Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería de Mecánica Eléctrica

PROPUESTA DE DISEÑO DEL MÓDULO DE IPv6 BÁSICO DEL LABORATORIO DE TELECOMUNICACIONES Y REDES LOCALES DE LA ESCUELA DE INGENIERÍA MECÁNICA ELÉCTRICA, FACULTAD DE INGENIERIA, UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Alejandra María Morales Cifuentes
Asesorada por la Inga. Ingrid Salomé Rodríguez de Loukota

Guatemala, julio de 2018

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

PROPUESTA DE DISEÑO DEL MÓDULO DE IPv6 BÁSICO DEL LABORATORIO DE TELECOMUNICACIONES Y REDES LOCALES DE LA ESCUELA DE INGENIERÍA MECÁNICA ELÉCTRICA, FACULTAD DE INGENIERÍA, UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

ALEJANDRA MARÍA MORALES CIFUENTES
ASESORADA POR LA INGA. INGRID SALOMÉ RODRÍGUEZ DE LOUKOTA

AL CONFERÍRSELE EL TÍTULO DE

INGENIERA EN ELECTRÓNICA

GUATEMALA, JULIO DE 2018

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Pedro Antonio Aguilar Polanco
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de León Rodríguez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Oscar Humberto Galicia Nuñez
VOCAL V	Br. Carlos Enrique Gómez Donis
SECRETARIA	Inga. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADOR	Ing. José Antonio de León Escobar
EXAMINADOR	Ing. Guillermo Antonio Puente Romero
EXAMINADOR	Ing. Sergio Leonel Gómez Bravo
SECRETARIA	Inga. Lesbia Magalí Herrera López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

PROPUESTA DE DISEÑO DEL MÓDULO DE IPv6 BÁSICO DEL LABORATORIO DE TELECOMUNICACIONES Y REDES LOCALES DE LA ESCUELA DE INGENIERÍA MECÁNICA ELÉCTRICA, FACULTAD DE INGENIERÍA, UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 2 de agosto de 2017.

Alejandra María Morales Cifuentes

Guatemala 12 de febrero de 2018

Ingeniero
Julio Cesar Solares Peñate
Coordinador del Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Apreciable Ingeniero Solares.

Me permito dar aprobación al trabajo de graduación titulado **¨Propuesta de diseño del módulo de IPv6 básico del laboratorio de Telecomunicaciones y Redes Locales de la Escuela de Ingeniería Mecánica Eléctrica, Facultad de Ingeniería, Universidad de San Carlos de Guatemala¨**, de la señorita **Alejandra María Morales Cifuentes**, por considerar que cumple con los requisitos establecidos.

Por tanto, el autor de este trabajo de graduación y, yo, como su asesora, nos hacemos responsables por el contenido y conclusiones del mismo.

Sin otro particular, me es grato saludarle.

Atentamente,

Inga. Ingrid Rodríguez de Loukota
Colegiada 5,356
Asesora

Ingrid Rodríguez de Loukota
Ingeniera Electrónica
Colegiado 5356

NIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 26.2018.
19 DE ABRIL 2018.

Señor Director
Ing. Otto Fernando Andrino González
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: : PROPUESTA DE DISEÑO DEL MÓDULO IPv6 BÁSICO DEL LABORATORIO DE TELECOMUNICACIONES Y REDES LOCALES DE LA ESCUELA DE INGENIERÍA DE MECÁNICA ELÉCTRICA, FACULTAD DE INGENIERÍA, UNIVERSIDAD DE SAN CARLOS DE GUATEMALA, de la estudiante; Alejandra María Morales Cifuentes, que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

Ing. Julio César Solares Peñate
Coordinador de Electrónica

NIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 26.2018.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen el Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación de la estudiante: ALEJANDRA MARÍA MORALES CIFUENTES titulado: PROPUESTA DE DISEÑO DEL MÓDULO IPv6 BÁSICO DEL LABORATORIO DE TELECOMUNICACIONES Y REDES LOCALES DE LA ESCUELA DE INGENIERÍA DE MECÁNICA ELÉCTRICA, FACULTAD DE INGENIERÍA, UNIVERSIDAD DE SAN CARLOS DE GUATEMALA, procede a la autorización del mismo.

Ing. Otto Fernando Andrino González

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

GUATEMALA, 3 DE MAYO 2018.

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 246.2018

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **PROPUESTA DE DISEÑO DEL MÓDULO DE IPv6 BÁSICO DEL LABORATORIO DE TELECOMUNICACIONES Y REDES LOCALES DE LA ESCUELA DE INGENIERÍA MECÁNICA ELÉCTRICA, FACULTAD DE INGENIERÍA, UNIVERSIDAD DE SAN CARLOS DE GUATEMALA,** presentado por la estudiante universitaria: **Alejandra María Morales Cifuentes,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

Ing. Pedro Antonio Aguilar Polanco
Decano

Guatemala, julio de 2018

/gdech

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

ACTO QUE DEDICO A:

Dios	Por ser el pilar de mi vida, la fuente y fin de todo lo que hago, y por las infinitas bendiciones que le ha dado a mi vida.
Mi padre	Manuel Morales, por ser esa fortaleza, esa torre inquebrantable que me protege y me cuida. Por forjar en mi perseverancia, lucha y sentido de justicia.
Mi madre	Lorena Cifuentes, por ser luz en mi vida, aquella gota de esperanza cuando sentía rendirme, por forjar en mí bondad, confianza y un espíritu libre en busca de la verdad.
Mi hermano	Manuel Morales Cifuentes, por ser mi cómplice, mi mejor amigo de toda la vida, mi compañero más leal, por siempre tener para mí una palabra de aliento.
Mi novio	Javier Rodríguez, por llenarme con su luz y su amor, por mostrarme que soy capaz de lograr cada cosa que me proponga, por escucharme y ser la persona que me alienta a seguir adelante.

Mis abuelos Carmen Gómez y Juan Cifuentes, por ser parte importante de mi vida, por su apoyo y su gran amor. Ana María González y Mario Antonio Morales, por ser mis ángeles protectores.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala — Por ser mi *alma mater*, por la oportunidad de poder realizar mis estudios en tan prestigiosa universidad.

Mis padres — Por todo su sacrificio, apoyo incondicional y por brindarme los más sabios consejos. Este triunfo también es suyo.

Javier Rodríguez — Por todo su apoyo y ayuda en la realización de este trabajo, por brindarme su tiempo y siempre estar allí cuando lo necesito.

Mis padrinos — Anneliese de Escobar y Juan José Escobar, por siempre estar a mi lado en cada paso de mi vida y por estar presentes en cada meta lograda.

Ing. Ingrid de Loukota

Por su tiempo y asesoramiento en la realización de este trabajo, por su dedicación y entrega en los cursos que imparte en la Facultad.

Mi familia

Tíos, tías, primos, primas y sobrinos, porque cada uno ha aportado un granito de arena a mi vida, por recibir siempre muestras de cariño afecto y apoyo.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

AFRINIC African Network Information Center, es el Registrador Regional de Internet para África.

AH Authentication Header, protocolo que autentica el origen de paquetes IP y garantiza la integridad de los datos.

APNIC Asia Pacific Network Information Centre, es el Registrador Regional de Internet para la región de Asia-Pacífico.

ARIN American Registry for Internet Numbers, es el Registro Regional de Internet Anglosajona, varias islas de los océanos Pacífico y Atlántico.

ARPANET Advanced Research Projects Agency Network, redes creadas por encargo del Departamento de Defensa de los Estados Unidos.

AS Autonomous System, es un grupo de redes IP que poseen una política de rutas propias e independientes.

Bit Binary digit, es un dígito del sistema de numeración binario.

Byte	Conjunto ordenado de bits, generalmente ocho.
CIDR	Classless Inter-Domain Routing, es un esquema de direcciones IP sin tomar en cuenta las clases.
DNS	Domain Name System, es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP.
ESP	Encapsulating Security Payload, es un protocolo que provee autenticación, integridad y confidencialidad de los paquetes de datos de la red.
Flooding	Algoritmo donde se envían todos los paquetes entrantes por cada interfaz de salida.
Forwarding	Acción de redirigir puertos de red de un nodo de red a otro.
Host	Punto de inicio y final de las transferencias de datos.
IANA	Internet Assigned Numbers Authority, entidad que supervisa la asignación global de direcciones IP, sistemas autónomos, DNS, entre otros.
IIS	Internet Information Services, es un servidor web y un conjunto de servicios para el sistema operativo Microsoft Windows.

IP	Internet Protocol, protocolo principal de comunicación que proporciona la entrega de paquetes sin conexión no fiable para Internet.
IS-IS	Intermediate System to Intermediate System, protocolo de estado de enlace, maneja una especie de mapa con el que se fabrica a medida que converge la red.
ISP	Internet Service Provider, servicio que permite conectarse a Internet.
LACNIC	Latin American & Caribbean Network Information Centre, es el Registro Regional de Internet para América Latina y el Caribe.
Loopbacks	Interfaz de red virtual.
Multicast	Envío de información en múltiples redes a múltiples destinos simultáneamente.
NAT	Network Address Translation, mecanismo utilizado por *routers* IP para intercambiar paquetes entre dos redes que asignan direcciones incompatibles.
NDP	Neighbor Discovery Protocol, protocolo de Internet de la capa dos usado en IPv6; reconoce equipos vecinos en la red.

Next hop	Siguiente enrutador más cercano por el cual un paquete puede pasar.
Nibble	Conjunto de cuatro dígitos binarios o medio octeto.

RESUMEN

Actualmente, cada día aumenta la demanda de dispositivos que requieren acceso a Internet, por lo que requieren de una dirección IP, sin embargo, el protocolo actual no es suficiente para cubrir esta demanda y se da la necesidad de crear un nuevo protocolo capaz de cubrir y de prever el aumento de dispositivos.

Este nuevo protocolo implica el debido estudio para su correcta configuración e implementación, y de la forma adecuada en cómo debe realizarse la transición de IPv4 a IPv6. De igual forma, es importante recordar que existen servicios a los cuales se puede acceder a través de Internet, como lo son servidores WEB, DNS, NTP, entre otros, y que, por lo tanto, deben ser configurados para que puedan trabajar bajo el nuevo protocolo.

El laboratorio de telecomunicaciones y redes fue implementado hace algunos años, enseña los conceptos fundamentales en el manejo de redes bajo el protocolo de IPv4. Por esta razón, surge la necesidad de la propuesta de agregar un nuevo módulo para este laboratorio, con el objetivo de brindarle al estudiante el conocimiento básico de IPv6, presentando de manera breve y concisa la fases de agotamiento de IPv6, seguido de los mecanismos de transición, el protocolo de IPv6, la forma de ruteo, los tipos de servicios y finalmente una guía metodológica que incluya contenido teórico, ejemplos y prácticas propuestas, para que el estudiante inicie su aprendizaje del protocolo.

OBJETIVOS

General

Presentar una propuesta de diseño para el módulo de IPv6 Básico para el Laboratorio de Telecomunicaciones y Redes Locales de la Escuela de Ingeniería Mecánica Eléctrica.

Específicos

1. Dar a conocer las organizaciones e instituciones a nivel mundial que se encargan de administrar las direcciones asignadas en cada región y las peticiones de comentario al crear los estándares y generalidades de IPv6.

2. Detallar los métodos de transición a IPv6 existentes, la forma en la que se manejan y en que situaciones es conveniente utilizarlos mediante un estudio previo de la red.

3. Dar a conocer los diferentes tipos de configuración de ruteo en IPv6 y de los diversos servicios en IPv6 que pueden brindarse a través de este protocolo.

4. Proponer una guía metodológica para el óptimo aprendizaje del estudiante con el nuevo módulo de IPv6 básico mediante la cual tenga acceso a toda la información esencial para el conocimiento del protocolo.

INTRODUCCIÓN

En 1969 gracias al inicio de ARPANET (Red de la Agencia de Proyectos de Investigación Avanzada) se realizan las primeras definiciones con las cuales llega a crearse el Internet, siendo un esquema de conexión de una red descentralizada con múltiples caminos entre dos puntos. Dado el proceso, en 1981 se definió el protocolo de internet IPv4 (RFC791).

Sin embargo, hacia el año de 1990 se realizaron los primeros estudios sobre el agotamiento de direcciones de IPv4 (4,3 millones de direcciones) debido a que la explotación comercial estaba dando un incremento enorme de entradas de ruteo. Como consecuencia para el año de 1997 ya existían más de 26 millones de *host* conectados. Por lo tanto, cualquier dispositivo que quiera enviar o recibir datos en internet debe tener una dirección IP, esto ocasionó que el número de usuarios conectados incrementara exponencialmente dando como resultado un agotamiento de direcciones de IPv4, siendo insuficientes ante la demanda.

Debido a la problemática de agotamiento de direcciones y al aumento de dispositivos capaces de conectarse a Internet, se crea en 1998 el protocolo de Internet IPv6 definido en la RFC2468 con una capacidad de 3.4×10^{38} de direcciones. Este nuevo protocolo previene el crecimiento de la red, se realiza una configuración más simplificada y facilita la complejidad de la red.

Dada esta nueva forma de configuración, surge la necesidad de implementar un nuevo módulo para el laboratorio de Telecomunicaciones y Redes Locales, para abordar los temas básicos de IPv6 para que los estudiantes se familiaricen con este nuevo protocolo, capacitándolos para afrontar los retos laborales que se les presenten.

1. CONCEPTOS BÁSICOS

Internet es una red mundial de computadoras conectadas por diferentes medios a través de satélites, fibra óptica, líneas telefónicas, entre otros. Esto permite que millones de usuarios puedan estar conectados a esta red y así poder intercambiar, extraer o introducir información. El protocolo de Internet (IP) es el soporte lógico para controlar el sistema de redes, especificando el proceso de cómo encaminar la información desde un equipo emisor hasta un equipo receptor.

1.1. Historia del Internet

En el año de 1969 inicia lo que se conoce como ARPANET, que no es más que un sistema de comunicación y control distribuido con fines militares. Su principal objetivo era crear un esquema de conexión de una red descentralizada con múltiples caminos entre dos puntos. Este inicio de esquema fue transformándose hasta lo que se conoce actualmente como Internet.

En 1981 se realiza la petición de comentario (RFC) 791, en donde se define el protocolo IPv4 con dos funciones básicas: la fragmentación, permitiendo el envío de paquetes de información de mayor tamaño, los cuales no eran soportados por los enlaces debido al límite de tráfico establecido, mediante la división de paquetes de información más pequeños; y el direccionamiento, permitiendo identificar el destino y origen de los paquetes de información gracias a un encabezado del protocolo en donde se almacena la dirección.

Inicialmente ARPANET trabajaba con distintos protocolos de comunicación, pero a medida que aumentaba el número de *hosts*, en el año 1983 adoptaron finalmente el protocolo TCP/IP para su utilización absoluta, permitiendo el crecimiento ordenado de la red junto con la eliminación de restricciones que presentaban los protocolos anteriores. Sin duda alguna, este protocolo demostró ser una versión bastante robusta y de fácil implementación, sin embargo, no previó el significativo incremento exponencial de las redes, lo que iba a generar el agotamiento de las direcciones IP, así también el crecimiento de las tablas de enrutamiento, problemas de seguridad y prioridad de entregas de determinados paquetes. Por lo que en 1990 se realizan los primeros estudios sobre el agotamiento de IPv4 y las posibles soluciones a utilizar para solventar este problema. En 1992 ya existían aproximadamente 1 millón 130 mil *hosts* conectados a la red, y en 1997 el número de *hosts* había aumentado a los más de 26 millones. Ante estas circunstancias, en 1998 se define por el RFC 2468 un nuevo protocolo, llamado IPv6, capaz de solventar todos los inconvenientes de la versión 4.

