UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

PLAN PARA IMPLEMENTAR LA TRANSICIÓN DE IPV4 A IPV6, EN LAS AULAS DE REDES DE LA UNIVERSIDAD DE QUINTANA ROO

T E S I S
PARA OBTENER EL GRADO DE

INGENIERO EN REDES

PRESENTA
BYRON AMADO SIERRA

DIRECTOR DE TESIS
M.S.I. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE

ASESORES
M.T.I. VLADIMIR VENIAMIN CABAÑAS VICTORIA
DR. JAVIER VÁZQUEZ CASTILLO
DR. JAIME SILVERIO ORTEGÓN AGUILAR
M.S.I. MELISSA BLANQUETO ESTRADA

CHETUMAL QUINTANA ROO, MÉXICO, OCTUBRE DE 2019

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

TRABAJO DE TESIS TITULADO

"PLAN PARA IMPLEMENTAR LA TRANSICIÓN DE IPV4 A IPV6, EN LAS AULAS DE REDES DE LA UNIVERSIDAD DE QUINTANA ROO"

ELABORADO POR

BYRON AMADO SIERRA

BAJO SUPERVISIÓN DEL COMITÉ DE ASESORÍA Y APROBADO COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE

INGENIERO EN REDES

COMITÉ DE TESIS

DIRECTOR _____
M.S.I. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE

ASESOR _____
M.T.I. VLADIMIR V. CABAÑAS VICTORIA

ASESOR _____
DR. JAVIER VAZQUEZ CASTILLO

ASESOR SUPLENTE _____
DR. JAIME SILVERIO ORTEGÓN AGUILAR

ASESORA SUPLENTE _____
M.S.I. MELISSA BLANQUETO ESTRADA

CHETUMAL QUINTANA ROO, MÉXICO, OCTUBRE DE 2019

Agradecimientos

A: Los Maestros de la DCI

Agradezco a todos los maestros de la DCI por ofrecer la ayuda necesaria para completar mi etapa en ingeniería en redes. Siempre estuvieron atentos a mis preguntas y estaban dispuestos a ayudar con cual quiere duda. En especial, quiero agradecer a M.S.I. Rubén González, M.T.I Vladimir Cabañas, Dr. Javier Vázquez, Dr. Jaime Ortegón y M.S.I Melissa Blanqueto Estrada. Este grupo de maestros siempre estuvieron presentes desde el principio de mi carrera y dispuestos a ayudarme.

Quiero agradecer a todos mis amigos que hice en la Universidad, especialmente a Aida Rivas, Guillermo Rivas y Miriam Rivas. Gracias por ayudar con las dudas de papeleo de migración y la Universidad.

A mi familia que siempre estuvo apoyándome y motivándome durante cada semestre. Gracias a mi madre y padre que todos los días me llamaban desde Belice y oraban por mí. A mi esposa Stephany Espat que igual que mis padres, me estuvo motivando para seguir adelante

Dedicatoria

Dedico este trabajo a mis Padres, Byron Absalon Sierra Polanco y Elubia Sierra Hernández. Siempre creyeron en mi incluso cuando yo les daba razón para no creer en mí. Nunca se dieron por vencidos y siempre me vieron graduado de una Universidad. Gracias al apoyo de ellos puedo decir que logré llegar al final de mi carrera en la Universidad de Quintana Roo.

Resumen

El proyecto se enfocará en desarrollar un plan para poder implementar una transición de IPv4 a IPv6 en las aulas de redes de la Universidad de Quintana Roo. La primera parte cubrirá la parte teórica básica y avanzada de IPv6. Otros temas que son necesarios abordar son el de direccionamiento, OSPF, EIGRP y Dual Stack.

La segunda parte se dedicará a implementar un laboratorio emulado, simulando a la topología de las Aulas. En esta parte se utilizará el software GNS3 con sus complementos, para poder emular la topología física de las Aulas. El enfoque será acercase lo más posible a un ambiente real donde el protocolo IPv6 pueda utilizarse con máquina de Linux y de Windows.

Por último, se hará pruebas con máquinas físicas usando el protocolo IPv6. Estas pruebas incluyen funciones básicas tal como una carpeta compartida sobre la red, FTP y pruebas de conectividad. Se comparan las pruebas con su versión en IPv4 y determinar si IPv6 es más rápido que Ipv4.

Índice

Índice de Ilustraciones

Índice de tablas

Glosario

EIGRP: es un protocolo de encaminamiento de vector distancia, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancia. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace. 23

Global Unicast Address : son las equivalentes a las direcciones públicas en IPv4 y son únicas a nivel global. Al igual que las direcciones públicas en IPv4 son rutables a través de internet. 18

LACNIC : El Registro de Direcciones de Internet de América Latina y Caribe es una organización no gubernamental internacional establecida en Uruguay en el año 2002. Su función es la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), Números Autónomos y Resolución Inversa para la región. 2

link local address: es una dirección IP creada únicamente para comunicaciones dentro de una subred local. 23

multicast: es un método de envío simultáneo de paquetes (a nivel de IP) que tan sólo serán recibidos por un determinado grupo de receptores, que están interesados en los mismos. ... 11

NAT: es un mecanismo utilizado por routers y equipos para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo. 4

Capítulo 1 Introducción

1.1 Introducción

La presente tesis tiene por objetivo investigar y evaluar un método de transición del protocolo IPv4 al protocolo IPv6. El motivo de esta investigación se da por el agotamiento de direccionamiento IPv4 y que proveedores de *Internet* están migrando a IPv6. El distribuidor de bloques IPv4 de América del Norte, ARIN, reportó que desde el 24 de septiembre del 2015 que ya no había direcciones disponibles. Latinoamérica tiene su distribuidor llamado LACNIC, que en este momento está repartiendo direcciones del último bloque que tiene disponible. Aunque LACNIC reporta que se ha disminuido la cantidad de solicitudes de IPv4, es estimado que para Latinoamérica ya no habrá direcciones IPv4 disponibles empezando el 18 de octubre del 2019 [1]. Por esta razón, es necesario investigar métodos de transición e implementación para en un futuro próximo poder migrar la infraestructura de la Universidad de Quintana Roo basada en IPv4 a una infraestructura que dependerá del protocolo IPv6.

La tesis se enfocará en estudiar las características, funcionamiento y rendimiento de IPv6. Se explicará la importancia de IPv6 por la falta de direcciones de IPv4 y se explorará las características básicas como la estructura y sus beneficios. Se documentará las funciones de los diferentes tipos de direcciones de IPv6, se explicará direccionamiento IPv6 y los protocolos que se usarán tales como ICMPv6, EIGRP y OSPF. Para poder medir el rendimiento, se implementarán simulaciones usando los softwares GNS3® y VMware®. Al terminar la simulación se implementará una prueba física en un ambiente controlado, donde se medirá el rendimiento en tiempo real.

1.2 Definición del problema

La Universidad en este momento cuenta con direcciones IPv4 que están repartidas en las diferentes divisiones académicas y administrativas. Para poder satisfacer las necesidades de alrededor de 1500 estudiantes, se emplean técnicas como el uso de *Network Address Translation* –NAT, para proporcionar una dirección IP a cada estudiante conectado a la red universitaria. Aunque el servicio de NAT soluciona el problema de la escasez de direcciones IP

temporalmente, para el funcionamiento de este servicio requiere que los dispositivos de redes, tal como los ruteadores o firewalls, realicen un procesamiento extra. Estos procesos extra generan como consecuencia una latencia en la red.

Por otra parte, con el incremento de estudiantes en la Universidad de Quintana Roo, también han aumentado el número de dispositivos que se conectan a la red universitaria. En estos momentos, la red de la universidad soporta la demanda de dispositivos que se quieren conectar a la red, sin embargo, no podrá ser suficiente en cuanto el *Internet* de las Cosas se popularice. En este sentido, la Universidad tendrá que proveer direccionamiento no sólo para las computadoras institucionales, sino que también para las computadoras personales (Laptops), teléfonos IP, celulares, tabletas, GPS y cualquier otro dispositivo que requiera una dirección IP. De lo anterior, podemos observar que falta planear los diversos factores involucrados para que en un futuro la universidad pueda migrar al protocolo IPv6, expandir y fortalecer su crecimiento tecnológico.

1.3 Justificación:

LANIC está cerca de agotar sus direcciones IPv4 para Latinoamérica. Con la población general creciendo y conectándose al *Internet*, las redes IPv4 actualmente implementadas, ya no podrán competir con la demanda de IP. Para en un futuro poder cumplir con la demanda de direcciones, es necesario que la Universidad implemente un plan para migrar a IPv6. Este proyecto tiene la finalidad de crear a detalle el método de transición del protocolo IPv4 al protocolo IPv6. Con IPv6 implementado, se debe incrementar el rendimiento de las redes y aumentar el número de equipos conectados. Con una dirección IPv6, la Universidad tendrá acceso a 65.356 subredes y se podrá conectar alrededor de 18 quintillones de dispositivos por subred.

1.4 Objetivos

General:

Realizar el plan para la transición de IPv4 a IPv6 que facilite migrar la red IPv4 establecida en las Aulas de Redes de la Universidad de Quintana Roo a una red IPv6 más eficiente y segura.

Específicos:

i. Investigar y documentar cambios hechos al protocolo IPv6.
ii. Investigar y escoger el mejor método de transición del protocolo IPv4 al protocolo IPv6.
iii. Diseñar un laboratorio en GNS3®, y simular los equipos que se encuentran en las Aulas de Redes.
iv. Implementar configuraciones simuladas en un ambiente físico y controlado.
v. Evaluar el desempeño de la transición en el ambiente controlado.

1.5 Metodología

La metodología que se usará en la tesis es explicativa. Se investigará sobre el protocolo IPv6 para su implementación, técnicas de migración, identificar sus beneficios, describir las ventajas y para documentar el proceso de migración del protocolo IPv4 al IPv6 en una red operando en las Aulas de Redes ubicadas en el edificio “L” de la División de Ciencias e Ingeniería de la Universidad de Quintana Roo.

Capítulo 2 Marco Teórico

2.1 Introducción al Protocolo IPv6

2.1.1 Introducción

IPv6 fue diseñado para relevar al protocolo IPv4, que está a punto de gastar sus últimos bloques de direccionamiento. En los años setenta, nadie se imaginó que el éxito del *Internet* iba a explotar una industria digitalizada y enfocada en IP (*Internet Protocol*.). Al darse cuenta de que IPv4 ya no sustentaría la demanda, un equipo de trabajo fue delegado para crear un protocolo que reemplazaría a IPv4 y que pudiera sustentar direcciones por un largo plazo. En el año 1994, el *Internet Engineering Task Force* (IETF), introdujo un conjunto de protocolos y estándares que hoy en día se conocen como *Internet Protocol* Version 6 (IPv6) [2].

Es importante conocer los cambios y los beneficios que traerá el nuevo protocolo. Organizaciones alrededor del mundo tienen que estar listas para la migración que tarde o temprano se dará.

2.1.2 Agotamiento de IPv4

IPv4 fue diseñado usando direcciones de 32-bits, que proporciona 4.26 billones de direcciones o 2^{32} direcciones [3]. Cuando primero se implementó este protocolo, sólo había 600 computadoras conectadas a *Internet*. Con la tecnología avanzando y el *Internet* llegando a todas las esquinas del mundo, hoy en día hay aproximada mente 15 billones de dispositivos conectados al *Internet*.

Para resolver el problema temporalmente, se creó una solución llamada NAT (*Network Address Translation*.). NAT permite múltiples equipos con direcciones privadas conectarse a una red pública, usando una o más direcciones públicas. Con esta solución NAT ha alargado la vida y utilidad de IPv4, pero al mismo tiempo NAT causa que los equipos realicen extra procesamiento lo que causa lentitud. Los siguientes puntos son unos de los principales problemas con NAT:

- Recálculo del Checksum- cuando se transporta segmentos con TCP se modifica el encabezado, lo que sígnica que hay que volver a recalcular el *checksum*.
- Manipulación de ICMP

- Problemas con Ipsec – Ipsec usa el encabezado de autenticación, la traducción NAT corrompe la prueba de integridad ya que el paquete es modificado.
- Quiebra el alcance de extremo a extremo. – NAT dificulta el acceso a direcciones privadas IPv4.
- Rendimiento – tener que estar traduciendo cada paquete que entra o sale causa retraso.

Otra solución que a ayudo a retrasar el agotamiento de IPv4 es *Classless* Inter-Domain Routing (CIDR). CIDR es un conjunto de estándares IP que se utiliza para crear identificadores para redes y dispositivos individuales [4]. Lo que permite CIDR es poder asignar bloques de acuerdo con las necesidades de la organización.

Con las soluciones temporáneas se ha logrado administrar bien las direcciones restantes, aunque en este momento está a punto de terminarse. América del Norte teniendo una penetración de 89% de sus 360 millones de habitantes y Asia 46% de sus 4 billones de habitantes; IPv4, incluso usando NAT, ya no puede competir en el mercado de hoy. En el 31 de enero, del 2011, IANA repartió los últimos dos bloques de IPv4, 39.0.0.0/8 y 109.0.0.0/8 a APNIC, el Registro Regional de *Internet* (RIR) de Asia. El 24 de septiembre, del 2015, ARIN el RIR de América del Norte, oficialmente se les acabo las direcciones IPv4. Actualmente, cuatro de las cinco RIR ya no tienen más direcciones IPv4 para asignar. AFRINIC, el RIR de África, es el último RIR que todavía tiene direcciones IPv4 [3].

2.1.3 Introducción de IPv6

IPv6 se introdujo mundialmente en 1994 por el IETF. El uso del *Internet* fue expandiendo drásticamente que se empezaron a agotar las direcciones de IPv4. Teniendo en mente el agotamiento de IPv4, IPv6 fue diseñado para poder sustituir y mejorar el funcionamiento protocolo IPv4.

Al observar el rápido consume de IPv4, el IETF creo un protocolo con direcciones de 128-bits llamado IPv6. Al utilizar 128-bits, IPv6 proporcionara 340 undecillón de direcciones o 2^{128} direcciones. Las organizaciones e industrias de tecnología ya están implementando IPv6 en lo que es hardware y software. IPv6 viene activado por default en los sistemas operativos más comunes como Windows, MAC OS y Linux. Con una magnitud enorme de direccionamientos,

podemos emplear todos los dispositivos que se quieran conectar y tener seguridad que habrá direcciones suficientes. Con el *Internet* de las Cosas (IoT, por sus siglas en inglés), hay varios dispositivos que utilizan una dirección IP y se estima que para al año 2020, IoT agregará alrededor de 35 billones de nuevos dispositivos.

2.1.4 ¿Por qué migrar a IPv6?

Como se ha mencionado en la sección anterior, una de las razones para hacer el cambio es que se está agotando las direcciones de IPv4. Con la conectividad de dispositivos aumentando con el tiempo, IPv4 ya no puede proveer las direcciones que son demandadas. Con el tiempo los ISP, dejarán de ofrecer direcciones IPv4 y sólo estará disponible IPv6.

Hay sitios donde la conectividad es sólo en IPv6. Por el agotamiento de IPv4, hay sitios que fueron diseñados usando el protocolo de IPv6. Aunque hay técnicas que se pueden implementar, como Dual Stack, para que un sitio pueda aceptar ambos protocolos, no es lo óptimo y normalmente es acompañado de un rendimiento degradado. Por ejemplo, si se navega la siguiente dirección http://ipv6.cybernode.com/ , no tendrá acceso si la red de donde se navega no está configurada con IPv6. Al contrario, si entramos a http://cybernode.com lograremos la conexión por IPv4.

