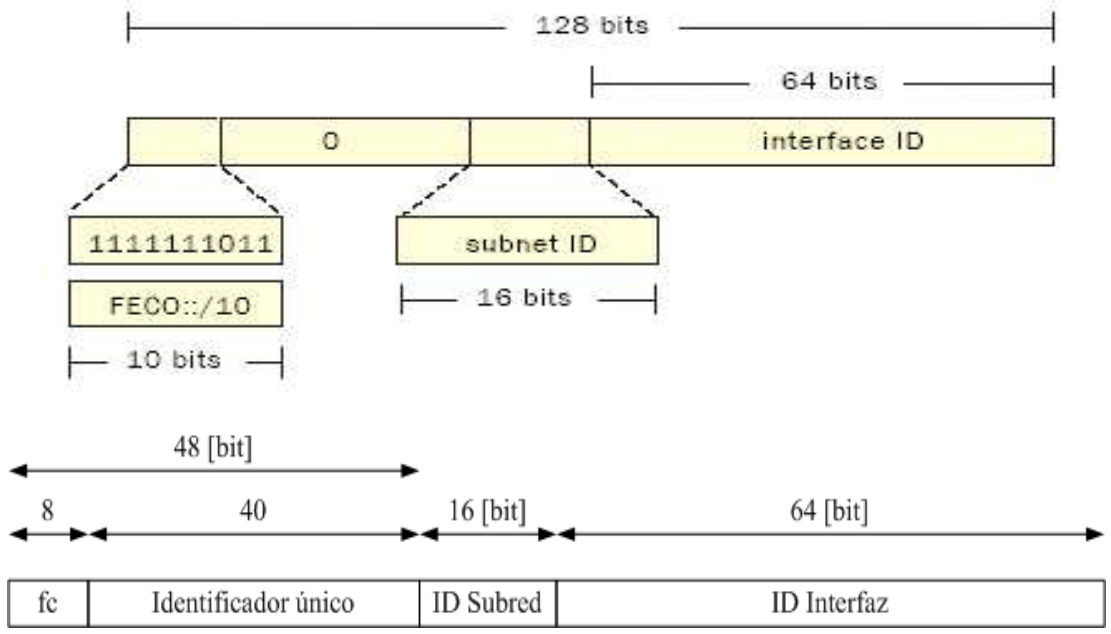


Figura 9 Estructura de una dirección local única.

Todas las direcciones locales únicas se encuentran dentro del rango dado por el prefijo fc00::/8. Los campos de una dirección “unicast” local única son:

- Identificador único: Es un valor de 40[bit] que identifica a un sitio en particular. Dado que este tipo de direcciones no son publicadas en Internet, pueden existir distintos sitios con el mismo identificador.

- Identificador subred: Permite crear un plan de direccionamiento jerárquico,

identificando a cada una de las 2^{16} posibles subredes en un sitio.

- Identificador de interfaz: Individualiza a una interfaz presente en una determinada subred del sitio. A diferencia de las direcciones locales al enlace, este identificador no se genera automáticamente.

2.4.1.3 Direcciones "unicast" Globales:

Las direcciones unicast globales son usadas para comunicar 2 nodos a través de Internet. Son el equivalente a las direcciones públicas en IPv4. Son el único tipo de direcciones que pueden ser enrutadas a través de Internet. El espacio reservado actualmente para este tipo de direcciones es de 2001:: a 3fff:ffff:ffff:ffff:ffff:ffff:ffff (2001::/3).

Todas las subredes en el espacio de direccionamiento unicast global tienen un prefijo de red fijo e igual a /64. Esto implica que los primeros 64 [bit] (los primeros 4 campos en formato hexadecimal) corresponden al identificador de red, y los siguientes corresponden a la identificación de la interfaz de un determinado nodo. En la Figura 10 se observa la estructura de una dirección unicast global.

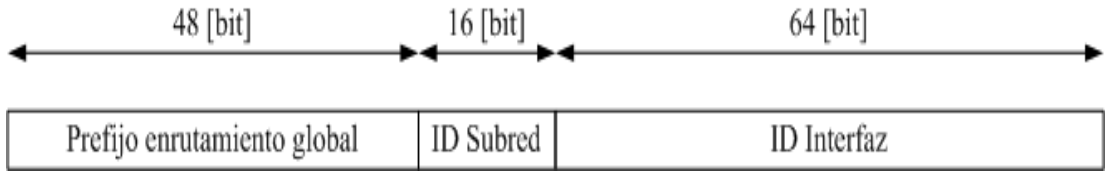


Figura 10 Estructura de una dirección "unicast" global.

El prefijo de enrutamiento global es aquel que identifica a un sitio conectado a Internet. Dicho prefijo sigue una estructura jerárquica, con el fin de reducir el tamaño de la tabla de enrutamiento global en Internet. En la Figura 11 se presenta la estructura utilizada actualmente para la delegación de prefijos.

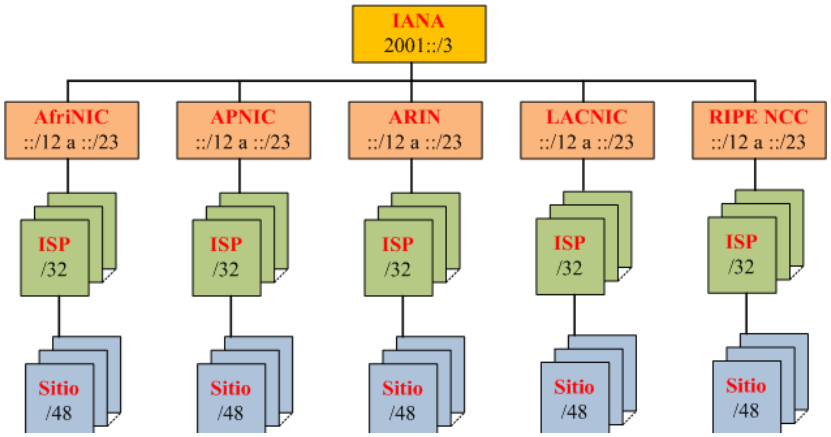


Figura 11 Jerarquía de delegación de prefijos "unicast" globales.

Del espacio total de direcciones Global Unicast administrador por el IANA, cada registro regional (RIR) maneja un prefijo /23, del cual entrega prefijos /32 a los proveedores de servicios presentes en cada región del planeta.

Los usuarios finales obtienen un prefijo /48 delegado directamente por sus proveedores de servicios. Un prefijo /48 permite que cada usuario cuente con un sitio o intranet compuesto por 2^{16} subredes, cada una con capacidad para conectar hasta 2^{64} dispositivos a Internet. O a su vez el usuario puede crear en sus instalaciones 65.535 subredes diferentes, que son las combinaciones creadas variando w,x,y,z en el grupo: **2001:db8:wxyz::/64**

Cada una de esas 65.535 subredes que nuestro cliente puede crear, puede a su vez tener más de 18 trillones de direcciones IP diferentes, que pueden ser de asignación por el cliente.

2.4.2 Multicast

Una dirección multicast en IPv6, identifica a un grupo de interfaces. Además, un interfaz puede pertenecer a cualquier número de grupos multicast. Estas direcciones tienen el siguiente formato:

Figura 12 Formato de direcciones "multicast".

Donde el prefijo 11111111 ó 0xFF identifica la dirección como multicast, el campo flag es un conjunto de 4 flags, el campo scope indica el alcance de cada dirección multicast en concreto (desde alcance de interfaz hasta alcance global) y el group ID identifica al grupo multicast.

En IPv6 el tráfico "multicast" opera de la misma forma que en IPv4. Dispositivos IPv6 ubicados en distintos lugares pueden recibir tráfico dirigido a una única dirección "multicast". Las direcciones IPv6 "multicast" tienen la estructura presentada en la Figura 13

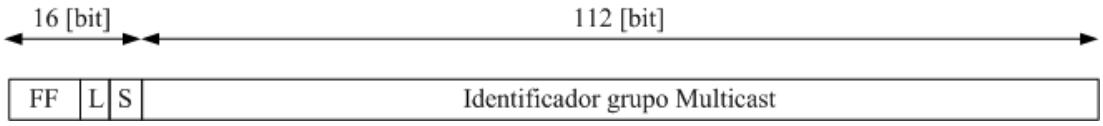


Figura 13 Estructura direcciones "multicast".

El campo L indica el tiempo de vida de un grupo "multicast", tomando el valor de 0 cuando es un grupo permanente y 1 cuando es un grupo "multicast" temporal. El campo S indica el contexto o alcance del grupo, de acuerdo a los valores presentados en la Tabla 2.1.

Valor de S (hexadecimal de 4 [bit])	**Contexto del Grupo**
1	Interfaz
2	Enlace
5	Sitio
8	Organización

E	Global
Otros valores	Sin asignar o reservado

Tabla 1 Códigos de contexto en una dirección "multicast".

IPv6 elimina el uso de las direcciones "broadcast", sustituyéndolas por direcciones "multicast". Esto permite hacer una selección más precisa de los destinatarios de una solicitud, evitando sobrecarga de mensajes en redes de muchos nodos. En la Tabla 2.2 se muestran algunos de los grupos multicast fijos existentes.

Direcciones IPv6 Multicast	**Descripción**
FF02::1	Todas las direcciones de todos los nodos son usadas para alcanzar a todos los nodos en el mismo enlace.
FF02::2	Todas las direcciones de los routers son usadas para alcanzar a todos los routers en el mismo enlace.
FF02::4	La dirección es usada para alcanzar a todos los protocolos de enrutamiento multicast de vector distancia (DVMRP) que usan los routers multicast en el mismo enlace.
FF02::5	La dirección es usada para lcanzar a todos los routers que usan OPSF en el mismo enlace.
FF02::1:FFXX:XXXX	La dirección solicitada del nodo es usada en el proceso de resolución de direcciones para resolver la dirección IPv6 de un nodo en el mismo enlace, a una dirección de capa de red. Los 24 bits últimos de la derecha de la dirección del

	nodo, son los mismos 24 bits últimos de la derecha de una dirección unicast.

Tabla 2 Direcciones reservadas para Multicast.

2.4.2.1 Dirección multicast de nodo solicitado

Para realizar la asociación entre direcciones capa 2 (MAC) y direcciones IPv6, se utiliza la dirección "multicast" de nodo solicitado. Esta dirección contiene parte de la dirección IPv6 que se desea consultar y posee la estructura descrita en la Figura 14

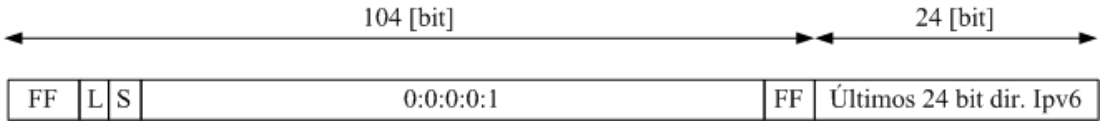


Figura 14 Estructura dirección "multicast" de nodo solicitado

Cada vez que un nodo se configura con una dirección IPv6, se une automáticamente al grupo multicast indicado por su dirección de nodo solicitado. Dado que dicha dirección toma solo los últimos 24 bit de la dirección IPv6, en un mismo grupo multicast pueden existir varios nodos con distintas direcciones IP. En la Tabla 2.3 se pueden observar algunas direcciones IPv6 y sus correspondientes direcciones multicast de nodo solicitado.

Dirección IPv6	**Dirección multicast de nodo solicitado**
2800:270:bcd0:3::1	ff02::1:ff00:1
2800:270::1230:1000:a34:9e9a	ff02::1:ff34:9e9a
2800:270::34de:2000:a34:9e9a	ff02::1:ff34:9e9a
fc00:0:0:1::aaaa:a1	ff02::1::ffaa:a1

Tabla 3 Ejemplos direcciones "multicast" de nodo solicitado.

Cuando un nodo desea enviar un paquete a un vecino presente en el mismo enlace y no tiene su dirección física, envía un mensaje que contiene la dirección IPv6 a consultar al grupo "multicast" de nodo solicitado correspondiente dicha dirección. Todos los nodos que estén en dicho grupo multicast reciben el mensaje, pero solo responde el nodo configurado con la dirección IPv6 solicitada.

2.4.3 Anycast

Una dirección "anycast" es aquella que identifica a un grupo de interfaces. Los paquetes enviados a una dirección anycast son reenviados por la infraestructura de enrutamiento hacia la interfaz más cercana al origen del paquete. Con el fin de facilitar la entrega, la infraestructura de enrutamiento debe conocer las interfaces que están asociadas a una dirección anycast y su distancia en métricas de enrutamiento

Para configurar una dirección "anycast", basta con configurar una misma dirección unicast en distintos dispositivos, junto con configurar en cada "router" una ruta directa hacia dicha dirección (/128). La idea es que cada "router" posea en su tabla de enrutamiento varias entradas hacia la misma dirección, con sus métricas asociadas. Al fallar la ruta más cercana, se selecciona automáticamente la siguiente.

El uso de "anycast" permite entre otras cosas implementar balanceo de carga y tolerancia a fallas. Por lo general, su uso se suele restringir al contexto de un sitio o red local. Las direcciones "anycast", al igual que las "multicast" solo son válidas como direcciones de destino en los paquetes IPv6.

2.4.4 Dirección de Loopback (::1)

La dirección 0:0:0:0:0:0:0:1 es llamada dirección de loopback. Ésta, sirve para enviar un paquete de IPv6 de un nodo a sí mismo. No puede ser asignada a ningún interfaz físico, sino que debe entenderse como la dirección link-local asignada a un interfaz virtual unido a un enlace que no va a ninguna parte. Al igual que la dirección unspecified, la dirección de loopback no puede ser usada como dirección origen en paquete salientes, y si un paquete tiene la dirección de loopback como destino no debe ser enviado fuera del nodo ni debe ser encaminado por los routers.

Direcciones	Uso
0:0:0:0:0:0:0:1 (::1)	Es la equivalente a 127.0.0.1 (localhost)
0:0:0:0:0:0:192.168.1.1	Formato para escribir IPv4 en una red IPv6/IPv4.
2000::/3 a 3fff:ffff:ffff:ffff:ffff:ffff:ffff	Rango de direcciones global unicast. 2 nodos a través de Internet
FC00::/7	Rango de direcciones unique local unicast. Intranet
FE80::/10	Rango de direcciones link-local unicast.
FF00::/8	Rango de direcciones multicast.
3FFF:FFFF::/32	Reservado para ejemplos y documentación.
2001:0DB8::/32	También reservado para ejemplos y documentación.

Tabla 4 Rango de direcciones IPv6

2.5 Protocolos de Enrutamiento

El uso de IPv6 no implica cambios significativos en la forma en que operan los protocolos de enrutamiento en las redes IP. Sin embargo, para aprovechar las nuevas características de IPv6, se han desarrollado nuevas versiones o complementos a los protocolos de enrutamiento más utilizados. En la Tabla 2.5 se presentan las nuevas versiones desarrolladas para IPv6.

Protocolo enrutamiento	Versión IPv6
RIP	RIPng
OSPF	OSPFv3
STATIC	STATIC for IPv6

Tabla 5 Protocolos de enrutamiento en IPv6

2.5.1 Mecanismos de configuración de direcciones STATICOS, RIPng, OSPFv3

2.5.1.1 Enrutamiento Staticos

En esta guía se describe cómo configurar rutas estáticas para IPv6. Este enrutamiento define las rutas que los paquetes viajan por la red. Al configurar manualmente las rutas estáticas para redes pequeñas ya no es necesario utilizar protocolos de enrutamiento dinámico.

Los dispositivos Ethernet reenvían los paquetes con información de la ruta que está configurado de formas manuales aprendidas mediante el protocolo de enrutamiento estático, además definen un camino de modo explícito entre dos dispositivos de red. A diferencia de un protocolo de enrutamiento dinámico, las rutas estáticas no se actualizan automáticamente y debe volver a configurar manualmente si cambia la topología de la red.

Las ventajas de usar rutas estáticas:

- Incluyen la seguridad y la eficiencia de los recursos.
- Las rutas estáticas utilizan menos ancho de banda que protocolos de enrutamiento dinámico y ciclos de CPU no se utilizan para calcular y comunicar las rutas.

La principal desventaja de usar rutas estáticas:

- Es la falta de reconfiguración automática, si cambia la topología de red.

2.5.1.1.1 Rutas estáticas recursivas

Una ruta estática recursiva, es cuando sólo el siguiente salto se especifica. Y la interfaz de salida se deriva del siguiente salto.

2.5.1.2 Enrutamiento RIPng

RIPng es un protocolo de vector de distancia. RIPng debe ser implementado solo en Routers que soporte IPv6 provee otros mecanismos para descubrimiento de rutas. El protocolo cuenta sobre el acceso de cierta información acerca de cada una de esas redes,

de lo cual lo más importante es su métrica. La métrica RIP de una red es un entero entre 1 y 15, inclusive. Esto es establecido en alguna forma no especificada en este protocolo; sin embargo, dado el máximo número de saltos es de 15, usualmente es usado un valor de 1. Las implementaciones deben permitir al administrador del sistema establecer la métrica de cada red. En adición a la métrica, cada red tendrá un prefijo de dirección destino y la longitud del prefijo asociado a este. Estos son establecidos por el administrador del sistema de una manera no especificada en este protocolo.

Cada router que implementa RIP es asumido que tiene una tabla de ruteo. Esta tabla tiene una entrada para cada destino que es asequible desde todas partes por el Sistema Operativo RIP. Cada entrada contiene al menos la siguiente información:

- El prefijo IPv6 del destino.
- Una métrica, la cual representa el costo total de obtener un datagrama desde el router a este destino. Esta métrica es la suma de los costos asociados con las redes que serian recorridas para obtener el destino.
- La dirección IPv6 del próximo router pertenece al camino del destino. Si el destino está sobre una de las redes directamente conectadas, este punto no es necesario.

Las entradas para las redes directamente conectadas son establecidas por el router usando información recolectada que en ningún caso es especificada en este protocolo. La métrica para una red directamente conectada es establecer el costo de esta red.

Los implementadores pueden también seleccionar el permitir al Administrador del Sistema introducir rutas adicionales. Esto sería más parecido a rutear hosts o redes fuera del alcance del Sistema de ruteo. Esto es referido como “Rutas Estáticas”. Las entradas para otros destinos que son inicialmente son sumadas y actualizadas por ciertos algoritmos.

2.5.1.2.1 Sus Limitaciones

RIP es una clase de algoritmos conocidos como Algoritmos de Vector de Distancia. Y tiene ciertas limitaciones:

- El protocolo está limitado a redes las cuales el tamaño máximo de saltos es de 15. Los diseñadores creen que el diseño básico del protocolo es inapropiado para redes grandes.

- El protocolo depende de "contar hasta el infinito" para resolver ciertas situaciones inusuales. Si el sistema de red tiene cientos de redes, y un lazo de ruteo es creado para envolverlos a todos, la resolución del lazo requeriría mucho tiempo o mucho consumo de ancho de banda. Tal como un lazo podría consumir una gran cantidad de ancho de banda en la red antes de que sea corregido.

- Este protocolo usa métricas fijas para comparar rutas alternativas. Esto no es apropiado para situaciones donde las rutas necesitan ser seleccionadas, basadas en parámetros tales como una medida de retardo, confiabilidad o carga. Las extensiones obvias permiten métricas de este tipo que son parecidas a introducir las características de una clase que los protocolos no están diseñados para manejar.

2.5.1.3 Enrutamiento OSPFv3

Este protocolo está diseñado para ejecutarse como un protocolo de enrutamiento para un único sistema autónomo. OSPF para IPv6 es una adaptación del protocolo OSPFv2 para IPv4.

El costo de OSPF para cada enlace es un número único, el cual es asignado por el administrador de la red y puede incluir factores como retraso, ancho de banda y costo monetario. El costo acumulado en los segmentos de red debe ser inferior a 65535. Los mensajes de OSPF se envían como PDUs de capa superior.

Este protocolo de estado de enlace para IPv6 presenta los siguientes cambios en relación a la versión 2:

- La estructura de los paquetes OSPF ha sido modificada para eliminar las dependencias del direccionamiento en IPv4 y utilizar IPv6.

- Los Nuevos paquetes LSAs son definidas para los prefijos y direcciones en IPv6. OSPF se ejecuta en cada enlace en lugar de ejecutarse en cada subred.
- Cada router tiene su LSA que describe su estado actual. La LSA de cada router OSPF se propaga de manera eficiente en toda la red a través de las relaciones lógicas entre los vecinos, llamadas también adyacencias; cuando la propagación de todas las LSAs se ha completado se puede decir que la red OSPF ha convergido.
- Mecanismos para el descubrimiento de vecinos llamada también de adyacencias, cuando la propagación de todas las LSAs se ha completado se puede decir que la red OSPF ha convergido.
- Utiliza mecanismos estandarizados de autentificación
- Utiliza direcciones de enlace local

Sus semejanzas son:

- Tipos básicos de paquetes
- Hello, DBD, LSR, LSU, LSA
- Mecanismos para el descubrimiento de vecinos y la formación de adyacencias
- Tipos de Interfaces
- P2P, P2MP, Broadcast, Virtual
- Propagación y remoción de LSAs
- Tipos muy similares de LSAs

Basado en la colección de LSAs de conocidos como base de datos del estado del enlace (LSDB) OSPF calcula el camino de menor costo para cada ruta y esos caminos se convierten en rutas en la tabla IPv6 de enrutamiento. Para reducir el tamaño de los LSDBs, OSPF permite la creación de zonas. Un área OSPF es la agrupación de segmentos de redes contiguos. En todas las redes OSPF debe haber por lo menos un área llamada el área de backbone.

En el LSA se almacena en una base de datos de enlace del Estado. El contenido de la base de datos, se crea la tabla de enrutamiento OSPF. La diferencia entre la base de

datos y la tabla de enrutamiento es que la base de datos contiene una completa colección de datos en bruto; la tabla de enrutamiento contiene una lista de rutas más cortas a destinos específicos conocidos a través de puertos de interfaz del router.

2.6 Mecanismos de transición de IPv4/IPv6

IPv6/IPv4 coexistirán durante muchos años. Una amplia gama de técnicas se han definido que permiten la coexistencia y proporciona una transición fácil. Hay tres categorías principales que a continuación indicamos:

- Mecanismo Dual-stack. Permiten a IPv4 y a IPv6 coexistir en los mismos dispositivos y redes

- Mecanismo de Tunneling. Permiten el transporte de tráfico de IPv6 a través de la infraestructura de IPv4 existente.

Estos mecanismos pueden y probablemente se usarán combinándolas entre sí. La migración a IPv6 puede hacerse paso a paso, empezando con un solo host o subnet. Se puede igualmente emigrar su red corporativa, o partes de la misma, mientras su ISP todavía trabaja sólo con IPv4. O su ISP puede actualizar a IPv6 mientras su red corporativa todavía ejecuta IPv4. Este capítulo describe las principales técnicas disponibles y factibles de implementar hoy en día. Conforme IPv6 siga creciendo en nuestras redes, se definirán nuevas herramientas y mecanismos para que la transición sea fácil de realizar.

A continuación vamos a describir brevemente cada técnica para luego pasar a analizar los métodos más importantes y que se usan con más frecuencia en el proceso de migración.