1.2. Jerarquía de asignación de direcciones

La asignación de direcciones IP lleva un sistema jerárquico formando un árbol invertido, en donde la parte más alta de este sistema la ocupa IANA (Internet Assigned Numbers Authority) que es el organismo responsable de los recursos numéricos de Internet, direcciones IP y los números de sistemas autónomos. La IANA asigna todos estos recursos a las RIR, según sus necesidades y políticas globales.

Las RIR (Regional Internet Registry) son las organizaciones sin ánimo de lucro basadas en un sistema de membresía. Existen cinco RIR cubriendo cada una de las regiones geográficas: LACNIC (Latin American and Caribbean IP

Address Regional Registry), ARIN (American Registry for Internet Numbers), RIPE NCC (RIPE Network Coordination Centre), APNIC (Asia Pacific Network Information Centre) y AFRINIC (African Network Information Centre). Cada RIR es distinta, todas reciben cantidades distintas de direcciones, tienen distintos ritmos de consumo y cada una maneja distintas políticas. Estas RIR a su vez asignan a un NIR (National Internet Registry), encargado de asignar direcciones en cada país y a las ISP (Proveedor de Servicios de Internet), que finalmente proporcionan servicio a los usuarios finales, es decir los clientes.

- LACNIC

LACNIC es el RIR encargado de asignar direcciones en la región de América Latina y el Caribe. Es una organización no gubernamental ubicada en Uruguay en el año 2002 y es responsable de la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), Números Autónomos y Resolución Inversa, entre otros.

1.3. Protocolo de IPv4

La cabecera IP determina el número de bits utilizados para codificar la dirección IP. Está definida en el RFC 791, en donde utiliza direcciones de 32 bits que la limitan a 4 294 967 296 direcciones únicas utilizables.

- Direcciones y espacio disponible

Estas direcciones están divididas en 256 prefijos /8, cada uno contiene 16 777 216 direcciones IPv4 únicas. De estos /8, 35 078 direcciones están reservadas a diferentes usos como *multicast*, identificadores locales, *loopbacks*,

usos privados o bien para usos futuros no especificados. El resto de direcciones prefijo /8 están disponibles para ser usadas en la Internet IPv4 pública.

Debido a que el número de bits en las direcciones de este protocolo es de 32, está limitado a aproximadamente 4,3 millones de direcciones. Estas direcciones, en una política inicial, están distribuidas en diferentes tipos: Clase A reservada para Gobierno, Clase B, Clase C y las direcciones reservadas. Esta forma de distribución solo ocasionó el poco aprovechamiento y mala distribución de las direcciones. Debido al incremento exponencial del Internet, en 1992 se crea el grupo ROAD (Routing and Addressing), el cual crea el CIDR definido en RFC 4632, que no es más que la utilización de bloques sin pensar en las clases, solo es necesario utilizar pequeños prefijos de tamaños apropiados y así aprovechar de mejor manera el número de direcciones, y poner fin al uso de clases.

1.4. Protocolo IPv6

La cabecera IP determina el número de bits utilizados para codificar la dirección IP. Está definida en el RFC 2468, en donde utiliza direcciones de 128 bits.

- Direcciones y espacio disponible

Debido a los estudios realizados sobre el agotamiento de IPv4, en 1998 se define en el RFC 2468 el protocolo IPv6 y se aumenta los bits de direccionamiento de 32 a 128, teniendo un cabezal base más simplificado junto con cabezales de extensión, incluye ahora un identificador de flujos de datos (QoS), realiza la fragmentación y reensamblaje de paquetes de origen y destino, y no en puntos intermedios como en IPv4, no se requiere de NAT, se

crean mecanismos que facilitan la configuración de la red y, sobre todo, prevé el crecimiento de la red. Gracias a que el número de bits aumentó a 128 el número de direcciones únicas de igual forma creció, teniendo una capacidad de aproximadamente $3{,}4 \times 10^{38}$ de direcciones. Todo el espacio de IPv6 se divide en 8 partes, de las cuales una pequeña parte del espacio se utiliza para asignaciones. Esta octava se divide en /32 y se asignó a cada RIR en octubre de 2006.

1.5. Fases de agotamiento

Enfocándose en LACNIC, por ser el RIR que administra la región latinoamericana, cuando se entra en una fase de agotamiento se hace referencia a que se inicia una etapa de reservas en que las asignaciones se van limitando en tamaño y periodicidad. Estas restricciones se definieron en las políticas presentadas por la comunidad en el Foro Público de Políticas. La finalización del protocolo IPv4 comprende 4 etapas fundamentales.

- Fase 0

Esta fase tuvo inicio en octubre de 2013 y se realizaron las asignaciones de recursos hasta alcanzar el último /9 disponible. Por esta misma razón se tenían disponibles 8 388 608 direcciones.

- Fase 1

Esta fase tuvo inicio el 19 de mayo de 2014 y se alcanzó el último /9, incluyendo los dos /10 reservados para la terminación gradual de IPv4 y para nuevos integrantes. La cantidad de direcciones a asignar era menor a 8 388 608.

- Fase 2

Esta fase tuvo inicio el 10 de junio de 2014 y se asignó el último bloque /10, es aquí donde se activa el punto 11.2 de Manual de Políticas, en el que se reserva un bloque /10 para terminación gradual, hasta este punto el número de direcciones disponibles era menor a 4 194 304.

- Fase 3

Esta fase tuvo inicio el 15 de febrero de 2017 y terminará cuando se asigne el último bloque /10 de terminación gradual y será la última reserva que asigne LACNIC, está compuesto por bloques recuperados y devueltos y por bloques postagotamiento asignados por la IANA. Solo se le asignará a miembros nuevos entre un /22 y un /24.

2. MECANISMOS DE TRANSICIÓN

Al momento de querer realizar la transición se debe tener presente que IPv4 e IPv6 son protocolos incompatibles, esto con el fin de agregarle mejorías al protocolo. En el momento de querer migrar de IPv4 a IPv6, se debe buscar la mejor manera de transición tomando en cuenta la coexistencia con IPv4, por lo que debe permitirse una transición amigable con IPv4 sin interferir con el funcionamiento de IPv4, así que se persiguen dos objetivos: la conectividad IPv6 en las redes y solucionar la escasez de IPv4. Para realizar esta transición se pueden seguir ciertas vías generales:

- IPv6 debe coexistir con IPv4.
- Se debe seguir el mismo esquema que IPv4.
- Se debe realizar cualquiera de las tres estrategias: IPv6 nativo, túneles o traducción.
- Tomar en cuenta que cada caso es distinto (debido a que cada red podrá ser manejada con distinta estrategia).

Existen tres mecanismos para realizar la transición a IPv6, los cuales pueden utilizarse de manera combinada:

- IPv6 Nativo, el cual utiliza la cabecera de IPv6 desde origen hasta destino, y puede tener dos opciones: *dual-stack* (doble pila) o solo IPv6.
- Túneles, el cual consiste en encapsular una versión en otra.
- Traducción, la cual logra realizar la comunicación entre dos *host* que solo hablen una versión, con diferente versión IP.

2.1. IPv6 Nativo

Paquete IPv6 nativo usando la cabecera IPv6 desde origen hasta destino, por lo que toda la red, tanto del proveedor como del cliente, debe ser puramente con IPv6. Este es el mecanismo de transición recomendado, debido a que IPv6 no se encuentra encapsulado ni se utiliza traducción.

Entre las ventajas de optar por este mecanismo se encuentra el esquema de la red, el direccionamiento, la monitorización queda establecida de manera definitiva, sin quedar pendientes posteriores a cambios, y sobre todo que el paso a IPv6 se realiza en una sola etapa, mientras que el resto de los métodos son de carácter temporal. La importancia hay al trabajar solamente con IPv6 es que la cantidad de direcciones IPv4 es insuficiente, por lo que se aumenta la disponibilidad de direcciones con IPv6, de igual forma, con IPv6 se puede realizar una gestión más fácil, se crean granjas de servidores solo IPv6 con *front-end*, y es una implementación válida para siempre.

Sin embargo, surge un inconveniente: no se puede permitir contenidos solo IPv4 a los nodos en red, solamente IPv6. Debido a esto, se crea ciertas soluciones que pueden ser implementadas y que se entrelazan con los demás mecanismos de transición:

- DS-LITE (túneles): permiten ofrecer IPv4 a los usuarios finales.
- NAT64/DNS64, 464XLAT: que son soluciones de traducción, pero incompletas.

A medida que IPv6 crezca y se vaya implementando en más dispositivos, este inconveniente desaparecerá.

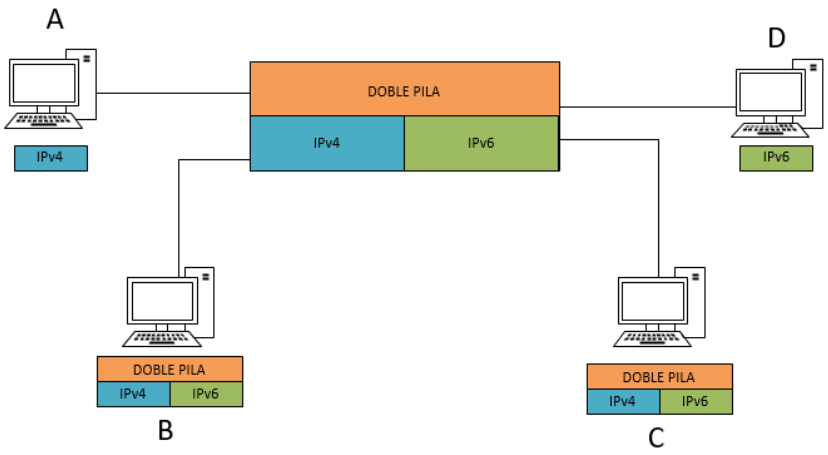
2.2. Doble pila

Con este mecanismo tanto IPv4 como IPv6 pueden funcionar simultáneamente, es decir en paralelo, por lo que habrá una red que maneje puramente el protocolo IPv4 y, por otro lado, una red que maneje puramente el protocolo IPv6 en donde el cliente será el encargado de decidir qué protocolo utilizar.

Este mecanismo es la opción más amigable con IPv4 y permite una transición gradual hacia IPv6. Por defecto se le dará preferencia a IPv6 sobre IPv4. Sin embargo, este esquema se vuelve más complejo y costoso, ya que aumenta la cantidad de recursos, se debe realizar una doble configuración y seguridad.

En la figura 1 se muestra un pequeño ejemplo de cómo se manejaría doble pila, en esta red que se llamará RED1 se cuenta con 4 computadoras nombradas A,B,C,D. Se supone que cada computadora ingresa a una página web, está página está montada en un servidor que maneja doble pila, es decir maneja el protocolo IPv4 e IPv6.

Figura 1. **Doble pila**



Fuente: elaboración propia.

El protocolo a utilizar lo decidirá la máquina cliente, así que el *host* A, que solo trabaja con el protocolo IPv4, realiza la conexión bajo este protocolo y guardará esta información para futuras conexiones. Por otro lado, el *host* D solamente trabaja bajo el protocolo IPv6, por lo que realiza la conexión bajo este protocolo. Y, finalmente, los *hosts* B y C trabajan bajo ambos protocolos, así que realizarán la conexión bajo el protocolo IPv6, debido a que este tiene prioridad mayor sobre IPv4.

2.3. Túneles

Este mecanismo consiste en encapsular una versión IP en otra, con el objetivo de atravesar una red que no soporte IPvX, pudiendo ser que IPv4 se encapsule en IPv6, o bien que IPv6 se encapsule en IPv4. Los túneles pueden ser, dependiendo de cómo se configuren:

- Estáticos: cuando se configuran de manera estática los extremos del túnel, que es como normalmente se realiza.

- Automáticos: cuando su configuración o parte de esta se establece en manera automática.

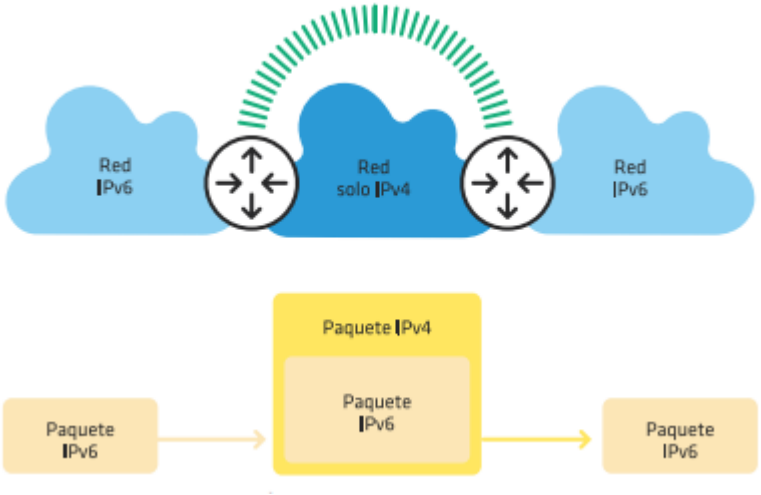
O bien dependiendo de cómo se conectan:

- Punto a punto: cuando solamente se conectan dos puntos de red, es decir dos interfaces de túnel, en un extremo se encapsulan y en el otro se desencapsulan.
- Multipunto: en donde se conectan varios puntos de red o interfaces de túneles de forma que un paquete que entra en el túnel se encapsula y puede ser entregado en uno de los varios puntos de salida del túnel.

En la práctica se pueden encontrar los siguientes túneles:

- 6in4: este encapsula IPv6 en IPv4, es un túnel estático, punto a punto y de configuración manual. Esta configuración consiste en definir las direcciones IPv4 de origen y destino utilizadas en cada extremo del túnel. Este tipo de túnel puede ser utilizado para evitar que un equipo, o bien un enlace que no soporte IPv6, quede sin poder comunicarse, o bien para interconectar dos redes IPv6, las cuales atraviesan Internet IPv4.

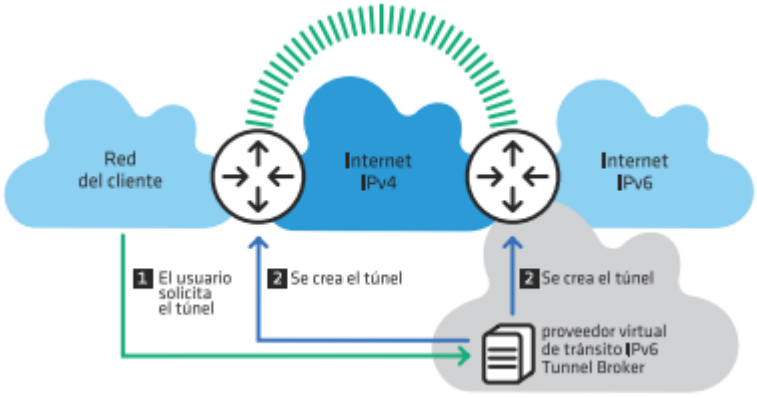
Figura 2. **Túnel 6IN4**



Fuente: MOREIRAS, Antonio. *IPv6 operadores de red.* P. 66

- *Broker*: parecido al 6in4, solo que cierta parte del proceso se automatiza configurando un servidor de túneles. Este puede ser considerado como un proveedor de acceso IPv6 virtual. Para su uso es necesario ingresar a un sitio web y crear una cuenta para solicitar el servicio. Una vez aprobado el servicio el proveedor lo configura en un servidor de túneles y se envian las instrucciones para que el usuario pueda configurar su extremo del túnel. Al configurarlo correctamente, el túnel logra quedar establecido y es ahí cuando puede proveer conectividad IPv6 sobre la Internet IPv4.