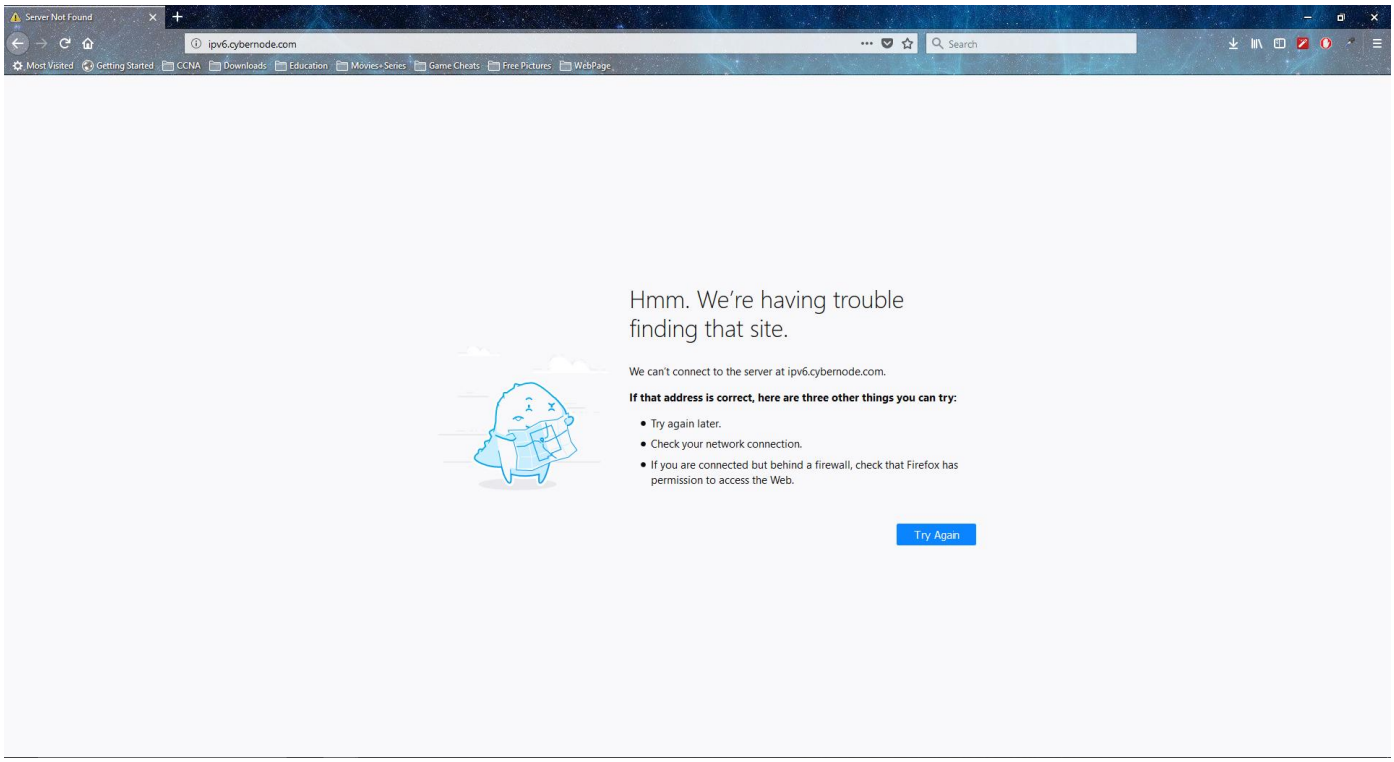
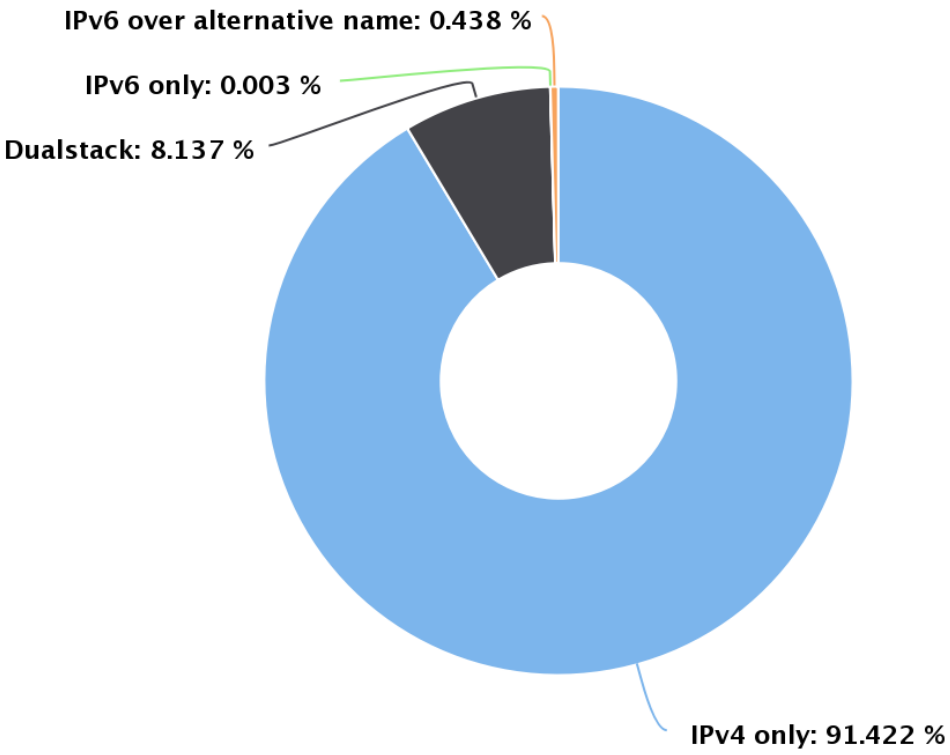


Ilustración 1: Conexión falla sin configuración IPv6

Por el momento, los sitios IPv4 todavía dominan el mercado, pero cambiará cuando se acaben las direcciones. Acuerdo con lo que publica 6lab.cz, alrededor de 8.5% de las páginas de *Internet* ya usan IPv6. Con Dual Stack teniendo 8.137%, IPv6 con nombre alternativo 0.438% y sólo IPv6 con 0.003% [5].



Gráfica 1 Protocolos en uso

2.1.5 Características de IPv6

Las características del protocolo IPv6 son las siguientes:

- Nuevo formato y encabezado – El nuevo formato ayuda a minimizar el procesamiento del encabezado en los routers. IPv6 no tiene los mismos campos que contiene el encabezado de IPv4 y eso ayuda en que se procese más rápido. Como hay diferencias significativas entre el paquete de IPv4 y IPv6, los dos protocolos no pueden intercambiar información sin ayuda de otro protocolo.
- Espacio de direcciones más grandes – En comparación con IPv4, IPv6 usa 4 veces más bits en su dirección. IPv4 usa 32 bits, mientas IPv6 usa 128 bits. Debido a que tiene un espacio más amplio y la ausencia de NAT, hay menos complejidad en la red y simplifica

los procesos. También se puede usar una dirección única para cada dispositivo en un casa u oficina.

- Auto Configuración – Para que un dispositivo obtenga su dirección usa mensajes de ICMPv6 Router Advertisement. El router IPv6 manda estos mensajes periódicamente o cuando recibe un mensaje de solicitud de un dispositivo.
- Seguridad – IPv6 por default trae incorporado el protocolo IPSec que provee seguridad y nivel de red o en la aplicación.

2.1.6 Comparación entre IPv4 y IPv6

Es importante notar que IPv6 no es sólo una extensión de IPv4, si no que IPv6 trae mejoramientos que faltaban en IPv4. En Tabla 1 se provee una comparación entre IPV4 y IPv6 con las diferencias en aplicación.

Tabla 1 IPv4 vs IPv6

Descripción	IPv4	IPv6
Dirección	32 bits (4 bytes) de largo. La dirección está compuesta de una porción de red (Network) y la otra porción de nodos (Host) y depende de la clase de direccionamiento. Hay varias clases de direccionamiento: A, B, C, D o E, dependiendo en los bits iniciales.	128 bits (16 bytes). Arquitectura básica es de 64 bits para la porción de red (Network) y 64 bits para el numero de nodos (Host). Normalmente la parte del host deriva su dirección usando la MAC de la interface.
Asignación de direcciones	Originalmente se asignaban por el tipo de clase, pero con el agotamiento de direcciones ahora se usa Classless *Inter-Domain Routing* (CIDR).	Asignación está en sus etapas principales. El IETF y la asociación de *Interactive Advertising Bureau*, AIB han recomendado que toda organización, hogar, o

Descripción	IPv4	IPv6
		entidad se le otorgue un prefijo de /48. Esto dejara 16 bits para que la organización use para sus subredes.
Vida de la dirección	Generalmente no es un concepto que aplica para IPv4, solamente si la dirección es asignada usando DHCP.	Direcciones IPv6 tiene dos vidas. Preferida y Válida, con la preferida siendo menor o igual a la válida.
Máscara de la Dirección	Usada para señalar la porción de network de la porción de host.	No se usa. Se usa Prefijo de la dirección.
Address Resolution Protocol (ARP)	ARP es usado por IPv4 para encontrar la dirección física o MAC asociada con una dirección IPv4	IPv6 empotra estas funciones dentro del protocolo IP como parte del algoritmo de SLAAC y Neighbor Discovery usando ICMPv6. No hay un ARP6.
Address Scope	Para direcciones *unicast*, este concepto no aplica.	In IPv6, el *address* scope es parte de la arquitectura. Direcciones *unicast* tiene definidas dos scopes. Incluyendo el link-local y global. *Multicast* tiene 14.
Tipos de direcciones	Las direcciones de IPv4 se categorizan en tres tipos: *Unicast address*, *multicast address* y *broadcast address*.	Las direcciones de IPv6 se categorizan en tres tipos: *Unicast address*, *multicast address* y *anycast address*.

Descripción	IPv4	IPv6
Configuración	Se tiene que configurar un nuevo sistema para que se logre comunicación, es decir que direcciones IP y rutas se tiene que asignar.	Configuración es opcional dependiendo de las funciones requeridas. Las interfaces de IPv6 se autoconfiguran usando SLAAC. Se puede configurar manualmente en la interfaz. Entonces el sistema puede comunicarse con otros sistemas IPv6 que estén en una red local o remota, dependiendo del tipo de red y si hay un router IPv6.
Domain Name System (DNS)	Aplicaciones aceptan nombres de host y después usan DNS para conseguir una dirección IP. Las aplicaciones también aceptan direcciones IP y usando DNS consiguen el nombre de host.	Tiene el mismo soporte IPv6.
Dynamic Host Configuration Protocol (DHCP)	DHCP es utilizado para obtener una dirección IP y otros tipos de configuraciones dinámicamente.	El mismo soporte llamado DHCPv6. En este caso un host no recibe una dirección de IPv6 del DHCP, pero puede conseguir otros tipos de configuraciones.
File Transfer Protocol (FTP)	FTP te permite enviar y recibir archivos atreves de redes.	Mismo soporte para IPv6
Fragmentos		Para IPv6, la fragmentación solo puede ocurrir en la

Descripción	IPv4	IPv6
	Cuando un paquete es muy grande para el enlace, puede ser fragmentado por el equipo que lo envía (Host o Router).	fuente de donde se originó y solo se rearma cuando llega al destino. El encabezado de extensión de fragmentación es utilizado.
Internet Control Message Protocol (ICMP)	Usado por IPv4 para comunicar información sobre la red.	Usado similarmente por IPv6, pero ICMPv6 provee nuevos atributos. Los nuevos atributos agregaron soporte para Neighbor Discovery y funciones que se relacionan.
Encabezado IP	Longitud variable de 20-60 bytes, dependiendo de las opciones IP presentes.	Longitud estática de 40 bytes. No hay opciones de encabezado de IP. Generalmente el encabezado de IPv6 es más simple que el de IPv4.
Opciones del Encabezado IP	Hay varias opciones que pueden acompañar a un encabezado IP (Antes de cualquier encabezado de transporte).	El encabezado de IPv6 no tiene opciones. IPv6 agrega encabezados de extensión adicionales.
Byte de protocolo de cabecera IP		El tipo de encabezado que sigue inmediatamente al encabezado IPv6. Utiliza los mismos valores que el campo de protocolo IPv4. Pero el efecto arquitectónico es permitir un rango actualmente

Descripción	IPv4	IPv6
	El código de protocolo de la capa de transporte o packet *payload*	definido de los siguientes encabezados, y se extiende fácilmente. El siguiente encabezado será un encabezado de transporte, un encabezado de extensión o ICMPv6.
IP header type of service byte	Usado por QoS y diferentes servicios para designar una clase de tráfico.	Usa diferentes códigos para asignar una clase de tráfico IPv6. Actualmente IPv6 no soporta ToS.
Conexión LAN	La conexión LAN es usada por una interface IP para llegar a una red física. Hay varios tipos por ejemplo Ethernet.	IPv6 puede ser usado por cualquier tipo de adaptador Ethernet y también tiene soporte sobre Ethernet virtual entre particiones lógicas.
Capa Dos Protocolo de Túnel (L2TP)	L2TP puede verse como PPP virtual y trabaja sobre cualquier línea soportada.	El mismo soporte para IPv6
Dirección Loopback	Una dirección loopback es una interfaz que utiliza la dirección de 127.*.*.* (Normalmente 127.0.0.1) que solo es usada por un nodo para mandar paquetes a sí mismo.	El concepto es igual que in IPv4. La dirección loopback es ::1
Maximum Transmission Unit (MTU)		IPv6 tienen un límite más bajo en su MTU con 1280 bytes. IPv6 no fragmenta paquetes

Descripción	IPv4	IPv6
	El Maximum Transmission Unit de un enlace es el número máximo de bytes que un enlace particular, como ethernet o modem puede soportar.	que estén bajo el límite. Para mandar IPv6 sobre un enlace con un MTU menor a 1280 bytes, la capa de enlace debe de fragmentar transparentemente y desfragmentar los paquetes IPv6.
Netstat	Netstat es una herramienta que se usa para observar el estatus de conexiones TCP/IP, interfaces o rutas.	Mismo soporte con IPv6
PING	Ping es una herramienta básica TCP/IP para poder probar conectividad.	Mismo soporte con IPv6
Puertos	TCP y UDP tienen espacios de puertos separados, cada uno identificado por un numero entre el rango 1-65535.	Para IPv6, los puertos trabajan de la misma manera que IPv4. Porque estos están en una familia nueva de direcciones, ahora hay cuatro espacios separados.
Quality of Service (QoS)	Quality of Service te permite pedir prioridad para los paquetes y ancho de banda para aplicaciones TCP/IP.	Mismo soporte con IPv6
Renumeración	Renumeración es hecha reconfigurando manualmente, con la posible	Renumeración es un elemento de diseño importante de IPv6 y es

Descripción	IPv4	IPv6
	excepción de DHCP. Generalmente, para un sitio u organización, remuneración tiene dificultad y es un proceso tedioso. Hay que evitar cuando sea posible.	automático, especialmente en el prefijo /48.
Simple Network Management Protocol (SNMP)	SNMP es un protocolo para administrar un sistema.	Mismo soporte con IPv6
Telnet	Telnet te permite acceder remotamente a un equipo	Mismo soporte con IPv6
Trace Route	Trace Route es una herramienta básica de TCP/IP para determinar el camino del paquete.	Mismo soporte con IPv6
Virtual Private Network (VPN)	VPN te permite extender seguramente una red privada sobre una red pública.	Mismo soporte con IPv6

2.2 Estructura y Direccionamiento de IPv6

2.2.1 Encabezado IPv6

El encabezado de IPv6, tomó varios conceptos de los que ya estaban definidos para IPv4. Para poder simplificar el procesamiento, algunos elementos que se encuentran en IPv4, ya no están en IPv6. En los siguientes puntos se explicará los campos de IPv6.

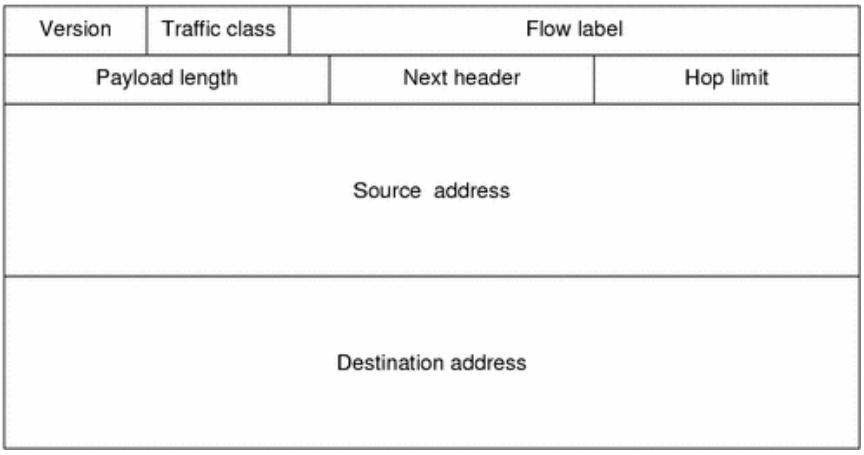


Ilustración 2: Encabezado IPv6(docs.oracle.com [6])

- ***Version –*** Es el primer campo de IPv6 que contiene el número de versión del encabezado de *Internet* Protocol. Este campo simplemente denota la versión de IP que está en uso. Si es IPv4, usa un número 4 y si es IPv6 usa el número 6. Este campo es de 4-bits.
- ***Traffic Class –*** Este campo es para especificar qué tipo de tratamiento recibirá un paquete por parte de los routers, lo que ayuda a brindar un poco de calidad de servicio (QoS). El IETF mejoró este campo usando una técnica llamada Differentiated Services (DS). IPv6 usa 6 bits para el DSCP (Differenciated Service Code Point) que permite 64 posibles marcas. Esto provee mucha más granularidad en selección de prioridades que la versión de IPv4 que sólo usa 3 bits.
- ***Flow Label –*** Este es un campo nuevo que se utiliza para etiquetar una secuencia o flujo de paquetes IPv6 enviados desde un origen a uno o más destinos. El campo ayuda a organizar los paquetes dándoles un número de identificación para que se pueda reconocer paquetes del mismo flujo. Esto asegura que cada paquete recibirá el mismo trato en los routers IPv6. Un Flow Label con 0 significa que el tráfico no está asociado con ningún flujo.
- ***Payload Length –*** Este campo es de 16-bits que indica la longitud en bytes de sólo la carga que sigue al encabezado principal de IPv6, en otras palabras, la porción de datos de un paquete. El campo no incluye el encabezado principal de IPv6. Si hay extensiones son incluidas en el número de bytes contenidas en el campo de *Payload* length.

- **Next Header -** El campo especifica los tipos de encabezados que es esperado después del encabezado principal de IPv6.
- **Hop Limit –** Este campo se asegura que los paquetes no transiten en las redes por un tiempo indefinido. El campo disminuye por 1 cada vez que un router recibe un paquete IPv6. Cuando llega a 0 el paquete es descartado y un mensaje ICMPv6 Time Exceeded (Tiempo Excedido) es enviado de regreso al origen del paquete.
- **Source and Destination *Address* (origen y destino)-** El primer campo es el de origen, es de donde surge el paquete. La dirección origen siempre será una dirección *unicast*, puede ser una link-local, unique local o un unspecified. El segundo campo es el campo destino, donde se dirige el paquete o recipiente. Estas direcciones pueden ser *unicast multicast* o *anycast*. Los routers usan este campo para poder enviar el paquete en el camino correcto.

2.2.2 *Unicast, Multicast y Anycast*

Hay tres categorías de direcciones IPv6. *Unicast* para una interfaz, *multicast* para un conjunto de interfaces en una red, un paquete es enviado a todas las interfaces asociadas con esta dirección. Por último, *anycast* que es una dirección que identifica a una o más interfaces [7].