2.6.1 Mecanismo Dual Stack Transition Mechanism o Doble Pila

Un nodo dual-stack tiene el apoyo completo de ambas versiones protocolares. Este tipo de nodo es a menudo llamado un nodo IPv6/IPv4. En la comunicación con un nodo IPv6, este se comporta como un nodo IPv6 único, y en la comunicación con un nodo

IPv4, este se comporta como un nodo IPv4 único. Las aplicaciones tienen un interruptor de configuración probablemente para habilitar o desactivar una de las pilas. Así que este tipo de nodo puede tener tres modos de funcionamiento. Cuando la pila de IPv4 se habilita y la pila de IPv6 es desactivada, el nodo se comporta como un nodo IPv4 único. Cuando la pila de IPv6 se habilita y la pila de IPv4 es desactivada, se comporta como un nodo IPv6 único. Cuando se habilitan las pilas tanto en IPv4 y de IPv6, el nodo puede usar ambos protocolos. Un nodo IPv6/IPv4 tiene una dirección por lo menos para cada versión protocolar.

La desventaja de esta técnica es que se debe realizar una actualización de software de red para ejecutar las dos pilas del protocolo separadas. Esto significa que todas las tablas (por ejemplo, las tablas de ruteo) se guarda simultáneamente, mientras los protocolos de ruteo se configuran para ambos protocolos. Para la administración de red, se tiene comandos separados dependiendo del protocolo (por ejemplo, ping.exe para IPv4 y ping6.exe para IPv6) y esto consume más memoria y poder del CPU.

2.6.1.1 Tipos de DSTM (Dual Stack Transition Mechanism o Doble pila)

El DSTM se compone de dos métodos en particular:

AIIH (Asignación de direcciones de IPv4 a IPv6 para host) y DTI (Interfaz Dinámica de Tunel):

- AIIH es un método que permite asignar temporalmente direcciones IPv4 a hosts Dual Stack dentro de una red IPv6, El entorno DSTM trabaja solamente con hosts Dual Stack. Se necesita un servidor encargado de asignar temporalmente direcciones IPv4 a los hosts, el cual generalmente utiliza DHCPv6, ya que DHCPv4 no puede ser utilizado dentro de una red IPv6. También se necesita un servidor para resolución de DNS y un enrutador frontera con soporte Dual Stack para comunicar el dominio IPv6 a un dominio exterior o al Internet.
- DTI es una interface diseñada para encapsular paquetes IPv4 dentro de paquetes IPv6. La unión de ambos métodos da como resultado el mecanismo DSTM, el cual tiene como objetivo que un host IPv6 obtenga una dirección IPv4 para establecer comunicación con hosts que manejen exclusivamente direcciones IPv4. DSTM permite también ejecutar aplicaciones IPv4 sin modificación

alguna, y solo se puede aplicar dentro de una red IPv6. A continuación se muestra un esquema del mecanismo DSTM

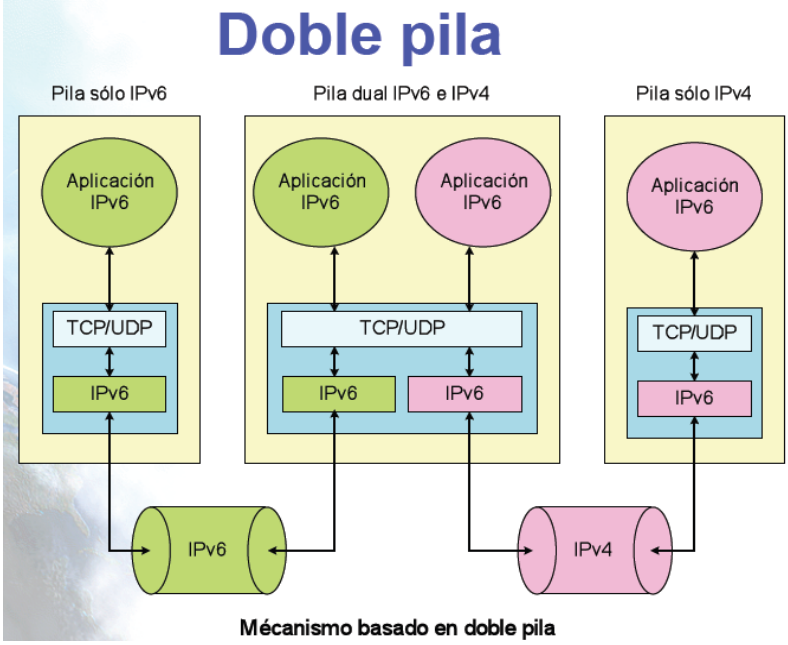


Figura 15 Esquema Dual Stack

2.6.2 Mecanismo de Tunneling o Túnel

Los mecanismos de **Tunneling** pueden usarse para desplegar una infraestructura IPv6 mientras la infraestructura IPv4 todavía sea la base. El Tunneling puede usarse para llevar trafico IPv6 encapsulándolo en los paquetes IPv4 y además sobre una infraestructura de ruteo IPv4. Por ejemplo, si un proveedor todavía tiene una infraestructura IPv4 única, el tunneling permite tener una red IPv6 corporativa y un túnel a través de la red IPv4 de su ISP para localizar otro host o red IPv6.

Estos son algunos mecanismos de transición basados en túneles:

- 6in4 (*) [6in4]
- TB (*) [TB]
- 6over4 [6over4]
- Teredo (*) [TEREDO], [TEREDOC]

2.6.2.1 Tipos de túneles

Los siguientes son los principales tipos de túneles y los más utilizados:

- Túneles de tipo 6to4. Permiten a dominios IPv6 aislados que cuenten con una conexión directa a una red IPv4 o al Internet, poder establecer comunicación con otros dominios IPv6 con una mínima configuración manual. Este tipo de túneles se utiliza comúnmente en redes aisladas o privadas.

- Tunnel Broker Es un intermediario al que el usuario final se conecta, normalmente con un interfaz web, que usuario solicita al TB la creación de un túnel y este le asigna una dirección IPv6 y le proporciona instrucciones para crear el túnel en el lado del usuario.

Los túneles manualmente configurados han sido de gran ayuda hasta la fecha, pero requieren una estricta supervisión y mantenimiento de parte de los administradores de las redes, por lo cual este tipo de túneles ya son muy poco utilizados y están al borde de desaparecer

2.6.2.1.1 Tunnel Broker

Desde el comienzo de IPv6 y durante su crecimiento, se ha tenido la necesidad de utilizar la infraestructura de red existente, es decir, la infraestructura IPv4. La mayoría de ellas están conectadas por una variedad de túneles de distintos tipos, cada uno de ellos con un objetivo en especial, pero al mismo tiempo con ciertos problemas o limitaciones.

2.6.2.1.1.1 Descripción de TB

La idea principal de este método es tener servidores dedicados, llamados TB’s, que se encarguen de configurar túneles de una manera automática en respuesta a requisiciones hechas por los usuarios de este servicio, y de esta manera aumentar el número de hosts que se encuentran actualmente conectados a una red IPv6. Se espera que en un futuro existan varios tipos de TB’s, de manera que el usuario pueda seleccionar de una lista el que mejor se acomode a sus necesidades, por ejemplo el

más cercano, el más barato, etc.

El método de TB permite a hosts Dual Stack que cuenten con una conexión a una infraestructura IPv4, crear túneles automáticamente para poder establecer una comunicación con dominios IPv6.

A continuación se muestra el entorno de un TB de una manera gráfica:

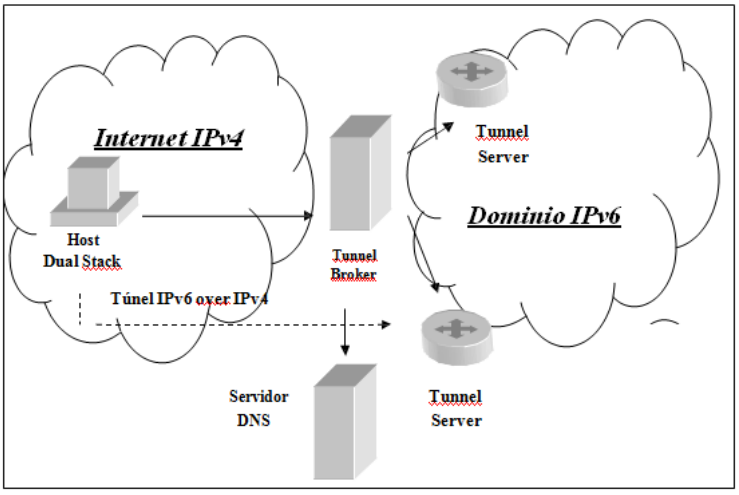


Figura 16 Entorno Tunnel Broker

El TB es en ocasiones una interface de tipo Web, donde el usuario se registra para obtener un túnel. En esta interface los túneles pueden ser creados, modificados o eliminados, de acuerdo a las necesidades del usuario. El TB puede repartir la carga entre varios Tunnel Servers (TS), e indicarles la configuración del túnel en cuestión. El TB también se encarga de dar de alta la dirección IPv6 del usuario, así como su nombre en el DNS. El TB debe tener una dirección IPv4 a la cual pueda comunicarse el usuario. También puede tener una dirección IPv6, pero ésta es opcional. La comunicación entre el TB y el usuario se puede realizar por medio de IPv4 o IPv6.

Un TS es un enrutador de tipo Dual Stack que se encarga de crear, modificar o eliminar túneles, basándose en las órdenes recibidas por el TB. El TS también puede guardar una estadística del uso de los túneles que administra y enviársela al TB para la toma de decisiones sobre los distintos túneles. Un TS debe tener una conexión directa a un dominio IPv6 o al Internet IPv6.

2.6.2.1.1.2. Funcionamiento de TB

Como se había mencionado anteriormente, el usuario o cliente del TB es un nodo Dual Stack, ya sea un host o un enrutador.

El TB debe contar con algún tipo de verificación de autenticidad del cliente, para evitar el uso no autorizado del servicio. El cliente debe proveer cierta información al TB para que se pueda configurar el túnel. Además, debe indicarle su dirección IPv4, un nombre para asociar la dirección IPv6 y también le debe indicar si es un host o un enrutador.

En caso de ser un enrutador IPv6 que va a proporcionar servicio a varios hosts IPv6, debe indicar también la cantidad de hosts para que le sea asignado un prefijo de acuerdo a sus necesidades, en lugar de una sola dirección.

Con la información necesaria y provista por el cliente, el TB decide que TS asignarle, basándose en la carga de tráfico que tenga cada TS. Después decide el prefijo IPv6 que va a asignarle al cliente. Este prefijo puede ir desde 0 hasta 128 bits, los más comunes son 48 (prefijo de sitio), 64 (prefijo de subred) o 128 (prefijo de host). Las direcciones IPv6 asignadas a ambos extremos del túnel deben ser globales y pertenecer al espacio de direcciones del TB.

Otras de las funciones del TB son decidir el tiempo de vida del túnel, registrar el nombre asociado con la dirección IPv6 en el DNS, configurar el TS y notificar al cliente la configuración del túnel y su nombre de dominio en el DNS.

2.6.3 Túnel 6to4

Este método es también conocido como Connection of IPv6 Do mains via IPv4 Clouds (conexión de dominios IPv6 por medio de nubes IPv4). Y actualmente es el más recomendado y utilizado, esencialmente por que este método permite a sitios o hosts IPv6 comunicarse entre ellos a través de una red IPv4, sin necesidad de configuración manual de túneles, y permite que dichos sitios o hosts se comuniquen

con el Internet IPv6 por medio de enrutadores 6to4 Relay.

Este método debe ser temporal, y se utilizará mientras se obtenga una conexión IPv6 nativa, es decir, mientras se lleva a cabo la transición de IPv4 a IPv6. No fue diseñado como una solución permanente.

El esquema de este método se muestra en la figura siguiente:

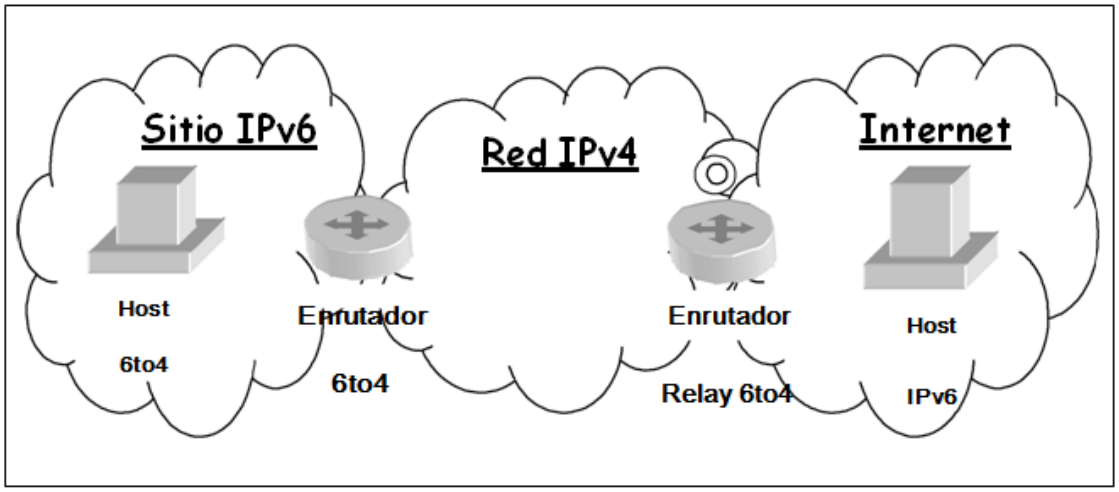


Figura 17 Entorno 6to4

Dentro de este entorno encontramos principalmente 3 elementos:

- Un host 6to4 es un host IPv6 que tiene configurada al menos una dirección de tipo 6to4. Estos hosts no requieren configuración manual, comúnmente cuentan con un mecanismo de autoconfiguración.

- Un enrutador 6to4 es un enrutador Dual Stack que soporta el uso de túneles 6to4, el cual sirve para intercambiar paquetes de tipo 6to4 entre enrutadores del mismo tipo y sitios o hosts IPv6. Estos enrutadores requieren configuración manual adicional, ya que son los encargados de encapsular y decapsular los paquetes.

- Un enrutador 6to4 Relay se puede definir como un enrutador 6to4 configurado para soportar el enrutamiento de tránsito entre direcciones 6to4 y direcciones IPv6 nativas. Este enrutador debe tener al menos una interface 6to4 y una interface IPv6 nativa, para poder establecer comunicación entre dominios

IPv4 e Pv6.

2.6.3.1 Dirección 6to4

Una dirección de tipo *6to4*, está conformada por distintas partes como se muestra en la siguiente figura:

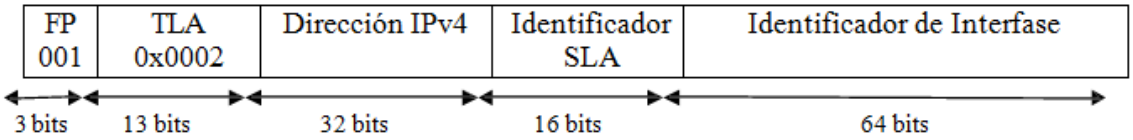


Figura 18 Estructura de Dirección Unicast Globales Agregables

Este tipo de dirección utiliza el prefijo 001, el cual identifica a las direcciones Unicast Globales Agregables, seguido por un identificador TLA de 13 bits asignado por IANA, cuyo valor es 0x0002. Después le sigue la dirección IPv4 del sitio, así como un identificador SLA y el identificador de interface.

Todo esto se puede expresar 2002:DirecciónIPv4::/48. La forma en que se convierte la dirección IPv4 al formato para estas direcciones se muestra a continuación:

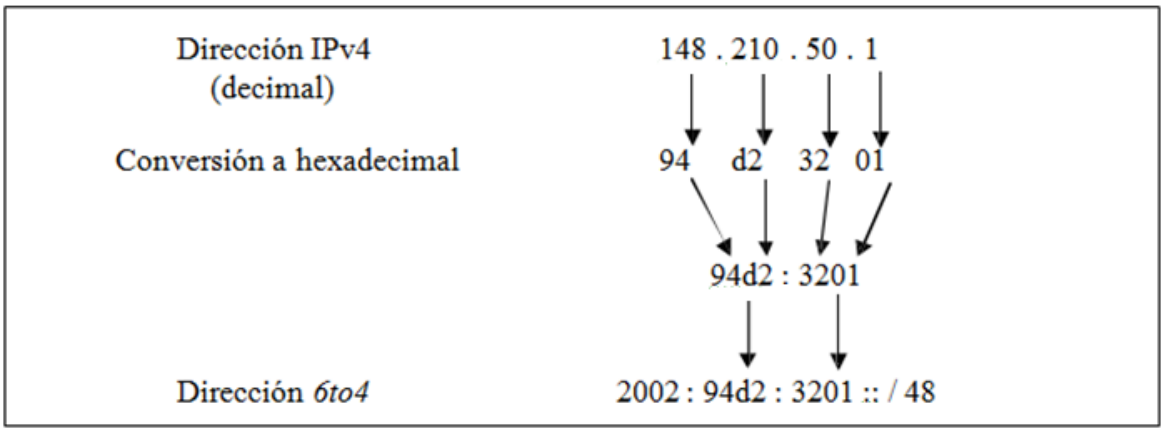


Figura 19 Conversión de dirección IPv4 a dirección 6to4

2.6.3.1.1 Selección de dirección

En caso de que un host tenga una dirección 6to4, y el host con el que quiere establecer

comunicación tenga una dirección 6to4 y una dirección IPv6 nativa, es recomendable que ambos hosts establezcan la comunicación utilizando 6to4. En caso de que ambos hosts tengan direcciones 6to4 y direcciones IPv6 nativas, se puede establecer la comunicación siempre y cuando ambos hosts utilicen el mismo tipo de direcciones, aunque es recomendable que la comunicación se realice por medio de direcciones IPv6 nativas.

2.6.3.2 Encapsulación 6to4

En el método de 6to4 se utiliza la encapsulación de paquetes IPv6 dentro de paquetes IPv4. El campo "Protocolo" de la cabecera IPv4 debe ser igual a 41, que es el número asignado para este tipo de encapsulación o túneles. Las direcciones de destino y origen, ubicadas en la cabecera IPv4, pueden ser las mismas direcciones del campo que contiene la dirección IPv4 en el prefijo formado para las direcciones 6to4.

2.6.3.3. Tipos de comunicación

Los enrutadores IPv6 dentro de un mismo sitio publican prefijos 2002:DirecciónIPv4:IdentificadorSLA::/64 para permitirle a los hosts crear direcciones 6to4 auto configuradas. Los hosts o subredes individuales se configuran automáticamente con una ruta de 64 bits de una subred para intercambio directo entre hosts vecinos. Cualquier paquete IPv6 que no contenga un prefijo de 64 bits similar al de alguna de las subredes del sitio, será enviado al enrutador 6to4 colocado en la frontera del sitio.

Con el método de 6to4 se pueden efectuar varios tipos de comunicación. A continuación se muestra un entorno para ejemplificar los diferentes tipos de comunicación:

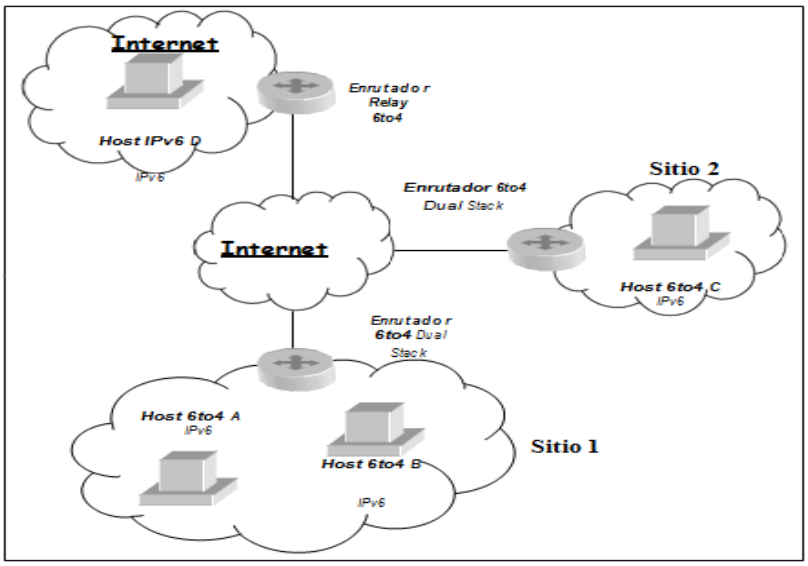


Figura 20 Comunicación 6to4

2.6.3.3.1 Comunicación del Host A al Host B. Un host 6 to4 puede establecer comunicación con un host 6to4 dentro de su mismo sitio. El host origen (Host A) envía el paquete al host solicitado (Host B) utilizando la infraestructura del sitio local (Sitio 1).

2.6.3.3.2 Comunicación del Host A al Host C. Un host 6to4 puede establecer comunicación con hosts 6to4 en otros sitios. Lo primero que hace el host origen (Host A) es mandar el paquete al enrutador 6to4 local (Sitio 1). Después este se encarga de hacerlo llegar al enrutador 6to4 del sitio solicitado (Sitio 2) por medio de la creación de túneles en la infraestructura IPv4. Por último, el enrutador en el sitio destino (Sitio 2) se encarga de decapsular el paquete y entregarlo al host solicitado (Host C) utilizando la infraestructura IPv6 del sitio.

2.6.3.3.3 Comunicación del Host A al Host D. Un host 6to4 puede establecer comunicación con hosts en el Internet IPv6. Lo primero que hace el host origen (Host A) es mandar el paquete al enrutador 6to4 local (Sitio 1). Después este se encarga de hacerlo llegar a un enrutador

6to4 Relay, el cual tenga acceso a ambos entornos, Internet IPv4 e Internet IPv6. Por último, el enrutador 6to4 Relay se encarga de decapsular el paquete y entregarlo al host solicitado (Host D) utilizando la infraestructura IPv6 del sitio.

2.6.3.4 Mantenimiento de los túneles

Los túneles ocupan muchos recursos de los TS's, tales como memoria y tiempo de procesamiento, y por eso es indispensable contar con un mecanismo encargado de la administración y manejo de estos túneles.

En la mayoría de los casos esto puede ser controlado con el tiempo de vida que asigne el TB, pero el problema surge cuando el cliente está utilizando una conexión en la que las direcciones se asignan dinámicamente. Por ejemplo, los usuarios que se conectan a su proveedor de Internet mediante módems, en donde un servidor DHCP se encarga de asignarles una dirección cada vez que accedan, la cual la mayoría de las veces es diferente a la que habían usado previamente.

En este caso es recomendable que el cliente utilice el túnel, y al terminar su conexión, el túnel sea eliminado, ya que al volver a acceder al Internet tendría una nueva dirección IPv4 y tendría que reconfigurar el túnel. Esta reconfiguración consumiría tal vez los mismos recursos que crear un nuevo túnel, y no es recomendable. Otra opción sería que los TS's informaran continuamente al TB acerca del estado del túnel, y contar con un mecanismo encargado de revisar el estado de la conexión del cliente, y tan pronto éste se desconecte, el túnel sea eliminado.