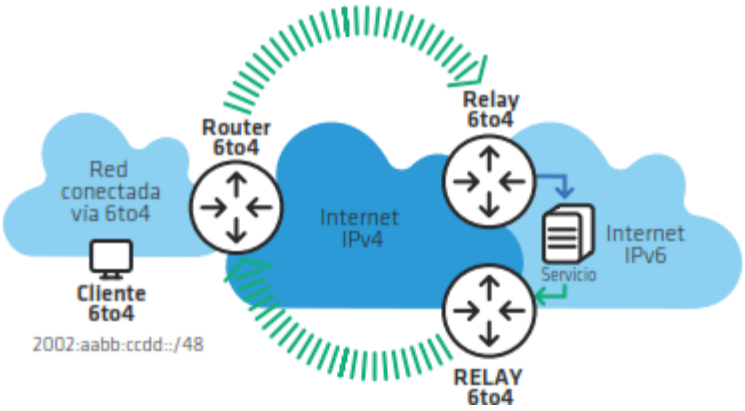
Figura 3. **Túnel *broker***



Fuente. MOREIRAS, Antonio. *IPv6 operadores de red.* P. 67

- 6to4: encapsula IPv6 en IPv4, es un túnel automático, multipunto y con un prefijo reservado para su configuración: 2002::/16, al cual se le incluyen los 32 bits de dirección IPv4, por lo que necesita un dirección pública IPv4. Se tienen tres elementos elementales: clientes 6to4, los *routers* 6to4 y los *relays* 6to4. Por clientes se hace referencia a las computadoras conectadas a una red que utiliza este tipo de túnel y que quiere conectividad IPv6, un *router*, por su lado, se refiere a aquel dispositivo que en la red del cliente oficia como extremo del túnel y debe tener una dirección IPv4 válida. Por lo que el otro extremo del túnel lo proveen los *relay*, que son *routers* con conectividad nativa IPv4 e IPv6. En modo de funcionamiento: el *router* encuentra el *relay* más cercano, gracias al envío a la dirección IPv4 *anycast* (192.88.99.1), este *relay* desencapsula el paquete y lo envía a su destino en la Internet IPv6. Luego el destino enruta la respuesta del *relay* más próximo, el cual es el *router* para 2002::/16, el cual encapsula nuevamente el paquete y lo envía al *router* cuya dirección IPv4 es parte de la dirección IPv6 de destino.

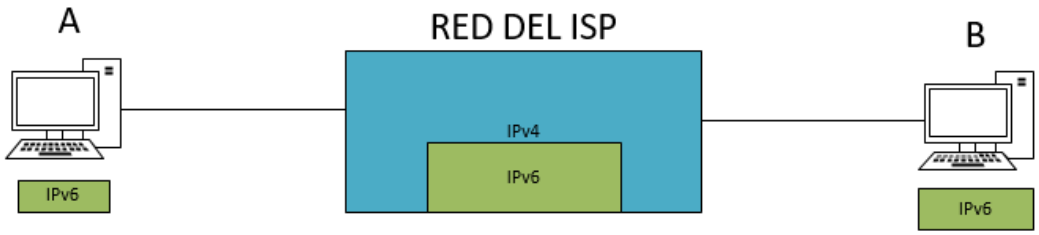
Figura 4. **Túnel 6to4**



Fuente. MOREIRAS, Antonio. *IPv6 operadores de red.* P. 68

- 6RD: parecido a 6to4, solo que puede configurarse con direcciones IPv4 privadas y no necesita un prefijo reservado. Con esta técnica se resuelven los problemas de asimetría y de falta de control sobre los *relays* utilizados en la red.

Figura 5. **Diagrama general de un túnel**



Fuente: elaboración propia.

En la figura 5 se observa un diagrama de lo que sería el mecanismo de túneles, como ejemplo se tomará el esquema en el cual dos *hosts*: el *host* denominado como A y el *host* denominado como B, quieren establecer una comunicación entre ellos. Estos dos host manejan solamente IPv6, el problema radica en que la red del ISP, por la cual se transmite la información, solamente

tiene la capacidad de trabajar con IPv4, por lo que se necesita de un *router* que realice el encapsulamiento de IPv6 en IPv4 y luego que desencapsule IPv6 de IPv4. Con esto, los dos *hosts* que solo hablan IPv6 pueden comunicarse a través de una red que solo habla IPv4.

2.4. Traducción

Este mecanismo es necesario para comunicar 2 *hosts* que solo hablen una versión diferente de IP, es el método menos recomendado, pero se utiliza cuando un *host* solo maneja un protocolo, es decir cuando es necesaria lo comunicación entre un nodo solo IPv6 y un solo IPv4, en cualquiera de los dos sentidos. Sin embargo, en la práctica solo se encontrará traducciones de IPv6 a IPv4. Este mecanismo solo debe usarse si no es posible la configuración en doble pila o túneles.

Figura 6. **Traducción**

Fuente: elaboración propia.

En la figura 6 se muestra un esquema del mecanismo de traducción, se tiene un *host* que solamente maneja el protocolo de IPv6, este *host* quiere acceder a Internet, específicamente a una página web que solamente trabaja baja el protocolo IPv4, sin embargo, el ISP que se encarga de brindarle el servicio de Internet al *host* trabaja también bajo el protocolo de IPv6, por lo que

la comunicación entre toda la red del ISP hacia el *host* trabaja sin ningún tipo de problema. Debido a que el *host* desea comunicarse con una página web que solamente trabaja con el protocolo IPv4, se necesita un *router* que realice un NAT en el extremo entre el ISP e Internet, este NAT realizará la traducción de la dirección IPv6 que tiene asignado el *host* y la convertirá en una dirección IPv4 que permitirá que el *host* finalmente pueda acceder a la página web.

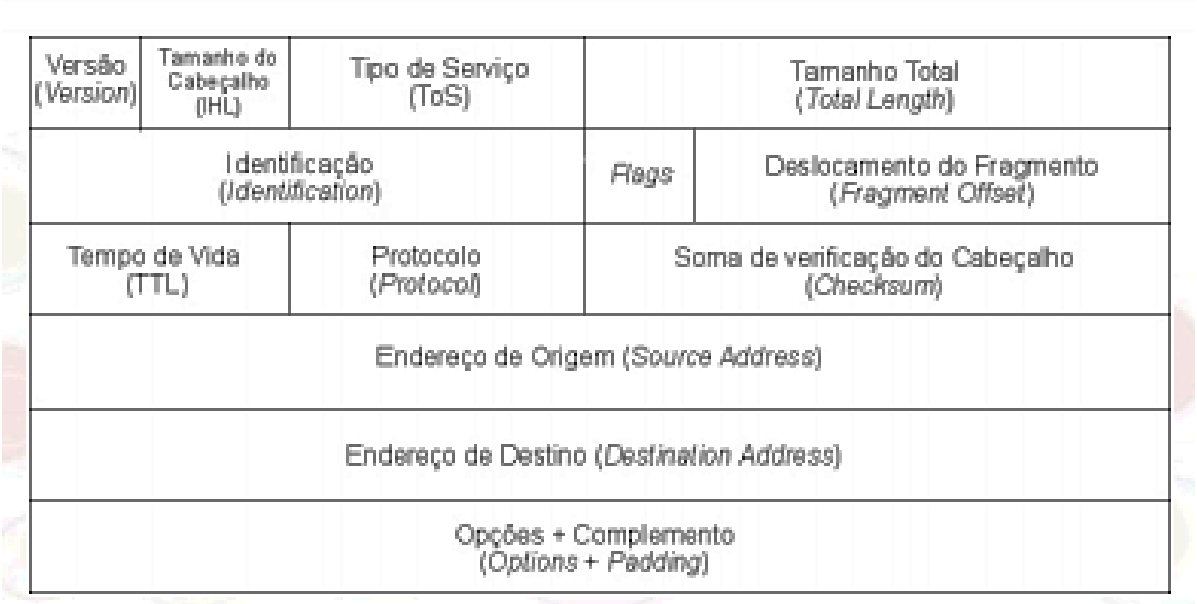
3. PROTOCOLO IPV6

Es importante conocer cómo se encuentra compuesto en sí el protocolo IPv6, es decir, cómo es su cabezal, qué campos lo componen y cuáles son los cambios y diferencias con el cabezal de IPv4, como también los tipos de direcciones y configuraciones de IPv6.

3.1. Cabezal IPv6 básico

El cabezal del protocolo IPv4 se encuentra compuesto por 12 campos fijos, pudiendo contener o no opciones, provocando que su tamaño pueda variar entre 20 y 60 bytes. En la figura 7 se puede observar los distintos campos por los cuales se encuentra compuesto el cabezal del protocolo IPv4:

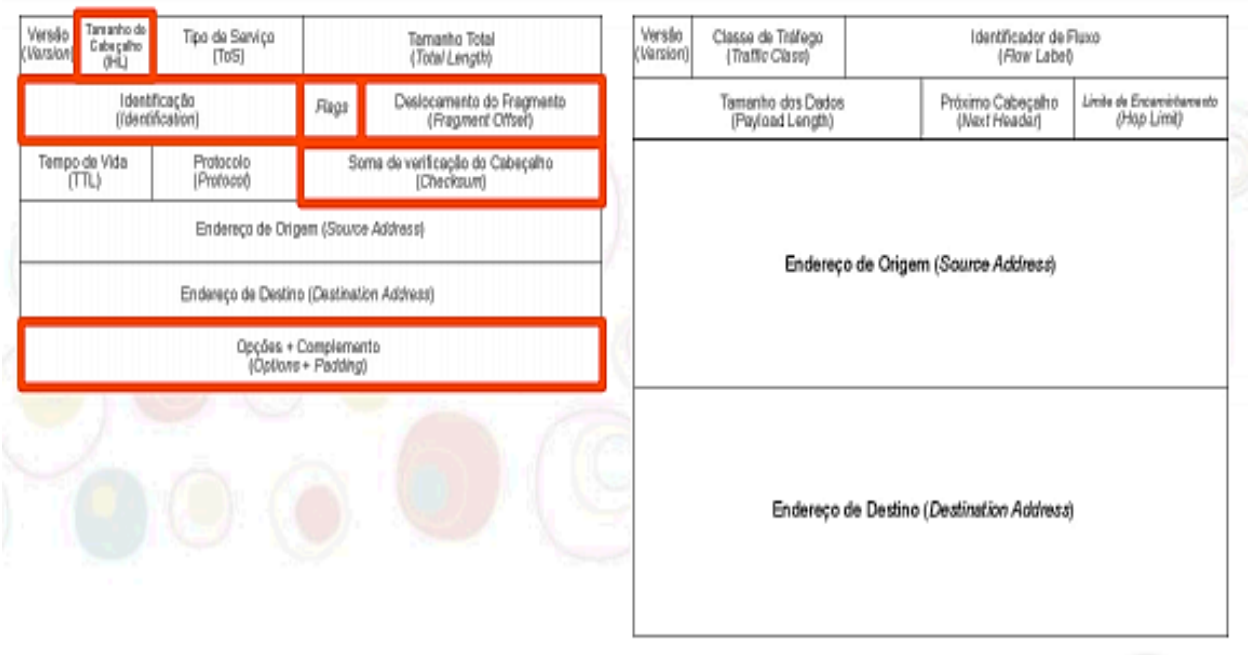
Figura 7. **Cabezal IPv4**



Fuente: LACNIC. *Tutorial IPv6 01.* P. 3

Ahora bien, IPv6 es una evolución de IPv4, y algo importante de identificar es que el cabezal ha sido simplificado, ya no contiene campos opcionales, por lo que su tamaño es de 40 bytes (fijo), apenas dos veces mayor que el cabezal de IPv4. Este cabezal resulta ser más flexible gracias a la implementación de cabezales adicionales, los cuales se describirán a lo largo de este capítulo. Este cabezal se vuelve más eficiente gracias a la minimización del *overhead* en los cabezales y reduciendo el costo del procesado de paquetes. En las siguientes figuras se comparan el cabezal de IPv4 e IPv6, y las modificaciones y cambios que se realizaron para dar origen al cabezal IPv6 básico, en las cuales se puede observar la eliminación de seis campos del cabezal IPv4, el cambio de nombre y de ubicación de cuatro campos, y la inclusión de un nuevo campo identificador de flujo en que solamente tres campos permanecieron intactos.

Figura 8. **Eliminación de campos**

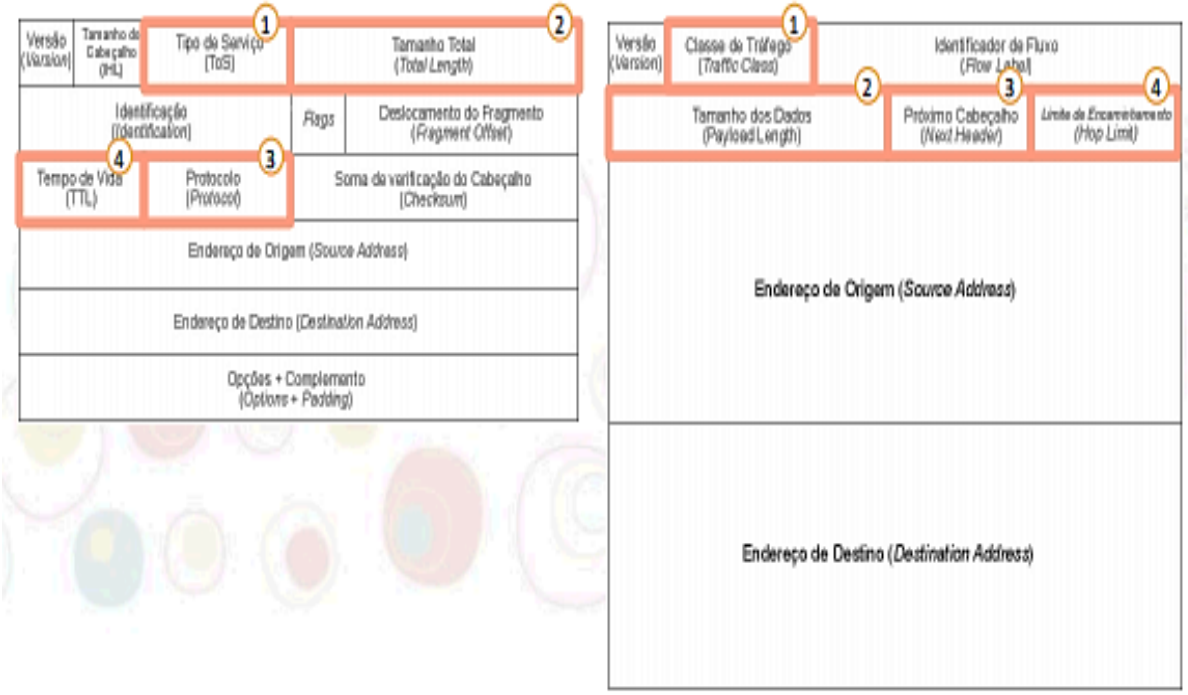


Fuente: LACNIC. *Tutorial IPv6 01.* P. 5.