Una interfaz es identificada por una dirección *unicast*. Cuando un dispositivo en una red envía un paquete a una dirección *unicast*, ese paquete es entregado específicamente a esa interface identificada por la dirección *unicast*. Entonces el propósito de una *unicast* es que haya comunicación entre un dispositivo con otro dispositivo. Cuando se implementa una red IPv6 las siguientes direcciones *unicast* pueden ser utilizadas:

- Global *Unicast Address* – es una dirección IPv6 única que se le asigna a la interfaz de un dispositivo conectado a una red. Estas direcciones tienen un alcance global y tiene el mismo propósito que una dirección pública en IPv4. Las direcciones se pueden conmutar o enrutar sobre el *Internet*.
- Link-local IPv6 *Address* – Estas direcciones permiten que dispositivos dentro de la misma red local se puedan comunicar. Link-local tiene un alcance local y no pueden ser enrutados fuera de la red local. Se identifican con el prefijo FE80::/10.

- Loopback IPv6 *Address*- Tiene el mismo funcionamiento que el loopback de IPv4. Las direcciones Loopback IPv6 es representa como 0:0:0:0:0:0:0:1 o puede ser escrita como ::1/128.
- Unspecified *Address* – es representada como ::/128.

Una dirección *Multicast* identifica a un conjunto de interfaces normalmente localizadas en diferentes nodos. Cuando un dispositivo de la red manda un paquete con una dirección *multicast*, el dispositivo se lo manda a todas las interfaces que se identifican con esa dirección. IPv6 no soporta *broadcast*, en su lugar, utiliza las direcciones *multicast* para mandar los paquetes.

Las direcciones *multicast* soportan hasta 16 diferentes tipos de alcances, incluyendo nodos, enlaces, sitios, organizaciones y alcances globales. Un campo de 4-bits en el prefijo identifica a estas direcciones, usan el prefijo FF00::/8. Los siguientes tipos de direcciones *multicast* se puede utilizar en una red:

- Solicited-node *Multicast Address*- Mensajes de Neighbor Discovery (ND) son enviados con esta dirección, ff02:0:0:0:0:1:ff00::/104.
- All-nodes *Multicast Address* – Mensajes de Router Advertisement (RA) son mensajes no solicitados envidos perdiódicamente a la dirección FF02::1.
- All-routers *Multicast Address* -Mensajes de Router Solicitation (RS) son enviados por el host con IPv6 para descubrir la presencia de routers con IPv6 en el enlace a la siguiente dirección FF02::2.

Una dirección *anycast* identifica a un conjunto de interfaces que normalmente pertenecen a diferentes nodos. Las *anycast* son similar a los *multicast*, excepto que los paquetes son enviados a solo una interfaz y no a todas las interfaces. El protocolo de enrutamiento normalmente calcula que interfaz física está localizada a una distancia mínima, dentro del conjunto de interfaces. Cuando se identifica la más cercana el paquete es enviado a esa interfaz y no a las demás.

2.2.3 Global *Unicast Address*

Las direcciones Global *Unicast* son direcciones enrutables y alcanzables globalmente por el *Internet* IPv6. Son el equivalente a las direcciones públicas de IPv4. Las direcciones actualmente son asignadas por el *Internet* Assigned Numbers Authority (IANA) y comienzan con el valor binario de 001 o el prefijo de 2000::/3. Esto resulta en un rango de direcciones de 2000::/3 hasta 3FFF::/16 [8]. Las direcciones pueden ser configuradas manualmente, usando SLAAC o por DHCP. Como se puede apreciar en la ilustración 3, el Global *Unicast Address* está compuesto por tres partes, el *global routing prefix, subnet ID* y la *interface ID.*

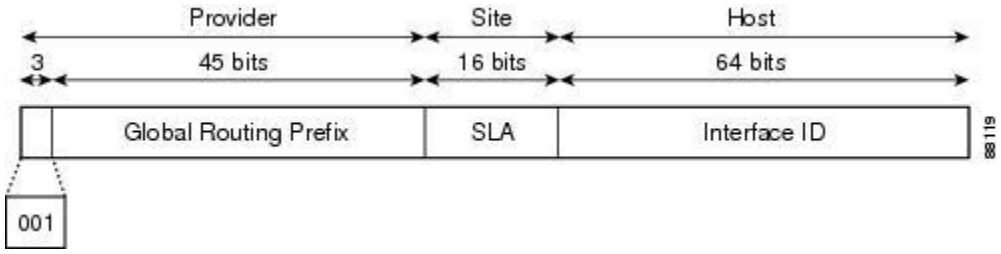


Ilustración 3: Estructura de una Global Unicast Address (cisco.com [9])

El global routing prefix es el prefijo o la sección de red de una dirección que es asignada por un proveedor de *Internet* (ISP). El American Registry for *Internet* Numbers (ARIN) tiene la política de que cada sitio, no importando el tamaño, tiene que recibir al menos un global routing prefix de 48 bits [9]. Los primeros tres bits del routing prefix son reservados, 001, seguidos de 45 bits asignados por el ISP. La reservación de los primeros 3 bits le dan un rango de 2000 a 3FFF a las direcciones *global unicast address*.

Usando los primeros 48 bits de los 128 bits, los siguientes 16 bits son para el Subnet ID. Con un global routing prefix de /48 con una Interface ID de 64-bits resulta un Subnet ID de 16 bits. Esto permite 65.536 subredes. El Prefix Length (Longitud del prefijo) es la longitud total del prefijo de la dirección que incluye el Global Routing Prefix y el Subnet ID.

El Interface ID identifica a una interface en una subred. Es recomendado en la mayoría de los casos que se use un Interface ID de 64-bits para todas las LANs y otras redes, incluyendo conexiones point-to-point. Teniendo una Interface ID de 64-bits en los usuarios de una red, facilita el uso de SLAAC que utiliza 64-bits para automáticamente crear una Interface ID. Otra

razón es que facilita el proceso de subneteo. Con 64-bits tenemos accesos cerca de 18 quintillones de direcciones por subred (18,446,744,073,709,551,616).

Consideremos la siguiente dirección 21DA:D3::/48 que es un routing prefix, tenemos los primeros tres bits reservados más los 45 restantes. Para darle un Subnet ID, hay que darle valores en la cuarta parte de la dirección, serían los 48-bits más 16-bits de la Subnet ID para completar 64-bits. La dirección sería como la siguiente 21DA:D3:0:2F3B::/64, con 2F3B siendo la parte del Subnet ID.

2.2.4 Link-Local *Unicast Address*

Una dirección link-local está diseñada para uso en un solo enlace y no deben de ser enrutadas. Estas direcciones no dependen de un prefijo global y se puede autoconfigurar. Las link-local se usan normalmente para mecanismos de autoconfiguración, para detectar a vecinos y para crear redes locales y temporales donde no hay routers presentes [10].

Teniendo la capacidad de autoconfigurarse le da muchas ventajas a IPv6 que IPv4 no tenía. Por ejemplo, un dispositivo puede auto asignarse una dirección al encender sin depender de un servidor DHCPv6. Esta dirección puede usarse para comunicación con otros dispositivos incluso con un router o servidor DHCPv6 para obtener una dirección global *unicast*. Esta opción facilitaría la conexión de impresoras, sistemas de entretenimiento o dispositivos del *Internet* de las Cosas.

Las direcciones link-local son representadas por el prefijo de FE80::/10 y los últimos 64 bit son usados como la interface ID. Usando el prefijo de FE80::/10 se obtiene un rango de FE80::/10 hasta el FEBF::/10. Aunque hay varias direcciones en los rangos, es recomendable usar el rango FE80::/10 para no causar problemas potenciales en ciertos sistemas operativos.

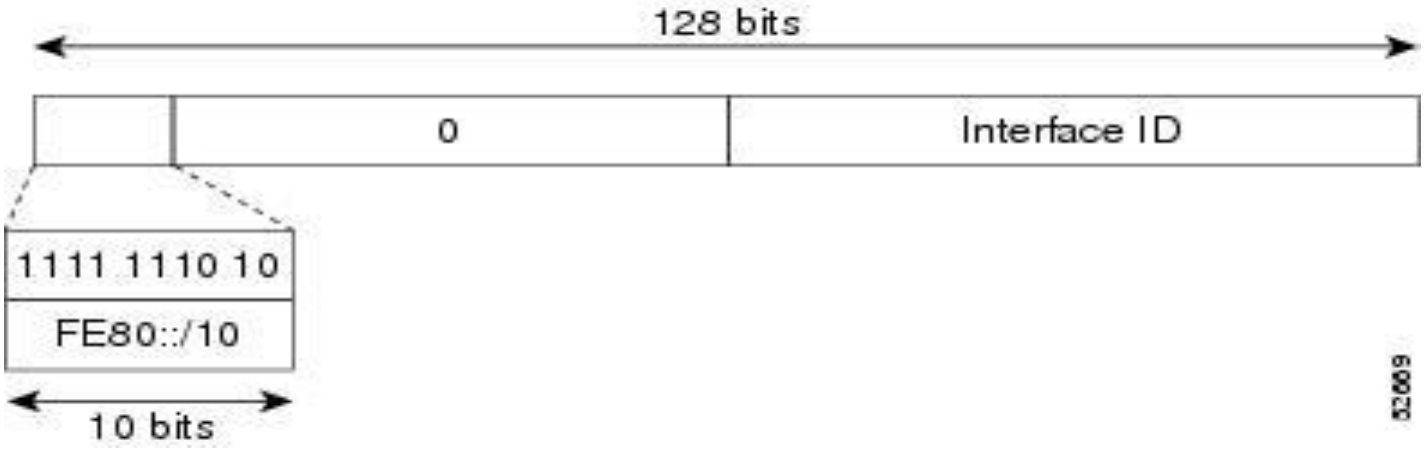


Ilustración 4: Estructura de Link-Local Address

Hay dos formas de configurar una dirección link-local, automática o manualmente. Los sistemas operativos como Windows y Linux vienen configurados para IPv6 por default, lo que les permite configurar automáticamente la dirección. El prefijo normalmente es FE80::/64 seguido de una interface ID de 64-bits generada por una de las siguientes dos maneras:

- EUI-64: usado por cisco IOS, MAC OS X y Linux.
- Generado Aleatoriamente: usado por Windows.

Extended Unique Identifier o EUI-64, toma la dirección MAC de una interfaz y la modifica para luego poder adherírsela a los 64-bits principales. La modificación es la inserción de un valor de 16-bits, FFFE, entre el OUI y el identificador de dispositivo de una MAC. Al insertar estos bits, el bit universal es volteado. Este proceso se puede lograr en tres pasos:

- Primer Paso - Convertir la dirección MAC a números binarios. Después partir la MAC en dos con el OUI de 24-bits en el lado izquierdo y el Identificador de 24-bits al lado derecho.
- Segundo Paso – insertar FFFE de 16-bits, 1111 1111 1111 1110, entre el OUI y el Identificador. FFFE es un valor reservado que indica que se ha usado EUI-64 para generar la dirección.
- Tercer Paso – voltear el séptimo bit llamado Universal/Local (U/L).

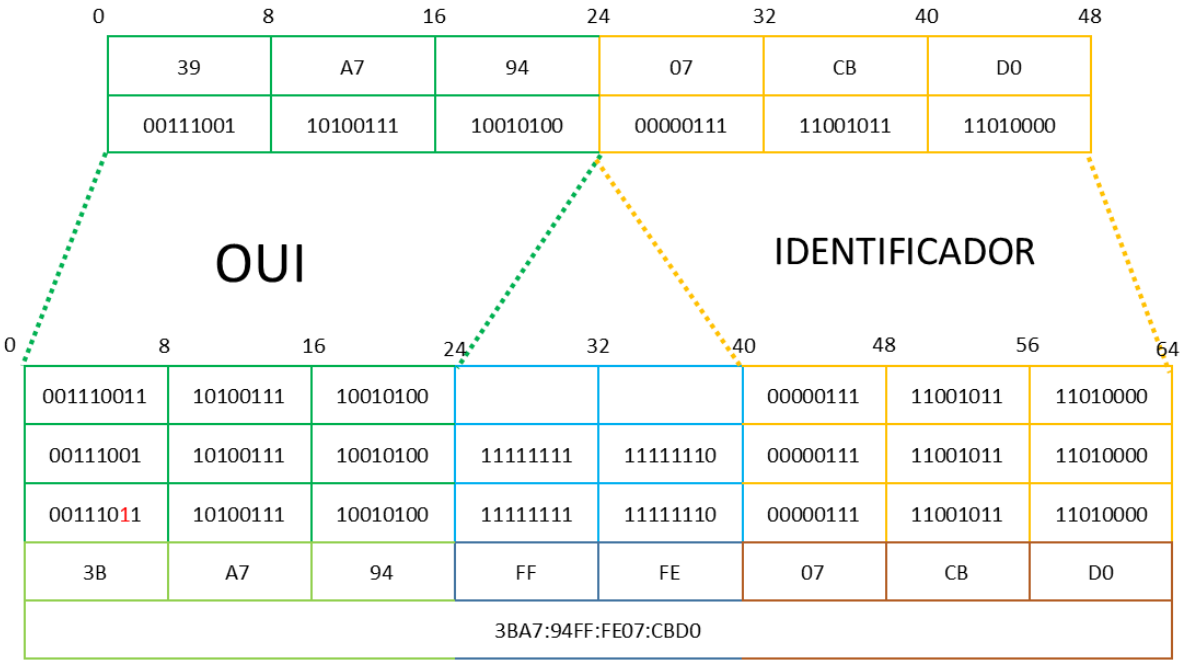


Ilustración 5: Proceso de EUI-64

2.2.5 *Multicast Address*

Una dirección *multicast*, es una dirección que manda un paquete a varios recipientes, al contrario, a un *unicast* que sólo se lo manda un recipiente. En IPv6 las direcciones *multicast* tiene un prefijo de ff00::/8, que se le denomina como el grupo *multicast* o *Multicast Group* y es el equivalente al 224.0.0.0/24 de las direcciones IPv4. Una dirección *multicast* sólo puede ser una dirección de destino y nunca una dirección de fuente.

Para mejorar el rendimiento los paquetes de *multicast* tienen un campo llamado Scope, que ayuda al router a determinar el enfoque en que tiene que propagar los paquetes de *multicast*. Con este mecanismo implementado, el router puede prevenir que paquetes sean entregados en el área correcta.

Hay direcciones mulitcast que son bien conocidas y están predefinidas y reservadas para el uso de grupos *multicast*. Estas direcciones tiene el prefijo de ff00::/12. Estas direcciones son utilizadas para operaciones de descubrimiento de routers o para protocolos de enrutamiento. A continuación, una lista de los más comunes [3]:

- FF02::1 - Todos los Nodos
- FF02::2 – Todos los routers
- FF02::5 – Routers OSPF
- FF02::a – Routers EIGRP

IPv6 no tiene direcciones *broadcast*, pero utiliza direcciones como FF02::2, todos los routers, que tiene un efecto similar.

Otro tipo de *multicast address* son las Solicited-Node *multicast*. Estas direcciones son creadas automáticamente y asignadas a una interfaz para cada global *unicast*, unique local *address*, y link local *address* que se encuentran en esa interfaz. Las solicited-node *multicast* son utilizadas localmente en la capa 2 por el protocolo Neighbor Discovery Protocol (NDP). NDP utiliza direcciones *multicast* para poder descubrir direcciones link-local que pudieran estar en la red local.

2.3 Direccionamiento Dinámico

IPv6 es configurable manualmente, pero tiene cierta dificultada por el tamaño de las direcciones. Al igual que IPv4, IPv6 está diseñado para poder proporcionar automáticamente una dirección, usando métodos dinámicos de direccionamiento. En esta parte se describirá los tres métodos que dispositivos pueden utilizar para conseguir sus direcciones. Los métodos son:

1. Stateless *Address* Autoconfiguration (SLAAC)
2. SLAAC y un Stateless DHCPv6
3. Stateful DHCPv6

Para poder hacer cualquier tipo de direccionamiento, los dispositivos de la red deben de mandar mensajes solicitando una dirección o anunciar que hay direcciones disponibles. Estos mensajes son llamados Router Advertisement (RA) o Router Solicitation(RS). Los mensajes fueron diseñados para la comunicación entre los router y dispositivos localizados en una red local.

Router Advertisement se originan de los routers para anunciar que están presente en la red local y para ofrecer parámetros para direccionamiento. Estos parámetros pueden incluir el prefijo, el tamaño del prefijo, el gateway y el Maximum Transmission Unit (MTU). Los routers mandan los RS usando la dirección *multicast* predeterminada FF02::1, todos los nodos IPv6.

Hay que notar que los mensajes RA se pueden mandar como *multicast* o se puede mandar como *unicast* sólo cuando el router responde a un mensaje de RS [11]. Cisco por default, manda los mensajes cada 200 segundos.

Router Solicitation son mensajes originados de dispositivos que son configurados a obtener su direccionamiento automáticamente. Los dispositivos tienen una dirección *multicast*, FF02::2 que utilizan para descubrir cualquier router que esté disponible en la red loca.

Paro poder visualizar mejor el proceso a continuación se darán los pasos que estos mensajes toman para solicitar o anunciar parámetros.

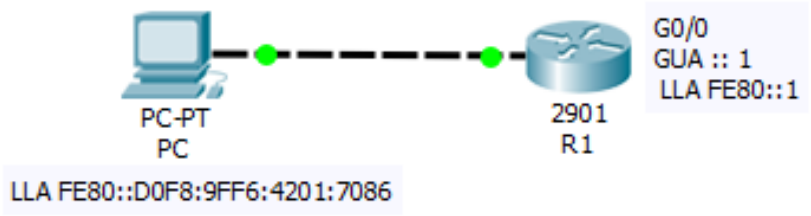


Ilustración 6 Mensajes RS y RA

1. **Primer Paso**: La computadora, denominada PC, está configurada para obtener su dirección automáticamente. Desde que se encendió, no ha recibido oferta, Router Advertisement, de un router y al pasar el tiempo manda una solicitud a la dirección FF02::2, todos los routers. Este mensaje es para informar a cualquier router que la computadora necesita un mensaje RA. El mensaje RS esta encapsulado en un paquete IPv6 y su contenido es el siguiente:
    - Dirección de la fuente - fe80::d0f8:9ff6:4201:7086
    - Dirección destino – FF02::2
2. **Segundo Paso**: El router recibe el mensaje RS de la computadora y responde con un RA. El mensaje RA le sugiere a la PC como pude crear su dirección *unicast* global y le provisiona otros tipos de parámetros. El prefijo y el tamaño del prefijo están incluidos en le mensaje RA. El Gateway por default es la dirección del interfaz del router, fe80::1. El mensaje incluye lo siguiente:
    - Dirección fuente: FE80::1

- Dirección destino: FF02::1
- Método Sugerido:
    i. SLAAC
    ii. SLAAC con Stateless DHCPv6
    iii. Stateful DHCPv6

Para que los métodos dinámicos puedan funcionar, el router manda cierto tipo de bandera en el mensaje de RA. Estas banderas (Flags) se configuran en la interfaz y son mandadas a los dispositivos para poder sugerirles los tres tipos de direccionamiento que pueden utilizar. Las banderas de dominan por las letras M, O y A. Los siguientes pasos se explican las tres banderas.