El mantenimiento de un túnel utiliza muchos recursos de los TS's, lo que implica un costo extra, pero evitaría algunos problemas. De esta manera, cuando el cliente se conecte al Internet, aunque sea con una dirección IPv4 diferente, solamente tendría que accesar al TB y proveer su nueva dirección IPv4 y crear el túnel de nuevo. Así, el cliente podría utilizar las mismas direcciones IPv6 asignadas e incluso el mismo nombre de dominio en el DNS.

CAPITULO III

3. ANÁLISIS COMPARATIVO DE IPV4/IPV6 Y DEL MECANISMO DE TRANSICIÓN Y COEXISTENCIA

3.1 Introducción

El protocolo IP fue desarrollado en 1973 junto con el protocolo TCP, como parte de un proyecto patrocinado por la Agencia de Programas Avanzados de Investigación (ARPA) del departamento de Defensa de los Estados Unidos (DoD). Se encuentra en la capa de red del modelo OSI, es un protocolo no orientado a conexión y no confiable; cada paquete es tratado de manera independiente de todos los demás y la entrega de paquetes no se garantiza.

El protocolo IP permite la interconexión de redes, proporcionando un esquema de transporte para el envío de paquetes desde un origen a un destino sin importar si se encuentran o no en diferentes redes. El envío de paquetes lo realiza a través de la transmisión de bloques de datos conocidos como datagramas. El origen y destino son identificados mediante direcciones fijas conocidas como direcciones IP en donde cada dispositivo debe tener una dirección única.

Existen dos versiones del protocolo IP a nivel de capa de red que actualmente están siendo usadas; la versión 4 (IPv4) y la versión 6 (IPv6). Esta última fue desarrollada debido a la gran masificación que ha tenido el Internet en el mundo global provocando el agotamiento de direcciones IPv4.

IPv6 está siendo implementada en algunas áreas debido a las exigencias que son cada vez mayores por el fuerte crecimiento y desarrollo del Internet, además de la evolución de las redes actuales. IPv6 llegará a reemplazar paulatinamente a IPv4.

3.2 Análisis de la Estructura de un paquete IPv4/IPv6

Un paquete IPv6 tiene una cabecera de tamaño fijo e igual a 40 [byte], el doble de la cabecera IPv4. Este aumento se debe a que el tamaño de los campos “Source Address” y “Destination Address” aumentaron su tamaño de 32 a 128 [bit] cada uno.

La cabecera Ipv6 posee los siguientes campos:

- Versión (“Version”): Indica la versión del protocolo IP, en este caso su valor es igual a 6.

- Clase de tráfico (“Traffic Class”): Incluye información que permite a los “routers” clasificar el tipo de tráfico al que el paquete pertenece, aplicando distintas políticas de enrutamiento según sea el caso. Realiza la misma función que el campo “Type of Service” de IPv4.

- Etiqueta de flujo (“Flow Label”): Identifica a un flujo determinado de paquetes, permitiendo a los “routers” identificar rápidamente paquetes que deben ser tratados de la misma manera.

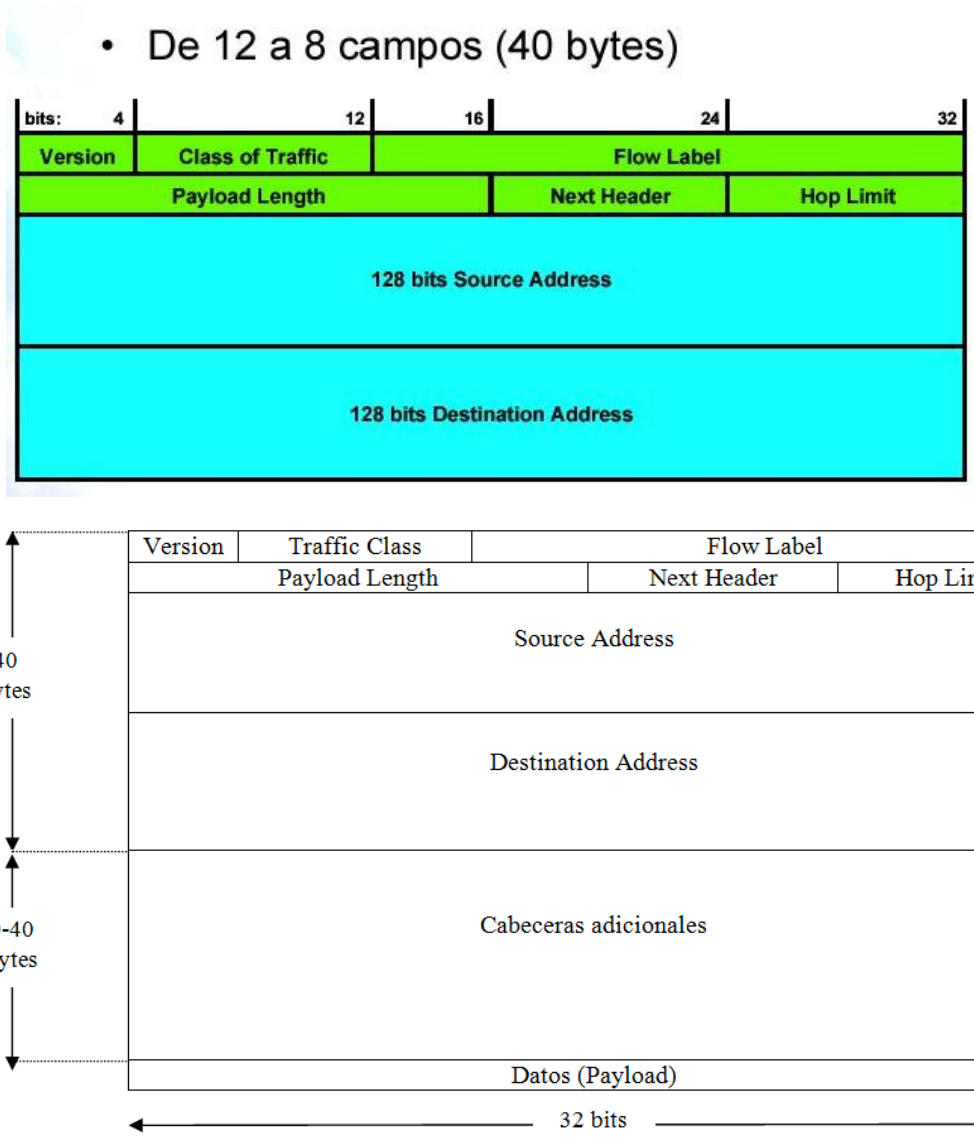
- Tamaño de la carga útil (“Payload Length”): Indica el tamaño de la carga útil del paquete. Las cabeceras adicionales son consideradas parte de la carga para este cálculo.

- Próximo encabezado (“Next Header”): Indica cual es el siguiente cabecera es la siguiente cabecera adicional presente en el paquete. Si no se utilizan, apunta hacia la cabecera del protocolo capa 4 utilizado.

- Límite de saltos (“Hop Limit”): Indica el máximo número de saltos que puede realizar el paquete. Este valor es disminuido en uno por cada “router” que reenvía el paquete. Si el valor llega a cero, el paquete es descartado.

- Dirección de origen (“Source Address”): Indica la dirección IPv6 del nodo que generó el paquete.

- Dirección de destino (“Destination Address”): Indica la dirección de destino final del paquete.



La Figura 21 muestra la estructura de un paquete IPv6.

El protocolo IPV6 reemplazó cierto campo del protocolo IPv4 por las denominadas cabeceras adicionales. Estas cabeceras permiten expandir el funcionamiento de IPv6, sin verse restringidas a un campo de tamaño fijo como el presente en IPv4.

Y a continuación en la en la Figura 22 se pueden apreciar los cambios de la cabecera IPv6 respecto a la cabecera IPv4.

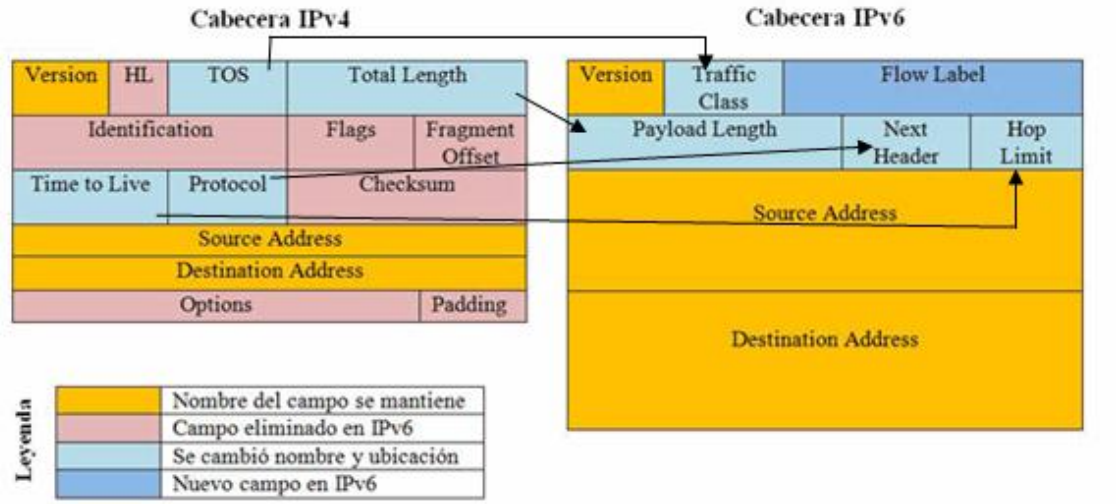


Figura 22 Cambios en la cabecera de los paquetes de IPv4 aIPv6.

3.3 Comparación de las características de IPv4/ IPv6

IPv6 mantiene varias funciones usadas en IPv4; en cambio, funciones que eran usadas en muy pocas ocasiones o no eran usadas han sido eliminadas. Esto permite añadirle a este nuevo protocolo nuevas características que provean nuevas funcionalidades para la comunicación a través del Internet.

Las diferencias más importantes entre IPv4 e IPv6 se muestran en la Tabla 6 a continuación:

	IPv4	**IPv6**
Direcciones	Las direcciones de origen y destino tienen una longitud de 32 bits (4 bytes).	Las direcciones de origen y destino tienen una longitud de 128 bits (16 bytes).
Formato de las direcciones	Notación decimal con puntos: 192.149.252.76	Notación hexadecimal: 3FFE:F200:0234:AB00:0123:4567:8901:ABCD
Notación de prefijos	192.149.0.0/24	3FFE:F200:0234::/48
Cantidad de direcciones	232 = ~4,000,000,000	2128 = ~340,000,000,000,000,000,000,000,000,000,000,000

Fragmentación	La llevan a cabo los enrutadores y el host que realiza el envío.	No la llevan a cabo los enrutadores, sino únicamente el host que realiza el envío.
Encabezado	Incluye una suma de comprobación.	No incluye una suma de comprobación.
Opciones	El encabezado lo incluye.	Todos se trasladan a los encabezados de extensión IPv6.
Marcos de solicitud ARP	El Protocolo de resolución de direcciones (ARP) utiliza los marcos de solicitud ARP de difusión para resolver una dirección IPv4 como una dirección de capa de vínculo.	Los marcos de solicitud ARP se sustituyen por mensajes de solicitud de vecinos de multidifusión.
Administrar la pertenencia a grupos locales de subred	Se utiliza el Protocolo de administración de grupos de Internet (IGMP).	IGMP se sustituye con los mensajes de Descubrimiento de escucha de multidifusión (MLD).
Determinar la dirección IPv4 de la mejor puerta de enlace predeterminada	Se utiliza el Descubrimiento de enrutadores ICMP, y es opcional.	El Descubrimiento de enrutadores ICMP queda sustituido por la Solicitud de enrutadores ICMPv6 y los mensajes de anuncio de enrutador, y es obligatorio.
Direcciones de multidifusión	Se utilizan para enviar tráfico a todos los nodos de una subred.	No hay direcciones de multidifusión IPv6. De forma alternativa, se utiliza una dirección de multidifusión para todos los nodos de ámbito local del vínculo.
Configuración manual	Debe configurarse manualmente o a través de	No requiere configuración manual o a través de DHCP.

	DHCP.	
DNS	Utiliza registros de recurso (A) de dirección de host en el Sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv4.	Utiliza registros de recurso (AAA) de dirección de host en el Sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv6.
Direcciones IP relacionados con host	Utiliza registros de recurso (A) de puntero en el dominio DNS IN-ADDR.ARPA para correlacionar direcciones IPv4 con nombres de host.	Utiliza registros de recurso (PTR) de puntero en el dominio DNS IP6.INT para correlacionar direcciones IPv6 con nombres de host.
Tamaño de paquete	Debe admitir un tamaño de 576 bytes (posiblemente fragmentado).	Debe admitir un tamaño de 1280 bytes (sin fragmentación).

Tabla 6 Comparativa entre IPv4/IPv6.

3.4. Direcciones IPv4 /IPv6 equivalentes

Para resumir la relación entre el direccionamiento IPv4 y el direccionamiento IPv6 la Tabla 7 muestra los conceptos de direccionamiento IPv4 y sus equivalentes en IPv6.

Direcciones IPv4	***Direcciones IPv6***
Internet address classes	No es aplicable en IPv6
Direcciones Multicast (224.0.0.0/4)	Dirección multicast IPv6 (FF00::/8)
Dirección de Broadcast	No es aplicable en IPv6
La dirección no especificada es 0.0.0.0	La dirección no especificada es ::
La dirección de Loopback es	La dirección de Loopback es ::1

127.0.0.1	
Direcciones IP públicas	Direcciones globales unicast
Dirección IP privada (10.0.0.0/8,)	Direcciones Site-local (FEC0::/48) 1 / 2.16.0.0/12 and 192.168.0.0/16
La representación de las direcciones se realiza con notación decimal.	La representación de las direcciones se la realiza con notación hexadecimal y la supresión de los ceros.
La máscara de subred se representa con notación decimal con puntos o longitud del prefijo.	Los bits de red se representan solo con la longitud del prefijo.

Tabla 7 Direcciones IPv4 equivalentes con IPv6.

3.5 Análisis de Soporte de IPv6 en los Routers Cisco serie 2800

Se requiere que todos los equipos involucrados para la transición y coexistencia que van hacer conectados a la red en este caso los routers y que brinden el servicio de Internet cuenten con soporte para IPv6. En la Tabla 8 se presenta un resumen del equipo a utilizado para el desarrollo de la investigación.

Equipo	Funciones	¿Soporta IPv6?	Acción a realizar
Router CISCO 2800	Enrutamiento Ipv6	Cisco 2800 IOS IP Base **"c2800nm-ipbase-mz"** no soporta	Actualización Cisco 2800 IOS Advanced IP Services **"c2800nm-advipservicesk9-mz"** que es la que soporta

Tabla 8 Equipo utilizado en la implementación

3.6 Análisis de Soporte de IPv6 en sistemas operativos

Prácticamente todos los sistemas operativos desarrollados actualmente cuentan con soporte IPv6. Para las organizaciones y empresas, dicha característica es vista como una garantía de que dichos productos funcionaran adecuadamente en los próximos años. Sin embargo, los ciclos de adopción de los sistemas operativos son extensos, lo que hace necesario revisar el soporte IPv6 en versiones anteriores de dichos sistemas. En la Tabla 9 se presenta un resumen con el soporte IPv6 de los sistemas operativos más utilizados por usuarios y servidores en la red institucional de la UNACH.

Sistema Operativo	**Soporte IPv6**	**Observaciones**
Windows 7	Sí	
Windows Vista	Sí	
Windows XP	Sí	A partir de Service Pack 2
Windows 2003	Sí	A partir de Service Pack 2
Windows Server 2008	Si	

Sistema Operativo	**Soporte IPv6**	**Observaciones**
Linux	Sí	Desde kernel 2.2
Windows Mobile (Windows CE)	Sí	Desde versión 2003

Tabla 9 Soporte IPv6 en sistemas operativos Windows utilizados en la red UNACH

3.7 Migración o transición

Es el Traslado de una aplicación de un ordenador o dispositivo a otro en condiciones de compatibilidad. Migrar es también elevar una versión de un producto software a otra de más alto nivel, o bien el movimiento de una arquitectura a otra que en este caso es lo que se va a realizar.

Toda red existente esta sujeta a la obsolescencia de su hardware y software. Cuando las empresas deciden mejorar sus sistemas, la migración de configuración y de datos no es tarea fácil.

3.7.1 Mecanismos de Migración o transición IPv4/IPv6

Características de migración IPv4/IPv6

IPv4 e IPv6 son incompatibles a nivel de paquete:

- Los nodos finales actuales de Internet no generan ni recogen IPv6.
- Los routers IP actuales de Internet descartan los paquetes IPv6.
- IPv6 ha sido diseñado pensando en la coexistencia

La principal dificultad es migrar la red Internet:

- Durante la etapa de transición, a nivel lógico, habrá Internet IPv4 e IPv6.

Los Mecanismos de migración o Transición de IPv4-IPv6: Permiten la coexistencia y/o interacción de los sistemas IPv4 e IPv6, mediante algunos procesos ya existentes en la actualidad.

3.7.2 Entender la convivencia y la migración

La coexistencia se produce cuando se tiene nodos IPv4 o IPv6, estos nodos se comunican a través de una infraestructura IPv4, una infraestructura IPv6 o una infraestructura que contiene tanto IPv4 como IPv6. Para comunicarse con nodos sólo IPv6, los nodos IPv4 puede utilizar una pasarela de traducción o una dirección IPv4 a IPv6. La migración es totalmente sólo cuando todos los nodos IPv4 se convierten en nodos IPv6.

A continuación se especifican las normas de migración:

- Usted puede desplegar IPv6 en los hosts en cualquier momento.
- Puede actualizar un host de IPv4 a IPv6 existentes, independientemente de la mejora de sus anfitriones y de otros routers.
- Un host IPv4 que ha instalado IPv6 todavía puede utilizar su dirección IPv4.

Los diferentes tipos de nodos existentes son:

- *Sólo IPv4-nodo* : Este es un nodo que asignan las direcciones IPv4. IPv4-nodos sólo no soporta IPv6.
- *IPv6 sólo nodo* : Este nodo se le asigna direcciones IPv6, y sólo puede comunicarse con otros nodos IPv6 y aplicaciones.
- *Nodo IPv6/IPv4* : Este nodo contiene una dirección IPv4 y la implementación de IPv6.
- *Nodo IPv4* : Este nodo puede enviar y recibir paquetes IPv4, y puede ser cualquiera de los siguientes:
    - Nodo IPv6/IPv4
    - Sólo IPv4-nodo
- *Nodo IPv6* : Este nodo puede enviar y recibir únicamente los paquetes IPv6, y puede ser cualquiera de los siguientes:
    - Nodo IPv6/IPv4
    - IPv6 sólo nodo

La dirección se utiliza normalmente cuando se utiliza el mecanismo de túnel automático. 6over4 direcciones IPv6 se asignan a los nodos que están conectados a una infraestructura multicast IPv4.

- *Direccionamiento 6to4* : Esta direccionamiento se utiliza para crear prefijos globales de direcciones de los sitios y direcciones globales para los nodos IPv6 en los diferentes sitios.
- *Direcciones ISATAP* : El direccionamiento ISATAP utiliza los identificadores de interfaz, se asignan a los nodos IPv6/IPv4. el direccionamiento ISATAP :
    - Válida los 64 bits de direcciones unicast

Los mecanismos que pueden utilizarse para la coexistencia con una infraestructura IPv4 son:

- *De doble capa IP* : La aplicación IP de doble capa tiene las siguientes características:
    - Una implementación del TCP / IP que tiene una dirección IPv4 y una capa de Internet IPv6.
    - Consta de una aplicación de la Casa de los protocolos de la capa de host
    - Los protocolos de la capa superior puede comunicarse a través de IPv4, IPv6, o IPv6 en túnel sobre IPv4.

El mecanismo de doble capa IP es usado por nodos IPv6/IPv4 para permitir la comunicación con nodos IPv4 e IPv6 nodos.

- *IPv6 sobre IPv4*: En este mecanismo de encapsular los paquetes IPv6 con una cabecera IPv4, para que estos paquetes que se transmiten a través de la infraestructura IPv4. Los parámetros de la cabecera IPv4 son:
    - IPv4 campo Protocolo establece en 41, lo que indica que el paquete como un paquete IPv6 encapsulado.
- El campo de Origen y Destino de campo contienen las direcciones IPv4 de los extremos del túnel.

CAPITULO IV

4. IMPLEMENTACIÓN DE LA GUÍA METODOLÓGICA

La presente guía, se desarrolló con el objeto de poder brindar a la comunidad universitaria y la comunidad en general, una guía que facilite las herramientas necesarias para impulsar y fomentar la adopción de los protocolos IPv6 en los diferentes entornos, motivados, además, por las preocupaciones que respecto a su adopción tardía.

La guía está desarrollada por procesos para cada entorno específico, de esta forma explica de una manera clara y exenta de tecnicismos innecesarios, los pasos y requerimientos para configurar e implementar la nueva versión del Protocolo IP en ámbitos tan variados como son las Redes Residenciales, Redes Académicas.

4.1 Parámetros empleados en la Guía Metodológica

Proceso 1: Sistemas Operativos con los que puede Implementar.

Objetivo: Determinar que sistemas operativos se va a utilizar para la implementación de IPv6, y su respectiva configuración.

Descripción: Se trabajará con los siguientes sistemas operativos que son Windows y Linux, además se tratara los temas de instalación comprobación, configuración, y desinstalación del protocolo Ipv6 en estos sistemas.

Software: Sistema operativo Windows, Linux

Actividades No.	Contenido
1	Contemplación de los Sistemas Operativos a utilizar
2	Instalación de IPv6 en Sistemas Operativos Windows
3	Instalación de IPv6 en Sistemas Operativos Linux
4	Comprobación de la instalación IPv6 en los Sistemas Operativos Windows y Linux

5	Configuración avanzada de IPv6 en Sistemas Operativos Windows y Linux
6	Desinstalación de IPv6 en Sistemas Operativos Windows y Linux

Tabla 10 Actividades para la implementación de IPv6

Proceso 2: Entorno académico y de investigación.

Objetivo: Determinar los requerimientos tanto de equipo y direccionamiento en la infraestructura dentro de los laboratorios de la Facultad de Ingeniería.

Descripción: Se determinan los equipos con los que se trabaja y el rango de direcciones IPv6 con los que se implementarán en el laboratorio.

Actividades No.	Contenido
1	Desplegando IPv6 en la universidad/laboratorio informático
2	Equipamiento a tener en cuenta
3	Cómo asignar direcciones IPv6 en una Universidad
4	Implementación de una red "SOHO"

Tabla 11 Pasos a tener en cuenta para la implementación

Proceso 3: Configuración de equipos

Objetivo: Configurar los diferentes protocolos de enrutamiento disponibles para IPv6 y el mecanismo de túnel para la coexistencia de IPv6'IPv4.

Descripción: Se configurará los cada uno de los protocolos de enrutamiento con son STATIC, Ripng, Ospf y el mecanismo de coexistencia para IPV4-IPV6 como es el 6to4.