Como puede observarse en la figura 8, del cabezal IPv4 se han eliminado seis campos, los cuales son innecesarios para el funcionamiento del nuevo protocolo:

- Tamaño del encabezado
- Identificador
- Bandera
- Fragmento
- *Checksum*
- Opciones adicionales

Figura 9. **Modificaciones de los campos**



Fuente: LACNIC. *Tutorial IPv6 01.* P. 6.

En la figura 9 se muestra la reubicación y renombramiento de cuatro campos:

- El campo “Tipo de Servicio”, ubicado como tercer campo en IPv4, cambia su nombre por “Clase de Tráfico”, ubicado en el segundo campo en IPv6.
- El campo “Tamaño Total”, ubicado en el cuarto campo en IPv4, cambia su nombre por “Tamaños de Datos”, ubicado en el cuarto campo en IPv6.
- El campo “Protocolo”, ubicado como noveno campo en IPv4, cambia su nombre por “Próximo Cabezal”, ubicado en el quinto campo en IPv6.
- Y por último el campo “Tiempo de Vida,” ubicado como octavo campo en IPv4, cambia su nombre por “Límite de Saltos”, ubicado en el sexto campo en IPv6.

Asimismo, puede observarse un nuevo campo: “Identificador de Flujo”, con un tamaño de 20 bits, el cual define el flujo de datos a los que se les podrá aplicar calidad de servicio, y que los únicos tres campos que no tuvieron modificaciones son Versión, Dirección de Origen y Dirección de Destino.

3.2. Cabezales de extensión de IPv6

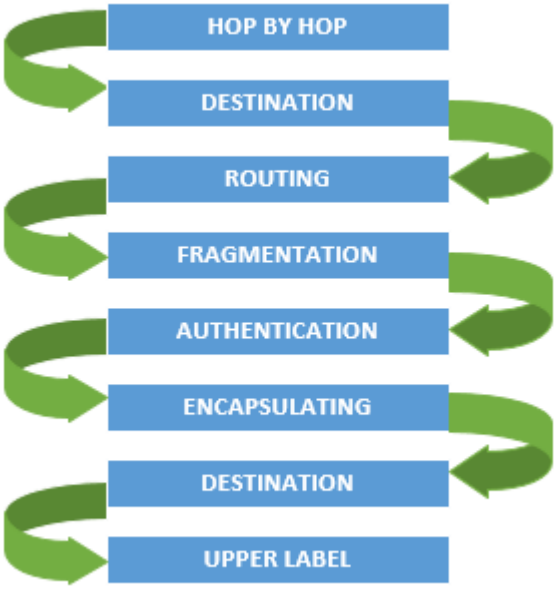
Los cabezales de extensión en IPv6 añaden funcionalidades en capa 3, es decir funcionalidades a capa IP, lo que hace que el cabezal sea más flexible. Pero hay que tener en cuenta que son limitados, deben ser configurados de forma ordenada y usados como máximo una vez (a excepción de *Destination*).

- *Hop-by-hop*, este cabezal es procesado por cada *router* (nodo) a lo largo del camino que siga el paquete, y se identifica por el valor “0” en el campo “Próximo Cabezal”.
- *Destination*, este cabezal es procesado por el *router*/nodo destino del paquete, y se identifica por el valor 60 en el campo “Próximo Cabezal”.

- *Routing*, este cabezal enlista uno o más *routers*/nodos intermedios que deberían atravesar el paquete antes de llegar a su destino y se identifica por el valor 43 en el campo “Próximo Cabezal”.
- *Fragmentation*, este cabezal es procesado en el *router*/nodo de destino, es el encargado de cargar información sobre los fragmentos de los paquetes IPv6 y se identifica por el valor 44 en el campo “Próximo Cabezal”.
- *Authentication*, (AH), este cabezal es utilizado por IPSec, el cual provee autenticación y garantía de integridad en los paquetes, y es identificado por el valor 51 en el campo “Próximo Cabezal”.
- *Encapsulation* (ESP), este cabezal cifra el contenido, también es utilizado por IPsec, el cual garantiza la integridad y confidencialidad de los paquetes y es identificado por el valor 52 en el campo “Próximo Cabezal”.
- *Destination*, este cabezal solamente es procesado por el *router*/nodo destino.
- *Upper Label*, este cabezal es utilizado para protocolos de capa superior.

En el caso de que se utilice más de un cabezal, se recomienda que se siga el siguiente orden:

Figura 10. **Orden de cabezales de extensión**



Fuente: elaboración propia.

3.3. Características generales de direccionamiento de IPv6

Los aspectos fundamentales del direccionamiento en IPv6 son los siguientes:

- Reglas básicas de notación

- De los 128 bits que componen el direccionamiento de IPv6, se realiza la división de 8 grupos de 16 bits cada uno, separados por dos puntos ":".
- La notación utilizada es la hexadecimal en cada grupo de *nibble* (4 bits).
- El uso de mayúsculas y/o minúsculas es indiferente.

Como ejemplo, se tiene el siguiente direccionamiento en IPv6:

2001:0db8:0321:0D10:0000:0000:0000:1000

- Reglas de compresión

- Los ceros a la izquierda en cada grupo se pueden eliminar.
- Si uno o más grupos contienen solamente ceros, estos pueden cambiarse por "::". Para el uso de esta regla se debe tener en cuenta que se puede suprimir y expandir sin ningún problema, y que esta regla puede utilizarse solamente una vez.
- Se puede usar corchetes "[ ]" para indicar algún puerto. Esto es importante, ya que logra evitar confundir un puerto con la nomenclatura de IPv6.

A modo de ejemplo:

- 2001:0db8:0321:0D10:0000:0000:0000:1000, existen grupos que contienen en su lado izquierdo un cero, por lo que se puede proceder a eliminarlo, seguidamente se logra observar que tres grupos constan solamente de ceros, estos grupos pueden ser comprimidos, por lo que el direccionamiento queda de la siguiente manera: 2001:db8:321:D10::1000.

- Ahora bien, si el direccionamiento a comprimir fuese: 2001:db8:0000:0000:0ABC:0000:0000:1234, se puede observar que existen dos grupos seguidos diferentes que constan solamente de ceros, por lo cual debe recordarse que la regla de aplicar doble dos puntos puede utilizarse una sola vez; una solución para realizar la compresión sería de la siguiente manera: 2001:db8:0:0:ABC::1234.

Nota: para los prefijos en IPv6 se sigue notación CIDR (prefijo/longitud de prefijo), a lo cual se le puede aplicar las reglas de compresión vistas anteriormente.

3.4. Tipos de direcciones en IPv6

En el direccionamiento IPv6 se puede encontrar tres tipos principales de direcciones: *unicast*, *multicast* y *anycast.*

- Unicast

Las direcciones *unicast* se refieren a paquetes que van de uno a uno, es decir existe un solo destino y un solo origen. Las *unicast* tienen una subdivisión de direcciones:

- Direcciones *Link-Local*: la cual es válida solamente en un enlace y se encuentra presente en una interfaz con IPv6 habilitado. En la práctica se debe utilizar el siguiente direccionamiento: fe80::/64.
- Direccionamiento *Unique-Local* (ULA): válido únicamente en un ámbito de un sitio de red, en la práctica se debe utilizar el siguiente direccionamiento: fc00::/17.
- IPv4 – *mapped*: utilizada para la configuración de un mecanismo de transición, en la práctica se debe utilizar el siguiente direccionamiento: ::FFFF:IPv4/128.

- Multicast

Las direcciones *multicast* se refieren a paquetes que van de uno a varios, es decir existe un solo origen, pero varios destinos. Hay definidos ciertos tipos

de direcciones *multicast*: FF01::1, FF02::1 utilizadas en todos los nodos; FF01::2, FF02::2 y FF05::2 para todos los dispositivos encargados de encaminar los paquetes.

- Anycast

Las direcciones *anycast* son similares a las *multicast*, sin embargo, la diferencia radica en que esta dirección es asignada a más de una interface situada en nodos diferentes y en donde se enruta a la interface más cercana que tenga dicha dirección. Entre sus implementaciones se encuentra el enrutamiento BGP.

3.5. Configuración de IPv6

Para poder realizar configuraciones bajo el protocolo IPv6, es importante activar IPv6 en los equipos, por lo que se puede seguir estos dos pasos:

1. Activar el reenvío de tráfico IPv6 en el equipo
2. Configurar las interfaces que requieren IPv6

En el siguiente ejemplo se observa la configuración de IPv6 en una interfaz de un *router*:

Figura 11. **Configuración de interface IPv6**

A

```
A>enable
A#conf t
A(conf)#ipv6 unicast-routing
A(conf)#int fa0/0
A(conf-if)#ipv6 address 2001:A:A:A:C::5/64
A(conf-if)#no shutdown
A(conf-if)#end
```

Fuente: elaboración propia.

Primero debe activarse el reenvío de tráfico IPv6 mediante el comando *ipv6 unicast-routing*, al activarlo se puede realizar la configuración de la interface con el protocolo de IPv6, lo cual es bastante similar al de IPv4.

4. ENRUTAMIENTO EN IPV6

Los *routers* tienen dos funcionalidades: intercambiar información en el plano de control, lo cual da lugar a tablas de rutas, y el reenvío (*forwarding*) de paquetes en el plano de control, dando lugar a tablas de reenvío, encargadas de seleccionar la información de las rutas en las tablas según la ruta más específica. La información de enrutamiento puede ser:

- De origen estático o de origen manual
- Aprendida por ser de interfaces conectadas directamente
- Aprendida mediante protocolos de *routing* dinámico

Los *routers* configurados en doble pila contienen la información de enrutamiento, tanto para IPv4 como para IPv6, la cual se gestiona de manera independiente y en paralelo. Se tienen tres elementos importantes a la hora de querer comunicar una red A con una red B:

- Información sobre redes/prefijos.
- El *next hop* o dirección donde se puede alcanzar esa red/prefijo.
- La comunicación entre vecinos, es decir los *routers* conectados entre sí.

Ahora bien, trabajar con un *routing* dinámico requiere un *router* ID que logre identificar cada uno de los *routers* participantes, para lo cual se utiliza un número entero de 32 bits. El formato para IPv4 sigue la forma a.b.c.d y este mismo servirá de igual forma y bajo las mismas reglas para IPv6:

- Configurarse de forma explícita: a.b.c.d

- Si no, se busca la mayor dirección IPv4 que se encuentre configurada en las interfaces de *loopback*.
- Si no, se busca la mayor dirección IPv4 de cualquier interfaz no *loopback.*

4.1. Enrutamiento estático

Una ruta estática es una ruta que es introducida manualmente en la tabla de rutas de un *router*, para que esta ruta exista debe ser creada de forma explícita y es una de las múltiples fuentes de información que posee un *router* para elaborar su tabla de reenvío. La diferencia que tiene con una ruta dinámica es que es incapaz de reaccionar a cambios en la red de forma automática.

Ventajas del enrutamiento estático:

- Simplicidad a la hora de planificar e implementar.
- Rapidez para implementar y que esa ruta sea efectiva.
- El uso y sintaxis de rutas estáticas en IPv6 es similar al de IPv4, en Cisco IOS por ejemplo, el comando tendría el siguiente formato: *ipv6 route prefix /length (outgoing interface [next-hop-address]* | *next-hop- address) [admin-distance]*. Sin embargo, hay que destacar ciertas diferencias, ya que como dirección *next-hop* puede utilizarse cualquiera del *router* vecino, incluida la *link local*; si se utiliza la dirección *link local* hay que configurar tanto la interfaz de salida como la dirección de *link local* (todas las interfaces tienen *link local* en el *router,* entonces no se sabría por dónde salir).

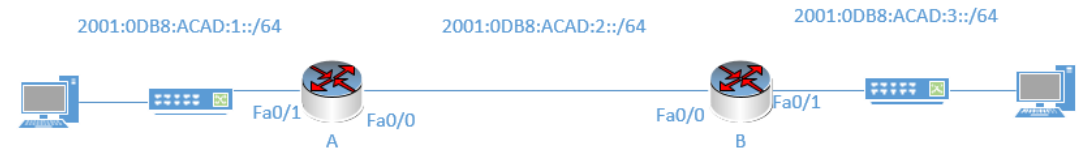
Inconvenientes del enrutamiento estático:

- Es una mala solución a nivel escalable para una red grande con muchas rutas y *routers.*
- No resulta una buena solución si la red sufre cambios constantes.

- Configuración de enrutamiento estático en IPv6

En la figura 12 se puede observar un diagrama de red, en el cual se requiere comunicar dos equipos finales (computadoras) ubicados en diferentes redes. Entre ellas se encuentran dispositivos de capa 2, como lo son los *switches,* y dispositivos de capa 3, como lo son los *routers*, en los cuales se configurará las rutas necesarias para establecer la comunicación entre ambas redes.

Figura 12. **Configuración de ruta estática IPv6**




```
A>enable
A#conf t
A(conf)#ipv6 unicast-routing
A(conf)#int fa0/0
A(conf-if)#ipv6 address 2001:0DB8:ACAD:2::1/64
A(conf-if)#no shutdown
A(conf-if)#exit
A(conf)#int fa0/1
A(conf-if)#ipv6 address 2001:0DB8:ACAD:1::1/64
A(conf-if)#no shutdown
A(conf-if)#exit
A(conf)#ipv6 route 2001:0ODB8:ACAD:3::/64 2001:0DB8:ACAD:1::2
```

```
B>enable
B#conf t
B(conf)#ipv6 unicast-routing
B(conf)#int fa0/0
B(conf-if)#ipv6 address 2001:0DB8:ACAD:2::2/64
B(conf-if)#no shutdown
B(conf-if)#exit
B(conf)#int fa0/1
B(conf-if)#ipv6 address 2001:0DB8:ACAD:3::1/64
B(conf-if)#no shutdown
B(conf-if)#exit
B(conf)#ipv6 route 2001:0ODB8:ACAD:1::/64 F0/0
```

Fuente: elaboración propia.

Resulta necesario habilitar ipv6 en ambos *routers* para poder configurar las direcciones IPv6 en las interfaces. En este ejemplo se utilizó un /64, el cual

es sugerido para conexiones punto a punto, por lo que se deduce que el *host* ubicado en la red LAN A tendrá una dirección 2001:0DB8:ACAD:1::2/64, mientras que el *host* ubicado en la red LAN B tendrá una dirección 2001:0DBI:ACAD:3::2/64. Es importante destacar que al realizar la configuración de la ruta se puede especificar, ya sea el siguiente salto, o bien la interface de salida.

4.2. Enrutamiento dinámico IGP en IPv6

Un enrutamiento IGP, de sus siglas en inglés de Interior Gateway Protocol, es el protocolo de enrutamiento dinámico para enrutar redes dentro de un mismo Sistema Autónomo o AS. Un enrutamiento dinámico puede clasificarse de la siguiente manera: por vector distancia (el número de saltos que toma un paquete para llegar a su destino), o bien por estado enlace (el mejor ancho de banda de un enlace para llegar al destino), y con base en esta clasificación existen varios protocolos IGP: RIP, OSPF, IS-IS, entre otros, los cuales siguen distintos criterios de selección para seguir una ruta y siguen las mismas directrices tanto en IPv4 como para IPv6.