1. Managed *Address* Configuration Flag (Bandera M): La bandera M representa configuraciones de direcciones administradas y le avisa al dispositivo que recibe el RA, que hay un servidor de DHCPv6 en la red y que debe de mandar una solicitud para conseguir todos sus parámetros con el servidor. En este caso toda la información necesaria para la configuración es proveída por un servidos DHCPv6. [12]. La única información que el dispositivo utiliza del mensaje RA es la dirección origen que se utiliza para la dirección Gateway.
2. Other Configuration Flag (Bandera O): La bandera O representa otra configuración, y le avisa al dispositivo recibiendo el mensaje RA que debe de utilizar un servidor DHCPv6 para conseguir otras configuraciones como la dirección del servidor DNS. El servidor DHCPv6 debe de ser un servidor stateless. [12]
3. *Address* Autoconfiguration Flag (Bandera A): la bandera A le avisa al dispositivo que debe de usar SLAAC para crear su dirección. Dependiendo del sistema operativo, se utilizará EUI-64 o Random 64 bit para procesar la dirección. [12]

Dependiendo de la opción seleccionada, se utiliza un servidor stateless o stateful. Un servidor stateful asigna una dirección única global a los clientes y mantiene información del estado, un registro de que cliente esta utilizando que dirección. Un servidor stateless no provee la dirección global única, solo provee información como la dirección del servidor DNS o el nombre de dominio.

La siguiente table muestra que bit deben de estar encendidos para que los métodos funcionen.

Metodo RA	Bandera A	Bandera B (Stateless)	Bandera M (Stateful)
SLAAC	1	0	0
SLAAC con DHCPv6 Stateless	0	1	0
DHCPv6 Stateful	0	0	1

Tabla 2 Métodos Dinámicos y Banderas RA

2.3.1 SLAAC

El método SLAAC es el que viene por default en los routers de cisco. SLAAC provee la habilidad de darle una dirección a un dispositivo basado en el prefijo de la red que un router anuncia usando los mensajes RA Los mensajes Router Advertisement son mandados periódicamente y incluyen la siguiente información:

- Uno o más prefijo IPv6
- Información del tiempo de vida de un prefijo
- Información sobre las banderas
- Información default del dispositivo

SLAAC es implementado cuando el dispositivo escucha para mensajes RA y toma el prefijo que se está anunciando para poder formar una dirección única que se puede utilizar en la red. Para que este proceso trabaje, el router debe de anunciar un prefijo de 64 bits, SLAAC dinámica creara la parte correspondiente que identificara al dispositivo. A continuación, se mostrará paso por paso como SLAAC funciona.

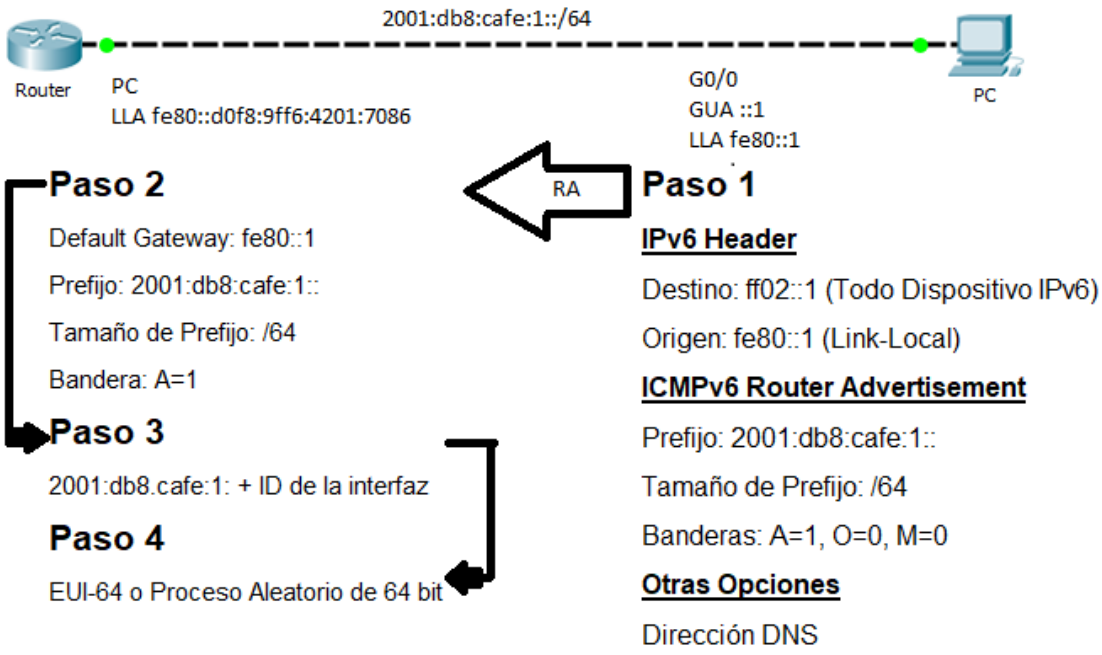


Ilustración 7 SLAAC mensaje RA

1. **Paso 1:** El mensaje Router Advertisement es encapsulado in un encabezado de IPv6 dirigido hacia la dirección multicas de todos los dispositivos IPv6, FF02::1. EL link-local configurado en R1, es la dirección de origen que se le asigna al encabezado, Esta dirección puede ser configurada automática o manualmente, es recomendado en estos casos configurar la interfaz manualmente. El link-local también es la dirección que los dispositivos usaran como su Gateway. El mensaje incluye el prefijo que se usara en esa red local y el tamaño del prefijo. Como se está utilizando SLAAC, la bandera A esta encendida y las otras dos apagadas. Se puede configurar otras opciones tal como la dirección del servidos DNS.
2. **Paso 2:** La PC recibe el mensaje RA y usa la dirección origen fe80::1, como su Gateway. Al recibir el mensaje la PC lee el bit de la bandera y reconoce que sus configuraciones se obtendrán por el proceso SLAAC.
3. **Paso 3:** La PC usa el prefijo 2001:DB8:CAFE:1: del RA como su prefijo para configurar su dirección global.
4. **Paso 4:** Para poder completar el proceso, la PC puede usar EUI-64 o un valor aleatorio de 64-bits.

2.3.2 SLAAC Con Stateless DHCPv6

Este método combina el método SLAAC con un Stateless Server. La primera parte ya se discutió y se sabe que un dispositivo autoconfigura su dirección global. En este caso el dispositivo vuelve a usar el método SLAAC y usa el servidor para obtener otras configuraciones. Un Stateless Server es un servidor que no provee direcciones globales. El servidor solo da información básica de la red que esta disponibles a todos los dispositivos conectados, tal como DNS o un dominio. A continuación, veremos el proceso que un dispositivo pasa para obtener una dirección utilizando este método.

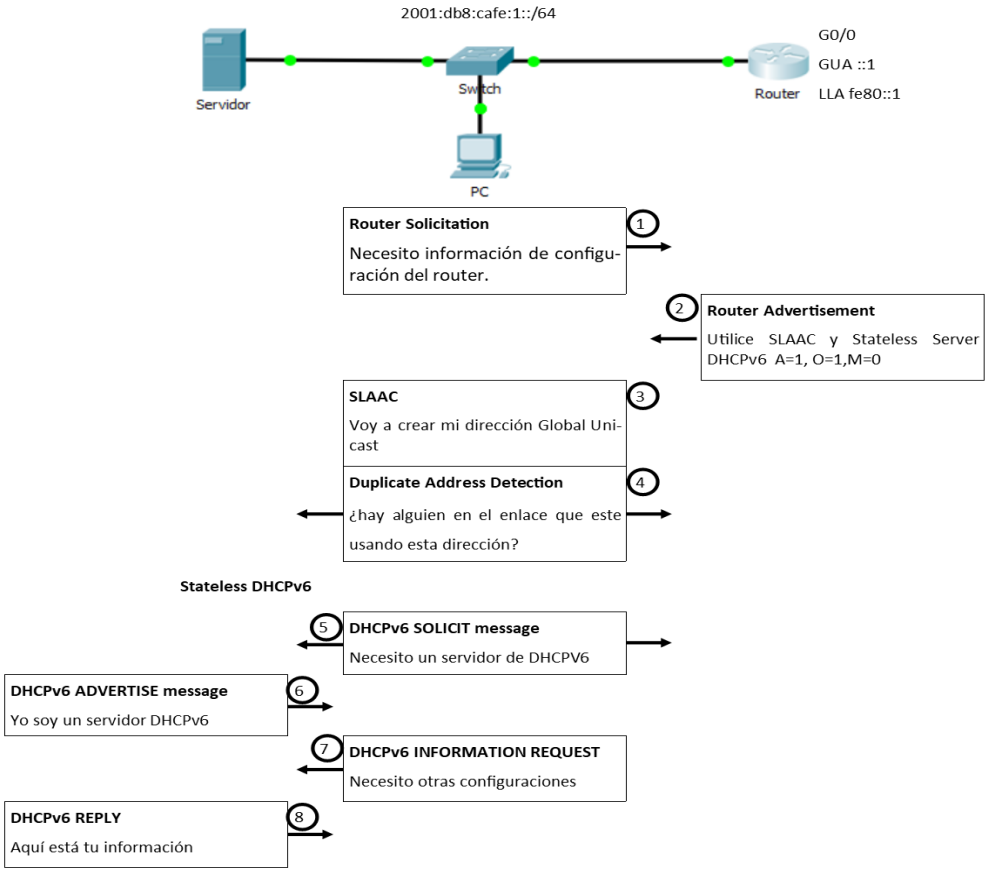


Ilustración 8 SLAAC con Stateless DHCPv6

1. **Paso 1:** La PC manda un mensaje Router Solicitation, no lo manda si ya ha recibido un mensaje de Router Advertisement del router.

2. **Paso 2:** El mensaje RA del router es mandado con la bandera A y O encendida y la bandera M apagada. Esta configuración le sugiere a la PC que genere su dirección global dinámicamente pero que cualquier otro tipo de dirección, debe de buscar a un servidor.
3. **Paso 3:** Al recibir el RA, la PC usa la dirección de origen del RA como su Gateway, fe80::1. Porque el paquete está configurado con la bandera A=1 la PC entiende que tiene que configurar su dirección global usando SLAAC.
4. **Paso 4:** Para asegurar que no hay otra dirección idintica en la red, la PC realiza un proceso llamado Duplicate *Address* Detection.
5. **Paso 5:** Porque la bandera O esta encendida, la PC entiende que cualquier otra información la debe de obtener de un servidor. La PC manda un mensaje DHCPv6 SOLICIT (Solicitud) a la dirección ff02::1:2, todos los servidores de DHCPv6.
6. **Paso 6:** Uno o más servidores pueden responder con un mensaje DHCPv6 ADVERTISE, indicando que están disponibles para dar el servicio.
7. **Paso 7:** La PC responde al servidor escogido con un mensaje INFORMATION REQUEST, solicitando otras configuraciones adicionales.
8. **Paso 8:** El servidor DHCPv6 responde con un mensaje REPLY conteniendo las otras configuraciones deseadas.

2.3.3 Stateful DHCPv6

El tercer método es el Stateful DHCPv6. Este método es similar al de IPv4, ya que provee una dirección única global y mantiene en récord de las IP’s asignadas. El proceso no involucra SLAAC para asignar direcciones. Lo único que tiene en común con las otras dos opciones, es que el default Gateway es proporcionada por el router. A continuación, se mostrará el proceso entre un dispositivo y el servidor DHCPv6

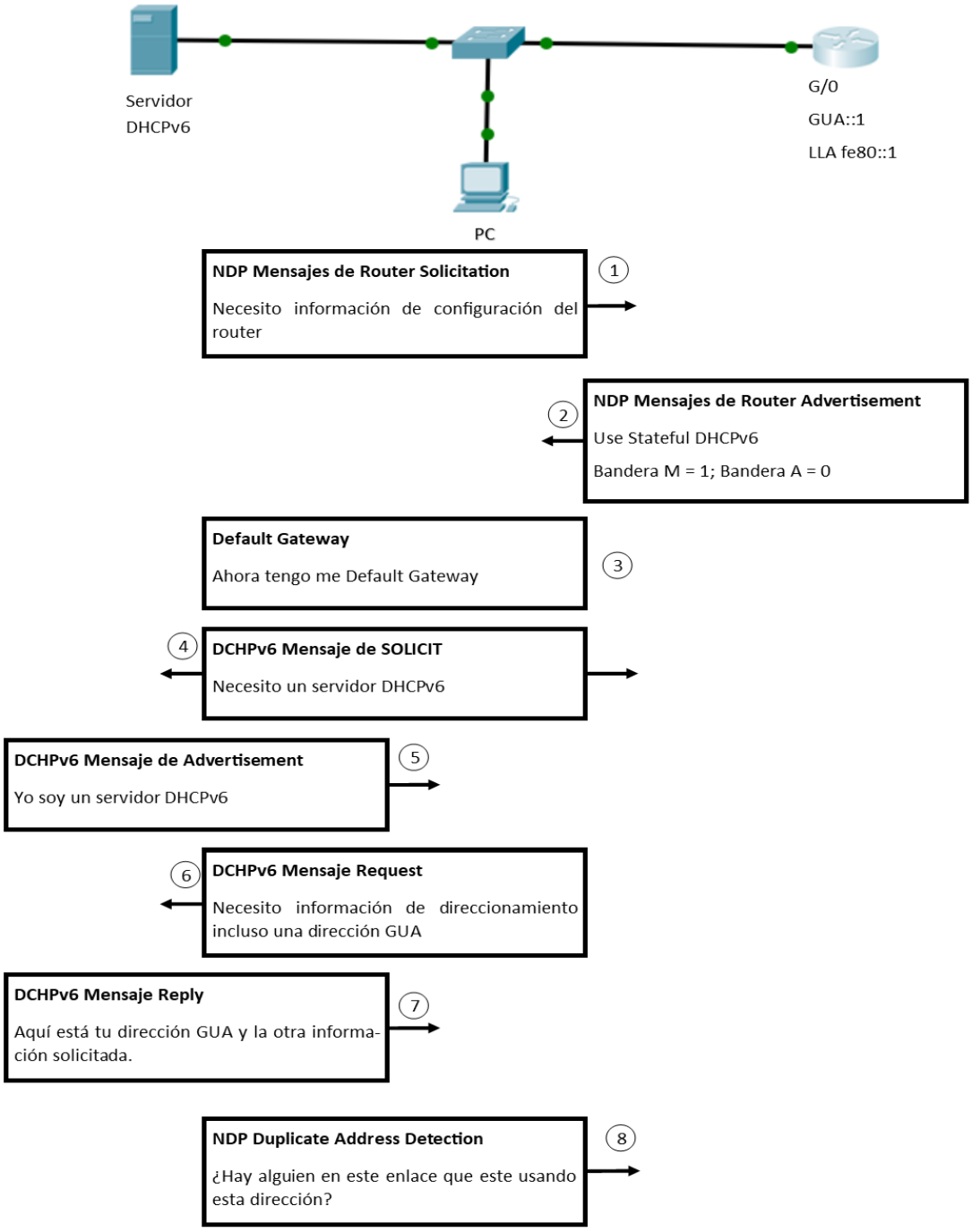


Ilustración 9 Stateful DHCP

1. **Paso 1:** La PC manda un mensaje ICMPv6 Router Solicitation, solicitando un mensaje de Router Advertisement.
2. **Paso 2:** El router le manda un mensaje de Router Advertisement con la bandera M igual a 1. Esto le sugiere a la PC que debe de usar un servidor DHCPv6 para poder obtener su direccionamiento. La bandera A esta apagada informándole al equipo que no será necesario el proceso de SLAAC:
3. **Paso 3:** Al recibir el Mensaje RA, la computadora usa tomo del paquete la dirección origen y la usa como el Gateway.
4. **Paso 4:** Como el mensaje recibido tiene la bandera M igual a uno, la PC manda un mensaje de DHCPv6 Solicit a la dirección ff02::1:2, la dirección *multicast* de todos los servidores DHCPv6.
5. **Paso 5:** Uno o más servidores pueden responder con un mensaje DHCPv6 Advertisement, indicando que están disponibles para proveer una dirección.
6. **Paso 6:** La PC responde al servidor de su elección con un mensaje Request pidiendo una dirección y otras configuraciones.
7. **Paso 7:** El servidor DHCPv6 responde con un mensaje Reply que contiene una dirección global y otras configuraciones.
8. **Paso 8:** La PC usa DAD para verificar si la dirección obtenida no está duplicada.

2.4 IMCPv6

El protocolo ICMP es uno de los protocolos utilizados in TCP/IP. ICMP es una aplicación muy importante para las conexiones de red, ya que con el protocolo diferentes dispositivos logran comunicarse uno con el otro. Un dispositivo puede recibir mensajes tipo ICMP que pueden indicar información o en mensaje de error. En lo más común y practico ICMP se utiliza en aplicaciones como ping o traceroute. ICMPv6 no es como el típico ICMP, la nueva versión es más robusta y aporta nuevas cualidades y funciones.