Equipo: Pc´s, routers.

Actividades No.	Contenido
1	Configuración de IPv6 en Interfaces del router
2	Configuración Rutas Estáticas en IPv6
3	Configuración RIPng para IPv6
4	Configuración OSPFv3 para IPv6
5	Configuración Túnel 6to4 para IPv6

Tabla 12 Detalle de pasos a tener en cuenta en la implementación

4.2 Desarrollo de la Guía Metodológica

"GUÍA METODOLÓGICA DE LOS MECANISMOS DE TRANSICIÓN Y COEXISTENCIA IPv4/IPv6"

La presente guía, se desarrolló con el objeto de poder brindar a la comunidad universitaria, una guía que facilite las herramientas necesarias para impulsar y fomentar la adopción del protocolo IPv6 en los diferentes entornos, motivados, además, por las preocupaciones que respecto a su adopción tardía.

La guía comprende procesos para cada entorno específico, de esta forma explica de una manera clara y exenta, los pasos y requerimientos para configurar e implementar la nueva versión del Protocolo IP en ámbitos tan variados como son las Redes Residenciales, Redes Académicas, etc.

Por su parte, el contenido de la guía ha contado con la colaboración de expertos en el área de redes de la Universidad Nacional de Chimborazo, que han brindado sus conocimientos para contribuir en este lento, pero inexorable camino hacia la adopción de IPv6.

Ing. Javier Haro

Instructor de la academia CISCO, UNACH

Ing. Daniel Santillán

Instructor de la academia CISCO, UNACH

Ing. Jorge Delgado

Director de la Escuela de Ing. en Sistemas y Computación

Como es ya de amplio conocimiento, el conjunto de direcciones IPv4 que aún se encuentran bajo la administración de IANA (www.iana.net) y que no han sido asignadas a los Registros Regionales de Internet, se reduce a un ritmo significativo y su terminación se acerca rápidamente. En otras palabras, el sistema global de direcciones de Internet se está agotando.

Por lo cual se ha creado IPv6 que es una nueva versión de Internet Protocolo, diseñada para suceder a la actual (IPv4). La transición entre ambas será un largo proceso durante el que se ha de garantizar la coexistencia.

La especificación IPv6 introduce en Internet Protocolo modificaciones fundamentales. No sólo la longitud de la dirección IP ha sido extendida a 128 bits; también ha sido modificado el formato de la cabecera IP y el modo en que se procesa la información que en ella se alberga. Pasar de IPv4 a IPv6 no es sencillo y los mecanismos que permiten la coexistencia y la transición entre las dos versiones han de estar estandarizadas.

Hoy, cientos de millones de personas están conectadas a Internet y un número equivalente de hosts y dispositivos implementan el protocolo IP. La migración al nuevo IP en tan corto periodo de tiempo requeriría la redefinición de un plan de direccionamiento IPv6 mundial, la instalación del protocolo en cada router y host, y la modificación de las aplicaciones actuales para que puedan soportarlo. Un proceso caro, sin duda, y que podría causar interrupciones del servicio inaceptables. Sencillamente, tal enfoque no tendría sentido, ya que muchas de las aplicaciones hoy operativas no han sido diseñadas para aprovechar las nuevas características de IPv6; ni siquiera las necesitan.

El nuevo protocolo IPv6, dispone de 340 billones de billones de billones (sextillones) de direcciones, lo que hace que la cantidad de direcciones IPv4 parezca insignificante. Con este mayor espacio de direcciones, IPv6 ofrece una variedad de ventajas en términos de estabilidad, flexibilidad y simplicidad en la administración de las redes. También es probable que la "Era IPv6" genere una nueva ola de innovación en las aplicaciones y las ofertas de servicios.

PROCESO I

1. Sistemas Operativos con los que puede Implementar

1.1 Introducción

En este capítulo se tratará de como realizar la instalación y configuración básica de IPv6 en diferentes plataformas de usuario final (sistemas operativos).

Se puede trabajar bajo los siguientes sistemas operativos y sus características:

- Windows XP
- Windows Server 2008
- Linux

Sistema Operativo	Soporte IPv6	Observaciones
Windows 7	Sí	
Windows Vista	Sí	
Windows XP	Sí	A partir de service pack 2
Windows 2003	Sí	A partir de service pack 2
Windows Server 2008	Si	
Linux	Sí	Desde kernel 2.2

Tabla 13 Soporte IPv6 en sistemas operativos Windows y Linux utilizados en una red

Obsérvese, que dado el gran número de versiones existentes en algunos casos, y especialmente en el de Linux, se presentan ejemplos genéricos, y por tanto, puede haber pequeñas diferencias dependiendo de la versión concreta, que habrán de ser solucionadas por el lector, con ayuda de documentación propia del sistema operativo que se trate.

1. 2. Instalación de IPv6

La mayor parte de los sistemas operativos, desde el año 2001 aproximadamente, tienen algún tipo de soporte de IPv6.

Es cierto, que en algunos casos, inicialmente no se trataba de un soporte "comercial", sino versiones de prueba, aunque dichos se incorporaban a sistemas operativos de "producción".

Tal es el caso del soporte de IPv6 en Windows 2000 (incluso en versiones anteriores de Windows NT, que por su antigüedad no describiremos en este documento), e incluso en la primera versión de Windows XP, antes del lanzamiento del denominado Service Pack 1 (SP1).

Cada vez es más frecuente que diversas plataformas o sistemas operativos, no solo incorporen IPv6, sino que además sea activado por defecto por el fabricante, sin requerir intervención alguna por parte del usuario.

Lo expuesto es válido no solo para sistemas operativos de computadores de sobremesa y portátiles, sino también para otros dispositivos que utilizan los mismos sistemas operativos, o versiones reducidas de los mismos, por ejemplo teléfonos celulares, agendas electrónicas, plataformas de juegos, etc. Es cierto, lógicamente, que en algunos casos, dichas versiones reducidas de los sistemas operativos, no incorporan todas las funcionalidades del sistema operativo original, y por tanto, se podría dar el caso de no poder acceder a todos las funciones que se mostrarán para la configuración y prueba de IPv6.

1.3 Instalación de IPv6 en Sistemas Operativos Windows

1.3.1 Instalación en XP y Server 2003

En realidad podríamos decir que IPv6 ya está instalado tanto en Windows XP como en Server 2003, y por tanto, más que instalación hablamos de activación.

Existen dos procedimientos para habilitar IPv6 en estas dos plataformas:

1.3.1.1 Línea de Comandos

En una ventana MS-DOS ejecutar: ipv6 install

Tras unos segundos, un mensaje de confirmación nos indicara la correcta instalación.

También se podría utilizar, dependiendo de la versión: netsh interface ipv6 install

1.3.1.2 Interfaz gráfica

A través del entorno gráfico o panel de control, nos situamos en "Conexiones de red", seleccionar la "red de área local" o "red inalámbrica", "Propiedades" con el pulsador derecho del ratón y a continuación pulsar sobre "instalar", "protocolo" y seleccionar "Microsoft TCP/IP versión 6".

El resultado será similar al mostrado en la siguiente captura de pantalla:

FIGURA 23: Pantalla De Instalación De Ipv6 En Xp/2003 Server

1.3.2. Instalación de IPv6 en Sistemas Operativos Linux

IPv6 esta soportado a partir de versión del kernel 2.4.x. Para comprobar si está instalado:

- #test -f /proc/net/if_inet6 && echo “Kernel actual soporta IPv6“

Para instalar el módulo IPv6:

- #modprobe ipv6

Se puede comprobar el módulo con:

- #lsmod |grep -w ‘ipv6’ && echo “modulo IPv6 cargado”

Se puede realizar la configuración permanente, en función de la versión de Linux.

1.3.2.1 Configuración en Centos 5.4 y similares

Para la configuración en Centos debemos seguir los siguientes pasos:

- Añadir a /etc/sysconfig/network: NETWORKING_IPV6=yes

Reiniciar la red:

- # service network restart o,
- #/etc/init.d/network restart

1.3.2.2. Comprobación de la instalación IPv6 en los Sistemas Operativos Linux y Windows

Una vez que hemos instalado IPv6, en función de las diferentes plataformas, tenemos una o varias opciones para verificar que dicha instalación ha sido realizada correctamente e incluso si tenemos conectividad tanto en la red local, como con otras redes IPv6.

1.3.3. Comprobación en Windows

Además de visualizar si la pila IPv6 ha sido instalada a través del entorno gráfico, como

hemos indicado en la sección de instalación, podemos utilizar el comando ipconfig o ipv6 if (no disponible en las últimas versiones de Windows).

El comando *ipconfig* nos facilitará la información de configuración IPv6 de las diferentes interfaces, al igual que de IPv4, mientras que *ipv6 if* sólo muestra información relativa a IPv6. Por ejemplo, si nuestra interfaz Ethernet fuese la número 5, el código seria:

- >ipv6 if 5

Una prueba adicional es comprobar que se puede "alcanzar" la propia interfaz, mediante el comando ping/ping6 (uno, otro o ambos, pueden estar disponibles dependiendo de la versión específica de cada sistema operativo). Ejemplo utilizando la dirección de "loopback":

- >Ping ::1

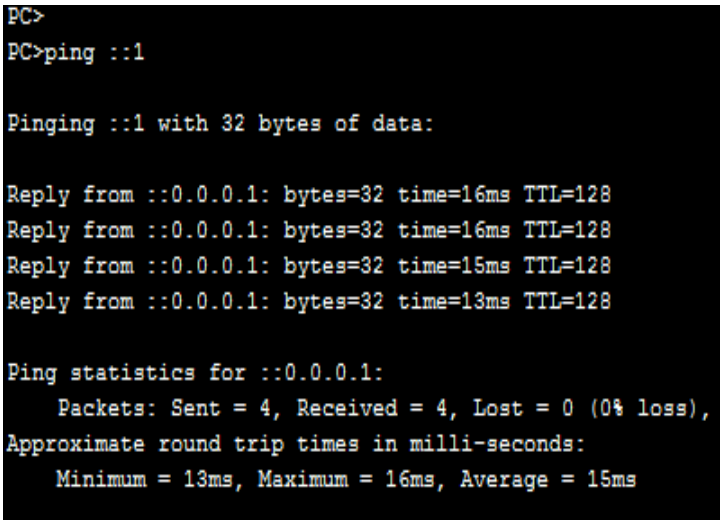


FIGURA 24: Ping A La Dirección De Loopback (:: 1)

Si se desea intentar con la dirección "link-local" (enlace local) propia, de una determinada tarjeta de red, por ejemplo

- >Ping fe80::71e7:cff:e6ad:8d67

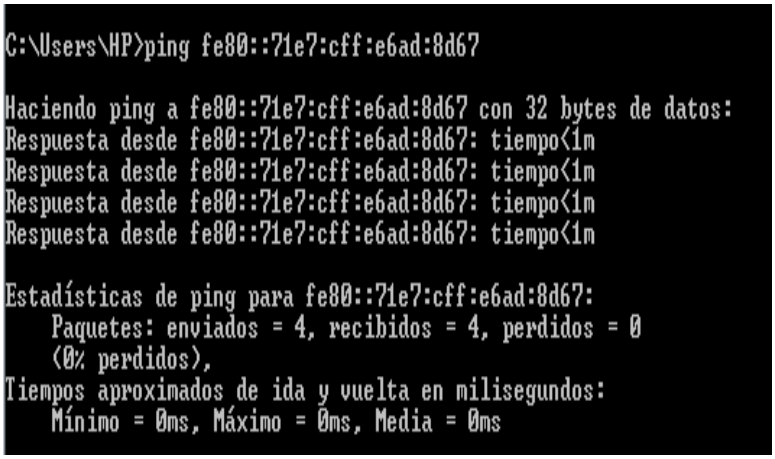


FIGURA 25: Ping a fe80::71e7:cff:e6ad:8d67

El paso siguiente es comprobar que existe conectividad con la red local. Esto sólo es posible si hay otras máquinas con IPv6 correctamente configurada en dicha red local (y la configuración de los cortafuegos permite usar el comando ping). El uso es equivalente al ejemplo anterior, pero utilizando la dirección de enlace local (o una dirección global), de la máquina a la que se desea hacer ping.

- Desde >ping 2001:db8:5::2
- Hasta >ping 2001:db8:5::1

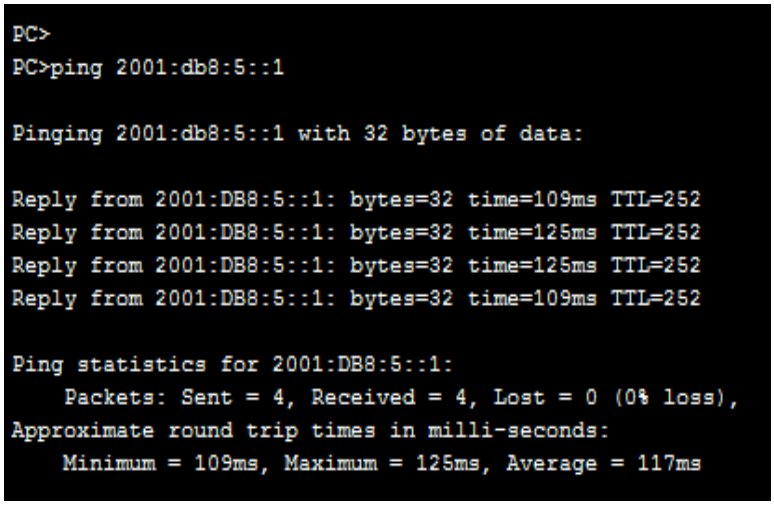


FIGURA 26: Ping desde 2001:db8:5::2 hasta 2001:db8:5::1

Igualmente, si se tiene conectividad con el exterior de la red local, es decir, con otras máquinas IPv6 situadas en Internet, es posible obtener un resultado similar a:

- ping www.ipv6tf.org

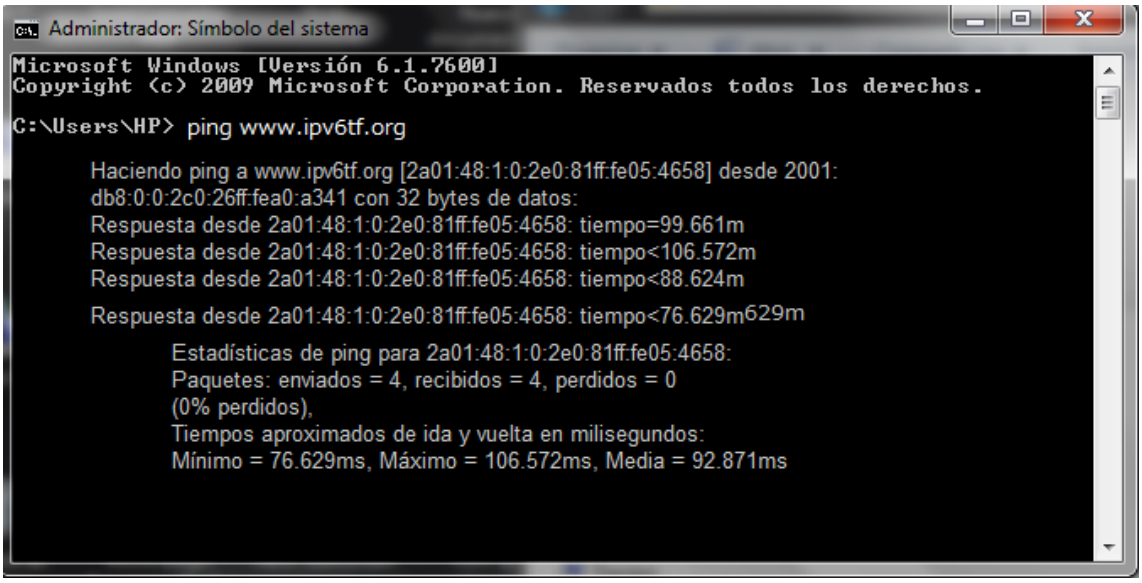


FIGURA 27: Ping a www.ipv6tf.org

Un paso adicional, es el uso de una herramienta que nos muestre los saltos entre los diferentes puntos de la red, desde nuestra propia máquina hasta la máquina destino, lo que se denomina un traceroute (traza de la ruta). Para ello se usa el comando tracert o tracert6 (según la versión/plataforma):

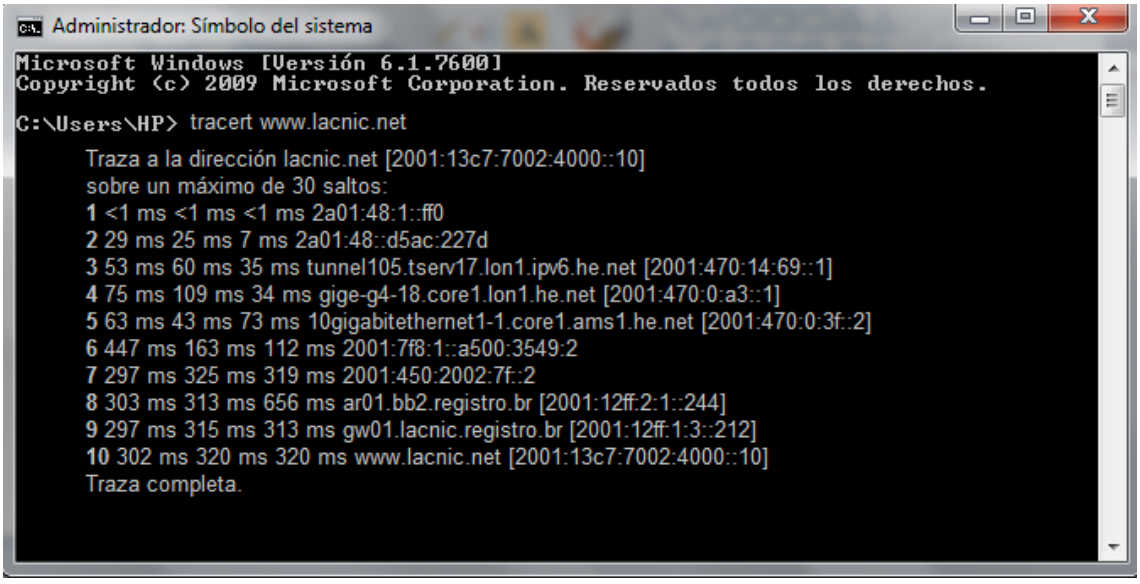


FIGURA 28: Uso Del Comando Tracert

1.3.4. Configuración avanzada de IPv6 en Sistemas Operativos Windows y Linux

En algunas ocasiones, es necesario realizar configuraciones avanzadas, por ejemplo configurar manualmente una dirección IPv6, modificar dicha configuración, o eliminarla.

Como en ocasiones anteriores, diversos sistemas operativos, realizan estas configuraciones de modos diferentes.

1.3.4.1. Configuración avanzada en Windows

Por diversos motivos, puede requerirse configurar manualmente una dirección IPv6. Para ello se usa el comando netsh con el formato siguiente:

- netsh interface ipv6 add address [interface=]<cadena (nombre de interfaz o índice)> [address=]<dirección IPv6>[/<entero>] [[type=]unicast|anycast] [[validlifetime=]<entero >|infinite] [[preferredlifetime=]<entero>|infinite] [[store=]active|persistent]

Netsh.- Es una utilidad de línea de comandos que nos ofrece varias opciones para la configuración de una red.

Add.- Permite añadir la dirección de red a la interfaz indicada.

Address.- Dirección de red IPV6

Type.- Indica el tipo de dirección

Unicast.- Nos indica que es una dirección única.

La última línea de comando nos valida los tiempos de conexión y los activa.

Ejemplo:

- netsh interface ipv6 add address 5 2001:db8::2 type=unicast

validlifetime=infinite preferredlifetime=10m store=active

Igualmente, se puede revisar la configuración con netsh (asumiendo que es la interfaz numero 5):

- netsh interface ipv6 show address 5

Show.- Nos da acceso para verificar la dirección IPv6 ingresada en la interfaz

Una vez configurada una dirección manualmente, se puede modificar con:

- netsh interface ipv6 set address [interface=]<cadena> [address=]<dirección IPv6>[[type=]unicast|anycast][[validlifetime=]<entero>|infinite] [[preferredlifetime=]<entero >|infinite] [[store=]active|persistent]

Set.- Nos permite modificar las variables de las direcciones IPv6 ingresadas.

Ejemplo:

- netsh interface ipv6 set address 5 2001:db8::2 preferredlifetime=infinite

Y finalmente, dicha dirección se puede eliminar con:

- netsh interface ipv6 delete address [interface=]<cadena> [address=]<dirección IPv6> [[store=]active|persistent]

Delete.- Nos permite borrar la dirección IPv6 asignada

Ejemplo:

- netsh interface ipv6 delete address 5 2001:db8::2 store=persistent

Finalmente, se puede agregar un servidor DNS con:

- netsh interface ipv6 add dnsserver [name=]<cadena> [address=]<dirección

IPv6> [[index=]<entero>]

Dnsserver.- Es el que nos permite ingresar al sistema de nombres de dominio para IPv6, para equipos y servicios de red que se organiza en una jerarquía de dominios.

En XP SP2/2003 SP2 se usa dns en lugar de dnsserver

Ejemplo:

- netsh interface ipv6 add dnsserver “Local área network” 2001:7f9:1000:1::947c 1

Y se pueden mostrar los servidores DNS configurados manualmente con:

- netsh interface ipv6 show dnsservers [[name=]cadena]

Ejemplo:

- netsh interface ipv6 show dnsservers

DNS servers in LAN interface

Index DNS server

------- ----------

1 2001:7f9:1000:1::947c

2 2001:7f9:1000:1::947c

Y por último, borrarlos con:

- netsh interface ipv6 delete dnsserver [name=]<cadena> [[address=]<dirección IPv6>|all]

Ejemplo:

- netsh interface ipv6 delete dnsserver “Local área network” all

1.3.4.2. Configuración avanzada en Linux

Añadir una dirección IPv6:

- # ifconfig <interface> inet6 add <ipv6address>/<prefixlength>

Eliminar unadirección IPv6:

- # ifconfig <interface> inet6 del <ipv6address>/<prefixlength>

Ver rutas IPv6:a

- # /sbin/ip -6 route show [dev <device>]
- # /sbin/route -A inet6

1.4. Mecanismos de transición con IPv6

Dado que no todos los ISPs, hoy en día, disponen de IPv6 en sus redes, es necesario utilizar lo que denominamos mecanismos de transición y coexistencia.

Básicamente, estos mecanismos, permiten que IPv4 e IPv6 coexistan, e incluso que cuando IPv6 no está disponible de forma “nativa”, se pueda utilizar IPv6 a través de la red IPv4, fundamentalmente mediante lo que denominamos “túneles”.

Los mecanismos de túneles, se ocupan de que IPv6 sea “empaquetado” o “encapsulado”, dentro de los paquetes IPv4, de tal forma que, como hemos indicado antes, IPv6 sea “transportado” en la red IPv4 existente.

Los siguientes gráficos permite visualizar como funcionan estos túneles y como se

"empaqueta" IPv6 en IPv4.