Tabla I. **Clasificación IGP**

TIPO	NOMBRE	IPv4	IPv6	COMENTARIOS
IGP	RIP	RIPv2	RIPng	Nueva versión solo IPv6
	OSPF	OSPFv2	OSPFv3	Nueva versión solo IPv6
	IS-IS	IS-IS	IS-IS	Se extendió para soportar IPv6

Fuente: elaboración propia.

- RIPng

Extensión de RIPv1 y RIPv2 para soportar direcciones de 128 bits, es decir direcciones IPv6, este protocolo es capaz de realizar el encaminamiento de prefijos IPv6: prefijo/longitud. En una topología en donde se maneja doble pila, si se utiliza RIP harán falta 2 procesos distintos: uno para IPv4 configurando RIPv2 y otro para IPv6 utilizando RIPng. Es importante destacar que RIPng solamente utiliza direcciones *link-local* como *next-hop.*

Cuando se habilita RIPng en una interfaz de un *router,* se realizarán tres cosas:

1. Se enviarán actualizaciones RIP por esta interfaz
2. Se procesan las actualizaciones RIP recibidas en esta interfaz
3. Anunciarán las rutas conectadas de esta interfaz

Para poder configurar RIP IPv6 es importante habilitar la configuración global de IPv6 con el comando "*ipv6 unicast-routing*" y luego habilitar IPv6 en aquellas interfaces en las cuales se requiera RIP, por lo que en forma resumida una simple configuración de RIP IPv6 sería:

Figura 13. **Configuración básica RIPng**

```
A>enable
A#conf t
A(conf)#ipv6 unicast-routing
A(conf)#int fa0/0
A(conf-if)#ipv6 rip process1 enable
```

Fuente: elaboración propia.

- OSPFv3

Es un protocolo de enrutamiento OSPF para IPv6, es una modificación de OSPFv2 y es capaz de soportar direcciones *next hop* y prefijos de 128 bits mediante nuevos LSAs, los cuales describen el estado de una red o un *router*. Esta nueva versión para IPv6 es muy similar a OSPFv2, solamente que este no funciona sobre una subred sino sobre un enlace, y puede usarse IPsec para ofrecer autenticación. El *router* ID consta de 32 bits, permite varias instancias por interfaz y se utilizan direcciones *multicast* IPv6 para la comunicación: FF02::5 o bien FF02::6. De igual forma, si se trabaja bajo una topología de doble pila debe configurarse tanto OSPFv2 para IPv4 como OPSFv3 para IPv6.

De igual manera es importante recordar que para configurar OSPFv3 primeramente se debe habilitar la configuración IPv6 con el comando "*ipv6 unicast-routing*", y luego se debe seleccionar la interfaz a la cual se le configurará OSPFv3 y finalmente se configura OPSFv3.

Figura 14. **Configuración básica OSPFv3**

```
A>enable
A#conf t
A(conf)#ipv6 unicast-routing
A(conf)#int fa0/0
A(conf-if)#ipv6 enable
A(conf-if)#ipv6 ospf 10 area 0
A(conf-if)#exit
A(conf)#ipv6 router ospf 10
A(conf-ospf)#router-id 1.1.1.1
A(conf-ospf)#log-adjacency-changes
A(conf-ospf)#end
```

Fuente: elaboración propia.

- IS-IS

IS-IS es un protocolo de encaminamiento OSI diseñado para soportar el protocolo IPv6, el cual es un correo sobre capa de enlace y ha sido extendido para poder soportar tanto IPv4 como IPv6. La información es enviada mediante TLVs: *tag, lenght, value*, en donde se definen 2 TLV para poder enviar información de *routing* IPv6 usando IS-IS: información del prefijo mediante IPv6 *reachability* e información de *next hop* mediante IPv6 *interface address*.

Existen dos modos de configuración: *single topology,* en la cual IPv4 e IPv6 comparten el cálculo de rutas, por lo que las interfaces IPv4 e IPv6 deben ser las mismas, y *multitopology,* en que el cálculo de rutas es independiente para IPv4 e IPv6 y, por lo tanto, las interfaces IPv4 e IPv6 pueden ser distintas.

Figura 15. **Configuración básica IS-IS IPv6**

```
A>enable
A#conf t
A(conf)#ipv6 unicast-routing
A(conf)#int fa0/0
A(conf-if)#ipv6 router isis alpha
A(conf-if)#exit
A(conf)#router isis alpha
A(conf-ospf)#net 49.1111.2222.3333.4444.00
A(conf-ospf)#end
```

Fuente: elaboración propia.

5. SERVICIOS CON IPV6

Migrar de IPv6 a IPv4 no solo conlleva la configuración de *switches* y *routers*, sino también de servicios como: servidores DNS, servidores WEB, NTP y la implementación de cierta seguridad para el resguardo de la información dentro de la red. Por lo que, si se ofrece un servicio alcanzable a través de una red, es importante que todos los usuarios puedan acceder sin problema, por eso es esencial recordar que existen redes que trabajan solo IPv4, solo IPv6 o bien redes que trabajan con el mecanismo de transición de doble pila.

El objetivo principal es que el servicio ofrecido sea accesible a cualquier usuario, independientemente del protocolo que utilice, por lo que es recomendable que se trabaje sobre IPv4 e IPv6, es decir, en doble pila. Esto permite que el servicio sea visible a todos los tipos de clientes y permite añadir IPv6 de forma gradual en la red.

5.1. Servidor DNS en IPv6

Un servidor DNS tiene como función ser una base de datos distribuida en donde los datos se van separando y ordenando según las etiquetas de texto separadas por un punto (nombre de dominio). Una idea muy importante es saber que el transporte, que se refiere a las consultas y respuestas que se hagan al servidor es totalmente independiente del contenido, es decir la información. Un servicio DNS tiene dos posibles resoluciones: la resolución directa, la cual resuelve de nombres a direcciones IP, y la resolución inversa, la cual resuelve de direcciones IP a nombres.

Un nombre de dominio suele estar dado por varios servidores:

- Maestro o primario: en que se hacen los cambios y se actualiza la versión del fichero de zona que contiene datos asociados al nombre de dominio.
- Esclavo o secundario: el maestro avisa de una nueva versión de datos y los esclavos solicitan actualización o transferencia de zona.

Para su configuración es común encontrar dos entornos que son los más usados: BIND, que trabaja sobre Linux, y Microsoft DNS Server, que trabaja sobre Windows.

5.2. Servidor web en IPv6

Al implementar un servidor web, se pueden encontrar dos configuraciones comunes: Apache, que trabaja sobre el sistema Linux, e IIS, que trabaja sobre el Sistema de Microsoft Windows. En cualquiera de las dos configuraciones se utiliza http o bien https, los cuales utilizan una conexión TCP, y pueden ser configurados tanto en IPv4 como en IPv6; una vez conectado el comportamiento es muy similar en ambos protocolos. Sin embargo, se requiere de una especial atención en la configuración del servidor y de los ficheros de *log* y su procesado.

En la configuración del servidor, en el campo donde se configura la dirección IP, se añade la dirección IPv6 designada a dicho servidor, o bien se puede utilizar directivas genéricas que incluyan IPv4 e IPv6. En Apache un simple asterisco “*” indica cualquier IP, es decir tanto IPv4 como IPv6:

- NameVirtualHost *:80

5.3. Servidor NTP en IPv6

Protocolo de sincronización de relojes, que funciona gracias al envío de paquetes UDP/IP, la última versión NTPv4 soporta el protocolo IPv4 y el protocolo IPv6. Existen dos modos de configuración: uno a uno, la cual puede funcionar en IPv4 e IPv6, y la configuración uno a muchos, la cual puede usar en IPv4 direcciones *multicast* o *broadcast,* y en IPv6 direcciones *multicast.* Como ejemplo, la siguiente dirección muestra un servidor capaz de ser alcanzado con IPv6 en Internet: 2.pool.ntp.or.

5.4. Seguridad en IPv6

Existen muchas mentiras sobre el tema de seguridad en IPv6, como que al estar en una etapa de transición y si una red trabaja aún bajo IPv4 no se corre ningún riesgo, o bien que IPv6 es más seguro que IPv4 debido a que es algo muy nuevo como para ser atacado, e infinidad de cosas más. Pero hay que tener en claro que ninguno de estas ideas es verdadera, y una idea muy precisa es que: IPv6 no es ni más ni menos seguro que IPv4.

- Clasificación de amenazas en IPv6

Existen tres categorías para las amenazas respecto a seguridad en IPv6:

- Aquellas amenazas que ya existían en IPv4 y se comportan de una manera muy similar en IPv6, como, por ejemplo: *sniffing*, ataques a otras capas, *flooding.*
- Aquellas amenazas que ya existían con IPv4 y se comportan distinto con IPv6, como, por ejemplo: el escaneo de la red, amplificación (*smurf*).

- Aquellas amenazas que aparecieron con la creación de IPv6, como por ejemplo: amenazas a NDP, *routing header* tipo O, cabeceras de extensión, etc.

    - Amenazas NDP

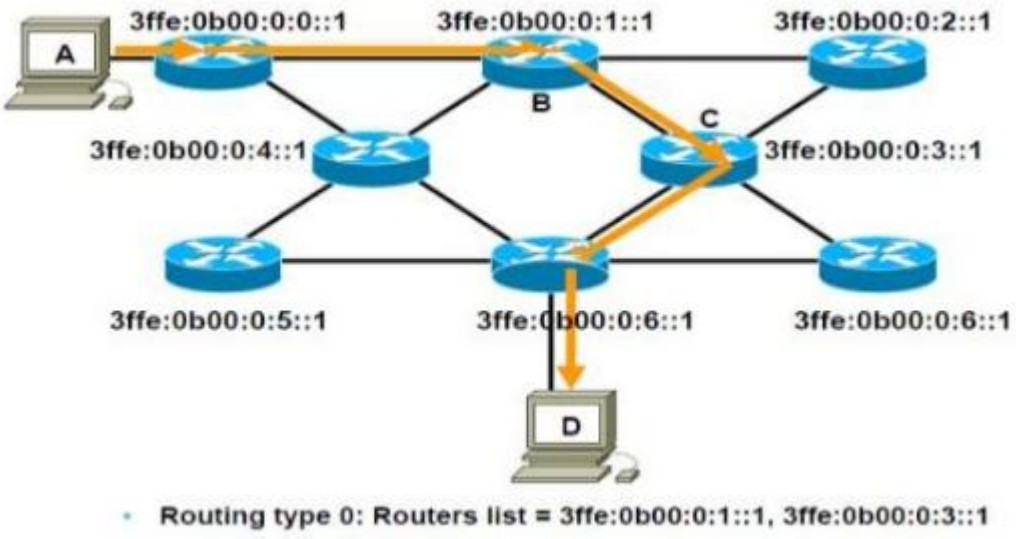
Neighbor Discovery Protocolo es un protocolo vulnerable a diversos ataques, autoconfigura nodos IPv6 y permite descubrir a otros nodos del mismo enlace, determinar su dirección de nivel de red y mantener información de la ruta IPv6 hacia otros nodos activos. Realiza la autoconfiguración de la dirección IPv6 por medio del envío de paquetes Router Advertisement (RA). Estos RA son utilizados para el ataque a NDP realizando las siguientes acciones: el atacante se hace pasar por un *router*, crea un prefijo falso en el enlace, crea un prefijo falso para la configuración de direcciones, crea parámetros falsos, estos ataques crean lo que se denominan ataques DoS.

    - Routing header Tipo 0

El RH0 puede ser usado para acumular tráfico sobre un camino remoto con el propósito de degradar el tráfico o DoS. Es considerado una amenaza grave por lo que se prohibió su uso en el RFC5095. Los atacantes pueden usar maliciosamente los encabezados de enrutamiento tipo 0 para eludir el filtraje de paquetes, es decir las políticas de listas de acceso de IPv6, o el enrutamiento y direccionamiento de difusión ilimitada. Este tipo de encabezados puede usarse para realizar ataques de DoS reflejados, *spoofing, spoofing* doble y ataques de ampliación, llamados también ataques *ping-pong* que causan saturación en el enlace, causando problemas de rendimiento a través del procesamiento adicional de la CPU.

En la figura 16 se muestra un ejemplo de un ataque RH0, se puede observar la intrusión de un *router* ilícito que se ha apropiado de la dirección IP de un *router* que sí pertenece a la red, por lo que la información ya no llega a su destino real si no que se traslada hacia el *host* atacante.

Figura 16. **Ataque RH0**



Fuente: SLIDESHARE. *Seguridad en IPv6.* P. 14

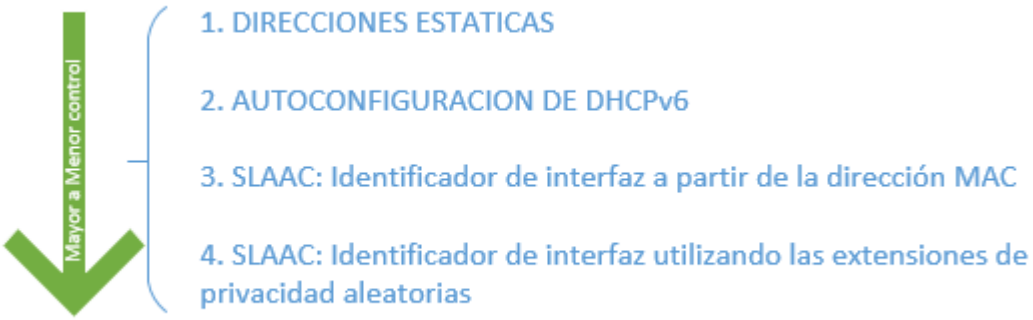
- Recomendaciones de seguridad en IPv6

Existen posibles soluciones ante las amenazas anteriores, algunas se encuentran estandarizadas y otras no, existiendo un nivel de soporte distinto entre cada fabricante. Entre las soluciones estandarizadas se puede encontrar: las extensiones de privacidad [RFC4941], IPSec [RFC4301, 4302, 4303, 4307, 7296, 7321], SEND [RFC3971, 3972] y RA-GUARD [RFC6104, 6105, 7113].

Una recomendación a destacar es la configuración de direcciones IPv6, de manera que se maneje un sistema jerárquico en que lo más alto será todo

aquello que puede tener un mayor control hasta terminar por aquello de que se tenga un menor control. Es importante manejar ciertos métodos de configuración y direcciones. Como forma de ejemplo se muestra la figura 17, en donde como cúspide de la pirámide se encuentran las direcciones estáticas, debido a que se configuran de manera manual, por lo que se tiene un mejor control al identificar qué dispositivo tiene configurada cierta dirección IP.

Figura 17. **Modelo jerárquico**



Fuente: elaboración propia.

Será común configurar varias direcciones IPv6 en una sola interfaz, y se debe seleccionar direcciones difíciles de poder ser adivinadas, debido a que los patrones de escaneo han cambiado para IPv6. Una de las ventajas de realizar este método jerárquico es la forma en la que se puede controlar y manejar de una mejor manera la red, obteniendo de esta manera una mayor seguridad. Una desventaja es que no siempre se podrá configurar una dirección estática, por lo que el esquema se rompería.