2.4.1 Formato General de ICMPv6

No hay tanta variación cuando se comparan los mensajes ICMPv4 con ICMPv6, el protocolo en IPv6 es similar, pero con mejoras. En el encabezado un paquete IPv6, si se encuentra el valor

58, quiere indicar que un mensaje de ICMPv6 es la próxima sección. A continuación, una gráfica de la representación del mensaje ICMPv6 y lo que significan los campos.

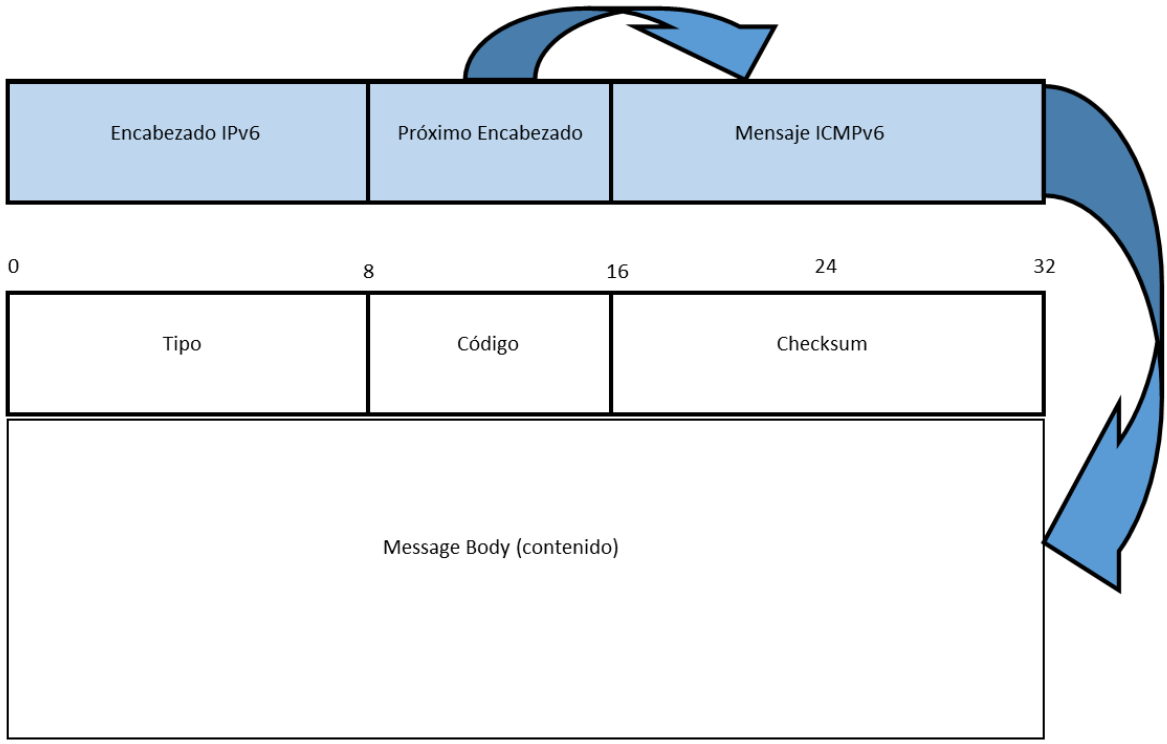


Ilustración 10 Formato ICMPv6

- **Tipo (8 bits):** Indica el tipo de mensaje de ICMPv6, por ejemplo, Echo Request, Destination Unreachable o Paquete Too Big.
- **Código (8 bits):** Provee más granularidad al campo de Tipo. Por ejemplo, se el Tipo fue Destino Inalcanzable, el código dará más información sobre porque no se pudo llegar al destino.
- **Checksum (16 bits)**: se utiliza para detectar corrupciones en la información enviada o recibida.

El campo de tipo se utiliza para categorizar los mensajes de ICMPv6 en dos grupos:

1. **Mensajes de Error:** Tipo = 0 hasta 127
2. **Mensajes de Información:** Tipo = 128 hasta 255

Los mensajes de error son utilizados para notificar porque el paquete que fue enviado no a llegado a su destino. Por ejemplo, si el *hop limit* de un paquete ha llegado a su límite entonces el paquete fue descartado por un router.

Los mensajes informativos no reportan errores, pero proveen información necesaria para varios tipos de pruebas o diagnósticos El más común sería los mensajes de ICMP, *Echo Request* y *Echo Reply*, que son utilizados en el comando *ping*.

2.4.2 Neighbor Discovery

Como se ha visto, ICMPv6 tiene varias similitudes con la versión 4, pero con IPv6 implementaron Neighbor Discovery (ND). Con esta adicción, ICMPv6 es más robusto que su contraparte. ICMPv6 ND incluye nuevas funcionalidades como *Prefix Discovery, Duplicate Address Detection* y *Neighbor Unreachability Detection*.

Para poder descubrir un dispositivo, el protocolo usa cinco mensajes ICMPv6.

1. Router Solicitation (RS)
2. Router Advertisement (RA)
3. Neighbor Solicitation (NS)
4. Neighbor Advertisement (NA)
5. Redirect Message

Los primeros 4 son nuevas adiciones al protocolo ICMPv6 y solo el Redirect Message es similar in IPv4. RS y RA son mensajes utilizados para la comunicación entre routers y otro tipo de dispositivos que están en la misma red. NS y NA son mensajes utilizados entre dos dispositivos, incluso los routers, que están en la misma red. Dispositivos y routers, usan ICMPv6 Neighbor Discovery en la siguiente manera:

- Descubrimiento de Router y el prefijo: Como se ha mencionado antes, SLAAC utiliza los mensajes RA y RS para poder asistir a un dispositivo conseguir su direccionamiento automáticamente.
- *Address* Resolution: Los mensajes NA y NS son utilizados para determinar la dirección de Capa 2.

- Duplicate *Address* Detection (DAD): Los mensajes NS y NA son utilizados para poder determinar si una dirección está en uso, ya sea dinámica o manual.
- Neighbor Unreachability Detection (NUD): Los mensajes NS y NA son utilizados para determinar se un dispositivo puede comunicarse con otro dispositivo.
- Redirection: Estos mensajes son utilizados para redirigir a un dispositivo a un router que tenga mejor siguiente salto - *next hop*.

2.5 Protocolos de Enrutamiento

Los protocolos de enrutamiento de IPv6 son muy similares a los del IPv4, incluso se puede considerar que es más fácil de implementar que su contraparte. En los siguientes puntos se explicará los siguientes temas:

1. Rutas Estáticas
2. EIGRP
3. OSPF

Para poder implementar cualquiera de estos protocolos in IPv6, tenemos que asegurarnos que el router esté habilitado para IPv6. Por ejemplo, en los equipos Cisco con IOS, con el comando **ipv6 *unicast*-routing** podemos habilitar IPv6 en un router. Al ingresar este comando, se habilita IPv6 y el router puede crear y procesar paquetes IPv6. Este comando hace que el router empiece a mandar mensajes RA (Router Advertisement) atreves de sus interfaces. Es posible configurar un router o interfaz de un router como si fuera un nodo, simplemente se agrega el comando **ipv6 enable** en la interfaz que se desea. Estos comandos causan que el router pertenezcan a los grupos de todos los dispositivos IPv6 ff02::1 y al grupo de todo los routers IPv6 ff02:2.

Para mantener un base de datos de redes conectadas, IPv6, igual que IPv4 tiene una tabla de rutas. Esta tabla tiene la misma función que en IPv4, pero tiene la ventaja que in IPv6 ya no existe las redes *Classful* ni las redes VLSM. Al no tener eso dos elementos, las tables de IPv6 son más directas y fáciles de entender.

Para poder visualizar la table de rutas, se ingresa el siguiente comando, **show ipv6 route.** Este comando nos permite agregar parámetros que puede proveer una tabla más específica o

detallada. Como en IPv4, se puede especificar que la tabla muestre rutas específicamente para una dirección IP o una interfaz. Se puede mostrar rutas que estén directamente conectadas, locales o estáticas.

2.5.1 Rutas Estáticas

Una ruta estática se puede establecer manualmente. En esta parte se mostrará como configurar una ruta estática básica. Las rutas estáticas deben tener ciertos parámetros para ser configuradas, la estructura es la siguiente:

Ipv6 route *ipv6-prefix/prefix-length {ipv6-address / interface-type interface-number} [next-hop-address]*

- Ipv6-prefix: Este parámetro es la dirección de la red destino con que se quiere establecer una conexión.
- /prefix-length: Esto se refiere a la longitud del prefijo IPv6. Por ejemplo, la longitud se define como /64.
- ipv6 *address*: la dirección del próximo salto se puede utilizar para alcanzar a una red deseada.
- interface-type: normalmente se usa para conexiones punto a punto tales como interfaces de serial o túneles.

La próxima imagen se utilizará para los siguientes puntos.

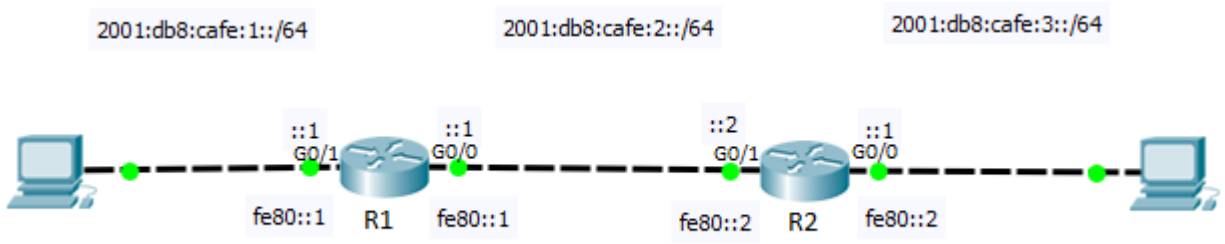


Ilustración 11 Rutas Estáticas

2.5.1.1 Rutas Estáticas Usando una Dirección Global.

Las rutas estáticas que utilizan una dirección global como la dirección del próximo salto, son una de las más usadas. A continuación, se configura R1 con una ruta estática hacia la red

2001:DB8:CAFE:3::/64 y se configurar la dirección 2001:DB8:CAFE:2::2/64 como el próximo salto.

R1(config) # **ipv6 route 2001:db8:cafe::3/64 2001:db8:cafe:2::2**

Con el comando de arriba, el router 1 ya podrá ver la red **2001:db8:cafe::3/64.**

2.5.1.2 Rutas Estáticas Usando Una Dirección Link Local

Normalmente las direcciones que se utilizan para el próximo brinco son direcciones que están en la misma red, entonces es común que se pueda utilizar una dirección de *link local* para el próximo salto. Las direcciones link local sólo se pueden alcanzar en un enlace o red compartida. Cuando se configura una ruta estática con un link local, hay que especificar la interfaz de salida porque hay posibilidades que haya un link local idéntica en el otro router. La configuración se hará en el router 2:

R2(config) # **ipv6 route 2001:db8:cafe:1::/64 gigabitethernet0/1 fe80::1**

2.5.1.3 Rutas Estáticas Por Default Usando Direcciones Link Local Como Próximo Salto

Configurando una ruta por default es similar a configurar una un IPv4, con un prefijo de todo cero y su longitud de /0. En IPv4 una ruta por default se configura con todos ceros 0.0.0.0 0.0.0.0, para representa esto en IPv6 se reescribe como ::0 /0. Por ejemplo:

R2(config) # **ipv6 route ::/0 gigabitethernet0/1 fe80::1**

2.5.2 EIGRP

EIGRP es un protocolo que fue creado por Cisco y fue diseñado como un protocolo vector distancia. La versión de IPv6 tiene las mismas funcionalidades que la versión IPv4, pero son protocolos totalmente diferentes. Hay dos maneras de configurar routers para EIGRP:

1. La Clásica
2. La nombrada

2.5.2.1 EIGRP Clásica

La forma clásica de configurar EIGRPv6 tiene sus raíces en la configuración de EIGRPv4. Para demostrar la configuración se usará la siguiente red:

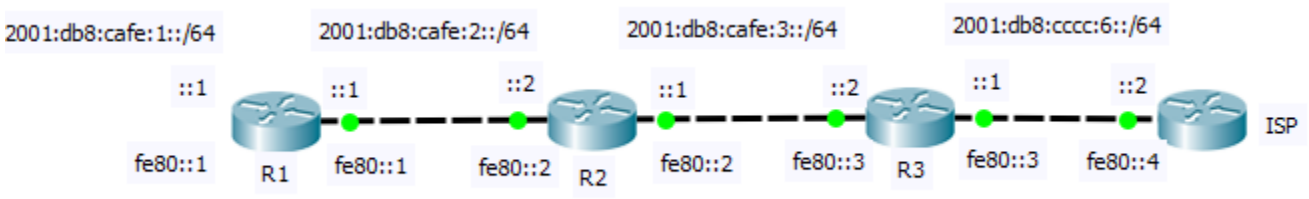


Ilustración 12 EIGRP

Primero se configura router 1:

R1(config)# ipv6 *unicast*-routing

R1(config)# ipv6 router eigrp 1

R1(config-rtr)# eigrp router-id 1.1.1.1

R1(config-rtr)# passive-interface gigabitethernet0/0

R1(config-rtr)# exit

R1(config)# interface gigabitethernet 0/0

R1(config-if)# ipv6 eigrp 1

R1(config-if)# exit

R1(config)# interface gigabitethernet 0/1

R1(config-if)# ipv6 eigrp 1

Los siguientes puntos son una breve explicación de la configuración realizada en R1:

- R1(config)# ipv6 router eigrp 1
  Este comando crea un proceso de EIGRP con el número autónomo de 1. El número Autónomo tiene que ser igual en todos los routers que estén en el mismo dominio.
- R1(config-rtr)# eigrp router-id 1.1.1.1
  Este comando configura la ID de EIGRP. Este comando es necesario si no hay una interfaz loopback activa o una interfaz física configurada con IPv4.
- R1(config-rtr)# passive-interface gigabitethernet0/0

  Este comando se usa cuando la interfaz no está conectada a un vecino que utiliza EIGRP. Provoca la cancelación de paquetes *hello* y actualizaciones de rutas.

- R1(config-if)# ipv6 eigrp 1

  EIGRP es habilitado directamente en la interfaz cuando se usa este comando.

Para crear un vínculo entre los routers, se tiene que configurar router 2 de la misma manera:

R2(config)# ipv6 *unicast*-routing
R2(config)# ipv6 router eigrp 1
R2(config-rtr)# eigrp router-id 2.2.2.2
R2(config-rtr)# exit
R2(config)# interface gigabitethernet 0/0
R2(config-if)# ipv6 eigrp 1
R2(config-if)# exit
R2(config)# interface gigabitethernet 0/1
R2(config-if)# ipv6 eigrp 1

Al configurar router 2, un mensaje debe de aparecer en los dos routers indicando que se ha establecido una relación.

Para configurar el router 3, es de la misma manera para su interfaz que se dirige hacia el router 2. Para tener acceso hacia el *Internet*, se debe de crear una ruta estática dirigida al ISP.

R3(config)# ipv6 *unicast*-routing
R3(config)# ipv6 route ::/0 gigabitethernet0/0 fe80::4
R3(config)# ipv6 router eigrp 1
R3(config-rtr)# eigrp router-id 3.3.3.3
R3(config-rtr)# exit
R3(config)# interface gigabitethernet 0/1
R3(config-if)# ipv6 eigrp 1
R3(config-if)# ipv6 summary-*address* eigrp 1 ::/0

Para poder verificar que se estableció una conexión EIGRP se puede usar los siguientes comandos:

- show ipv6 eigrp neighbors
- show ipv6 eigrp topology

- show ipv6 route eigrp
- show ipv6 protocols
- show ipv6 eigrp traffic
- show ipv6 eigrp interfaces
- show ipv6 interface
- ping
- show running-config

2.5.2.2 EIGRP Nombrada

El modo nombrado de EIGRP permite que se configure todo en un mismo entorno, el modo de configuración de EIGRP. Este método usa direcciones de familias para unificar en una misma instancia, configuraciones hechas en IPv6 y IPv4. Se usará la ilustración 12 para el ejemplo de EIGRP nombrado. A continuación, la configuración de router 1.

R1(config)# ipv6 *unicast*-routing

R1(config)# router eigrp REDES

R1(config-router)# *address*-family ipv6 *unicast* autonomous-system 1

R1(config-router-af)# eigrp router-id 1.1.1.1

R1(config-router-af)# af-interface gigabitethernet 0/0

R1(config-router-af-interface)# passive-interface

R1(config-router-af-interface)# exit-af-interface

R1(config-router-af)# exit-*address*-family

- R1(config)# router eigrp REDES
  Este comando configura la instancia virtual de REDES e ingresa al modo de configuración de EIGRPv6 nombrado. No es necesario que este nombre sea igual en los otros routers.
- R1(config-router)# *address*-family ipv6 *unicast* autonomous-system 1
  Este comando configura la instancia de EIGRPv6 para la familia de direcciones IPv6 y usa el número autónomo 1. El número autónomo si tiene que ser igual en todos los

routers participando en el mismo dominio. Al ingresar, el router se cambia al modo de configuración de direcciones de familias.

- R1(config-router-af)# eigrp router-id 1.1.1.1
  Este comando configura la ID de EIGRP. Este comando es necesario si no hay una interfaz loopback activa o una interfaz física configurada con IPv4.
- R1(config-router-af)# af-interface gigabitethernet 0/0
  Este comando se utiliza para configurar direcciones de familias en la interfaz gigabitethernet 0/0
- R1(config-router-af-interface)# passive-interface
  Este comando se usa cuando la interfaz no está conectada a un vecino que utiliza EIGRP. Provoca la cancelación de paquetes hello y actualizaciones de rutas.