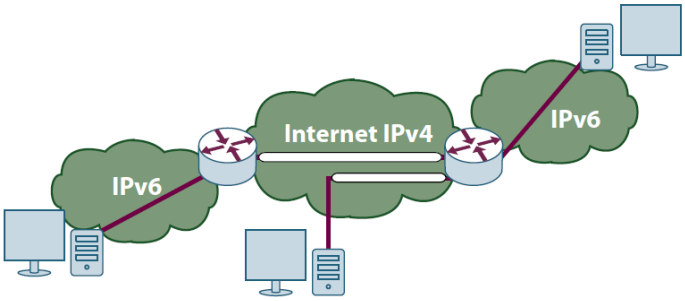


FIGURA 5: TÚNELES IPV6 EN IPV4

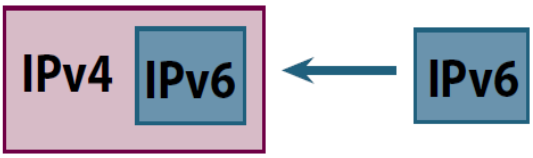


FIGURA 29: Encapsulado De Ipv6 En Ipv4

Hay muchos mecanismos de transición y se trata de un tema sumamente complejo, por lo que este apartado, se centra sólo en aquellos mecanismos de túneles que consideramos más útiles, y que se denominan túneles automáticos y más concretamente el denominado 6to4

6to4 sólo funciona cuando se dispone de direcciones IPv4 públicas. En este caso, sin entrar en detalles técnicos, lo que ocurre es que se utiliza la dirección IPv4 para configurar automáticamente una dirección IPv6 y un túnel automático, que como decíamos anteriormente, permite utilizar IPv6 a través de la red IPv4.

1.4.1 Configuración Túnel 6to4 para Sistemas Operativos Windows y Linux

6to4 para Windows solo se necesita activarlo por medio de la ventana de MS-DOS con el siguiente comando:

- > netsh int ipv6 6to4 set relay Direccion_6TO4_RELAY enabled 1440
- >ipconfig

Enable.- nos permite activar el puerto 1440

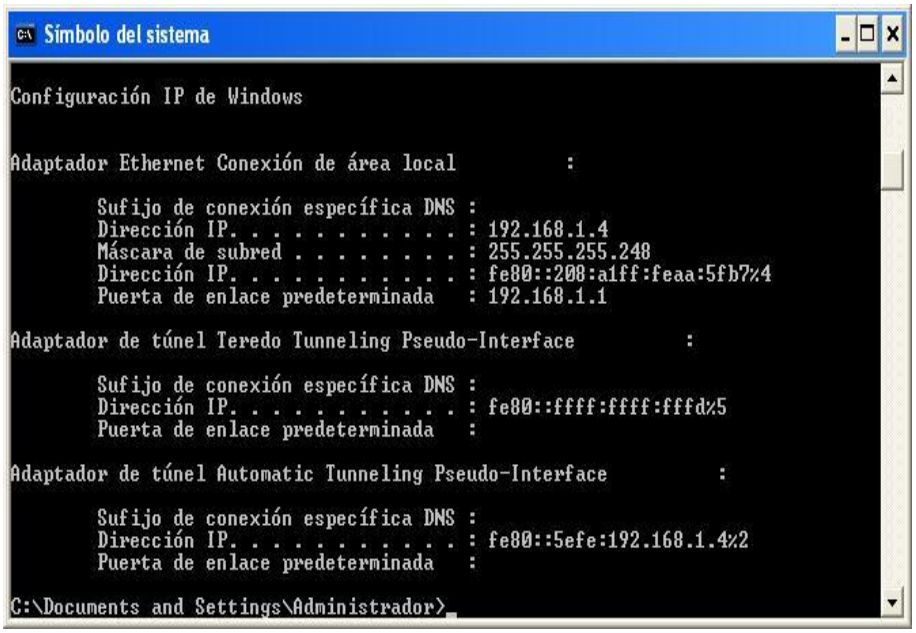


FIGURA 30: Configuración Ip De Windows

Y vemos como se ha creado el Adaptador de túnel Automatico que en este caso es nuestro túnel 6to4

Mientras que para Linux Centos desde ventana de comandos se utilizara los siguientes códigos.

- ip tunnel add tun6to4 mode sit ttl 80 remote any local Direccion_publica_IPv4_local
- ip link set dev tun6to4 up
- ip -6 addr add 2002:XXYY:ZZUU::1/16 dev tun6to4
- ip -6 route add 2000::/3 via ::192.88.99.1 dev tun6to4 metric 1

Note: Podemos notar que XXYY:ZZUU es la notación hexadecimal para

Direccion_publica_IPv4_local (la dirección IPv4 pública) según lo Siguiente:

- Direccion_publica_IPv4_local = 60.172.21.22 -> 60 -> 3C

• 172 -> AC

• 21 -> 15

• 222 -> DE

• 60.172.21.22 -> XXYY:ZZUU = 3CAC:15DE

Con estos códigos se crea una nueva interfaz En este caso así 2002:3CAC:15DE /16 o dependiendo con la dirección Ipv4 con la que quieras trabajar, a continuación escribimos:

- #ifconfig

Y veremos que se ha creado el túnel

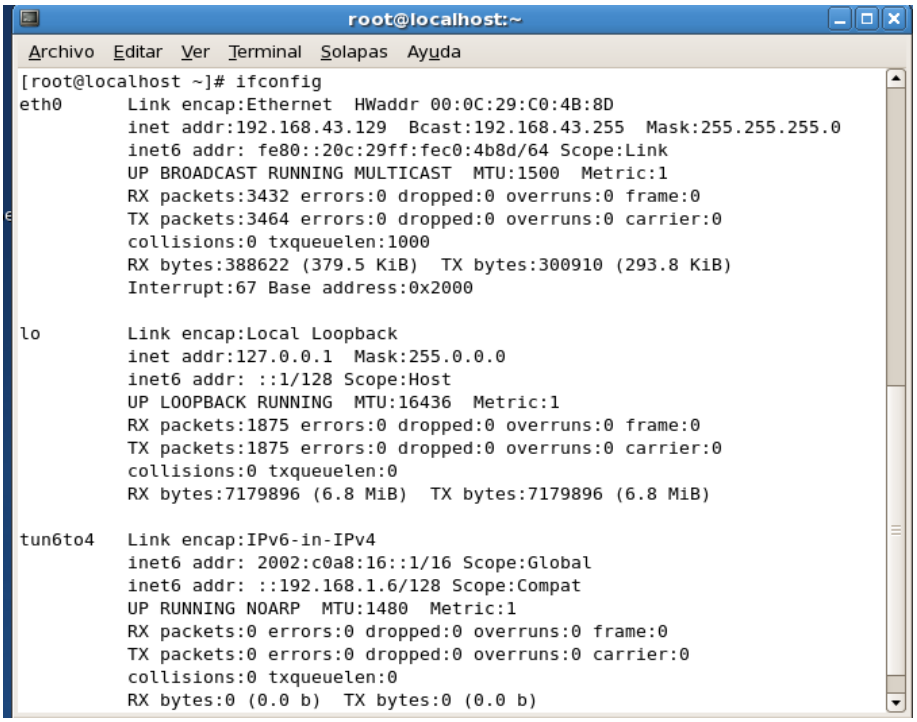


FIGURA 31: Visualización De Interfaces En Linux Con El Comando Ifconfig

1.4.2. Desinstalación de IPv6 en sistemas Operativos Windows y Linux

En general, no debería ser necesario desinstalar IPv6, pero si se precisa hacerlo, facilitamos a continuación la información relativa a las plataformas más relevantes.

1.4.2.1 Desinstalación en XP

En estas plataformas, se usa:

- ipv6 uninstall

En otros casos, dado que el comando ipv6.exe solo aparece hasta Windows XP, es necesario utilizar el comando netsh:

- netsh interface ipv6 uninstall

Uninstall.- Con este comando desinstalamos los componentes de IPv6

Por supuesto que también es posible usar el entorno gráfico, de forma contraria a la indicada para la instalación.

En general se requiere reiniciar el sistema operativo para evitar efectos indeseados.

Como alternativa, si lo que se requiere es inicializar la pila a la situación por defecto de "fábrica", se puede usar (en la mayoría de las plataformas):

- netsh interface ipv6 reset

Reset.- Permite arrancar la interfaz sin necesidad de cumplir las secuencias habituales de apagado y nuevo encendido.

Obsérvese que en Windows Vista, 2008 y 7, dado que la pila IPv6 esta totalmente integrada con la pila IPv4, no es posible desactivarlo por completo. En su lugar, se puede usar el entorno gráfico para desactivarlo en una interfaz de red concreta.

PROCESO II

2. ENTORNO ACADÉMICO Y DE INVESTIGACIÓN

2.1. Introducción

En este capítulo mostraremos las características que tiene el despliegue de IPv6 en el ámbito de las redes de investigación y educación. Estas redes están compuestas en general por universidades y centros de investigación, pudiendo en algunos casos incluir escuelas y otros organismos relacionados. Es importante destacar la experiencia de este sector ya que ha sido el que ha liderado el desarrollo de la nueva versión del protocolo IP y donde mayor experiencia en el despliegue se cuenta.

A lo largo del capítulo veremos algunas de las ventajas que IPv6 presenta para este entorno y mostraremos también las principales redes en el mundo que hoy cuentan con esta tecnología. Además, desde un punto de vista práctico, se proporcionará la información necesaria para que una universidad o centro de investigación pueda desplegar IPv6 en su red fácilmente.

2.2. Desplegando IPv6 en la universidad/laboratorio informático

En esta sección nos ocupamos de los pasos necesarios para poder hacer un despliegue de IPv6 en una red de una universidad o, más generalmente, en una institución de características educativas o científicas.

Si bien puede pensarse que no hay diferencias entre este tipo de institución y una red de una empresa o una oficina pequeña, hay algunas particularidades por las que veremos que vale la pena hacer una sección separada. Hacemos la salvedad de que estaremos hablando de las redes que están al servicio del investigador o del docente y no haremos mención a redes de administración, ya que esos casos son similares a los tratados en otros capítulos

2.3 Equipamiento a tener en cuenta

En una red podemos destacar los siguientes equipos a grandes rasgos:

- Routers

Equipo	Funciones	¿Soporta IPv6?	Acción a realizar
Router CISCO 2800	Enrutamiento Ipv6	Cisco 2800 IOS IP Base **"c2800nm-ipbase-mz"** no soporta	Actualización Cisco 2800 IOS Advanced IP Services **"c2800nm-advipservicesk9-mz"** que es la que soporta

- Servidores
- Estaciones de trabajo (PC, portátiles, otros dispositivos)

2.4. Cómo asignar direcciones IPv6 en una Universidad

Al momento de definir un rango IPv6 para una institución, debemos tener en cuenta que la mayoría de las universidades se encuentran conectadas a un proveedor de Internet que en la actualidad se encuentran funcionando con un direccionamiento de IPv4.

Es así que nosotros tratamos que tanto IPv6-IPv4 puedan coexistir en un entorno real.

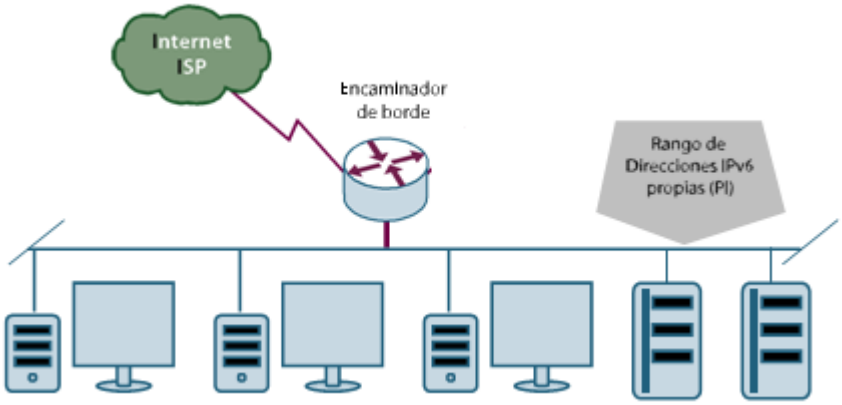


Figura 32: Esquema De Conectividad De Una Institución Final En Una Nren

2.5 Implementación de una red "SOHO"?

Se llama "SOHO" (Small Office Home Office) a una oficina pequeña, a una oficina montada en casa, o un laboratorio de práctica. En general, podría considerarse con esta denominación a cualquier conformación de oficina o grupo de profesionales independientes con una capacidad de hasta 10 trabajadores1 (Ver Figura 4 y Figura 5).

Basándonos en esta definición, cuando hablamos de Home Office en IPv6, nos referimos a la implementación de la red de un SOHO, de forma tal que cuente con la capacidad de operar con la nueva versión del protocolo IP: IPv6.

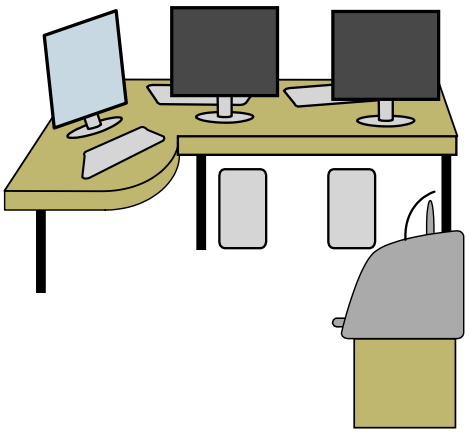


Figura 33: Ejemplo De Negocio Pequeño, Con Menos De 10 Empleados

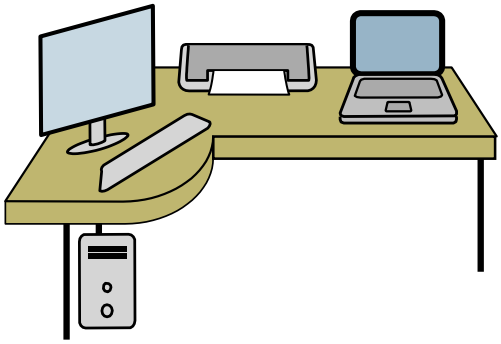


Figura 34: Ejemplo De Oficina En Casa O Red Residencial

2.5.1 Construyendo un SOHO con IPv6

Antes de comenzar la construcción de un SOHO que implemente IPv6 en su red es importante tener claro las diferentes partes que lo componen. Una vez que éstas estén identificadas, podremos ver cuáles de ellas será necesario configurar para que funcionen con IPv6. A partir de ahí, será apropiado ver cómo hacerlo.

En resumen, las etapas que debemos cumplir serán:

1. Identificar las partes del SOHO
2. Determinar cuáles de ellas requieren configuración para trabajar con IPv6
3. Configurar el SOHO con IPv6

2.5.2. Identificando las partes de un SOHO

Como hemos dicho en el párrafo anterior, este es el primer paso a la hora de pensar en la construcción de la red de un SOHO. Para llevar a cabo tal identificación, sugerimos hacerlo sobre tres aspectos bien delimitados:

2.5.2.1 Identificación del equipamiento que compone el SOHO, donde además habrá que distinguir entre:

2.5.2.1.1 Dispositivos de networking

2.5.2.1.2 Dispositivos terminales

2.5.2.2 Identificación de los sistemas operativos, en sus variantes:

2.5.2.2.1. Sistemas operativos de servidores

2.5.2. 2. Sistemas operativos de computadoras y laptops

2.5.2.3. Identificación de las aplicaciones

2.5.2.3.1. En servidores

2.5.2.3.2En estaciones terminales

Comencemos por el punto 2.5.2.1.:

- Dispositivos de Networking: deberemos identificar en nuestra red aquellos dispositivos que no constituyen nuestra interfaz de usuario, sino que son los que contribuyen a la comunicación de la red. En este conjunto podríamos incluir por ejemplo: el switch donde conectamos las terminales o computadoras, el router que el proveedor de Internet nos dejó instalado al contratar el servicio, el equipo que nos provee la conexión inalámbrica, entre otros.

- Dispositivos terminales: en este grupo encontramos aquellos dispositivos con los que interactuamos directamente, como por ejemplo: las computadoras de escritorio, las computadoras portátiles o laptops, PDAs, teléfonos IP, servidores de aplicaciones, entre otros.

En otra categoría podríamos identificar a las impresoras de red, que si bien no representan una interfaz directa con el usuario, tampoco es un dispositivo de networking, pero sin embargo vamos a querer su servicio dentro de la red y probablemente queramos tenerla en cuenta a la hora de trabajar con IPv6.

Siguiendo con el punto 2.5.2.2, deberemos identificar los sistemas operativos con los cuales trabajaremos, para ello tendremos en cuenta:

- Sistemas operativos de servidores: son los sistemas operativos que se ejecutan en aquellos dispositivos terminales que aportan servicios de red, como por ejemplo el servicio de e-mail. Podemos identificar entre ellos: sistemas operativos Linux, Windows, etc. Siendo los dos primeros los más utilizados en redes SOHO.

2.5.3. Configurando los componentes del SOHO con IPv6

Finalmente, con los dispositivos identificados, las versiones de software actualizadas para que soporten la nueva versión del protocolo IP y las modificaciones que hayan sido necesarias en las aplicaciones, estamos preparados para la etapa de la configuración.

Para ello, dividiremos la tarea en dos partes claramente separadas:

- configuración de la red interna de nuestro SOHO (LAN)

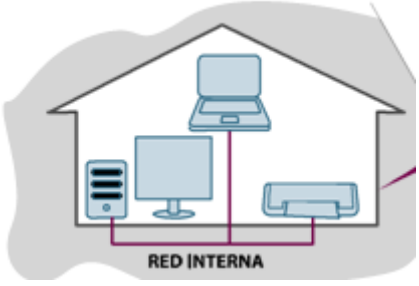


Figura 35. Límite Del Área De Una Red Interna

Antes de comenzar con la descripción de las tareas, trataremos el tema de cómo obtener las direcciones IPv6 con las que trabajaremos. Existen varias alternativas, algunas de ellas podrían ser:

- Disponer de direcciones propias, solicitadas al RIR correspondiente según la región donde nos encontremos.
- Que nuestro proveedor de Internet nos asigne un bloque de direcciones.
- Utilizar direcciones 6to4 (en este caso necesitaremos al menos una dirección IPv4 pública para hacerlo funcionar)
- Utilizar Túnel Brokers, de modo tal de establecer túneles automáticos con algún sitio capaz de proveer conectividad IPv6. Para esto solo es necesario disponer de un host dual-stack y un navegador para ver la web o interfaz del "broker" y configurar a partir de allí el túnel.

Con cualquiera de estas variantes u otras que no están descritas en este libro, lograremos disponer de direcciones IPv6, por lo que, ahora sí estamos listos para pensar en la configuración de la red.

PROCESO III

3. CONFIGURACIÓN DE EQUIPOS

A continuación daremos una breve descripción de la configuración en los distintos equipos que mencionamos antes, necesaria para implementar IPv6 en una red de una institución académica.

3.1 Routers

Los equipos de encaminado deberán tener configurados los prefijos IPv6 que correspondan a la institución en las interfaces que van a tener IPv6 habilitado. Es conveniente permitir que los prefijos de red sean anunciados en cada LAN, para permitir la autoconfiguración de dispositivos.

Una mención especial merece el protocolo de encaminado interno que utiliza la institución: dado que ahora será necesario incluir el intercambio de información de IPv6 además de IPv4, se deberá utilizar algún sistema de encaminado interno que soporte IPv6. La recomendación es entonces utilizar OSPFv3, RIP y Túneles 6to4, que permiten manejar diferentes topologías en cada versión de IP.

Protocolo enrutamiento	**Versión IPv6**	**Característica**
RIP	RIPng	Es un protocolo de enrutamiento que utiliza un algoritmo de vector distancia utilizando como métrica el número de saltos. Posee una métrica de 15 saltos. En comparación con otros protocolos de enrutamiento, RIP es más fácil de configurar. Además, es un protocolo abierto, soportado por muchos fabricantes. Desventaja No permite indicar subredes. Al introducir nuevas redes, tiempo de actualización largo. Al desaparecer ciertas redes, problema de conteo al infinito. El tamaño de las redes está limitado a un valor máximo de 16 saltos.

OSPF	OSPFv3	La secuencia básica de operaciones realizadas por los routers con OSPFv3 es: Descubrir vecinos OSPFv3, Elegir el DR (designed router). Formar adyacencias (elementos cercanos), Sincronizar bases de datos, Calcular la tabla de encaminamiento. Los "routers" efectuarán todos estos pasos durante su activación, y los repetirán en respuesta a eventos de red. Cada "router" debe ejecutar estos pasos para cada red a la que está conectado, excepto para calcular la tabla de encaminamiento. Cada "router" genera y mantiene una sola tabla de encaminamiento para todas las redes.
STATIC	STATIC for IPv6	El administrador debe actualizar manualmente cada entrada de ruta estática siempre que un cambio en la topología de la red requiera una actualización. A demás la ausencia de tolerancia a fallos. Si cayese una línea en cualquier parte de la red, esta no sería capaz de reaccionar y automáticamente dirigir los paquetes por otro camino, ya que solo tienen una única ruta para hacerlo. La desventaja de las rutas estáticas es la cantidad de rutas que tendríamos que configurar con redes grandes y complejas. La imposibilidad de reparto de tráfico entre varios caminos posibles (balanceo de carga). CARACTERISTICAS -Fácil de entender -Fácil de configurar en redes pequeñas

Tabla 14. Protocolos de enrutamiento y Mecanismo de Túnel para IPv6

3.2 Configuración de IPv6 en Interfaces del router

Antes de aprender a configurar rutas, primero aprenderemos a como ingresar las direcciones IPv6 a cada una de las interfaces del router con los que trabajemos.

Pasos a seguir

1. enable
2. configure terminal
3. interfaz tipo número
4. ipv6 address ipv6-prefix / prefix
   ipv6 enable

5. salida
6. ipv6 unicast-routing

Pasos detallados

	Comando o acción	**Propósito**
Paso 1	**enable** **Ejemplo:** Router> enable	Permite modo EXEC privilegiado. Ingrese su contraseña si es necesario.
Paso 2	**ipv6 unicast-routing** **Ejemplo:** Router(config)# ipv6 unicast-routing	Permite el envío de datagramas unicast IPv6.
Paso 3	**configure terminal** **Ejemplo:** Router # configure terminal	Entra en el modo de configuración global.
Paso 4	*número de tipo de* **interfaz** **Ejemplo:** Router (config) # interface ethernet 0 / 0	Especifica un tipo de interfaz y número, y coloca el router en modo de configuración de la interfaz.
Paso 5	**ipv6 address** *ipv6-prefix / prefix* **ipv6 enable**	Ingresamos una dirección Ipv6 en la interfaz con su respectivo prefijo o mascara Y Avilitamos la interfaz para que pueda

	no shutdown **Ejemplo:** Router(config-if)# ipv6 address 2001:0DB8:0:1::/64 Router(config-if)# ipv6 enable Router(config-if)# no shutdown	trabajar con IPv6 Y levantamos la interfaz
Paso 6	**exit** **Ejemplo:** Router(config-if)# exit	Salimos de la interfaz de configuración, y regresamos al modo de configuración global.