Una dirección estática tiene mayor control y manejo gracias a que es configurada manualmente, y se podrá conocer con certeza la dirección IP que tiene configurada un dispositivo, sin embargo, en una red demasiado grande

este mecanismo se vuelve tedioso y más difícil de implementar. Una autoconfiguración DHCPv6 permite que los dispositivos adquieran una dirección IP sin necesidad de configurarla manualmente, por lo que se ahorra tiempo y recursos para su implementación, sin embargo, debido a que la asignación la realiza dinámicamente, se vuelve más complicado reconocer qué dispositivo tienen asignada cada dirección IP.

Un SLAAC es un proceso de autoconfiguración de direcciones IPv6 que se vuelve un método más difícil de controlar, debido a que este depende, o bien de la MAC del dispositivo asociado, o de las extensiones de privacidad aleatorias, es decir la puede generar cualquier dispositivo, por lo que es una autoconfiguración sin estado, ya que no existe un equipo dedicado a mantener el arrendamiento de dichas direcciones ni hace seguimiento de esta autoasignación.

6. GUÍA METODOLÓGICA

PLANIFICACIÓN DEL MÓDULO DE IPv6 PARA EL LABORATORIO DE TELECOMUNICACIONES Y REDES LOCALES
ESCUELA DE INGENIERÌA DE MECÁNICA ELÉCTRICA
FACULTAD DE INGENIERÍA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CLASE TEÓRICA

Se propone una guía didáctica para el auxiliar encargado del Laboratorio de Telecomunicaciones y Redes, indicando tema, propósitos y contenidos. Para visualizar los materiales y prácticas propuestas para esta guía es útil dirigirse a la sección de apéndices.

- Nivel: universitario
- Semestre: noveno
- Género: mixto
- Asignatura: Telecomunicaciones y Redes Locales
- Encargado: auxiliar de laboratorio
- Eje temático: *networking*
- Bloque de contenidos: enseñanza de IPv6 Básico

Propósitos:

- Familiarizar a los estudiantes con el nuevo protocolo de Internet IPv6.
- Mostrar los diferentes mecanismos de transición, configuración y los distintos servicios que pueden entregarse a través del nuevo protocolo.

- Realizar ejercicios prácticos en un entorno simulado (*packet tracert*) utilizando las configuraciones necesarias para realizar ciertas topologías de red.

Contenidos:

- Conceptuales:

Historia del Internet, definición de IPv6, mecanismos de transición, configuraciones y servicios.

- DOS SANTOS, Rodrigo. *Curso IPv6 básico*. Brasil: Sao Paulo, 2010.
- ACOSTA, Alejandro. *IPv6 para operadores de red.* Argentina: Buenos Aires, 2014.

Procedimentales:

- Dar a conocer qué es el Internet, fases de agotamiento y los mecanismos de transición.
- Dar a conocer el protocolo IPv6 y sus diferentes configuraciones.
- Realizar ejercicios prácticos de configuraciones en interfaces de dispositivos, de ruteo y de servidores.

Actitudinales:

Manejar y utilizar el conocimiento en redes como instrumentos y formas de configuración y de solución de problemas en diferentes tipos de red, como medios de formación de conocimiento para su interacción en el ámbito laboral.

Actividades:

- Asistir a las clases programadas que exponen los temas de IPv6.
- Investigar sobre los diferentes mecanismos de transición y sus diferencias.
- Realizar prácticas simuladas supervisadas con el software Packet Tracer.

Procedimiento organizativo y métodos:

- Explicativo, demostrativo, práctica guiada, recursos teóricos.
- Individual, en parejas, en grupos, con ejercicios en laboratorio o tareas en casa.

Recursos o medios:

- Material didáctico
- Salón de clases
- Software Packet Tracer
- Computadoras

PLANIFICACIÓN DEL MÓDULO DE IPv6 PARA EL LABORATORIO DE TELECOMUNICACIONES Y REDES LOCALES
ESCUELA DE MECANICA ELÉCTRICA
FACULTAD DE INGENIERIA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CLASE I

- Nivel: universitario
- Semestre: noveno
- Género: mixto

- Asignatura: Telecomunicaciones y Redes Locales
- Encargado: auxiliar de laboratorio
- Eje temático: *networking*
- Bloque de contenidos: enseñanza de IPv6 básico

Propósito:

- Introducir al estudiante en los conceptos de Internet y las fases de agotamiento.
- Conocer el por qué de la creación de un nuevo protocolo.

Parte inicial:

- Presentación
- Indagación sobre conocimiento actual del tema
- Preguntas sobre el tema
- Propósito del tema

Parte principal:

- Con base en el material 1 se debe explicar sobre la creación de Internet y las fases de agotamiento.
- Realizar preguntas sobre los conceptos fundamentales del tema.

Parte final:

- Responder dudas sobre el tema.

- Como tarea, investigar sobre el Internet, el protocolo de IPv6 y las fases de agotamiento.

PLANIFICACIÓN DEL MÓDULO DE IPv6 PARA EL LABORATORIO DE TELECOMUNICACIONES Y REDES LOCALES
ESCUELA DE INGENIERÌA DE MECÁNICA ELÉCTRICA
FACULTAD DE INGENIERÍA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CLASE II

- Nivel: universitario
- Semestre: noveno
- Género: mixto
- Asignatura: Telecomunicaciones y Redes Locales
- Encargado: auxiliar de laboratorio
- Eje temático: *networking*
- Bloque de contenidos: enseñanza de IPv6 básico

Propósito:

- Introducir al estudiante en los conceptos de mecanismos de transición.
- Mostrarle al estudiante cuál es la diferencia entre cada mecanismo de transición.

Parte inicial:

- Presentación

- Indagación sobre conocimiento actual del tema
- Preguntas sobre el tema
- Propósito del tema

Parte principal:

- Con base en el material 2 se debe explicar sobre los diferentes mecanismos de transición.
- Realizar preguntas sobre los conceptos fundamentales del tema.
- Diferenciar en qué momento utilizar cuál mecanismo de transición.

Parte final:

- Responder dudas sobre el tema.
- Proponer un esquema de red (puede usarse el propuesto en la práctica del material 2) para que el estudiante analice y opine sobre cómo realizaría la transición de IPv4 a IPv6 de dicha red.

PLANIFICACIÓN DEL MÓDULO DE IPv6 PARA EL LABORATORIO DE TELECOMUNICACIONES Y REDES LOCALES
ESCUELA DE INGENIERÌA DE MECÁNICA ELÉCTRICA
FACULTAD DE INGENIERÍA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CLASE III

- Nivel: universitario
- Semestre: noveno
- Género: mixto

- Asignatura: Telecomunicaciones y Redes Locales
- Encargado: auxiliar de laboratorio
- Eje temático: *networking*
- Bloque de contenidos: enseñanza de IPv6 básico

Propósito:

- Introducir al estudiante en los conceptos del protocolo IPv6.
- Enseñar las reglas básicas del protocolo de IPv6, como los tipos de direcciones.

Parte inicial:

- Presentación
- Indagación sobre conocimiento actual del tema
- Preguntas sobre el tema
- Propósito del tema

Parte principal:

- Con base en el material 3 se debe explicar sobre el protocolo de IPv6, cabezales, reglas básicas y tipos de direccionamientos.
- Realizar preguntas sobre los conceptos fundamentales del tema.
- Realizar ejemplo (propuestos en el material 3).

Parte final:

- Responder dudas sobre el tema.

- Hoja de trabajo con los ejercicios propuestos en la práctica del material 3.

PLANIFICACIÓN DEL MÓDULO DE IPv6 PARA EL LABORATORIO DE TELECOMUNICACIONES Y REDES LOCALES
ESCUELA DE INGENIERÌA DE MECÁNICA ELÉCTRICA
FACULTAD DE INGENIERÍA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CLASE IV

- Nivel: universitario
- Semestre: noveno
- Género: mixto
- Asignatura: Telecomunicaciones y Redes Locales
- Encargado: auxiliar de laboratorio
- Eje temático: *networking*
- Bloque de contenidos: enseñanza de IPv6 básico

Propósito:

- Introducir al estudiante en los conceptos de enrutamiento en IPv6.
- Enseñar los diferentes tipos de enrutamiento en IPv6.

Parte inicial:

- Presentación
- Indagación sobre conocimiento actual del tema
- Preguntas sobre el tema

- Propósito del tema

Parte principal:

- Con base en el material 4 se debe explicar sobre los diferentes tipos de enrutamiento en IPv6.
- Realizar preguntas sobre los conceptos fundamentales del tema.
- Realizar ejemplo propuesto en el material 4.

Parte final:

- Responder dudas sobre el tema.
- Hoja de trabajo con los ejercicios propuestos en la práctica del material 4.

PLANIFICACIÓN DEL MÓDULO DE IPv6 PARA EL LABORATORIO DE TELECOMUNICACIONES Y REDES LOCALES
ESCUELA DE INGENIERÌA DE MECÁNICA ELÉCTRICA
FACULTAD DE INGENIERÍA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CLASE V

- Nivel: universitario
- Semestre: noveno
- Género: mixto
- Asignatura: Telecomunicaciones y Redes Locales
- Encargado: auxiliar de laboratorio
- Eje temático: *networking*

- Bloque de contenidos: enseñanza de IPv6 básico

Propósito:

- Introducir al estudiante en los conceptos de servicios con IPv6.
- Enseñar los diferentes tipos de servicios y seguridad en IPv6.

Parte inicial:

- Presentación
- Indagación sobre conocimiento actual del tema
- Preguntas sobre el tema
- Propósito del tema

Parte principal:

- Con base en el material 5 se debe explicar sobre los diferentes tipos de servicios en IPv6.
- Mostrar las amenazas y recomendaciones de seguridad en IPv6.
- Realizar preguntas sobre los conceptos fundamentales del tema.
- Realizar ejemplo propuesto en el material 5.

Parte final:

- Responder dudas sobre el tema.
- Hoja de trabajo con los ejercicios propuestos en la práctica del material 5.

CONCLUSIONES

1. Existen diferentes organizaciones que operan a nivel mundial, las cuales se encargan de la administración y de controlar las asignaciones de direcciones IP debidamente, tanto para el protocolo de IPv4 como para el protocolo IPv6, así mismo crean estándares y generalidades para el mejor manejo de IPv6 en cada región.

2. Es importante un buen estudio previo de la red junto con el conocimiento de los distintos métodos de transición a IPv6 que existen, para poder realizar una transición amigable y escalonada, permitiendo migrar al nuevo protocolo de manera eficaz y sin perder la conectividad a Internet.

3. El ruteo en IPv6 cuenta con algunas diferencias que su antecesor, sin embargo, la base en cada uno de los protocolos es la misma, permitiendo un aprendizaje más rápido. Los servicios que funcionan bajo el protocolo IPv4 pueden ser configurados para que sean compatibles con el protocolo IPv6 sin que el usuario note alguna diferencia.

4. Debido a la importancia del protocolo de IPv6 y de su pronta implementación, la guía metodológica de esta tesis se convierte en una extensión del Laboratorio de Telecomunicaciones y Redes Locales, otorgando al estudiante el concepto básico y las características principales que le ayudarán en su desempeño laboral.

RECOMENDACIONES

1. Que la persona encargada de dar el curso tenga un conocimiento básico de redes y de lo que son los protocolos IPv4 e IPv6, y que haya estudiado y comprendido el contenido de esta guía.

2. Realizar constantes actualizaciones al contenido de este curso, con base en los retos laborales que puedan llegar a enfrentar los estudiantes de la carrera de Ingeniería Electrónica.

3. Crear un laboratorio con equipo físico para que el estudiante pueda realizar las configuraciones en un entorno real y no solamente en un entorno simulado, bajo prácticas estructuradas. Crear un laboratorio mejor equipado da la posibilidad de que, en el futuro, se puedan implementar cursos de Cisco como tal en la carrera.

BIBLIOGRAFÍA

1. ACOSTA, Alejandro. *IPv6 para operadores de red*. Buenos Aires, Argentina: ISOC, 2014. 86 p.

2. DOS SANTOS, Rodrigo. *Curso IPv6 básico*. Sao Paulo, Brasil, 2010. 316 p.

3. ECIJA*. IPv6 aspectos legales del nuevo protocolo de Internet*. Inglaterra, Comisión Europea, 2005. 305 p.

4. LACNIC. *Curso IPv6 avanzado*. Montevideo, Uruguay, 2017. 100 p.

5. LACNIC. *Curso IPv6 básico*. Montevideo, Uruguay, 2017. 150 p.

6. LACNIC. *Despliegue de IPv6 para el desarrollo socioeconómico en América Latina y el Caribe*. Montevideo, Uruguay, 2015. 116 p.

APÉNDICES

Apéndice 1. **Material Didáctico**

Material 1

Conceptos Básicos

- Introducción

Bienvenidos a este módulo de IPv6 básico para el Laboratorio de Telecomunicaciones y Redes Locales, en esta clase se abarcarán diferentes temas que van desde un recordatorio de lo que es Internet hasta llegar a las fases de agotamiento de IPv4.

- Internet

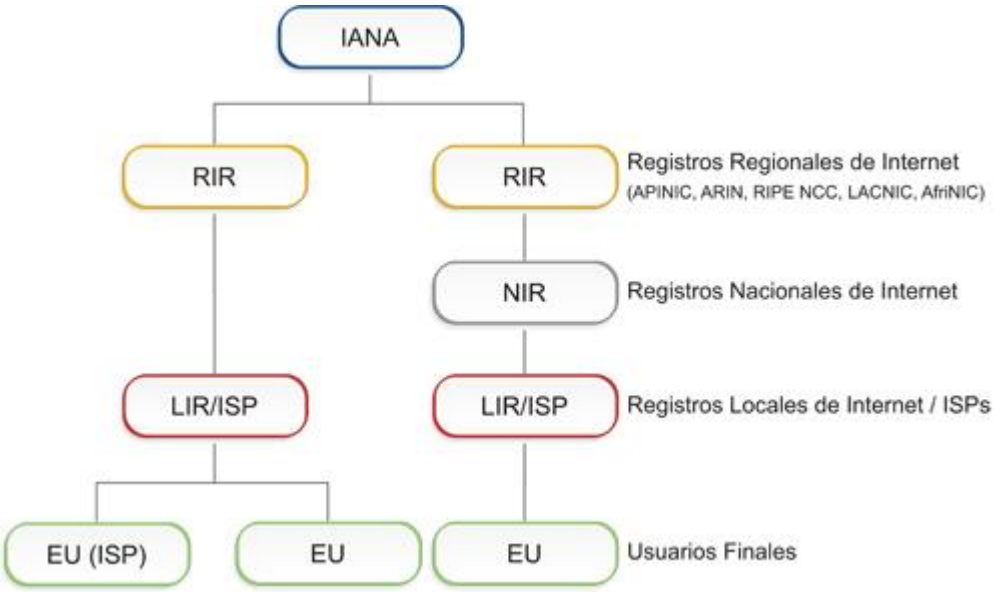
¿Qué es Internet? Una red mundial de computadoras conectadas por diferentes medios, ya sean satelitales, fibra óptica, líneas telefónicas, entre otros, permitiendo que millones de usuarios puedan estar conectados a esta red para así poder intercambiar, extraer o introducir información. ¿Cómo surgió esta gran red llamada Internet? En el año de 1969 da inicio ARPANET, un sistema de comunicación y control distribuido con fines militares, cuyo principal objetivo era crear un esquema de conexión de una red descentralizada con múltiples caminos entre dos puntos, convirtiéndose poco a poco en lo que se conoce actualmente como Internet. Más adelante se define el protocolo IPv4, el cual cumplía dos funciones básicas: la fragmentación, permitiendo el envío de paquetes de información de mayor tamaño, los cuales no eran soportados por los enlaces debido al límite de tráfico establecido, mediante la división de

paquetes de información más pequeños; y el direccionamiento, permitiendo identificar el destino y origen de los paquetes de información gracias a un encabezado del protocolo en donde se almacena la dirección. Ahora vemos la importancia del protocolo de internet (IP). Sin embargo, este protocolo no previó el aumento exponencial de las redes, lo que iba a generar el agotamiento de las direcciones IPv4.