Luego procedemos al router 2:

R2(config)# ipv6 *unicast*-routing
R2(config)# router eigrp REDES
R2(config-router)# *address*-family ipv6 *unicast* autonomous-system 1
R2(config-router-af)# eigrp router-id 2.2.2.2
R2(config-router-af)# exit-*address*-family
R2(config-router)# exit

En el router dos no entramos al modo *af-interface*, porque con EIGRP nombrado, todas las interfaces activadas con IPv6 son automáticamente configuradas con EIGRP. Para terminar la configuración, configuramos el router 3:

R3(config)# ipv6 *unicast*-routing
R3(config)# ipv6 route ::/0 gigabitethernet0/0 fe80::4
R3(config)# router eigrp CAFE-DOMAIN
R3(config-router)# *address*-family ipv6 *unicast* autonomous-system 1
R3(config-router-af)# eigrp router-id 3.3.3.3
R3(config-router-af)# exit
R3(config-router)#

2.5.3 OSPF

Open Shortes Path First (OSPF) es un protocolo *link-state* que fue desarrollado para reemplazar al protocolo vector distancia, Routing Information Protocol (RIP). La versión IPv6 de OSPF se denomina OSPFv3. OSPFv2 y OSPFv3 comparten ciertas funcionalidades y operaciones, pero hay cambios significantes en OSPFv3.

2.5.3.1OSPF tradicional

En la manera tradicional OSPFv3 sólo soporta direcciones IPv6, si un sistema dual stack está implementado, OSPFv3 mantiene una tabla de vecinos propia. Para configurar el el proceso tradicional es bastante similar al OSPFv2. Se utilizará la siguiente figura para mostrar la configuración.

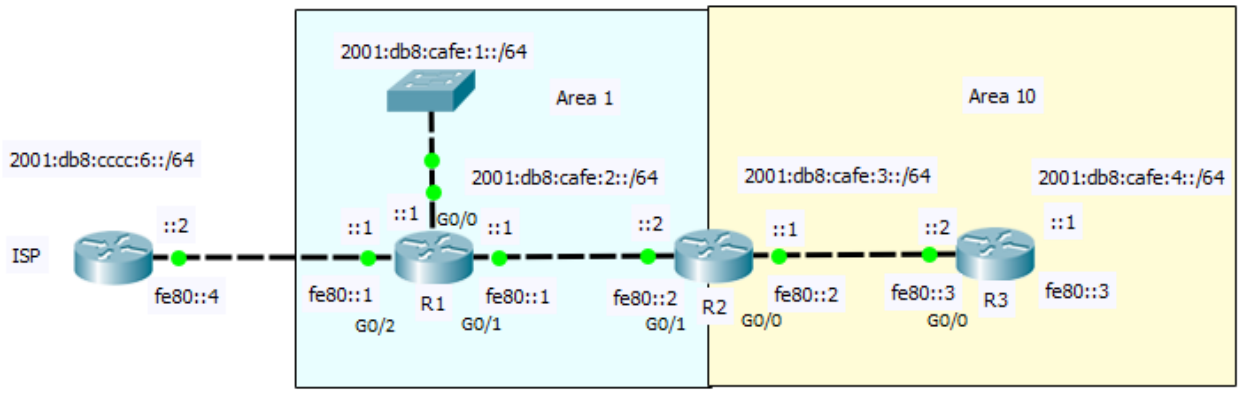


Ilustración 13 OSPF

Router 1 es un OSPF A*utonomous System Boundary Router* (ASBR), que tiene una interfaz externa conectada al ISP y tiene dos interfaces internas en el área 1. Router R2 es un *Area Border Router* (ABR) con una interfaz en el área 1 y la otra en el área 10. El router R3 está localizada en un área llamada *totally stubby area* que no recibe prefijos de otros routers, pero si recibe una ruta default del ABR.

Primero se configura el router R1:

R1(config)# ipv6 *unicast*-routing

R1(config)# ipv6 route ::/0 gigabitethernet0/2 fe80::4

R1(config)# ipv6 router ospf 1

```
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)# passive-interface gigabitethernet 0/0
R1(config-rtr)# default-information originate
R1(config-rtr)# exit
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ipv6 ospf 1 area 1
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/1
R1(config-if)# ipv6 ospf 1 area 1
R1(config-if)# exit
```

Se explicará puntos que son específicos a OSPF.

- R1(config)# ipv6 router ospf 1
  Esta configuración habilita el proceso de enrutamiento de OSPv3 usando el proceso ID 1. Este número solo tiene significado local y no es necesario que los de más routers en el mismo dominio tengan el mismo número.
- R1(config-rtr)# default-information originate
  Este comando es utilizado para redistribuir la ruta estática por default a todos los routers participando en el mismo dominio de OSPFv3.
- R1(config-if)# ipv6 ospf 1 area 1
  OSPFv3 se debe de habilitar en la interfaz que participara en el intercambio. La ID de procesamiento tiene que ser idéntica a la ID que se utilizó al principio y el área tiene que ser igual in todos los routers que están en el mismo dominio.
- Interface gigabitethernet que apunta al ISP no se configura con OSPF porque el router ISP no es un vecino habilitado con OSPF.

Ahora pasamos a la configuración del router 2:

```
R2(config)# ipv6 unicast-routing
R2(config)# ipv6 router ospf 1
```

R2(config-rtr)# router-id 2.2.2.2

R2(config-rtr)# area 10 stub no-summary

R2(config-rtr)# exit

R2(config)# interface gigabitethernet 0/1

R2(config-if)# ipv6 ospf 1 area 1

R2(config-if)# exit

R2(config)# interface gigabitethernet 0/0

R2(config-if)# ipv6 ospf 1 area 10

R2(config-if)# exit

Router 2 tiene una interfaz en el área 1 y la otra interfaz en el área 10 que es un *totally stubby area*. Para configurar un *totally stuby area*, se utiliza la configuración **stub no-summary** en el proceso de OSPFv3. Este comando le indica al router que esta área no recibe rutas resumidas o rutas externas.

El router R3 está completamente en el área 10 que es un *totally stuby area*. Para la configuración no es necesario poner **no-summary** porque sólo el ABR necesita saber que una de su interfaz está en un *totally stuby area*.

R3(config)# ipv6 *unicast*-routing

R3(config)# ipv6 router ospf 1

R3(config-rtr)# router-id 3.3.3.3

R3(config-rtr)# area 10 stub

R3(config-rtr)# exit

R3(config)# interface gigabitethernet 0/0

R3(config-if)# ipv6 ospf 1 area 10

R3(config-if)# exit

R3(config)# interface gigabitethernet 0/1

R3(config-if)# ipv6 ospf 1 area 10

R3(config-if)# exit

Para poder verificar que se estableció una conexión EIGRP se puede usar los siguientes comandos:

- show ipv6 route ospf
- show ipv6 ospf database
- show ipv6 protocols
- show ipv6 interface
- show ipv6 ospf neighbor
- show ipv6 ospf interface
- ping
- show running-config

2.5.3.2 OSPF con Direcciones de Familia (*Address* Family)

Con OSPFv3 usando direcciones de familias, se puede implementar IPv4 y IPv6 en el mismo proceso. OSPFv3 con *Address Family* -AF usa IPv6 para transportar mensajes de IPv6 e IPv4, entonces se requiere la configuración de direcciones *link local* y de *IPv6 unicast routing*, aunque sólo esté transportando IPv4. Se usará la misma ilustración que se utilizó en el ejemplo anterior, pero se agregarán redes de IPv4.

Empezaremos con router 1 que es el ASBR.

R1(config)# ipv6 *unicast*-routing

R1(config)# ipv6 route ::/0 gigabitethernet0/2 192.168.44.2

R1(config)# ip route 0.0.0.0 0.0.0.0 gigabitethernet0/2 fe80::4

R1(config)# router ospfv3 1

R1(config-router)# *address*-family ipv6 *unicast*

R1(config-router-af)# router-id 1.1.1.6

R1(config-router-af)# passive-interface gigabitethernet 0/0

R1(config-router-af)# default-information originate

R1(config-router-af)# exit-*address*-family

R1(config-router)# *address*-family ipv4 *unicast*

R1(config-router-af)# router-id 1.1.1.4

R1(config-router-af)# passive-interface gigabitethernet 0/0

R1(config-router-af)# default-information originate

R1(config-router-af)# exit-*address*-family

R1(config-router)# exit

- R1(config-router)# *address*-family ipv6 *unicast*
  Este comando hace que el router ingrese al modo de configuración de AF IPv6
- R1(config-router-af)# router-id 1.1.1.6
  Este comando configura la ID de EIGRP. Este comando es necesario si no hay una interfaz loopback activa o una interfaz física configurada con IPv4. Su puede utilizar el mismo ID para el AF de IPv4, pero para poder distinguir se puso un 6.

Sólo se explica la parte de *address-family* IPv6 ya que únicamente cambia el IPv4 en el ejemplo es el ID. Después de configurar los procesos, se tiene que ingresar a las interfaces que participarán y activarán el proceso en las interfaces señaladas.

R1(config)# interface gigabitethernet 0/0

R1(config-if)# ospfv3 1 ipv6 area 1

R1(config-if)# ospfv3 1 ipv4 area 1

R1(config-if)# exit

R1(config)# interface gigabitethernet 0/1

R1(config-if)# ospfv3 1 ipv6 area 1

R1(config-if)# ospfv3 1 ipv4 area 1

R1(config-if)# exit

Con router R2, igual que en el ejemplo tradicional se tiene que especificar que el área 10 es un *totally stuby area*. El comando *no-summary* se tiene que configurar en el proceso de IPv4 e IPv6.

R2(config)# ipv6 *unicast*-routing

R2(config)# router ospfv3 1

R2(config-router)# *address*-family ipv6 *unicast*

R2(config-router-af)# router-id 2.2.2.6

R2(config-router-af)# area 10 stub no-summary

R2(config-router-af)# exit-*address*-family

R2(config-router)# *address*-family ipv4 *unicast*

R2(config-router-af)# router-id 2.2.2.4

R2(config-router-af)# area 10 stub no-summary

R2(config-router-af)# exit-*address*-family

R2(config-router)# exit

R2(config)# interface gigabitethernet 0/1

R2(config-if)# ospfv3 1 ipv6 area 1

R2(config-if)# ospfv3 1 ipv4 area 1

R2(config-if)# exit

R2(config)# interface gigabitethernet 0/0

R2(config-if)# ospfv3 1 ipv6 area 10

R2(config-if)# ospfv3 1 ipv4 area 10

R2(config-if)# exit

Con el router 3 se omite el *no-summary* y sólo se configura con el comando *stub* que indica que todo el router está en el *totally stubby* área.

R3(config)# ipv6 *unicast*-routing

R3(config)# router ospfv3 1

R3(config-router)# *address*-family ipv6 *unicast*

R3(config-router-af)# router-id 3.3.3.6

R3(config-router-af)# area 10 stub

R3(config-router-af)# passive-interface gigabitethernet 0/0

R3(config-router-af)# exit-*address*-family

R3(config-router)# *address*-family ipv4 *unicast*

R3(config-router-af)# router-id 3.3.3.4

R3(config-router-af)# area 10 stub

R3(config-router-af)# passive-interface gigabitethernet 0/0

R3(config-router-af)# exit-*address*-family

R3(config-router)# exit

R3(config)# interface gigabitethernet 0/0

R3(config-if)# ospfv3 1 ipv6 area 10

R3(config-if)# ospfv3 1 ipv4 area 10

R3(config-if)# exit

R3(config)# interface gigabitethernet 0/1

R3(config-if)# ospfv3 1 ipv6 area 10

R3(config-if)# ospfv3 1 ipv4 area 10

R3(config-if)# exit

2.6 Dual Stack

Dual Stack es la técnica de combinar IPv6 e IPv4 en la misma red. Con este método, todos los dispositivos están configurados con dos direcciones, una IPv4 y una IPv6. Esta implementación ha sido la más popular de todas las tecnologías para implementar IPv6, esto es porque corre los dos protocolos en paralelo.

Aunque Dual Stack ofrece una oportunidad menos complicada de implementar IPv6, Dual Stack tiene ciertos conflictos. Hay que recordar que cuando se configurar Dual Stack, se está configurando dos veces. Eso quiere decir que habrá doble trabajo administrativo y técnico, provisionando direcciones, administrando equipos y solucionando problemas.

En el proceso de mandar paquetes, una aplicación que soporta IPv4 e IPv6 puede escoger qué protocolo mandar dentro del paquete. Si la aplicación manda en IPv6, al igual que IPv4, un número de puerto TCP o UDP es asignado al paquete. El campo de *Next Header* identifica el

protocolo de transporte. El paquete es encapsulado en una trama de ethernet que usa el tipo de campo 0x86dd. Una aplicación que soporta los dos protocolos manda los paquetes en los dos protocolos, y pide todas las direcciones disponibles al DNS. Si el DNS responde con direcciones IPv4 e IPv6, el sistema operativo escoge que protocolo usar. En la mayoría de los casos, las aplicaciones están por default configuradas para aceptar IPv6 primero.

Capítulo 3 Desarrollo

Para el desarrollo de este proyecto, se dará un ejemplo en cómo se puede implementar IPv6 en las aulas de redes de la DCI. La DCI tiene dos aulas de redes con un switch en cada aula. En la ilustración se demuestra la situación actual de las aulas.

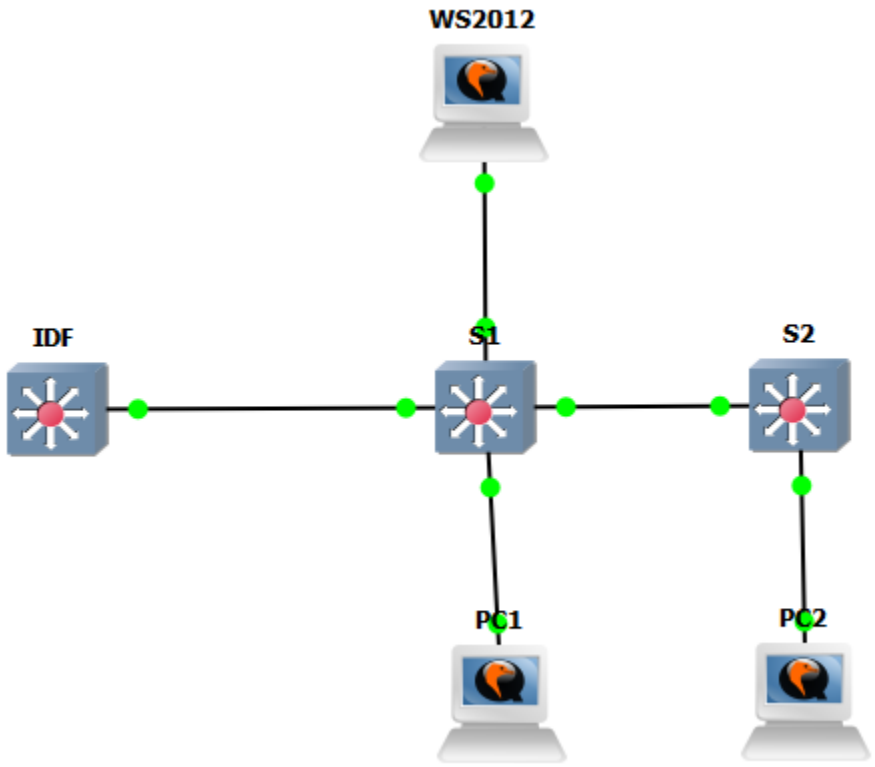


Ilustración 14 Aulas de Redes

Para poder implementar el protocolo, se sugiere utilizar un router como salida al *Internet*. Con un router, se tiene la opción de remover el servidor DHCP localizado en el Windows Server 2012, y utilizar SLAAC como método de asignación de direccionamiento para IPv6.

Para poder facilitar la transición en el aula de redes, se dejará el servidor de Windows como IPv4 y se utilizará el router como DHCP para IPv6. En la configuración actual, S1 tiene un enlace

troncal a un IDF que maneja la salida al *Internet*. Se pondrá el router entre el S1 y el IDF. Con la modificación, la topología quedaría como la siguiente.

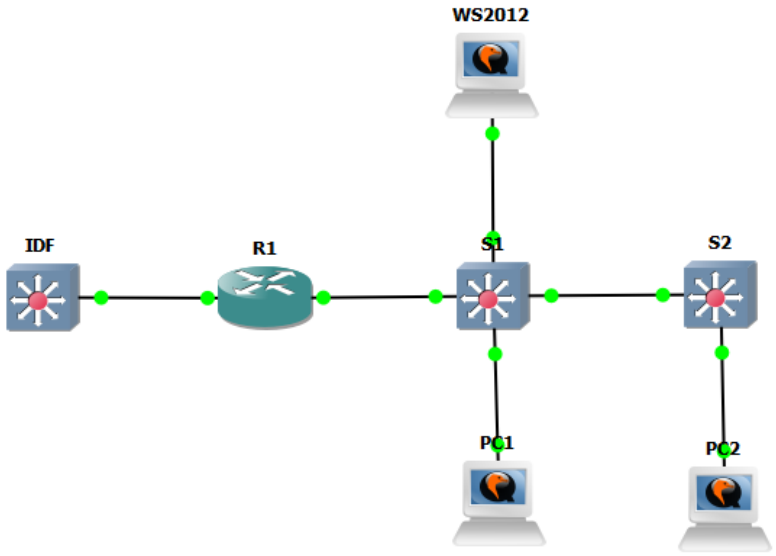


Ilustración 15 Aulas de Redes con Router

Se utilizará la red 10.10.10.0 /24 para IPv4 y la red IPv6 usara 2001:DB8:1:1:: /64. Se utilizará un prefijo de /64 para que los dispositivos puedan usar el método de SLAAC y puedan autoconfigurar su interfaz con una IPv4.