Tabla 15. Pasos detallados para la Configuración de IPv6 en Interfaces del router

3.3 Configuración Rutas Estáticas en IPv6

En esta guía se describe cómo configurar rutas estáticas para IPv6. Este enrutamiento define las rutas que los paquetes viajan por la red. Al configurar manualmente las rutas estáticas para redes pequeñas ya no es necesario utilizar protocolos de enrutamiento dinámico.

Los dispositivos Ethernet reenvían los paquetes con información de la ruta que está configurado de formas manuales aprendidas mediante el protocolo de enrutamiento estático, además definen un camino de modo explícito entre dos dispositivos de red. A diferencia de un protocolo de enrutamiento dinámico, las rutas estáticas no se actualizan automáticamente y debe volver a configurar manualmente si cambia la topología de la red.

3.3.1 Las ventajas de usar rutas estáticas:

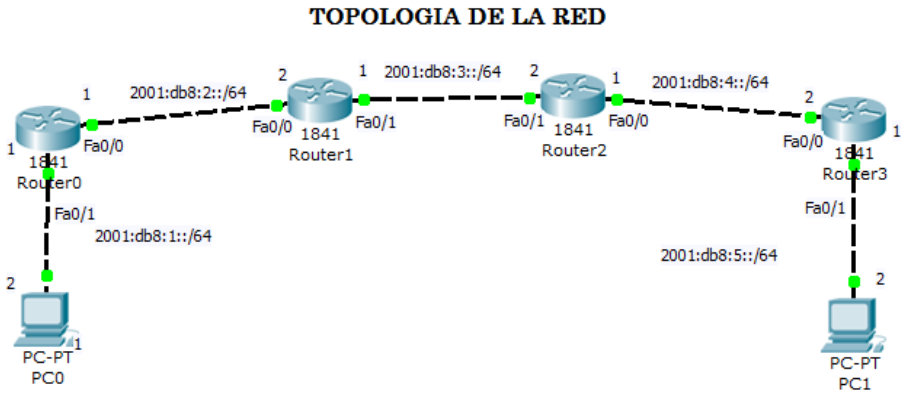
- Incluyen la seguridad y la eficiencia de los recursos.
- Las rutas estáticas utilizan menos ancho de banda que protocolos de enrutamiento dinámico y ciclos de CPU no se utilizan para calcular y comunicar las rutas.

3.3.2 La principal desventaja de usar rutas estáticas:

- Es la falta de reconfiguración automática, si cambia la topología de red.

Ejemplo de configuración de rutas estáticas IPv6:

Las pruebas se las realizó con router CISCO serie 2800.



Pasos detallados

	Comando o acción	Propósito
Paso 1	**Enable** **Ejemplo:** Router> enable	Permite modo EXEC privilegiado. Ingrese su contraseña si es necesario.

Paso 2	**configure terminal** **Ejemplo:** Router # configure terminal	Entra en el modo de configuración global.
Paso 3	**ipv6 unicast-routing** **Ejemplo:** Router(config)# ipv6 unicast-routing	Permite el envío de datagramas unicast IPv6.
Paso 4	**IPv6 ruta** *IPv6 prefijo* / *prefijo de longitud* / interfaz o wateway **Ejemplo:** Router (config) # IPv6 route:: / 0 serie 2 / 0 cambiar	Configura una ruta estática IPv6. • Una ruta estática por defecto IPv6 se configura en una interfaz de serie. • Vea los ejemplos de sintaxis que siguen inmediatamente a esta tabla para los usos específicos de la **ruta** de comandos para configurar**IPv6** rutas estáticas.

Tabla 16. Pasos detallados para la configuración de Rutas Estáticas en IPv6

3.4 Enrutamiento Estático en los Routers

ROUTER R1

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot system flash c2800nm-advipservicesk9-mz.124-25c.bin
boot-end-marker
!
no aaa new-model
!
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
!
voice-card 0
 no dspfarm
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:2::1/64
```

```
 ipv6 enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:1::1/64
 ipv6 enable
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 125000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 125000
!
ip forward-protocol nd
!
ip http server
no ip http secure-server
!
ipv6 route 2001:DB8:3::/64 2001:DB8:2::2
ipv6 route 2001:DB8:4::/64 2001:DB8:2::2
ipv6 route 2001:DB8:5::/64 2001:DB8:2::2
!
control-plane
!
line con 0
line aux 0
```

```
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end
```

ROUTER R2

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot system flash c2800nm-advipservicesk9-mz.124-25c.bin
boot-end-marker
!
no aaa new-model
!
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
!
voice-card 0
 no dspfarm
!
interface FastEthernet0/0
```

```
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:2::2/64
 ipv6 enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:3::1/64
 ipv6 enable
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 125000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 125000
!
ip forward-protocol nd
!
ip http server
no ip http secure-server
!
ipv6 route 2001:DB8:1::/64 2001:DB8:2::1
ipv6 route 2001:DB8:4::/64 2001:DB8:3::2
ipv6 route 2001:DB8:5::/64 2001:DB8:3::2
```

```
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end
```

ROUTER 3

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot system flash c2800nm-advipservicesk9-mz.124-25c.bin
boot-end-marker
!
no aaa new-model
!
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
```

```
!
voice-card 0
 no dspfarm
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:4::1/64
 ipv6 enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:3::2/64
 ipv6 enable
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 125000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 125000
!
ip forward-protocol nd
!
!
```

```
ip http server
no ip http secure-server
!
ipv6 route 2001:DB8:2::/64 2001:DB8:3::1
ipv6 route 2001:DB8:1::/64 2001:DB8:3::1
ipv6 route 2001:DB8:5::/64 2001:DB8:4::2
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end
```

ROUTER 4

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R4
!
boot-start-marker
boot system flash c2800nm-advipservicesk9-mz.124-25c.bin
boot-end-marker
!
no aaa new-model
!
ip cef
```

```
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
!
voice-card 0
 no dspfarm
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:4::2/64
 ipv6 enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:5::1/64
 ipv6 enable
!
interface Serial0/2/0
 no ip address
 shutdown
 no fair-queue
 clock rate 125000
!
interface Serial0/2/1
 no ip address
 shutdown
```

```
 clock rate 125000
!
ip forward-protocol nd
!
ip http server
no ip http secure-server
!
ipv6 route 2001:DB8:3::/64 2001:DB8:4::1
ipv6 route 2001:DB8:2::/64 2001:DB8:4::1
ipv6 route 2001:DB8:1::/64 2001:DB8:4::1
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end
```

3.5 Configuración RIPng para IPv6

RIPng es un protocolo de vector de distancia. RIPng debe ser implementado solo en Routers que soporte IPv6 provee otros mecanismos para descubrimiento de rutas. El protocolo cuenta sobre el acceso de cierta información acerca de cada una de esas redes, de lo cual lo más importante es su métrica. La métrica RIP de una red es un entero entre 1 y 15, inclusive. Esto es establecido en alguna forma no especificada en este protocolo; sin embargo, dado el máximo número de saltos es de 15, usualmente es usado un valor de 1. Las implementaciones deben permitir al administrador del sistema establecer la métrica de cada red. En adición a la métrica, cada red tendrá un prefijo de dirección destino y la longitud del prefijo asociado a este. Estos son establecidos por el administrador del sistema de una manera no especificada en este protocolo.

Cada router que implementa RIP es asumido que tiene una tabla de ruteo. Esta tabla tiene una entrada para cada destino que es asequible desde todas partes por el Sistema Operativo RIP. Cada entrada contiene al menos la siguiente información:

- El prefijo IPv6 del destino.
- Una métrica, la cual representa el costo total de obtener un datagrama desde el router a este destino. Esta métrica es la suma de los costos asociados con las redes que serian recorridas para obtener el destino.
- La dirección IPv6 del próximo router pertenece al camino del destino. Si el destino está sobre una de las redes directamente conectadas, este punto no es necesario.

Las entradas para las redes directamente conectadas son establecidas por el router usando información recolectada que en ningún caso es especificada en este protocolo. La métrica para una red directamente conectada es establecer el costo de esta red.

Los implementadores pueden también seleccionar el permitir al Administrador del Sistema introducir rutas adicionales. Esto es similar a rutear hosts o redes fuera del alcance del Sistema de ruteo. Esto es referido como “Rutas Estáticas”. Las entradas para otros destinos que son inicialmente son sumadas y actualizadas por ciertos algoritmos.

3.5.1 Pasos a seguir

1. enable
2. configure terminal
3. ipv6 unicast-routing
4. IPv6 router *rip nombre_del_proces*o
5. exit
6. número de tipo de interfaz
7. IPv6 rip *nombre_del_proceso* ***enable***

Pasos detallados

	Comando o acción	**Propósito**
Paso1	**Enable** **Ejemplo:** Router> enable	Permite modo EXEC privilegiado. Ingrese su contraseña si es necesario.
Paso2	**configure terminal** **Ejemplo:** Router # configure terminal	Entra en el modo de configuración global.
Paso3	**ipv6 unicast-routing** **Ejemplo:** Router(config)# ipv6 unicast-routing	Permite el envío de datagramas unicast IPv6.
Paso4	**Ipv6 router rip nombre_del_proceso** **Ejemplo:**	Configura un enrutamiento IPv6 RIP proceso y entra en el modo de configuración del router para el PIR de enrutamiento IPv6 proceso.

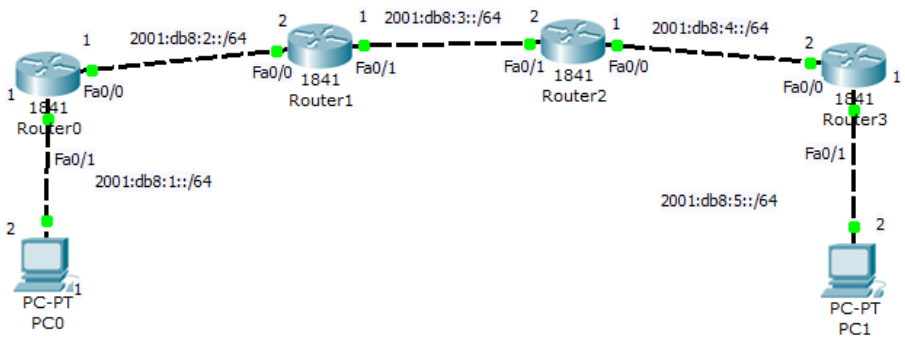
	Router (config) #IPv6 router rip proceso1	
Paso5	**Salida** **Ejemplo:** Router (config-if) # exit	Sale de la interfaz de configuración de modo y entra en el modo de configuración global.
Paso6	*número de tipo de* **interfaz** **Ejemplo:** Router (config) # interfaz Ethernet 0 / 0	Especifica el tipo de interfaz y número, y entra en modo de configuración de la interfaz.
Paso7	*Ipv6 rip* **nombre_del_proceso enable** *Ejemplo:* *Router (config-if) # Ipv6 rip* **proceso1 enable**	Permite una IPv6 Routing Information Protocol (RIP) proceso de enrutamiento en una interfaz.

Tabla 17. Pasos detallados para la Configuración de RIPng para IPv6

Ejemplo de configuración RIP par IPv6:

Las pruebas se las realizo con router CISCO serie 2800.

TOPOLOGIA DE LA RED



3.6 Enrutamiento RIPng en los Routers

ROUTER 1

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R1

!

boot-start-marker

boot system flash c2800nm-advipservicesk9-mz.124-25c.bin

boot-end-marker

!

no aaa new-model

!

ip cef

!

ip auth-proxy max-nodata-conns 3

ip admission max-nodata-conns 3

!

ipv6 unicast-routing

!

```
voice-card 0
 no dspfarm
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:2::1/64
 ipv6 enable
 ipv6 rip 1 enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:1::1/64
 ipv6 enable
 ipv6 rip 1 enable
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 125000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 125000
!
ip forward-protocol nd
!
ip http server
```

```
no ip http secure-server
!
ipv6 router rip 1
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end
```

ROUTER 2

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot system flash c2800nm-advipservicesk9-mz.124-25c.bin
boot-end-marker
!
no aaa new-model
!
!
ip cef
!
```

```
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
!
voice-card 0
 no dspfarm
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:2::2/64
 ipv6 enable
 ipv6 rip 1 enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:3::1/64
 ipv6 enable
 ipv6 rip 1 enable
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 125000
!
interface Serial0/0/1
 no ip address
```

```
 shutdown
 clock rate 125000
!
ip forward-protocol nd
!
ip http server
no ip http secure-server
!
ipv6 router rip 1
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end
```

ROUTER 3

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot system flash c2800nm-advipservicesk9-mz.124-25c.bin
boot-end-marker
```

```
!
!
no aaa new-model
!
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
!
voice-card 0
 no dspfarm
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:4::1/64
 ipv6 enable
 ipv6 rip 1 enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:3::2/64
 ipv6 enable
 ipv6 rip 1 enable
!
interface Serial0/0/0
 no ip address
```

```
 shutdown
 no fair-queue
 clock rate 125000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 125000
!
ip forward-protocol nd
!
ip http server
no ip http secure-server
!
ipv6 router rip 1
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end
```

ROUTER 4

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
!
hostname R4
!
boot-start-marker
boot system flash c2800nm-advipservicesk9-mz.124-25c.bin
boot-end-marker
!
no aaa new-model
!
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
!
voice-card 0
 no dspfarm
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:4::2/64
 ipv6 enable
 ipv6 rip 1 enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:5::1/64
```

```
 ipv6 enable
 ipv6 rip 1 enable
!
interface Serial0/2/0
 no ip address
 shutdown
 no fair-queue
 clock rate 125000
!
interface Serial0/2/1
 no ip address
 shutdown
 clock rate 125000
!
ip forward-protocol nd
!
ip http server
no ip http secure-server
!
ipv6 router rip 1
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
End
```

3.7 Configuración OSPFv3 para IPv6:

OSPF es un protocolo de enrutamiento de IP. Se trata de un vínculo de Protocolo del Estado, en contraposición a una distancia de protocolo de vector. Piense en un enlace como una interfaz en un dispositivo de red. Un enlace de Protocolo del Estado toma sus decisiones de encaminamiento basadas en los estados de los vínculos que conectan a máquinas de origen y de destino. El estado de un enlace es una descripción de la interfaz y su relación con sus dispositivos de red vecinos. La información de interfaz incluye el prefijo IPv6 de la interfaz, la máscara de red, y así sucesivamente entre todos los routers. Esta información se propaga en diversos tipos de anuncios de estado de enlace (LSA).

El LSA se almacena en una base de datos de enlace del Estado. El contenido de la base de datos, se crea la tabla de enrutamiento OSPF. La diferencia entre la base de datos y la tabla de enrutamiento es que la base de datos contiene una completa colección de datos en bruto; la tabla de enrutamiento contiene una lista de rutas más cortas a destinos específicos conocidos a través de puertos de interfaz del router.

OSPFv3 Es la versión de OSPF para IPv6, esta basada en OSPFv2, con varias adiciones, además es utilizada para distribuir prefijos de IPv6, y además Aunque tiene el mismo nombre que OSPFv2, sondos protocolos diferente

Similitud entre OSPFv2 y OSPFv3

- Mecanismos para el descubrimiento de vecinos y la formación de adyacencias
- Tipos de Interfaces
    - P2P, P2MP, Broadcast, Virtual
- Propagación y remoción de LSAs
- Tipos muy similares de LSAs
- Tipos básicos de paquetes

  Existen cinco tipos de mensajes del protocolo OSPF:

1. **HELLO o Saludo** se usa para:

   - Identificar a los vecinos, para crear una base de datos en mapa local.
   - Enviar señales de <estoy vivo>, al resto de routers para mantener el mapa local.
   - Elegir un router designado para una red multienvío
   - Encontrar al router designado existente.
   - Enviar señales de <estoy vivo>

2. **Database Description Packets o Descripción de la base de datos** se usa para:

   - Intercambiar información para que un router pueda descubrir los datos que le faltan durante la fase de inicialización o sincronización cuando dos nodos han establecido una conectividad.

3. **Link State Request o Petición del estado del enlace** se usa para:

   - Pedir datos que un router se ha dado cuenta que le faltan en su base de datos o que están obsoletos durante la fase de intercambio de información entre dos routers..

4. **Link State Request o Actualización del estado del enlace** se usa como:

   - Respuesta a los mensajes de Petición de estado del enlace y también para informar dinámicamente de los cambios en la topología de la red. El emisor retransmitirá hasta que se confirme con un mensaje de ACK.

5. **Link State ACK o ACK del estado del enlace** se usa para:

   - Confirmar la recepción de una Actualización del estado del enlace.

Diferencias entre OSPFv2 y OSPFv3

- OSPFv3 usan el enlace, en lugar de la subred
- Puedes tener varias instancias por enlace
- Topología de OSPFv2 no es específica para IPv6
    - Router ID
    - Link ID
- Mecanismos estandarizados de autentificación
- Utiliza direcciones de enlace local

3.7.1 Pasos a seguir

1. enable
2. configure terminal
3. ipv6 unicast-routing
4. interfaz *tipo número*
5. IPv6 *proceso ospf-Zona de id-ID* [ejemplo *ejemplo-id]*

Los pasos detallados

	Comando o acción	**Propósito**
Paso1	**Enable** **Ejemplo:** Router> enable	Activa el modo EXEC privilegiado. Introduzca su contraseña si se le pide.
Paso2	**configure terminal** **Ejemplo:**	Entra en el modo de configuración global.

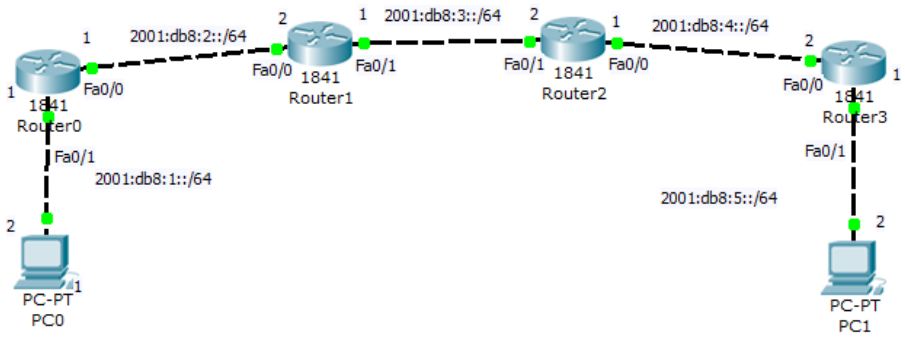
	Router # configure terminal	
Paso3	**ipv6 unicast-routing** **Ejemplo:** Router(config)# ipv6 unicast-routing	Permite el envío de datagramas unicast IPv6.
Paso4	*número de tipo* **de interfaz** **Ejemplo:** Router (config) # interface ethernet 0 / 0	Especifica un tipo de interfaz y el número, y coloca el router en modo de configuración de la interfaz.
Paso5	*Ip address ipv4 / mascara_de_la red* **Ejemplo:** *Router (config-if) #ip address 10.10.0.1 255.255.0.0*	Ingresa una dirección IPv4 para que esta se asigne como id para la configuración del router en OSPFv3
Paso6	**IPv6** *proceso* ***ospf-Zona*** *de id-ID***[ejemplo** *ejemplo-id]* **Ejemplo:** Router (config) # ipv6 ospf 1 area 0	Permite OSPF para IPv6 en una interfaz.

Tabla 18. Pasos detallados para la Configuración de OSPFv3 para IPv6

Ejemplo de configuración OSPFv3 par IPv6:

Las pruebas se las realizo con router CISCO serie 2800.

TOPOLOGIA DE LA RED



3.8 Enrutamiento OSPFv3 en los Routers

ROUTER 1

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R1

!

boot-start-marker

boot system flash c2800nm-advipservicesk9-mz.124-25c.bin

boot-end-marker

!

no aaa new-model

!

ip cef

!

ip auth-proxy max-nodata-conns 3

ip admission max-nodata-conns 3

!

ipv6 unicast-routing

!