- Jerarquía de asignación de direcciones

¿Entonces existe alguna organización encargada de administrar y controlar las direcciones IP? Sí, la asignación de direcciones IP lleva un sistema jerárquico formando un árbol invertido, en donde la parte más alta de este sistema la ocupa IANA (Internet Assigned Numbers Authoritity), que es el organismo responsable de los recursos numéricos de Internet, direcciones IP y los números de sistemas autónomos. IANA asigna recursos a las RIR (Regional Internet Registry), entre los cuales se encuentra LACNIC (Latin American and Caribbean IP Address Regional Registry), la RIR encargada de la administración de direcciones IP en Latinoamérica y el Caribe. Estas RIR a su vez asignan a un NIR (National Internet Registry) encargado de asignar direcciones en cada país y que, a su vez, asigna direcciones a los ISP (Internet Service Provider), o bien las NIR pueden asignar a los ISP y estos asignan a los usuarios finales.

Figura 18. **Jerarquía**



Fuente: LACNIC. Definiciones. P. 1

- Protocolo IPv4

¿Qué es el protocolo IPv4? Es el encargado de asignar una dirección IP a un dispositivo para que sea capaz de alcanzar la red llamada Internet, este protocolo utiliza direcciones de 32 bits que lo limitan a 4 292 967 296 direcciones únicas utilizables. Estas direcciones se encuentran divididas en 256 prefijos /8, de los cuales 35 078 direcciones se encuentran reservadas a diferentes usos, como multicas, identificadores locales, *loopbacks*, usos privados o bien para usos futuros no especificados. El resto están disponibles para ser usadas en la Internet IPv4 pública, la cual, a medida que ha aumentado la cantidad de dispositivos queriendo ingresar a la red de Internet,

se ha vuelto insuficiente, por lo que se empezó a afrontar un agotamiento de direcciones. Una fase de agotamiento se refiere a que se entra en una etapa de reservas en donde las asignaciones se van limitando en tamaño y periodicidad. La finalización del protocolo IPv4 comprende 4 etapas fundamentales:

- La fase 0, la cual dio inicio en octubre de 2013 y se realizaron las asignaciones de recursos hasta alcanzar el último /9 disponible.
- La fase 1, la cual dio inicio en mayo de 2014, donde se alcanzó el último /9, incluyendo los dos /10 reservados para la terminación gradual de IPv4 y para nuevos integrantes.
- La fase 2, la cual dio inicio en junio de 2014, donde se asignó el último bloque /10, es aquí donde se activa el punto 11.2 del Manual de Políticas, en donde se reserva un bloque /10 para terminación gradual. Hasta este punto el número de direcciones disponibles era menor a 4 194 304.
- La fase 3, la cual dio inicio en febrero de 2017 y terminará cuando se asigne el último bloque /10 de terminación gradual y será la última reserva que asigne LACNIC, el cual está compuesto por bloques recuperados y devueltos y por bloques postagotamiento asignados por IANA. Solo se le asignará a miembros nuevos entre un /22 y un /24.

Debido a estas fases de agotamientos de las direcciones IPv4, se crea un nuevo protocolo de internet: IPv6, el cual utiliza direcciones de 128 bits dando lugar a $3{,}4 \times 10^{38}$ direcciones, y con mejoras en su cabezal. Con este nuevo protocolo se puede ser capaz de cubrir la demanda de la red hoy en día.

Práctica 2 – Material 2

Investigación

Investigue sobre:

1. Los diferentes RIR que existen en las diferentes regiones del mundo.
2. ¿Cuáles son las fases de agotamiento en las regiones que administran estos RIR?
3. ¿Qué medidas se utilizaron para frenar el agotamiento de IPv4?
4. Encuentra usted alguna otra solución para evitar este agotamiento. Explique.

Material 2
Mecanismos de Transición

- Introducción

Bienvenidos a este módulo de IPv6 básico para el Laboratorio de Telecomunicaciones y Redes Locales, en esta segunda clase se abarcarán diferentes temas sobre los diferentes mecanismos de transición para realizar de forma amigable una transición de IPv4 a IPv6.

- Mecanismos de transición

¿Pueden convivir IPv4 e IPv6? Sí, sin embargo, hay que tener claro que son protocolos incompatibles, y que en el momento de querer migrar de IPv4 a IPv6 se debe buscar la mejor manera de transición, tomando en cuenta la coexistencia con IPv4 y sin interferir en su funcionamiento, persiguiendo así dos objetivos: la conectividad IPv6 en las redes y solucionar la escasez de IPv4.

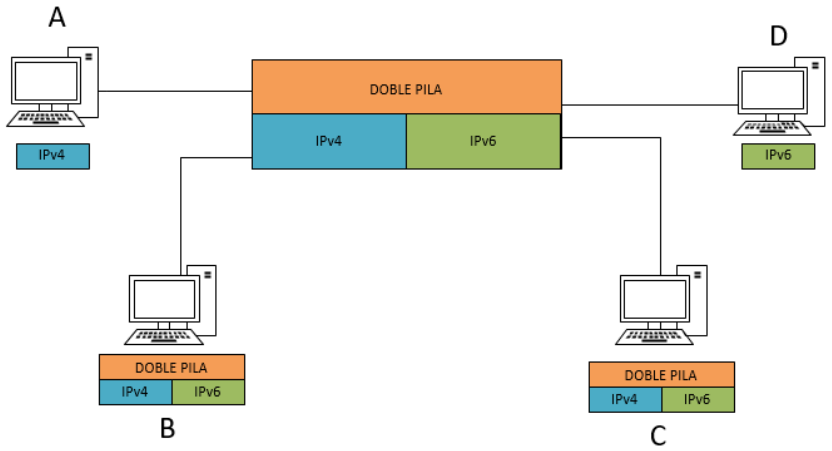
Para poder realizar esta transición podemos seguir ciertas vías generales:

- IPv6 debe coexistir con IPv4.
- Se debe seguir el mismo esquema que IPv4.
- Se debe realizar cualquiera de las tres estrategias: IPv6 nativo, túneles o traducción.
- Se debe tener en cuenta que cada caso es distinto, ya que cada red podrá ser manejada con distinta estrategia.

- Doble pila

Con este mecanismo tanto IPv4 como IPv6 pueden funcionar simultáneamente y en forma paralela, por lo que será necesario una red que maneje puramente IPv4 y, por otro lado, una red que maneje puramente IPv6, y donde el *host* cliente será el encargado de decidir qué protocolo utilizar. Este mecanismo es la opción más amigable con IPv4 y permite una transición gradual hacia IPv6, en donde por defecto se le dará preferencia a IPv6. Una desventaja con este mecanismo es que el esquema se vuelve más complejo y costoso, y ya que aumenta la cantidad de recursos se debe realizar una doble configuración y seguridad.

Figura 19. **Doble pila**



Fuente: elaboración propia.

En la figura 20 se muestra un ejemplo de cómo se manejaría doble pila. En esta red que llamaremos RED1 se cuenta con 4 computadoras nombradas A,B,C,D. Supongamos que cada computadora ingresa a una página web, esta página está montada en un servidor web que maneja doble pila, es decir maneja el protocolo IPv4 e IPv6. Como se ha mencionado antes, el protocolo a

utilizar lo decidirá la máquina cliente, así que el *host* A, que solo trabaja con el protocolo IPv4, realiza la conexión bajo este protocolo y guardará esta información para futuras conexiones. Por otro lado, el *host* D solamente trabaja bajo el protocolo IPv6, por lo que realiza la conexión bajo este protocolo. Y finalmente los *hosts* B y C trabajan bajo ambos protocolos, así que realizarán la conexión bajo el protocolo IPv6, debido a que este tiene prioridad mayor sobre IPv4.

- Túneles

Con este mecanismo se encapsula una versión IP en otra con el objetivo de atravesar una red. Existen dos opciones: encapsular IPv4 en IPv6, o bien, encapsular IPv6 en IPv4. Dependiendo de su configuración los túneles pueden ser:

  - Estáticos: se configura de manera estática los extremos del túnel, que es como normalmente se realiza.
  - Automáticos: cuando su configuración o parte de ella se establece en manera automática.

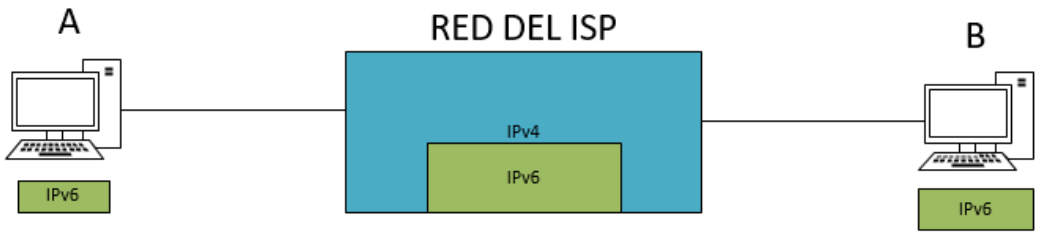
Dependiendo de cómo se conectan los túneles pueden ser:

  - Punto a punto: cuando solamente se conectan dos puntos de red, es decir dos interfaces de túnel, en un extremo se encapsulan y en el otro se desencapsulan.
  - Multipunto: en donde se conectan varios puntos de red o interfaces de túneles, de forma que un paquete que entra en el túnel se encapsula y puede ser entregado en uno de los varios puntos de salida del túnel.

En la práctica podemos encontrar los siguientes túneles:

- 6in4: en este túnel se encapsula IPv6 en IPv4, es un túnel estático, punto a punto y de configuración manual.
- *Broker*: parecido al 6in4, solo que cierta parte del proceso se automatiza configurando un servidor de túneles.
- 6to4: este túnel encapsula IPv6 en IPv4, es automático, multipunto y con un prefijo reservado para su configuración: 2002::16, al cual se le incluyen los 32 bits de dirección IPv4, por lo que es necesario una dirección pública IPv4.
- 6RD: parecido al 6to4, solo que puede ser configurado con direcciones IPv4 privadas, y no es necesario un prefijo reservado.

Figura 20. **Túnel**



Fuente: elaboración propia.

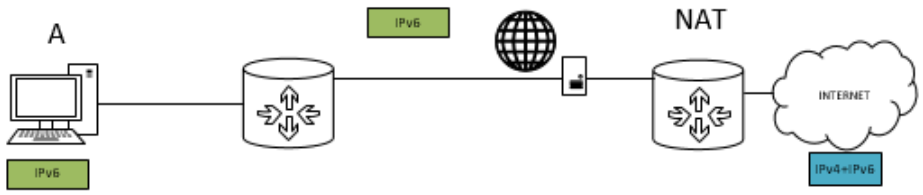
En la figura 21 podemos observar un diagrama de lo que sería el mecanismo de túneles, como ejemplo tomaremos el esquema en el cual dos *hosts*: el *host* denominado como A y el *host* denominado como B, quieren establecer una comunicación entre ellos; estos dos *host* manejan solamente IPv6, el problema radica en que la red del ISP (Proveedor de Servicio de Internet), por la cual se transmite la información, solamente tiene la capacidad

de trabajar con IPv4, por lo que se necesita de un *router* que realice el encapsulamiento de IPv6 en IPv4 y luego que desencapsule IPv6 de IPv4. Con esto, los dos *hosts* que solo hablan IPv6 pueden comunicarse a través de una red que solo habla IPv4.

- Traducción

Este mecanismo resulta necesario para comunicar 2 *hosts* que solo hablen una versión diferente de IP, es el método menos recomendado, pero es utilizado cuando un *host* solo maneja un protocolo. En la práctica solo se encontrarán traducciones de IPv6 a IPv4, y solo debe usarse si no es posible la configuración en doble pila o túneles.

Figura 21. **Ejemplo**



Fuente: elaboración propia.

En la figura 22 se muestra un esquema del mecanismo de traducción, se tiene un *host* que solamente maneja el protocolo de IPv6, este *host* quiere acceder a Internet, específicamente a una página web que solamente trabaja baja el protocolo Ipv4, sin embargo, el ISP que se encarga de brindarle el servicio de Internet al *host* trabaja también bajo el protocolo de Ipv6, por lo que la comunicación entre toda la red del ISP hacia el *host* trabaja sin ningún tipo de problema. Debido a que el host desea comunicarse con una página web que

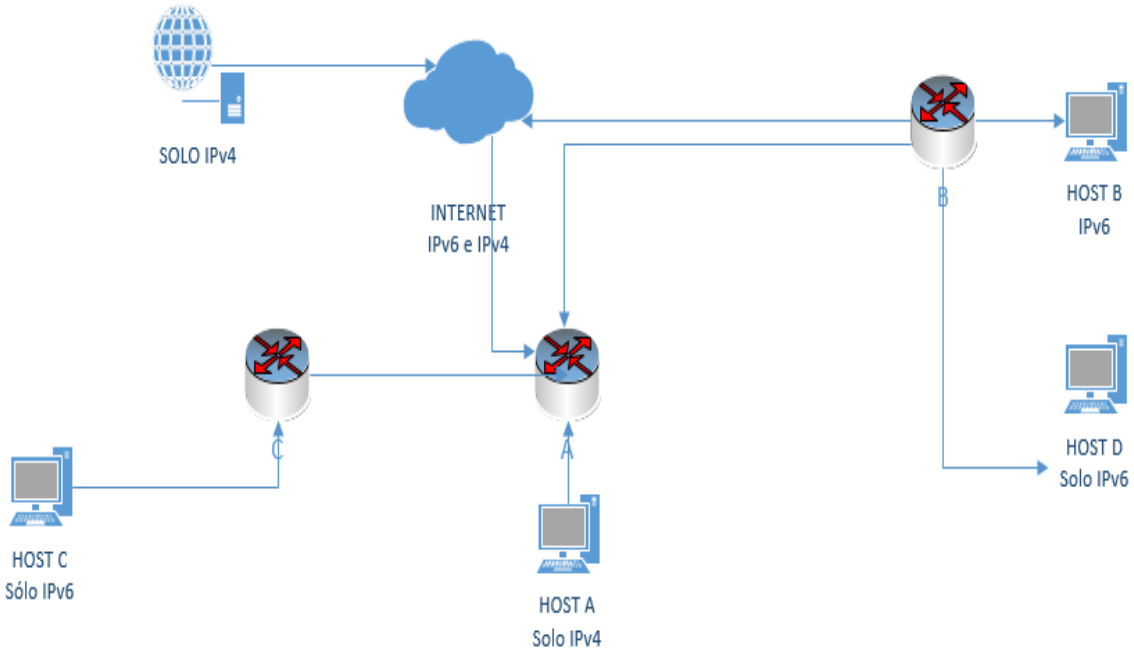
solamente trabaja con el protocolo Ipv4, se necesita un *router* que realice un NAT en el extremo entre el ISP e Internet, este NAT realizará la traducción de la dirección Ipv6 que tiene asignado el *host* y la convertirá a una dirección Ipv4 que permitirá que el *host* finalmente pueda acceder a la página web.