Para que las computadoras, PC1 y PC2, obtengan direccionamiento usando SLAAC, se tiene que configurar la interfaz del Router con una dirección IPv6. Antes de configurar la interfaz, hay que habilitar el router con IPv6 utilizando el comando **ipv6 *unicast*-routing**. Verificamos en la configuración con el comando **show**.

R1#show running-config | include ipv6 uni

ipv6 *unicast*-routing

Como la implementación de IPv6 es dual-stack, se configura una IPv6 y IPv4 en la misma interfaz.

R1#show running-config | section interface GigabitEthernet0/1

interface GigabitEthernet0/1

ip *address* 10.10.10.1 255.255.255.0

ipv6 *address* FE80::1 link-local

ipv6 *address* 2001:DB8:1:1::1/64

ipv6 enable

R1#

En la configuración se puede ver que la interfaz tiene ambas direcciones y una dirección link-local. Las direcciones link-local, son generadas automáticamente al habilitar IPv6 en el Router, En este caso, se configuró una dirección estática para poder identificar la red.

Con esta configuración, las computadoras ya deben de obtener una dirección IPv6. En las siguientes ilustraciones se puede ver que las computadoras, con sistemas operativos de Windows y Ubuntu, obtuvieron su direccionamiento. Se puede apreciar que los primeros 4 nibbles son los mismos que tiene la interfaz en el Router, los de más nibbles son agregados por el sistema operativo.

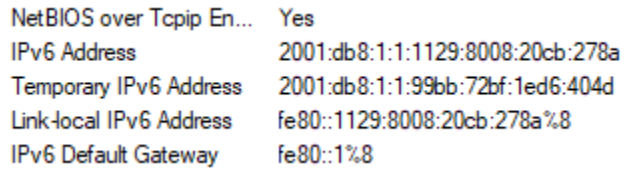


Ilustración 16 IPv6 Windows 10

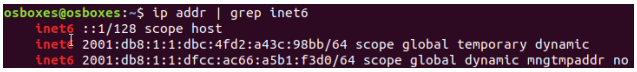


Ilustración 17 IPv6 Ubuntu 18.04.2

A continuación, se configura el Windows Server 2012. Este servidor actuará como el servidor de DHCP de la parte de IPv4. En el servidor, se tiene que habilitar la opción de DHCP. Al habilitar la opción, se procede a configurar un Scope. El scope contiene la información que usará el servidor para distribuir las IPs. Para esta red, se configuró el rango de 10.10.10.20-30/24. También se configuró para que las computadoras obtengan la puerta de enlace, también conocida como Gateway, 10.10.10.1. Se configuran las direcciones DNS de Google. En la ilustración 18, se muestra las opciones generales que fueron configuradas.

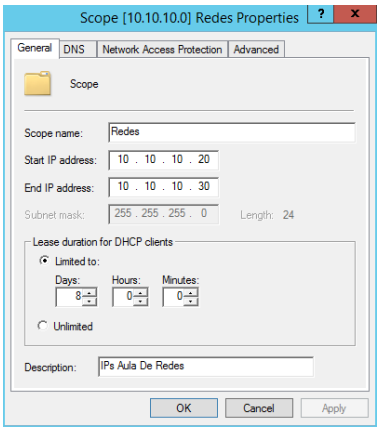


Ilustración 18 Opciones Generales DHCPv4

Al terminal, se reinicia el servicio de redes en cada computadora. En Windows 10, *ipconfig /release*, seguido de un *ipconfig /renew*. En Ubuntu se usa el comando *sudo service network-manager restart*. En las siguientes figuras, se puede verificar que las computadoras obtuvieron una IP dentro del rango configurado en el servidor.

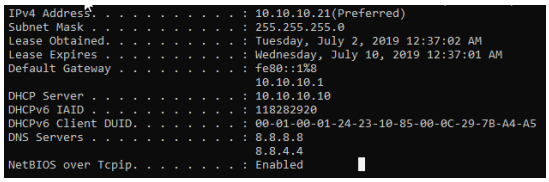


Ilustración 19 Windows IPv4

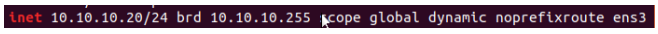


Ilustración 20 Ubuntu IPv6

3.1 Pruebas de funcionamiento

Para probar las funcionalidades de IPv6, se hicieron pruebas que trabajan en IPv4. En el servidor, se configuró un folder y se compartió en la red. Para poder montar un folder usando IPv6, se tiene que separar cada *nibble* con un guión en vez de utilizar los dos puntos. Después del último nibble se agrega *.ipv6-literal.net*. En este caso la dirección IPv6 del servidor es, 2001:db8:1:1:a809:9970:2ae7:de3c, y se convierte en 2001-0db8-00001-00001-a809-9970-2ae7-de3c.ipv6-literal.net. La carpeta de prueba se le llamó *Test1*, tiene un documento de texto llamado *IPv6* y se montará en la PC que tiene Windows 10. Para montarlo, se siguen los mismos pasos que en IPv4, la dirección de la carpeta es la siguiente, \\2001-0db8-00001-00001-a809-9970-2ae7-de3c.ipv6-literal.net\Users\Administrator\Desktop\Test1.

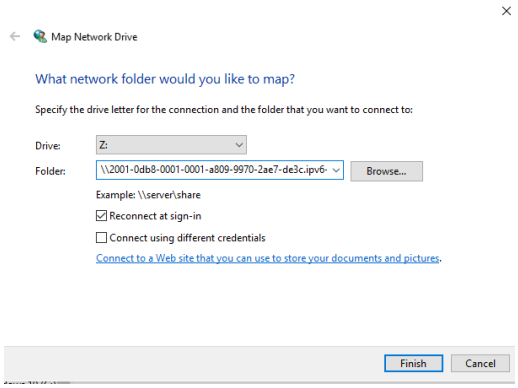


Ilustración 21 Montando Carpeta IPv6

Al terminal se puede ver la carpeta en las opciones de This PC.

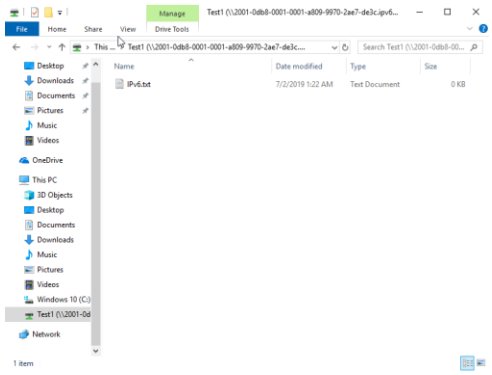


Ilustración 22 Carpeta Montada Usando IPv6

La próxima prueba se realizó con un el servicio de FTP. Se configuró el servidor FTP en el servidor de Windows 2012. Para poder configurar el servicio, se agregó el roll de IIS de Windows. Luego se habilito la opción de FTP. En las configuraciones del IIS, se habilitó un sitio FTP llamado Test-FTP y se dio permisos a usuarios anónimos para acceder el servicio. En las ilustraciones siguientes, se puede ver la configuración del servidor, la carpeta en Windows 2012 y la carpeta en Windows 10.

Para facilitar la conexión, se le configuró una IP estática al servidor Windows 2012. La dirección es la siguiente, 2001:db8:1:1::100.

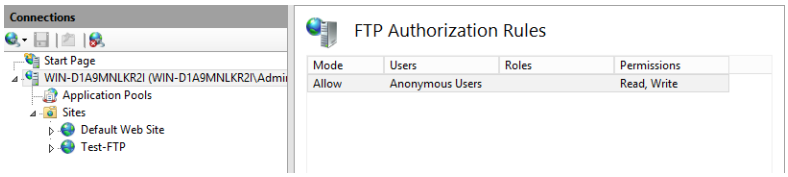


Ilustración 23 Configuraciones FTP

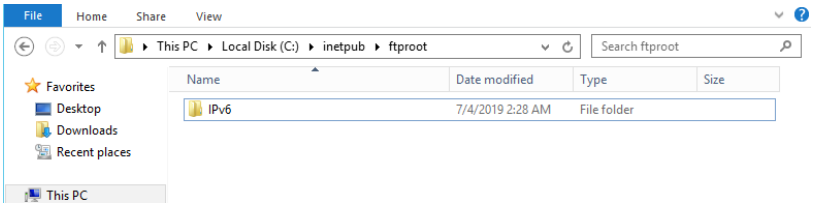


Ilustración 24 Carpeta local del FTP

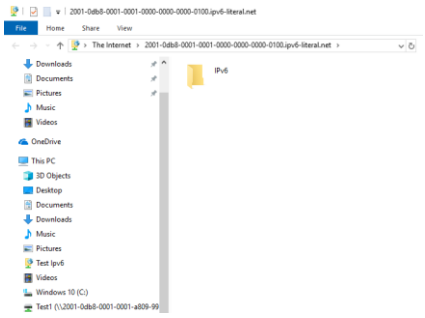


Ilustración 25 Carpeta FTP W10

En la ilustración 25, se puede ver que la carpeta se conectó al servidor FTP usando la dirección ftp://2001-0db8-0001-0001-0000-0000-0000-0100.ipv6-literal.net.

Capítulo 4 Resultados

Se hicieron varias pruebas para corroborar la funcionalidad de IPv6. Dentro de estas pruebas, se consideró una relacionada con la conectividad de una conexión FTP y de una carpeta compartida usando el servidor Windows 2012.

Para poder complementar las pruebas realizadas en GNS3, éstas también se realizaron para un ambiente de producción. Se comenta que, en esta red, hay conectividad hacia el *Internet* usando IPv6. La red ya está establecida y se configuró una máquina con Windows Server 2016 para poderlas llevar a cabo.

En el servidor Windows 2016, se le asignó una IPv6 estática de 2803:9a40:0:3::100. Se le configuró el *Gateway* de 2803:9a40:0:3::1, que es un servidor pfSense. Para complementar las pruebas se utilizó una laptop que obtuvo direccionamiento por el método de SLAAC. Al momento de la prueba, la laptop fue asignada la siguiente IPv6, 2803:9a40:0:3:3d79:55f5:d913:34cd.

4.1 Prueba de Conectividad

Para poder probar la conectividad dentro la red, se aseguró que cada dispositivo obtuvo su direccionamiento IPv6. Cada dispositivo en este caso logró la configuración de IPv6 utilizando SLAAC y el prefijo 2001:db8:1:1/64.

Desde la computadora PC1, Windows 10, se pudo hacer una prueba de ping hacia el Gateway, PC2 y el Servidor. Con la PC2, Ubuntu, se hicieron las mismas pruebas y el resultado fue positivo. Entre todos los dispositivos hay conectividad IPv6. En las ilustraciones 26 y 27 se puede ver el resultado de IPv4 y en las ilustraciones 28 y 29 de IPv6.

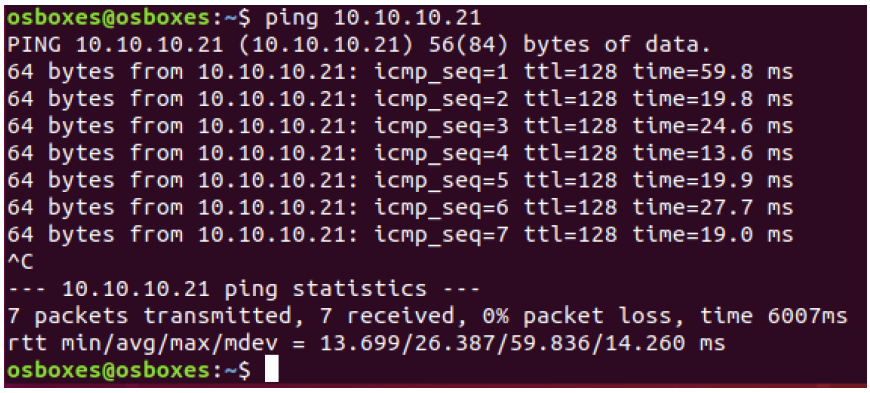


Ilustración 26 Conectividad IPv4 hacia la PC Windows 10

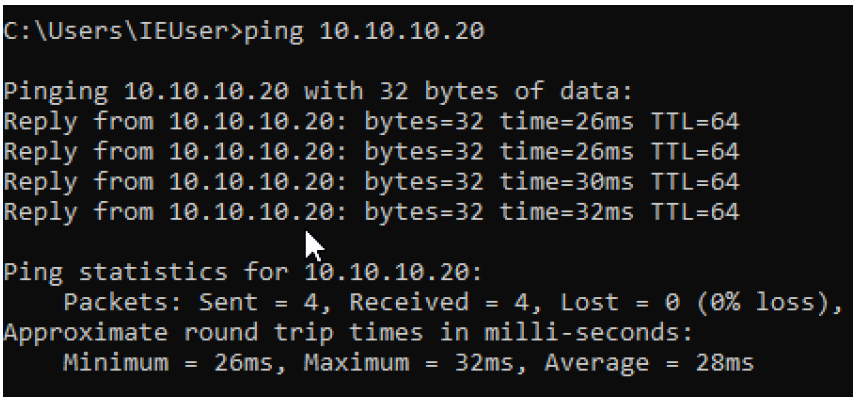


Ilustración 27 Conectividad IPv4 hacia la PC Ubuntu

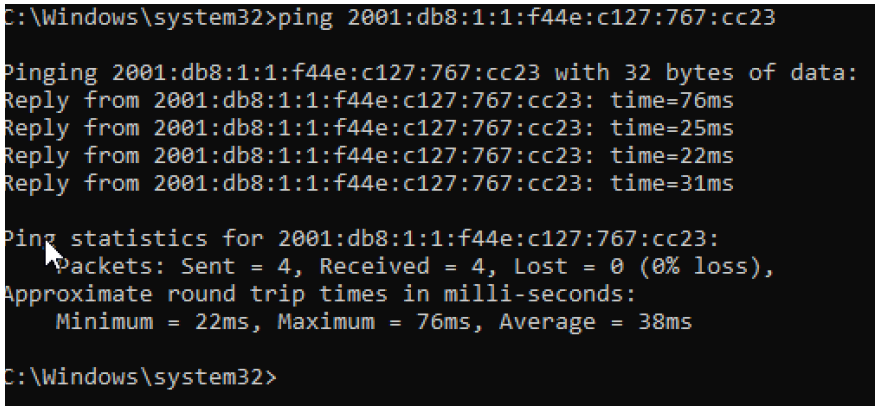


Ilustración 28 Conectividad IPv6 hacia PC Ubuntu

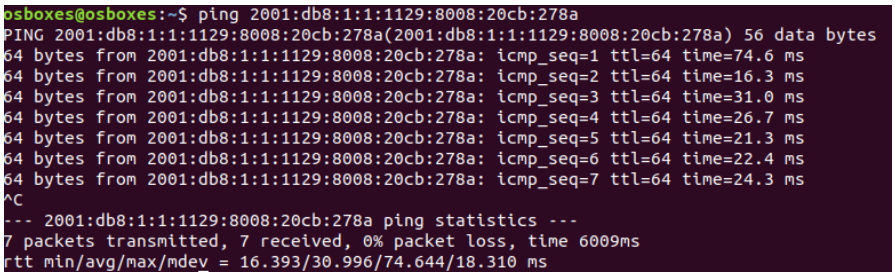


Ilustración 29 Conectividad IPv6 hacia PC Windows 10

Por ser una emulación en GNS3, no se puede apreciar la diferencia en el tiempo que toma para mandar los paquetes ICMP. Se puede notar que el tiempo en que se tomó para mandar 4 paquetes son similares. En la Tabla 3 se toma el promedio de tiempo de los primeros 4 paquetes de cada máquina.

Protocolo	Promedio de Tiempo
IPv4	28.98s
IPv6	37.85s

Tabla 3 Promedio de tiempos GNS3

Viendo el promedio del tiempo, se puede notar que usando GNS3 IPv6 es más lento que IPv4, aunque en teoría IPv6 debe de ser mucho más rápido que IPv4.

4.1.1 Conectividad ambiente de producción

Para poder tener una mejor comparación en los tiempos, se hizo una prueba de conectividad en un ambiente de producción. Como se mencionó antes, este ambiente tiene conectividad hacia el *Internet*. Se hizo pruebas de *ping* hacia los servidores de Google y entre el servidor Windows 2016 y la laptop.

La primera prueba se realizó entre el servidor y la laptop. Se hizo la prueba con IPv4 primero, seguido de IPv6.

```
C:\Users\sierr>ping 10.11.17.102

Pinging 10.11.17.102 with 32 bytes of data:
Reply from 10.11.17.102: bytes=32 time=1ms TTL=128
Reply from 10.11.17.102: bytes=32 time=1ms TTL=128
Reply from 10.11.17.102: bytes=32 time=1ms TTL=128
Reply from 10.11.17.102: bytes=32 time=1ms TTL=128

Ping statistics for 10.11.17.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\sierr>
```

Ilustración 30 Conectividad IPv4 hacia Servidor Windows 2016

```
C:\Users\Administrator>ping 10.11.17.149

Pinging 10.11.17.149 with 32 bytes of data:
Reply from 10.11.17.149: bytes=32 time=1ms TTL=128
Reply from 10.11.17.149: bytes=32 time=1ms TTL=128
Reply from 10.11.17.149: bytes=32 time=1ms TTL=128
Reply from 10.11.17.149: bytes=32 time=1ms TTL=128

Ping statistics for 10.11.17.149:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Ilustración 31 Conectividad IPv4 hacia Laptop

```
C:\Users\sierr>ping 2803:9a40:0:3::100

Pinging 2803:9a40:0:3::100 with 32 bytes of data:
Reply from 2803:9a40:0:3::100: time=1ms
Reply from 2803:9a40:0:3::100: time=1ms
Reply from 2803:9a40:0:3::100: time=1ms
Reply from 2803:9a40:0:3::100: time=1ms

Ping statistics for 2803:9a40:0:3::100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Ilustración 32 Conectividad IPv6 hacia Servidor 2016

```
C:\Users\Administrator>ping 2803:9a40:0:3:3d79:55f5:d913:34cd

Pinging 2803:9a40:0:3:3d79:55f5:d913:34cd with 32 bytes of data:
Reply from 2803:9a40:0:3:3d79:55f5:d913:34cd: time=1ms
Reply from 2803:9a40:0:3:3d79:55f5:d913:34cd: time=1ms
Reply from 2803:9a40:0:3:3d79:55f5:d913:34cd: time=1ms
Reply from 2803:9a40:0:3:3d79:55f5:d913:34cd: time=1ms

Ping statistics for 2803:9a40:0:3:3d79:55f5:d913:34cd:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Ilustración 33 Conectividad IPv6 hacia Laptop

En las ilustraciones anteriores, se demuestra que hay conectividad IPv6 entre los equipos, también que no hay diferencia entre los tiempos de los paquetes mandados. Esto se debe a que los dispositivos se encuentran en la misma red y están conectados a puertos Gigabit Ethernet.

En la siguiente prueba se utilizó la laptop y utilizamos el comando *ping* hacia los servidores de Google. Las computadoras tienden a preferir IPv6 sobre IPv4, esto quiere decir que si hago ping google.com, se resolverá primero usando IPv6.