```
voice-card 0
 no dspfarm
!
interface FastEthernet0/0
 ip address 10.10.0.1 255.255.0.0
 duplex auto
 speed auto
 ipv6 address 2001:DB8:2::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface FastEthernet0/1
 ip address 10.9.0.1 255.255.0.0
 duplex auto
 speed auto
 ipv6 address 2001:DB8:1::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 125000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 125000
!
ip forward-protocol nd
!
ip http server
```

```
no ip http secure-server
!
ipv6 router ospf 1
 log-adjacency-changes
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end
```

ROUTER 2

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot system flash c2800nm-advipservicesk9-mz.124-25c.bin
boot-end-marker
!
no aaa new-model
!
ip cef
!
```

```
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
!
voice-card 0
 no dspfarm
!
interface FastEthernet0/0
 ip address 10.10.0.2 255.255.0.0
 duplex auto
 speed auto
 ipv6 address 2001:DB8:2::2/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface FastEthernet0/1
 ip address 10.11.0.1 255.255.0.0
 duplex auto
 speed auto
 ipv6 address 2001:DB8:3::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 125000
!
interface Serial0/0/1
 no ip address
```

```
 shutdown
 clock rate 125000
!
ip forward-protocol nd
!
ip http server
no ip http secure-server
!
ipv6 router ospf 1
 log-adjacency-changes
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end
```

ROUTER 3

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot system flash c2800nm-advipservicesk9-mz.124-25c.bin
```

```
boot-end-marker
!
no aaa new-model
!
!
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
!
voice-card 0
 no dspfarm
!
interface FastEthernet0/0
 ip address 10.12.0.1 255.255.0.0
 duplex auto
 speed auto
 ipv6 address 2001:DB8:4::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface FastEthernet0/1
 ip address 10.11.0.2 255.255.0.0
 duplex auto
 speed auto
 ipv6 address 2001:DB8:3::2/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface Serial0/0/0
```

```
 no ip address
 shutdown
 no fair-queue
 clock rate 125000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 125000
!
ip forward-protocol nd
!
!
ip http server
no ip http secure-server
!
ipv6 router ospf 1
 log-adjacency-changes
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
End
```

ROUTER 4

```
version 12.4
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R4
!
boot-start-marker
boot system flash c2800nm-advipservicesk9-mz.124-25c.bin
boot-end-marker
!
no aaa new-model
!
ip cef
!
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
!
voice-card 0
 no dspfarm
!
interface FastEthernet0/0
 ip address 10.12.0.2 255.255.0.0
 duplex auto
 speed auto
 ipv6 address 2001:DB8:4::2/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface FastEthernet0/1
```

```
 ip address 10.13.0.1 255.255.0.0
 duplex auto
 speed auto
 ipv6 address 2001:DB8:5::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface Serial0/2/0
 no ip address
 shutdown
 no fair-queue
 clock rate 125000
!
interface Serial0/2/1
 no ip address
 shutdown
 clock rate 125000
!
ip forward-protocol nd
!
!
ip http server
no ip http secure-server
!
ipv6 router ospf 1
 log-adjacency-changes
!
control-plane
!
line con 0
line aux 0
line vty 0 4
```

```
 login
!
scheduler allocate 20000 1000
!
end
```

3.9. Configuración Túnel 6to4 para IPv6

6to4 es un mecanismo de transición de Internet para la migración de Protocolo de Internet versión 4 (IPv4) para IPv6, un sistema que permite que los paquetes IPv6 a ser transmitidos a través de una red IPv4 (por lo general la Internet IPv4). 6to4 también permiten comunicarse con las máquinas de la Internet IPv6. Generalmente se usa cuando un fin de sitio o el usuario final desea conectarse a Internet IPv6 usando su conexión IPv4 existente.

Cuando 6to4 es utilizado por una red local, toda la red local sólo necesita una dirección IPv4 único. Dentro de esa red, los hosts aprenden sus direcciones IPv6 y el enrutamiento utiliza protocolos de descubrimiento de router normal, así como en una red IPv6 nativa.

Mecanismo de Túnel	**Protocolo de enrutamiento que puede utilizar**
6to4	RIPng OSPFv3 STATIC for IPv6

3.9.1 Como Funciona 6to4

Exige que el extremo del túnel tenga una dirección IPv4 pública. Sin embargo, muchas máquinas están conectadas a Internet IPv4 a través de uno o varios dispositivos NAT, por lo general debido a la escasez de direcciones IPv4. En tal situación, la única disponible dirección IPv4 pública se asigna al dispositivo NAT, y el extremo del túnel

6to4 debe aplicarse en el dispositivo NAT en sí. Muchos dispositivos NAT actualmente se encuentran desplegados, sin embargo, no se puede actualizar para aplicar 6to4, por razones técnicas o económicas.

6to4 realiza tres funciones:

1. Asigna un bloque de espacio de direcciones IPv6 a cualquier host o de red que tiene una dirección IPv4 global.
2. Encapsula los paquetes IPv6 dentro de paquetes IPv4 para la transmisión a través de una red IPv4 utilizando 6in4.
3. Rutas de tráfico entre 6to4 y "nativo" de las redes IPv6.

3.9.1.1 Pasos a seguir

1. enable
2. configure terminal
3. ipv6 unicast-routing
4. *número de tipo* de interfaz
5. *Ip address ipv4 / mascara_de_la red*
6. ipv6 address *ipv6-prefix* / *prefix*

   ipv6 enable

   no shutdown
7. interface Tunnel0
8. ipv6 address *ipv6-prefix* / *prefix*

   ipv6 enable
9. Tunnel source *ipv6-prefix* / *prefix*
10. Tunnel destination
11. tunnel mode ipv6ip

    no shutdown
12. Ip route ipv4_destino/ mascara de subred / interfaz_gateway
13. Ipv6 route / dirección_IPv6 / prefijo /gateway

Los pasos detallados

	Comando o acción	**Propósito**
Paso1	**Enable** **Ejemplo:** Router> enable	Activa el modo EXEC privilegiado. • Introduzca su contraseña si se le pide.
Paso2	**configure terminal** **Ejemplo:** Router # configure terminal	Entra en el modo de configuración global.
Paso3	**ipv6 unicast-routing** **Ejemplo:** Router(config)# ipv6 unicast-routing	Permite el envío de datagramas unicast IPv6.
Paso4	*número de tipo* **de interfaz** **Ejemplo:** Router (config) # interface ethernet 0 / 0	Especifica un tipo de interfaz y el número, y coloca el router en modo de configuración de la interfaz.
Paso5	*Ip address ipv4 / mascara_de_la red* **Ejemplo:** *Route (config-if) #ip address 10.9.0.1 255.255.0.0*	Ingresamos dirección IPv4 en los routers para que estas se puedan comunicar por medio de ruteo estáticas

Paso6	**ipv6 address** *ipv6-prefix / prefix* **ipv6 enable** no shutdown **Ejemplo:** Router(config-if)# ipv6 address 2001:DB8:1::1/64 Router(config-if)# ipv6 enable Router(config-if)# no shutdown	Ingresamos una dirección Ipv6 en la interfaz con su respectivo prefijo o mascara Y Habilitamos la interfaz para que pueda trabajar con IPv6 Y levantamos la interfaz
Paso7	interface Tunnel0 **Ejemplo:** Router (config) # interface tunnel 0	Creamos la interfaz de túnel para que permita que los paquetes IPv6 puedan ser transmitidos a través de una red IPv4
Paso8	**ipv6 address** *ipv6-prefix / prefix* **ipv6 enable** **Ejemplo:** Router(config-if)# ipv6 address 2001:db8:6::1/64 Router(config-if)# ipv6 enable	Ingresamos una dirección Ipv6 en la interfaz con su respectivo prefijo o mascara Y Habilitamos la interfaz para que pueda trabajar con IPv6

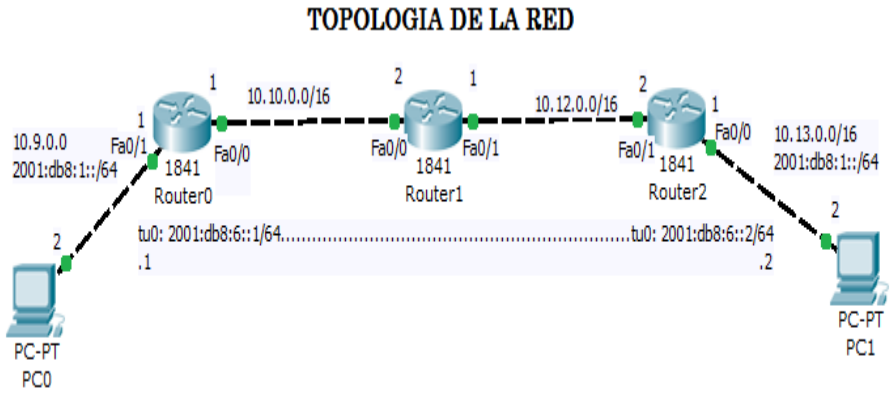
Paso9	**Tunnel source** *ipv6-prefix / prefix* **Ejemplo:** Router(config-if)# tunnel source 10.10.0.1	Colocamos la dirección IPv4 local del origen del túnel para la comunicación
Paso10	**Tunnel destination** **Ejemplo:** Router(config-if)# tunnel **destination** **10.12.0.2**	Colocamos la dirección IPv4 local del destino del túnel para la comunicación
Paso11	**tunnel mode ipv6ip** no shutdown **Ejemplo:** Router(config-if)# **tunnel mode ipv6ip** Router(config-if)# no shutdown	Le damos un modo o camino para que se comunique el túnel por medio de las direcciones IPV6 Y levantamos la interfaz
Paso12	Ip route ipv4_destino/ mascara de subred / interfaz_gateway Ejemplo: Router(config)# ip route 0.0.0.0 0.0.0.0 10.10.0.2	A lo que hacemos ruteo estático estamos permitiendo que se puedan comunicar las direcciones IPv4 entre los distintos routers

Paso13	Ipv6 route / dirección_IPv6 / prefijo /gateway Ejemplo: Router(config)# ipv6 route ::/0 2001:DB8:6::2	A lo que hacemos ruteo estático estamos permitiendo que se puedan comunicar las direcciones IPv6 entre los distintos routers y de esta forma podemos realizar la comunicación por medio del túnel

Tabla 19. Pasos detallados de Configuración del Túnel 6to4 para IPv6

Ejemplo de configuración RIP par IPv6.

Las pruebas se las realizo con router CISCO serie 2800.



3.9.2 Configuración Túnel 6to4 en los Routers

ROUTER R1

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R1

!

boot-start-marker

```
boot system flash c2800nm-advipservicesk9-mz.124-25c.bin
boot-end-marker
!
no aaa new-model
!
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
!
voice-card 0
 no dspfarm
!
interface Tunnel0
 no ip address
 ipv6 address 2001:DB8:6::1/64
 ipv6 enable
 tunnel source 10.10.0.1
 tunnel destination 10.12.0.2
 tunnel mode ipv6ip
!
interface FastEthernet0/0
 ip address 10.10.0.1 255.255.0.0
 duplex auto
 speed auto
 ipv6 enable
!
interface FastEthernet0/1
 ip address 10.9.0.1 255.255.0.0
 duplex auto
```

```
 speed auto
 ipv6 address 2001:DB8:1::1/64
 ipv6 enable
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 125000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 125000
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.10.0.2
!
ip http server
no ip http secure-server
!
ipv6 route ::/0 2001:DB8:6::2
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end
```

ROUTER R2

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot system flash c2800nm-advipservicesk9-mz.124-25c.bin
boot-end-marker
!
no aaa new-model
!
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
!
voice-card 0
 no dspfarm
!
interface FastEthernet0/0
 ip address 10.10.0.2 255.255.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.12.0.1 255.255.0.0
 duplex auto
```

```
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 125000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 125000
!
ip forward-protocol nd
ip route 10.9.0.0 255.255.0.0 10.10.0.1
ip route 10.13.0.0 255.255.0.0 10.12.0.2
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end
```

ROUTER 3

```
version 12.4
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot system flash c2800nm-advipservicesk9-mz.124-25c.bin
boot-end-marker
!
no aaa new-model
!
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
!
voice-card 0
 no dspfarm
!
interface Tunnel0
 no ip address
 ipv6 address 2001:DB8:6::2/64
 ipv6 enable
 tunnel source 10.12.0.2
 tunnel destination 10.10.0.1
 tunnel mode ipv6ip
!
interface FastEthernet0/0
 ip address 10.13.0.1 255.255.0.0
```

```
 duplex auto
 speed auto
 ipv6 address 2001:DB8:5::1/64
 ipv6 enable
!
interface FastEthernet0/1
 ip address 10.12.0.2 255.255.0.0
 duplex auto
 speed auto
 ipv6 enable
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 125000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 125000
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.12.0.1
!
ip http server
no ip http secure-server
!
ipv6 route ::/0 2001:DB8:6::1
!
control-plane
!
```

```
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
end
```

CAPITULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- El protocolo de internet Ipv6 soporta gran cantidad de direcciones jerárquicas que permiten un crecimiento de la infraestructura de red y nuevas capacidades de enrutamiento ordenado bajo las normativas de RFC 2460 Request for Comments 2460 (Petición de Comentarios: 2460) que es un conjunto de protocolos de comunicación entre routers como es enrutamiento estático, ripng, ospfv3.

- IPv6 Soporta aplicaciones en tiempo real, está proyectada para correr en redes de alta velocidad y a la vez ser eficiente en redes de ancho de banda bajo.

- Las prácticas desarrolladas en el laboratorio de la Facultad de Ingeniería de la UNACH es ampliamente adaptable para proyectos de gran tamaño, los requerimientos variaran según las necesidad de cada institución, ya sean estas de infraestructura o arquitectura, sin embargo la aplicación de Ipv6 es el misma.

- La guía detalla los pasos básicos que se debe tomar a consideración para la migración de Ipv4 a Ipv6, a demás cita procesos de enrutamiento y direccionamiento.

- El mecanismo de transición 6to4 es el que mejor se adapta para integrar un conjunto de computadoras con IPv6 en una infraestructura de red Ipv4.

- En la región de Sudamérica y el Caribe todavía trabaja con Ipv4, y no se encuentra desarrollado el enlace de tunnel bróker por lo cual dificulta dar el servicio de internet dentro de una intranet con ipv6.

5.2 Recomendaciones

- Hay que verificar si la IOS Internetwork Operating System, (Sistema Operativo de Interconexión de Redes) soporta protocolo IPV6, en nuestra implementación trabajamos con router Cisco serie 2800 la misma que poseía IOS IP Base **"c2800nm-ipbase-mz"** que no soporta dicho protocolo, teniendo que realizar una actualización a la versión Cisco IOS Advanced IP Services **"c2800nm-advipservicesk9-mz"**.

- Antes de implementar una red con el protocolo ipv6 debemos tener muy claramente los métodos de enrutamiento (revisar la Guía metodológica), estos son: estático, Ripng, OSPFv3, para de esta forma poder adaptarlas de acuerdo a las necesidades e infraestructura que posea la institución.

- Se recomienda el uso del método de transición y coexistencia 6to4 para la implementación de ipv6 ya que dicho método es el que se adapta de mejor forma a los protocolos de enrutamiento existentes esencialmente por que este método permite a sitios o hosts IPv6 comunicarse entre ellos a través de una red IPv4, sin necesidad de configuración manual de túneles, y permite que dichos sitios o hosts se comuniquen con el Internet IPv6 por medio de enrutadores 6to4 Relay.

TRABAJO FUTURO PARA EL ÁREA DE INFORMATICA DE LA FACULTAD DE INGENIERÍA DE LA UNACH

Plan de actualización de la red.

Tal como se describe en el capítulo 4 de este proyecto, está encaminado a la implementación de IPv6 dentro de la Facultad de Ingeniería de la UNACH. Pero en un futuro se deberá actualizar no solo la facultad, sino también toda de la red universitaria debiendose considerar los siguientes aspectos:

- De implementar IPv6 a los diferentes servicios que son:
  - Servidor PROXY
  - Servidor DNS
  - Servidor WEB
  - Servidor FTP

- Además de tener un direccionamiento IPv6 comenzando con en el Backbone principal, desde el proveedor de servicios de la institución "TELCONET", pasando por el switch de Core Cisco 4500 hasta los switch de distribución de cada una de las facultades.

  Y de esta forma ofrecer mejores prestaciones, lograr un mejor rendimiento y así solventar el problema existente del tunnel bróker.

BIBLIOGRAFÍA

- Blanchet, Marc. Migrating to IPv6: A practical Guide to Implemeting IPv6 in Mobile and Fixed Networks. Enero 3, 2006.
- Gai, Silvano. Internetworking IPv6 with Cisco routers. Mcgraw-Hill. Marzo 27 de 1998.
- Grosse, Erick. Lakshman. Network Processors Applied to IPv4/IPv6 Transition. Laboratorios Bell. Nueva Jersey, Estados Unidos. Agosto 2003.
- Kotal, Vladimír. PhD Thesis. Principles, implementation and transistion to IPv6 protocol. Universidad de Karlova, Praga.Abril 19 de 2005.
- Lund Kramshøj ,Henrik . MC Thesis. Designing Internetworks with IPv6. Dinamarca.
- Ramírez, Sergio, María Cervantes. Introducción al IPv6. Universidad de la República.
- Waddingtin, Daniel G, Fangzhe Chang. Realizing the Transition to IPv6. IEEE Communications Magazine. Vol. 6, issue 3., pp.38-48., Junio 2002.
- Mark A. Miller, M&T Books Implementing IPv6, 2nd Edition, 2000.

Bibliografía Electrónica

- http://portalipv6.lacnic.net/
- http://www.cisco.com/en/US/tech/tk872/tsd_technology_support_protocol_home.html
- http://es.wikipedia.org/wiki/IPv6
- http://www.rau.edu.uy/ipv6/queesipv6.htm
- http://lacnic.net/sp/index.html

Paginas web para implementar Tunnel Broker.

- http://www.tunnelbroker.net
- http://tb4.consulintel.euro6ix.org/es/registro.php
- http://www.ipv6tf.org/index.php?page=using/connectivity/test

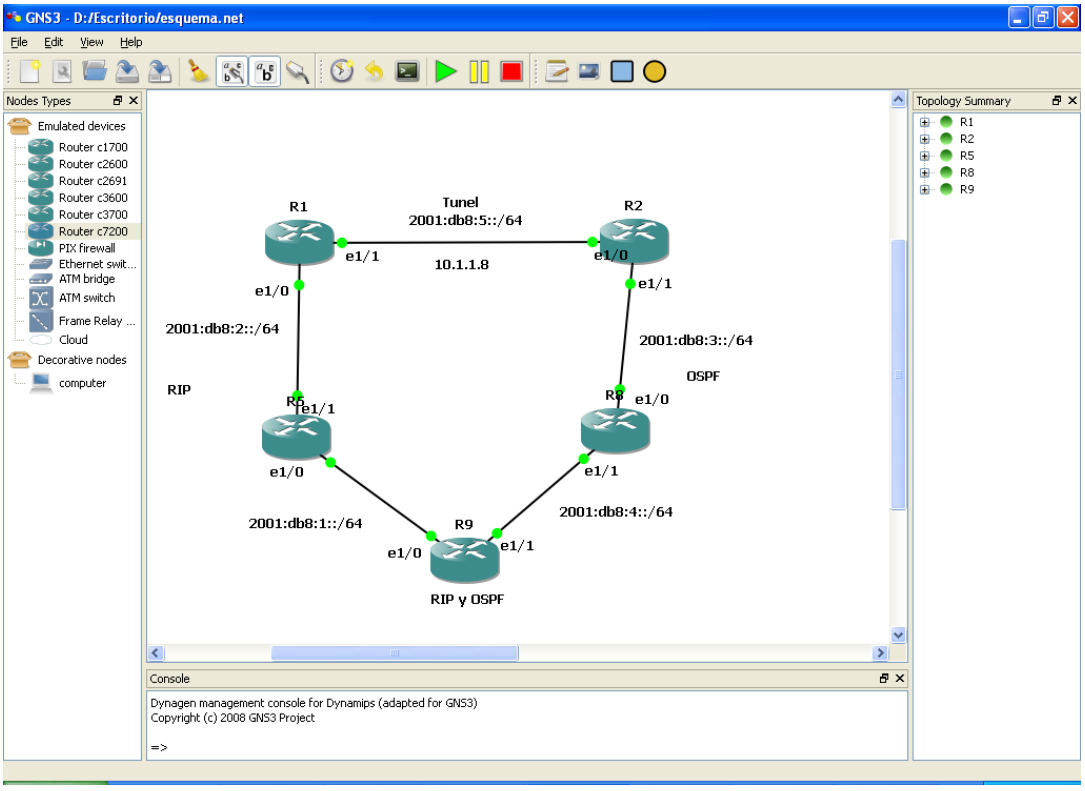
ANEXOS

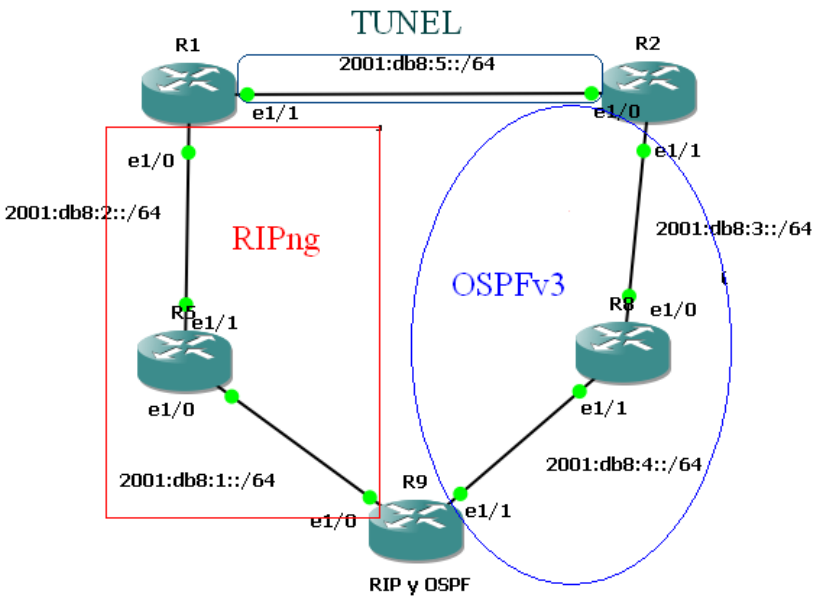
UNIVERSIDAD NACIONAL DE CHIMBORAZO
ESCUELA DE ING. EN SISTEMAS Y COMPUTACIÓN

ANEXO Nº 1

CONFIGURACIÓN DE ENRUTAMIENTOS DINAMICOS RIPNG Y OSPFV3 EN UNA RED

TOPOLOGÍA DE LA RED CON EL SIMULADOR GNS3

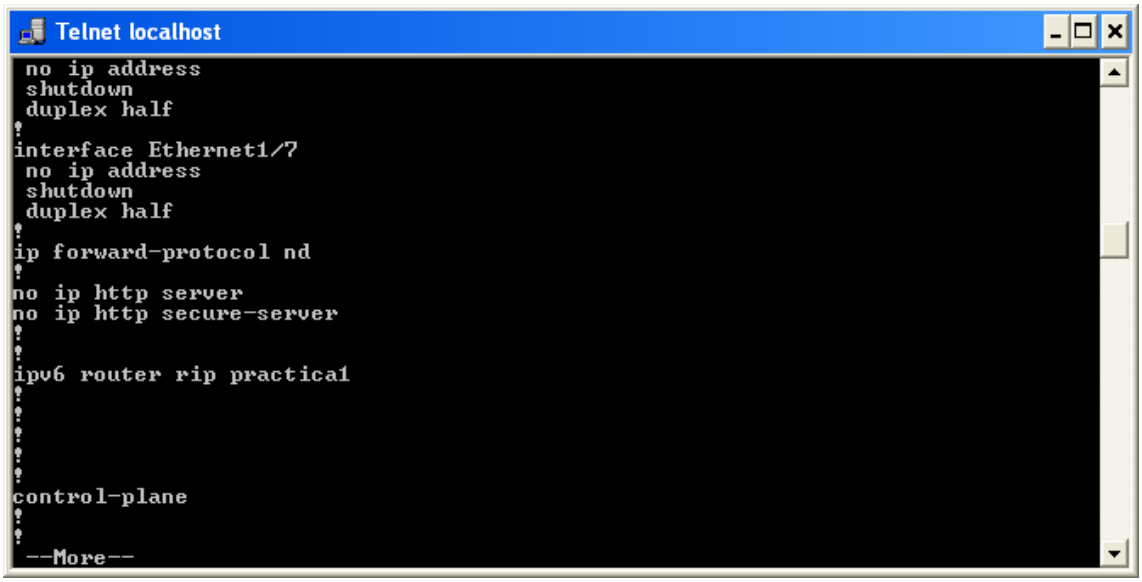




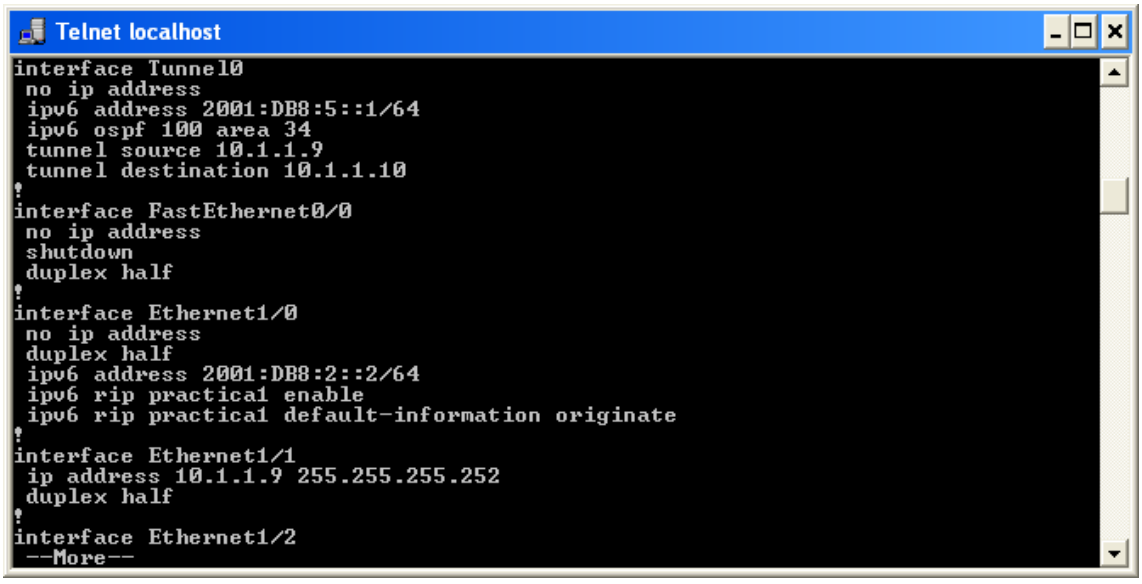
ROUTER 5

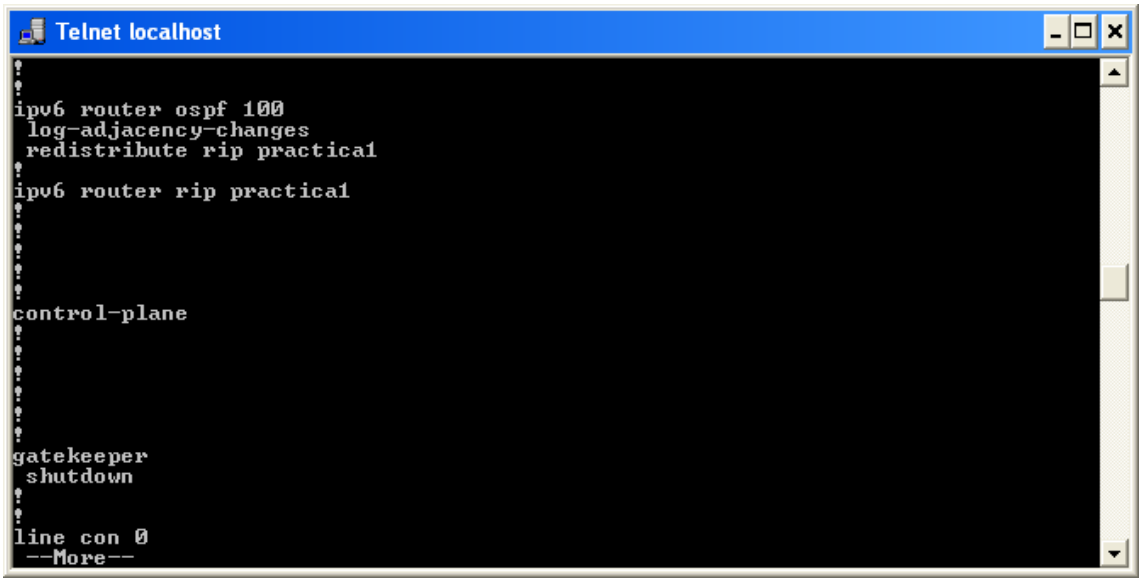
Telnet localhost

```
 duplex half
!
interface Ethernet1/0
 no ip address
 duplex half
 ipv6 address 2001:DB8:1::1/64
 ipv6 rip practica1 enable
!
interface Ethernet1/1
 no ip address
 duplex half
 ipv6 address 2001:DB8:2::1/64
 ipv6 rip practica1 enable
!
interface Ethernet1/2
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/3
 no ip address
 shutdown
 duplex half
!
 --More--
```

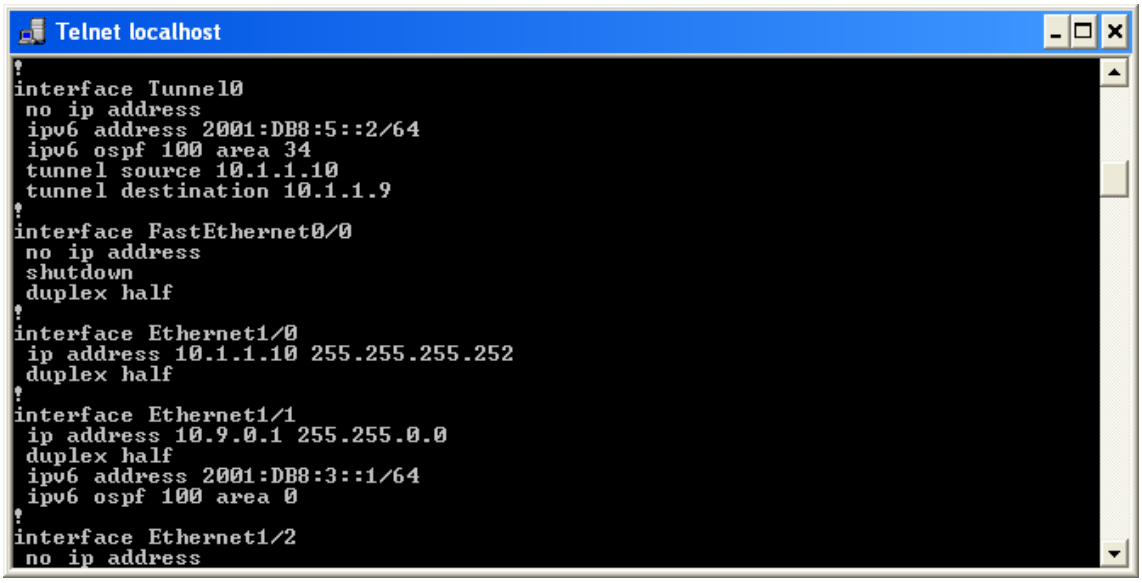

Telnet localhost
no ip address
shutdown
duplex half
!
interface Ethernet1/7
no ip address
shutdown
duplex half
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
ipv6 router rip practica1
!
!
!
!
!
control-plane
!
!
--More--

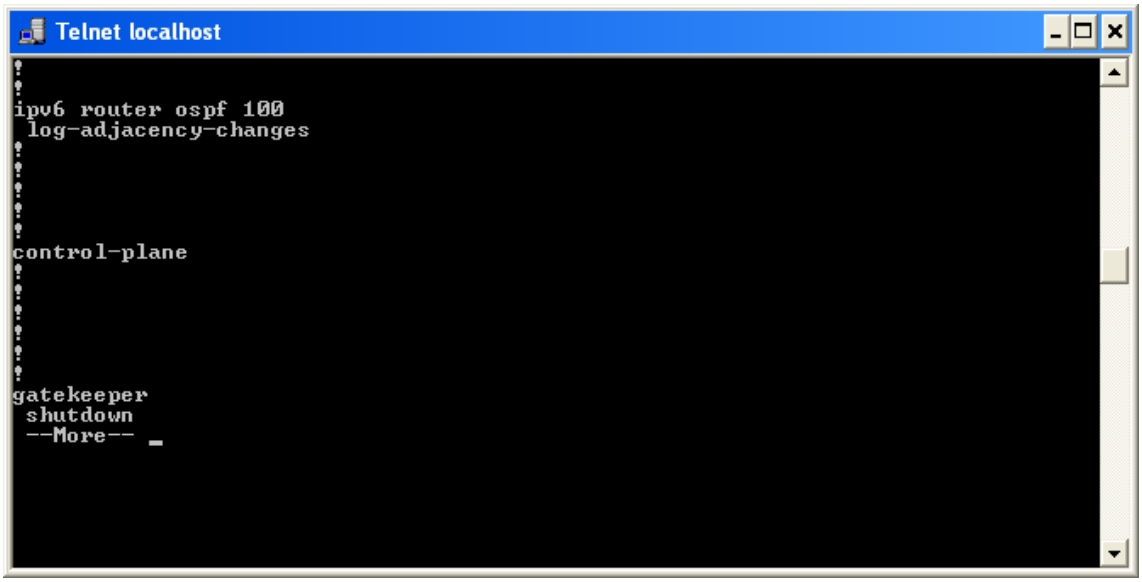
ROUTER 1


Telnet localhost
interface Tunnel0
no ip address
ipv6 address 2001:DB8:5::1/64
ipv6 ospf 100 area 34
tunnel source 10.1.1.9
tunnel destination 10.1.1.10
!
interface FastEthernet0/0
no ip address
shutdown
duplex half
!
interface Ethernet1/0
no ip address
duplex half
ipv6 address 2001:DB8:2::2/64
ipv6 rip practica1 enable
ipv6 rip practica1 default-information originate
!
interface Ethernet1/1
ip address 10.1.1.9 255.255.255.252
duplex half
!
interface Ethernet1/2
--More--

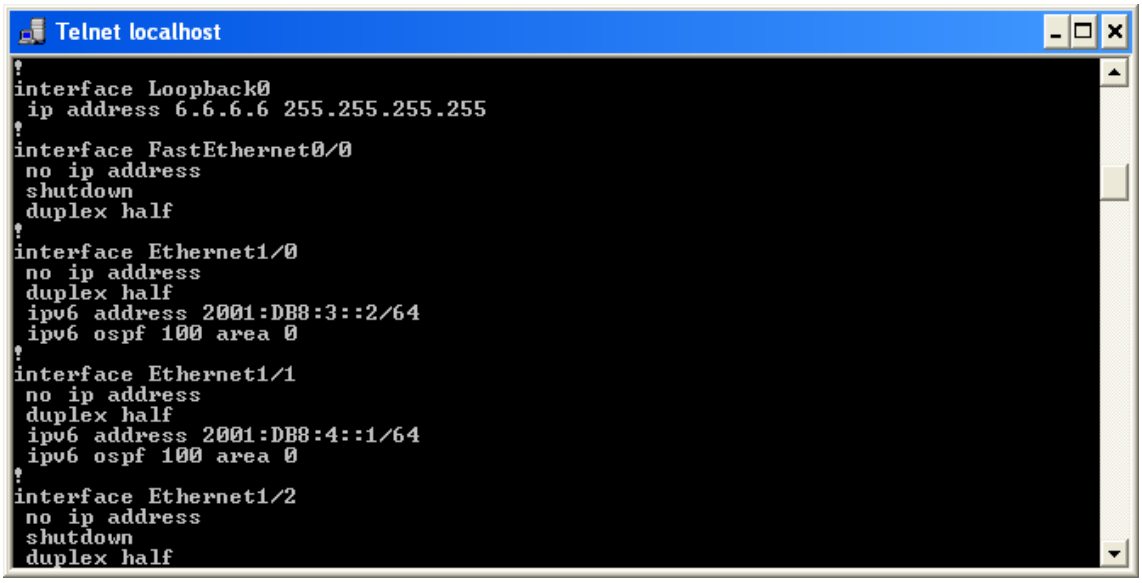

Telnet localhost
!
!
ipv6 router ospf 100
 log-adjacency-changes
 redistribute rip practica1
!
ipv6 router rip practica1
!
!
!
!
!
control-plane
!
!
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 --More--

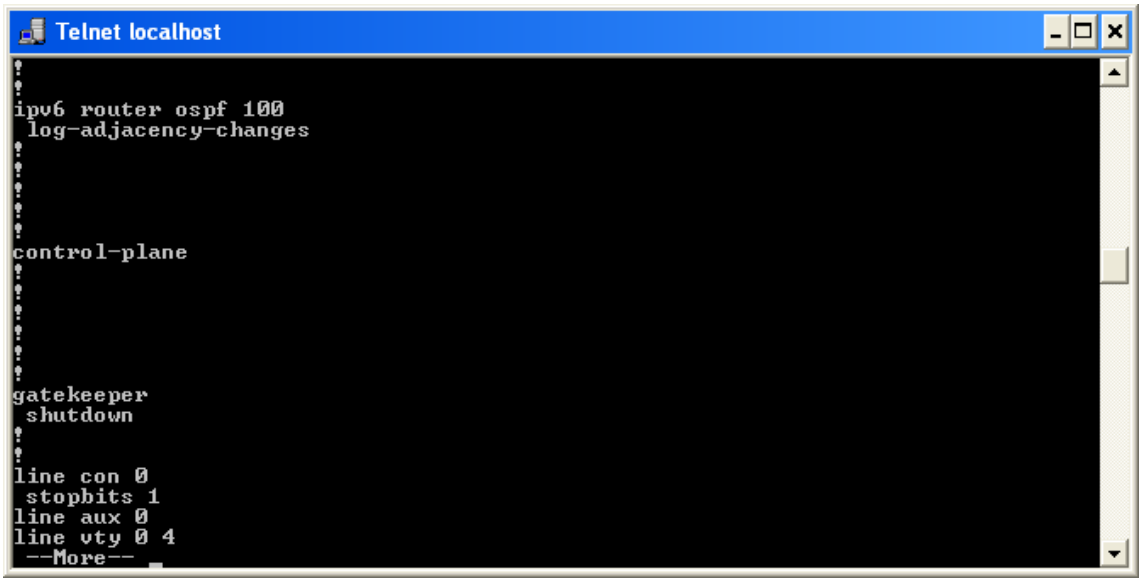
ROUTER 2


Telnet localhost
!
interface Tunnel0
 no ip address
 ipv6 address 2001:DB8:5::2/64
 ipv6 ospf 100 area 34
 tunnel source 10.1.1.10
 tunnel destination 10.1.1.9
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/0
 ip address 10.1.1.10 255.255.255.252
 duplex half
!
interface Ethernet1/1
 ip address 10.9.0.1 255.255.0.0
 duplex half
 ipv6 address 2001:DB8:3::1/64
 ipv6 ospf 100 area 0
!
interface Ethernet1/2
 no ip address

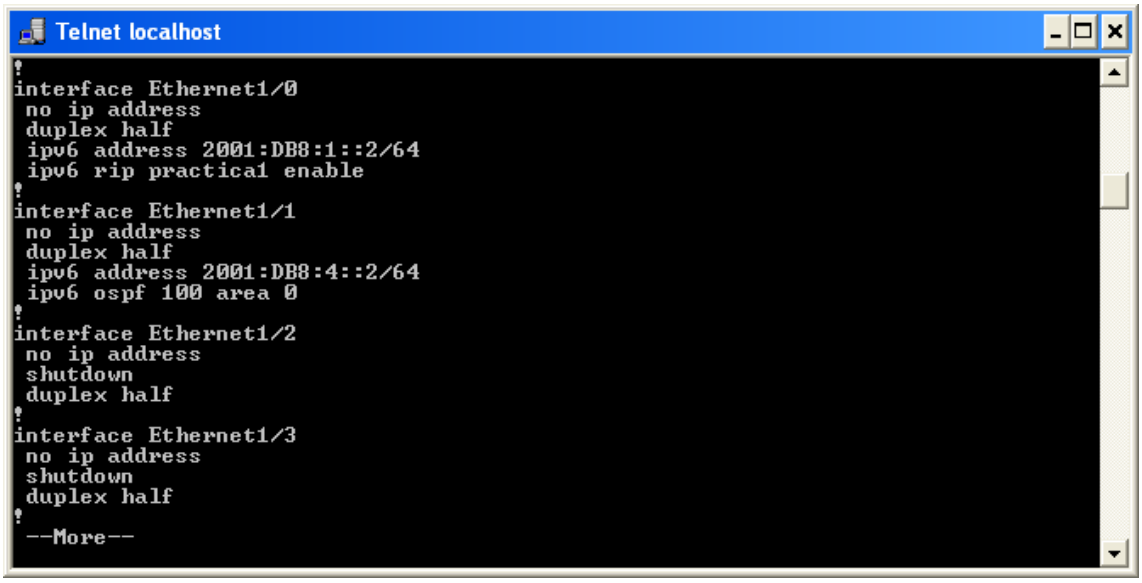

Telnet localhost
!
!
ipv6 router ospf 100
 log-adjacency-changes
!
!
!
!
!
control-plane
!
!
!
!
!
gatekeeper
 shutdown
 --More--

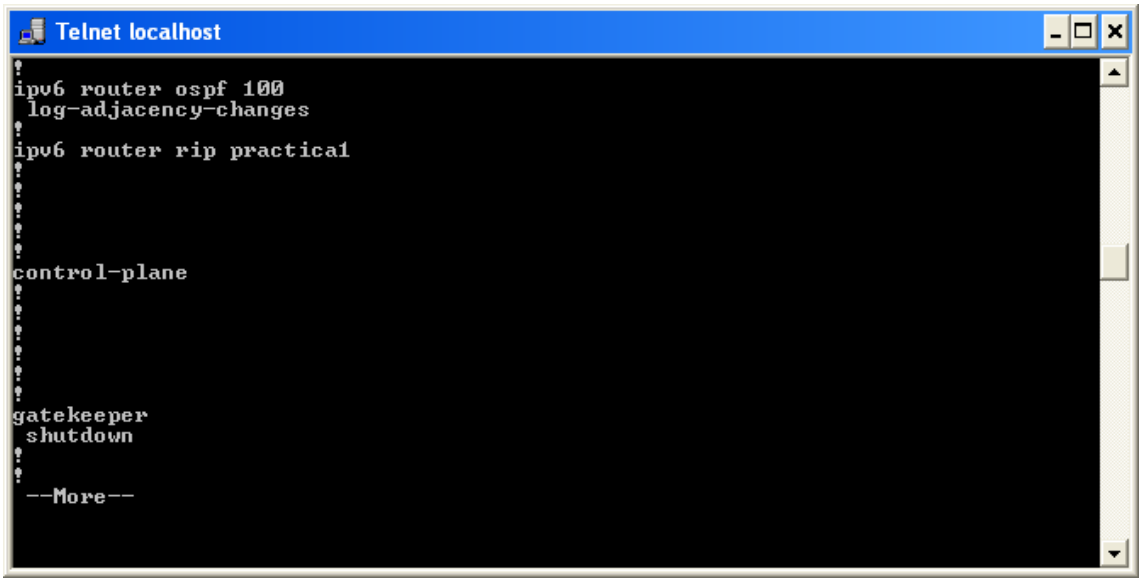
ROUTER 8


Telnet localhost
!
interface Loopback0
 ip address 6.6.6.6 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/0
 no ip address
 duplex half
 ipv6 address 2001:DB8:3::2/64
 ipv6 ospf 100 area 0
!
interface Ethernet1/1
 no ip address
 duplex half
 ipv6 address 2001:DB8:4::1/64
 ipv6 ospf 100 area 0
!
interface Ethernet1/2
 no ip address
 shutdown
 duplex half

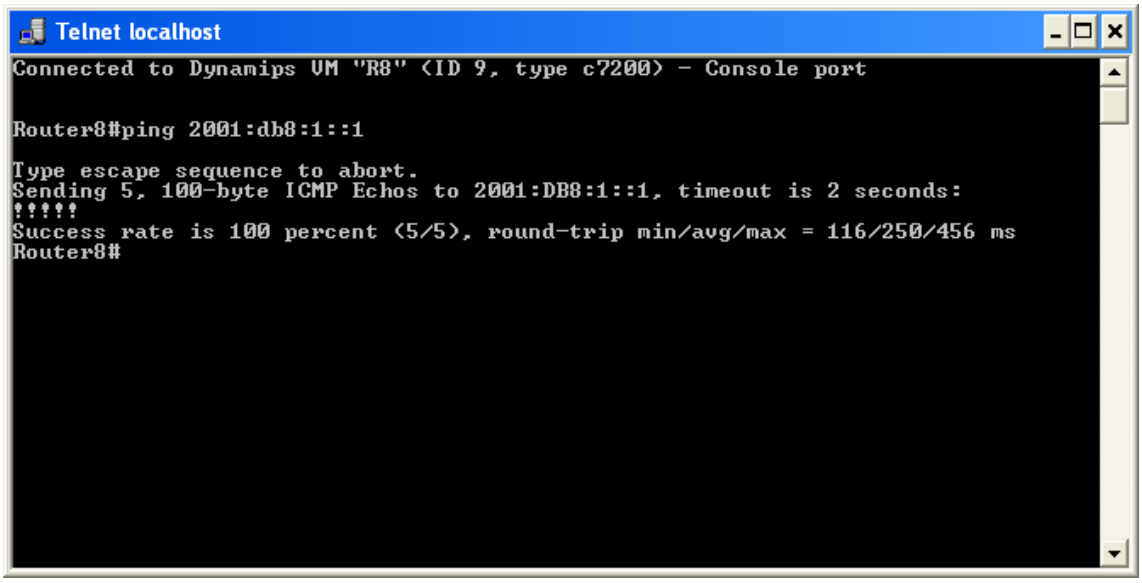

Telnet localhost
!
!
ipv6 router ospf 100
 log-adjacency-changes
!
!
!
!
!
control-plane
!
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 stopbits 1
line aux 0
line vty 0 4
 --More--

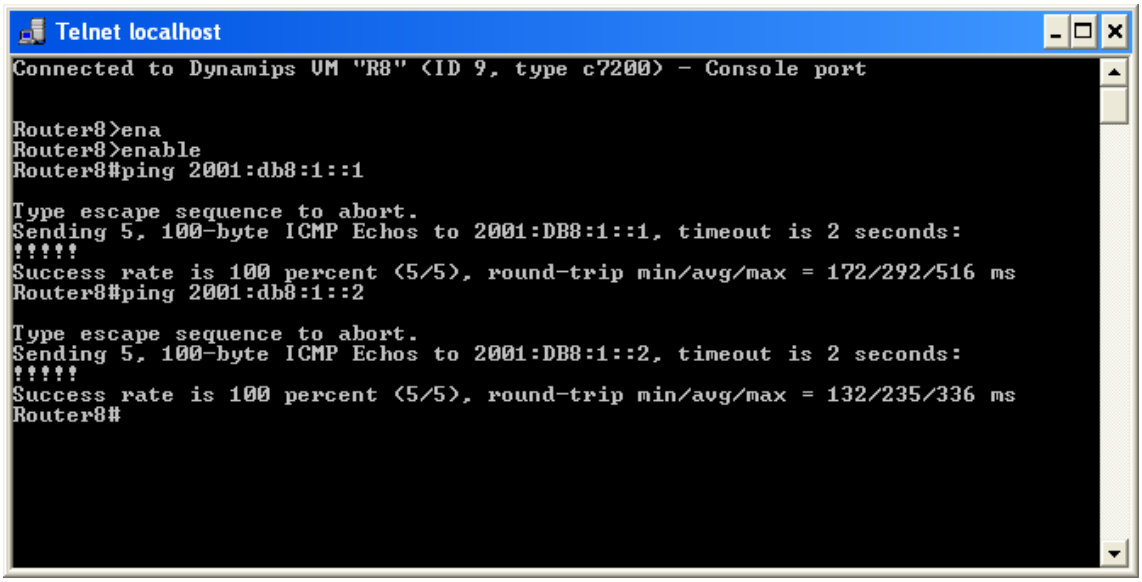
ROUTER 9


Telnet localhost
!
interface Ethernet1/0
 no ip address
 duplex half
 ipv6 address 2001:DB8:1::2/64
 ipv6 rip practica1 enable
!
interface Ethernet1/1
 no ip address
 duplex half
 ipv6 address 2001:DB8:4::2/64
 ipv6 ospf 100 area 0
!
interface Ethernet1/2
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/3
 no ip address
 shutdown
 duplex half
!
 --More--



PING ENTRE R8 QUE POSEE UN INTERFAZ CON RIP Y R9 QUE ESTA CONFIGURADO CON OSPF




Telnet localhost
Connected to Dynamips VM "R8" (ID 9, type c7200) - Console port
Router8>ena
Router8>enable
Router8#ping 2001:db8:1::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 172/292/516 ms
Router8#ping 2001:db8:1::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 132/235/336 ms
Router8#