```
Pinging google.com [2607:f8b0:4002:c09::64] with 32 bytes of data:
Reply from 2607:f8b0:4002:c09::64: time=42ms
Reply from 2607:f8b0:4002:c09::64: time=42ms
Reply from 2607:f8b0:4002:c09::64: time=42ms
Reply from 2607:f8b0:4002:c09::64: time=42ms

Ping statistics for 2607:f8b0:4002:c09::64:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 42ms, Average = 42ms
```

Ilustración 34 Ping al servidor de Google, IPv6

```
C:\Users\sierr>ping -4 google.com

Pinging google.com [173.194.219.102] with 32 bytes of data:
Reply from 173.194.219.102: bytes=32 time=46ms TTL=42
Reply from 173.194.219.102: bytes=32 time=47ms TTL=42
Reply from 173.194.219.102: bytes=32 time=46ms TTL=42
Reply from 173.194.219.102: bytes=32 time=46ms TTL=42

Ping statistics for 173.194.219.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 47ms, Average = 46ms
```

Ilustración 35 Ping al servidor de Google IPv4

A diferencia entre la prueba entre las estaciones, se puede aprecias en las ilustraciones 34 y 35, la deferencia en el tiempo. Se nota que en IPv4 el tiempo de transmisión fue mayor que en el protocolo IPv6. A continuación se puede ver la diferencia entre los tiempos.

Protocolo	Promedio de Tiempo
IPv6	42
IPv4	46.2

Hay una diferencia de 4.25ms entre los dos protocolos.

4.2 Prueba de FTP

Para realizar esta prueba, se instaló y configuró el servidor FTP en la máquina del servidor Windows 2012. La estalación no fue complicada, se siguió los mismos pasos que se siguen para instalar el servidor FTP en IPv4. En la computadora Windows 10, se habilitó el servicio de FTP para poder interactuar con el servidor.

En el servidor se creó una carpeta y se le puso un archivo llamado “Test6.txt”. En la PC1, se instaló el FTP y la carpeta con el archivo y se lograron ver. Al borrar el documento en el servidor, se pudo observar los mismo en la PC1. Dependiendo de los permisos dados, se puede crear y borrar desde PC1

4.2.1 FTP Ambiente Real

Para esta prueba se usaron las mimas máquinas que en la prueba de conectividad. Se activó la característica de IIS con el servicio de FTP in el servidor Windows 2016.

La primera prueba con FTP fue acceder el servicio usando un navegador de *Internet*, Chrome en este caso. La siguiente dirección fue utilizada para acceder el folder FTP

ftp://[2803:9a40:0:3::100]. Se puede ver que al solicitar la carpeta usando FTP, el navegador pide el usuario y contraseña que se configuro en el servidor.

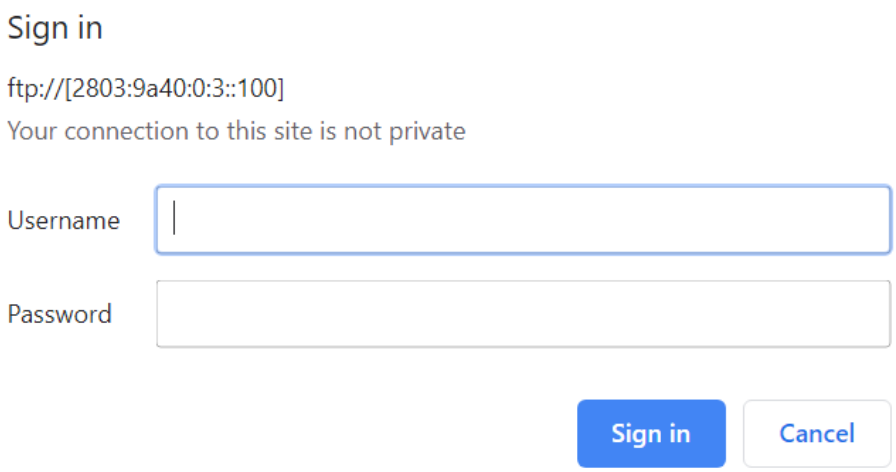


Ilustración 36 Autenticación FTP Navegador Chrome

Al autenticar, se muestran las carpetas que se configuraron en el Servidor Windows 2016.

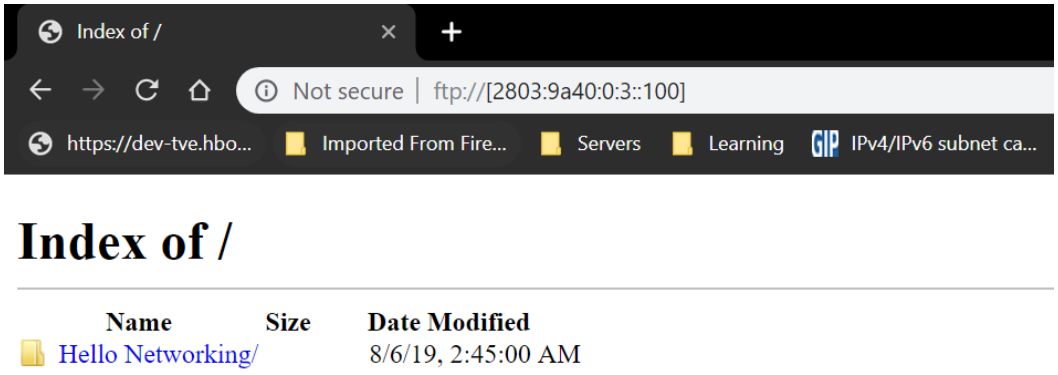


Ilustración 37 Carpetas FTP Chrome

En la siguiente prueba, se utilizó el software llamado FileZilla para poder transferir entre ambas computadoras. Primero se transfirió un archivo usando IPv4 y luego se hizo la prueba con IPv6. El archivo tiene tamaño de 6.89 GB. En la ilustración 38 se puede ver que la conexión fue exitosa.

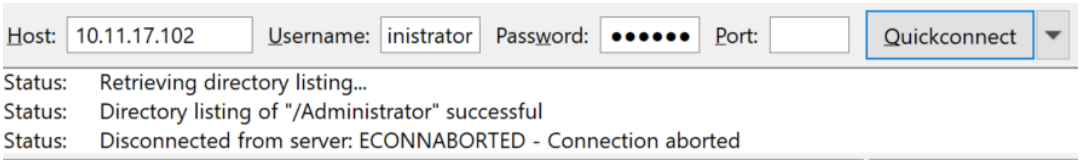


Ilustración 38 Conexión exitosa FTP FileZilla Ipv4

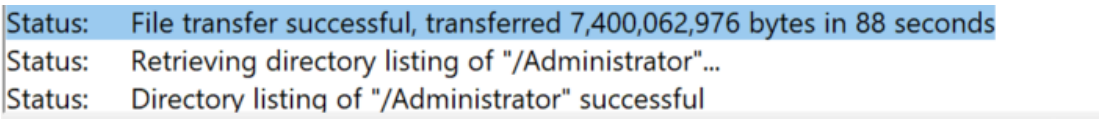


Ilustración 39 Transferencia FTP IPv4

En IPv4, el archivo fue transferido en 88 segundos.

Para IPv6, se hizo la misma prueba con el mismo archivo. En este caso la transferencia sólo duro 65 segundos, 23 segundos menos que en IPv4. En las ilustraciones siguientes se puede ver la conexión exitosa al servidor FTP y la transferencia.

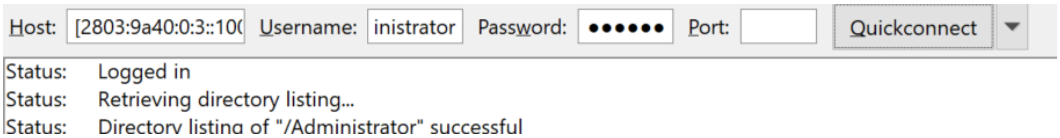


Ilustración 40 Conexión exitosa FTP FileZilla IPv6

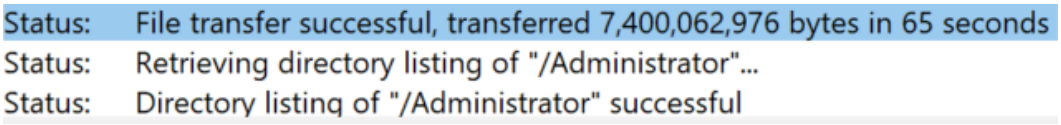


Ilustración 41 Transferencia FTP IPv6

4.3 Prueba de Carpeta Compartida

En esta prueba, se creó una carpeta para compartir sobre la red. Esta carpeta está localizada en el servidor y se llamó “Test1”. Dentro de la carpeta se puso un archivo llamado “IPv6.txt”.

En PC1 se montó la carpeta y se logra ver el archivo IPv6.txt. Para probar la carpeta compartida se le dio acceso al usuario para editar. Se creó otro archivo llamado Test2. Se verificó que el archivo está reflejado en el servidor.

4.3.1 Carpeta Compartida Ambiente Real

Al igual como en el ejemplo del FTP, se creó una carpeta compartida en el servidor Windows 2016. Esta carpeta se puso en el escritorio y se llamó Test_V6. En la ilustración 42, se puede ver la capeta Test_V6 montada usando IPv4 y IPv6.

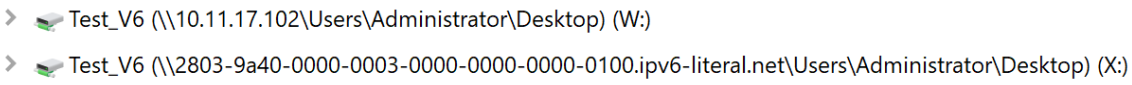


Ilustración 42 Carpeta Test_V6 con IPv4 y IPv6

La transferencia usando IPv4 duró aproximadamente 65s con una transferencia promedio de 108 MB/s.

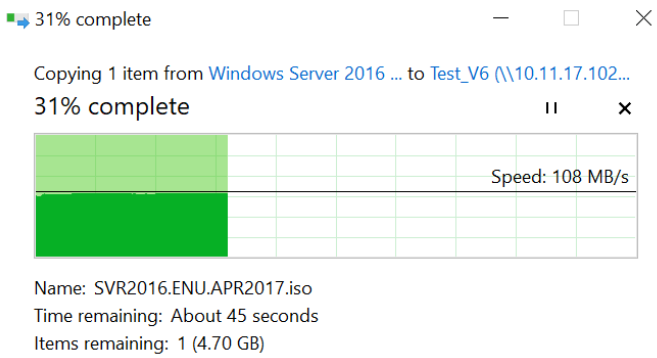


Ilustración 43 Transferencia IPv4 Carpeta Compartida

Con la prueba de IPv6, se obtuvieron los mismos resultados, no se pude ver una deferencia entre el tiempo y el promedio de transferencia.

Capítulo 5 Conclusiones

IPv6 fue creado en el año 1998 para poder enfrentar la crisis del agotamiento de IPv4. Aunque desde esa fecha hasta hoy, IPv6 todavía no ha ganado la popularidad que tiene IPv4. Hay muchos retos para que la adaptación de IPv6 sea aceptado globalmente, pero con el tiempo se ha incrementado el uso.

Aunque muchos consideran que IPv6 es un protocolo complicado, en realidad es más fácil usar IPv6 que IPv4. Como toda nueva tecnología el direccionamiento con IPv6 tiene su complejidad, pero sigue los mismos pasos que IPv4. El subneteo en IPv6 es mucho más fácil de aprender cuando uno no se enfoca en la dificultad del sistema hexadecimal. La asignación de IPv6's en una red puede hacerse con servidor DHCP o se puede hacer da manera dinámica usando SLAAC. La seguridad es mayor en la versión 6, al utilizar el protocolo de seguridad *Ipsec.*

Para las aulas de redes sería gran ventaja tener implementado IPv6, ya que la Universidad de Quintana Roo cuenta con la carrera de Ingeniería en Redes y el uso del direccionamiento con IPv6 es el futuro en la tecnología de redes. Aunque hasta el momento la Universidad no tenga conectividad a *Internet* usando IPv6, se puede crear una Intranet dentro de la Universidad y aprovechar las ventajas que aporta esta tecnología. La UQROO, perteneciendo a la región que es controlada por LACNIC, puede aplicar para direccionamiento IPv4 e IPv6 y luego formar vecinos usando el protocolo BGP.

Con las pruebas realizadas en el ambiente de producción, pude confirmar que IPv6 es mucho más fácil de implementar que IPv4. Al igual, transferencias entre equipos de cómputo son más rápidas que en IPv4. La Universidad cuenta con equipos que soportan IPv6 y tendría que hacer gastos adicionales mínimos para implementar el protocolo.

La experiencia al hacer la tesis fue única. IPv6 ha existido por muchos años, pero hoy en día todavía no existe mucha información sobre el tema. Bastante de la información que se encuentra es basada en IPv6 de hace 10 años o más, por suerte encontré un libro de Cisco del año 2017. Una de mis limitaciones fue el Hardware para poder correr GNS3 con sus accesorios. Aunque al principio pude utilizar mi computadora personal para configurar segmentos del laboratorio, no pude correr todas las computadoras el mismo tiempo. Para poder ejecutar en

todas las computadoras, implementé el sistema de GNS3 en un servidor localizado en mi trabajo, Central TV & *Internet*. Con el servidor pudo emular todas las computadoras necesarias sin usar recursos de mi computadora personal. Central TV & *Internet* ahora usa el sistema que implementé para hacer pruebas de redes y hacer tutoriales para nuevos empleados.

La tesis no fuera posible sin la experiencia que obtuve en las clases de la Universidad. Gracias a las asignaturas de redes pude configurar e implementar los routers y switches en la emulación. Usando la información que obtuve en Administración de Sistemas basados en Windows y Linux pude configurar las computadoras con sistemas operativos como Windows Server y Ubuntu. Mi enfoque fue usar el conocimiento impartido en las clases y reemplazarlo usando el protocolo de IPv6. En conclusión, mis experiencias prácticas durante los estudios universitarios me han permitido obtener los resultados en esta tesis.

Referencias

[1] LACNIC, «Lacnic,» [En línea]. Available: http://www.lacnic.net/en/web/lacnic/agotamiento-ipv4. [Último acceso: 13 febrero 2016].

[2] IPv6.com, «IPv6 – The History and Timeline,» 10 febrero 2006. [En línea]. Available: https://www.ipv6.com/general/ipv6-the-history-and-timeline/. [Último acceso: 2 febrero 2018].

[3] R. Graziani, IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6, vol. 2, Indianapolis: Cisco Press, 2017.

[4] What Is My IP Addess, «CIDR Notation,» [En línea]. Available: https://whatismyip*address*.com/cidr. [Último acceso: 3 febrero 2018].

[5] T. Podermanski, «http://6lab.cz,» [En línea]. Available: http://6lab.cz/live-statistics/. [Último acceso: 2018].

[6] Oracle, «docs.oracle.com,» Oracle, [En línea]. Available: https://docs.oracle.com/cd/E18752_01/html/816-4554/ipv6-ref-2.html.

[7] ComputerNetworkingNotes, «IPv6 *Address* Types & Format Explained with Examples,» https://www.computernetworkingnotes.com/ip-tutorials/ipv6-*address*-types-format-explained-with-examples.html, 18 enero 2018. [En línea]. [Último acceso: 15 febrero 2018].

[8] C. Schroder, «Calculating IPv6 Subnets in Linux,» 26 octubre 2017. [En línea]. Available: https://www.linux.com/learn/intro-to-linux/2017/10/calculating-ipv6-subnets-linux. [Último acceso: 15 febrero 2018].

[9] ARIN, «ARIN Number Resource Policy Manual,» 18 enero 2018. [En línea]. Available: https://www.arin.net/policy/nrpm.html#six41. [Último acceso: 15 febrero 2018].

[10] S. Hagen, IPv6 Essentials Integrating IPv6 Into Your IPv4 Network, Sebastopol: O'Reilly Media, 2014.

[11] ComputerNetworkingNotes, « ComputerNetworkingNotes,» 18 01 2018. [En línea]. Available: https://www.computernetworkingnotes.com/ip-tutorials/ipv6-neighbor-discovery-protocol-explained.html.

[12] T. Coffeen, «SLAAC-to-Basics (Part 2 of 2: Configuring SLAAC),» HexaBuild, 31 10 2017. [En línea]. Available: https://community.infoblox.com/t5/IPv6-CoE-Blog/SLAAC-to-Basics-Part-2-of-2-Configuring-SLAAC/ba-p/11646. [Último acceso: 07 05 2018].

[13] D. Bombal y J. Duponchelle, «Getting Started with GNS3,» GNS3, 18 August 2018. [En línea]. Available: https://docs.gns3.com/1PvtRW5eAb8RJZ11maEYD9_aLY8kkdhgaMB0wPCz8a38/index.html. [Último acceso: 10 October 2018].

Apéndices