Práctica 2 – Material 2
Análisis de los Mecanismos de Transición

A continuación se presenta el esquema de una red, analícela y responda las siguientes preguntas:

1. ¿Qué tipo de mecanismo de transición utilizaría para comunicar el *host* A al internet? Explique y detalle qué dispositivos se ven involucrados.
2. ¿Qué tipo de mecanismo de transición utilizaría para comunicar el *host* B a la página web? Explique y detalle qué dispositivos se ven involucrados.
3. ¿Qué tipo de mecanismo de transición utilizaría para comunicar el *host* C con el *host* D? Explique y detalle qué dispositivos se ven involucrados.

Figura 22. **Diagrama de red**



Fuente: elaboración propia.

Material 3

Protocolo IPv6

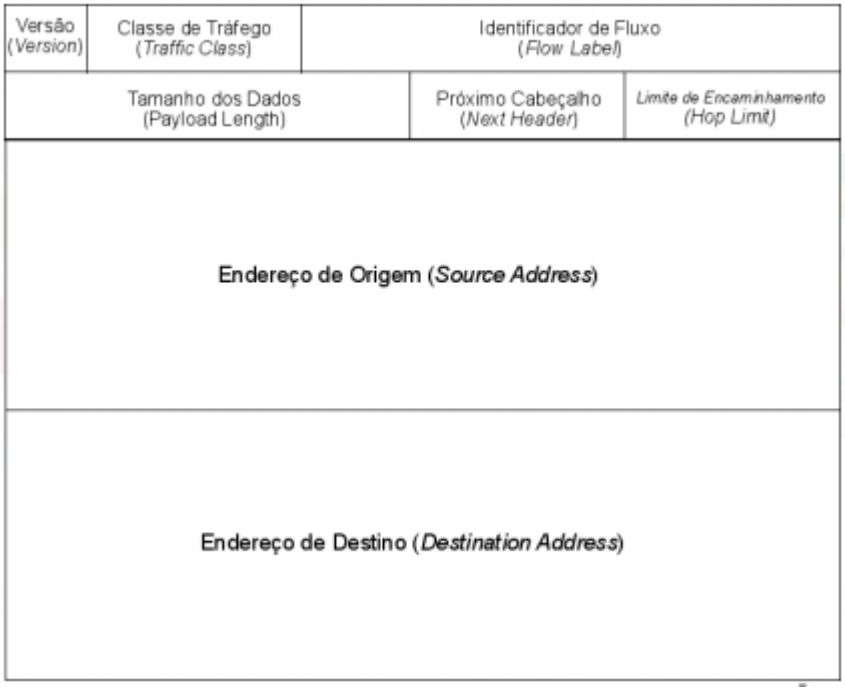
- Introducción

Bienvenidos a este módulo de IPv6 básico para el Laboratorio de Telecomunicaciones y Redes Locales, en esta tercera clase se abarcarán los temas del cabezal de IPv6, los cabezales de extensión y sus características de direccionamiento.

- Cabezal IPv6 básico

Recordando que IPv6 es una evolución de IPv4, algo muy importante para destacar es que el cabezal de IPv6 es bastante simplificado en comparación de IPv4, ya que este cabezal no contiene campos opcionales, por lo que hace que su tamaño sea fijo de 40 bytes. Es un cabezal más flexible gracias a la implementación de cabezales adicionales o de extensión. Para la creación de este cabezal se realizaron cambios y modificaciones del cabezal IPv4: la eliminación de los campos de tamaño del encabezado, identificador, bandera, fragmento, *checksum* y opciones adicionales. Al igual se realizaron cambios de nombre y posición de los siguientes campos: Tipo de Servicio, ubicado en el tercer campo en IPv4, cambia a Clase de Tráfico, ubicado en el segundo campo en IPv6; Tamaño Total, ubicado en el cuarto campo en IPv4, cambia a Tamaños de Datos, ubicado en el cuarto campo en IPv6; Protocolo, ubicado como noveno campo en IPv4, cambia su nombre por Próximo Cabezal, ubicado en el quinto campo en Ipv6, y, por último, Tiempo de Vida, ubicado en el octavo campo en IPv4, cambia su nombre por Límite de Saltos, ubicado en el sexto campo en IPv6.

Figura 23. **Cabezal básico de IPv6**



Fuente: LACNIC. *Tutorial IPv6 01.* P. 6

- Cabezales de extensión

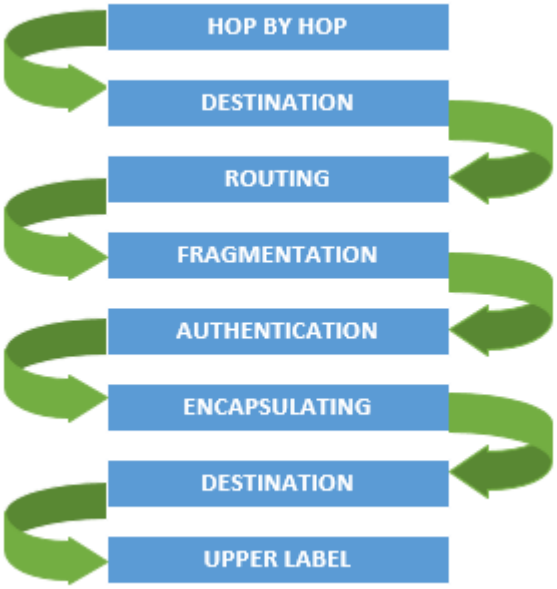
Estos cabezales añaden funcionalidades en capa 3, lo que hace que el cabezal sea más flexible. Estos cabezales son limitados y deben ser configurados de forma ordenada, así podrán ser utilizados como máximo una sola vez (a excepción de *Destination*).

  - *Hop-by-hop*, este cabezal es procesado por cada *router* (nodo) a lo largo del camino que siga el paquete, y se identifica por el valor “0” en el campo “Próximo Cabezal”.

- *Destination*, este cabezal es procesado por el *router*/nodo destino del paquete, y se identifica por el valor 60 en el campo “Próximo Cabezal”.
- *Routing*, este cabezal enlista uno o más *routers*/nodos intermedios que debería atravesar el paquete antes de llegar a su destino y se identifica por el valor 43 en el campo “Próximo Cabezal”.
- *Fragmentation*, este cabezal es procesado en el *router*/nodo de destino, es el encargado de cargar información sobre los fragmentos de los paquetes IPv6 y se identifica por el valor 44 en el campo “Próximo Cabezal”.
- *Authentication* (AH), este cabezal es utilizado por IPSec, el cual provee autenticación y garantía de integridad en los paquetes, y es identificado por el valor 51 en el campo “Próximo Cabezal”.
- *Encapsulation* (ESP), este cabeza cifra el contenido, también es utilizado por IPsec, el cual garantiza la integridad y confidencialidad de los paquetes, y es identificado por el valor 52 en el campo “Próximo Cabezal”.
- *Destination*, este cabezal solamente es procesado por el *router*/nodo destino.
- *Upper Label*, este cabezal es utilizado para protocolos de capa superior.

La siguiente imagen muestra el orden en que deben ser utilizados los cabezales en ocasiones en que se configure más de un cabezal.

Figura 24. **Orden de cabezales de extensión**



Fuente: elaboración propia.

- Características generales de direccionamiento de IPv6

Reglas básicas de notación:

- De los 128 bits que componen el direccionamiento de IPv6, se realiza la división de 8 grupos de 16 bits cada uno, separados por dos puntos ":".
- La notación utilizada es la hexadecimal en cada grupo de *nibble* (4 bits).
- El uso de mayúsculas y/o minúsculas es indiferente.

Como ejemplo podemos encontrar el siguiente direccionamiento en IPv6:

2001:0db8:0321:0D10:0000:0000:0000:1000.

- Reglas de compresión

    - Los ceros a la izquierda en cada grupo se pueden eliminar.
    - Si uno o más grupos contienen solamente ceros, estos pueden cambiarse por “::”. Para el uso de esta regla se debe tener en cuenta que se puede suprimir y expandir sin ningún problema, y que esta regla puede utilizarse solamente una vez.
    - Se puede usar corchetes “[ ]“ para indicar algún puerto. Esto es importante, ya que logra evitar confundir un puerto con la nomenclatura de IPv6.

A modo de ejemplo:

- 2001:0db8:0321:0D10:0000:0000:0000:1000, existen grupos que contiene en su lado izquierdo un cero, por lo que se puede proceder a eliminarlo, seguidamente se logra observar que tres grupos constan solamente con ceros, estos grupos pueden ser comprimidos, por lo que el direccionamiento queda de la siguiente manera: 2001:db8:321:D10::1000.

- Ahora bien, si el direccionamiento a comprimir fuese: 2001:db8:0000:0000:0ABC:0000:0000:1234, se puede observar que existen dos grupos seguidos diferentes que constan solamente de ceros, por lo cual debe recordarse que la regla de aplicar doble dos puntos puede utilizarse una sola vez; una solución para realizar la compresión sería de la siguiente manera: 2001:db8:0:0:ABC::1234.

Nota: para los prefijos en IPv6 se sigue notación CIDR (prefijo/longitud de prefijo), a lo cual se le puede aplicar las reglas de compresión vistas anteriormente.

- Configuración de IPv6

Existen dos pasos importantes que deben seguirse para configurar IPv6:

- Activar el reenvío de tráfico IPv6 en el equipo
- Configurar las interfaces que requieren IPv6

Para configurar una dirección IPv6 en un dispositivo (enrutador), es importante tomar en cuenta los siguientes comandos: ipv6 *unicast-routing* para activar el reenvío de tráfico en IPv6, e IPv6 *address* [dirección asignada], como se muestra a continuación:

Figura 25. **Configuración básica de una interface**

A

```
A>enable
A#conf t
A(conf)#ipv6 unicast-routing
A(conf)#int fa0/0
A(conf-if)#ipv6 address 2001:A:A:A:C::5/64
A(conf-if)#no shutdown
A(conf-if)#end
```

Fuente: elaboración propia.

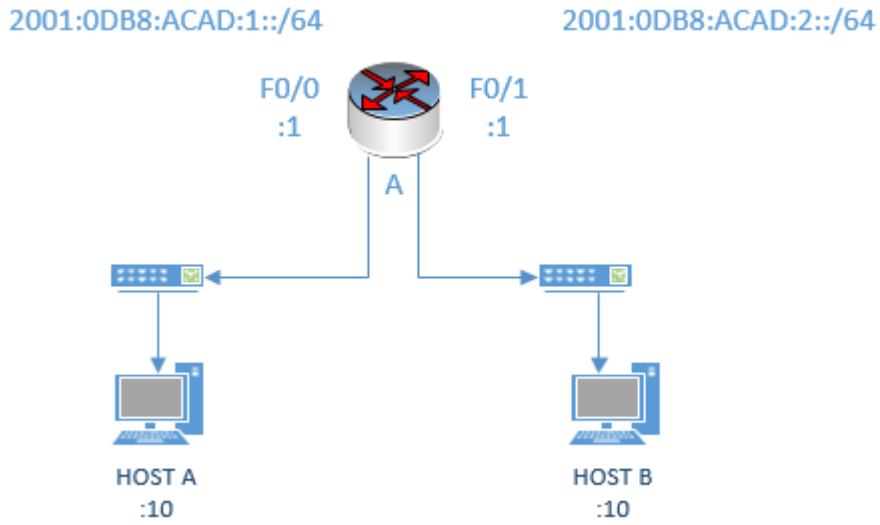
Práctica 3 – Material 3
Ejercicios de Direccionamiento de IPv6

A. Con base en las reglas de notación y compresión vistas en clase, realizar los siguientes ejercicios (escriba todas las posibles soluciones para cada uno):

1. 2001:0DB8:0000:0000:0000:0000:1428:57AB
2. 2031:0000:130F:0000:0000:09C0:876A:130B
3. E3D7:0000:0000:0000:51F4:00C8:C0A8:6420
4. 3FFE:0501:0008:0000:0260:97FF:FE40:EFAB
5. BA98:0074:3210:000F:0000:0000:FFFF puerto 554
6. 0000:0000:0000:0000:0000:0000:0001
7. FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
8. 0000:0000:0000:0000:0000:0000:ce7b:1f01 puerto 8003
9. FE80:0000:0000:0000:0000:0000:0000:0009
10. 3FF3:0B00:0C18:0001:0000:1234:AB34:0002 puerto: 443

B. Configuración de IPv6 en una interfaz de un enrutador:

En este esquema muy simple y sencillo se muestra un *router* A al cual se le configurarán las direcciones para cada una de las interfaces, de igual manera se configurarán las direcciones para el *host* A y el *host* B:



A>ena

A#conf t

A(config)# ipv6 unicast-routing

A(config)#int f0/0

A(config-if)#ipv6 address 2001:db8:acad:1::1/64

A(config-if)#no shutdown

A(config-if)#exit

A(config)#int f0/1

A(config-if)#ipv6 address 2001:db8:acad:2::1/64

A(config-if)#no shutdown

A(config-if)#exit

A(config)#exit

A#wr

Al tener configuradas las interfaces, nos dirigimos a la configuracion de la computadora:

HOST A

Direccion IPv6: 2001:db8:acad:1::10

Longitud del prefijo de red: 64

Puerta determinada (Gateway): 2001:db8:acad:1::1

HOST B

Direccion IPv6: 2001:db8:acad:2::10

Longitud del prefijo de red: 64

Puerta determinada (Gateway): 2001:db8:acad:2::1

Tarea:

A. Investigue sobre los diferentes tipos de direccionamiento en IPv6, escribiendo el uso y diferencia entre cada uno, y proporcione ejemplos de cada direccionamiento.

Material 4
Enrutamiento en IPv6

- Introducción

Bienvenidos a este módulo de IPv6 básico para el Laboratorio de Telecomunicaciones y Redes Locales, en esta cuarta clase se abarcarán diferentes temas sobre los diferentes protocolos de enrutamiento que pueden ser configurados en IPv6.

- **Enrutamiento estático**

¿Qué es enrutamiento estático? Una ruta estática es una ruta que es introducida manualmente en la tabla de rutas de un *router*, para que esta ruta exista debe ser creada de forma explícita y es una de las múltiples fuentes de información que posee un *router* para elaborar su tabla de reenvío. La diferencia que tiene con una ruta dinámica es que es incapaz de reaccionar a cambios en la red de forma automática.

Entre sus ventajas se encuentra la simplicidad a la hora de planificar e implementar la rapidez de implementación, y que el uso y la sintaxis es similar al de IPv4. Por otra parte, una desventaja es que no es una solución escalable para una red grande con muchas rutas y enrutadores si la red sufre cambios constantes.

- **Enrutamiento dinámico IGP en IPv6**

¿Qué es un enrutamiento dinámico? Un enrutamiento IGP, de sus siglas en ingles de Interior Gateway Protocol, es el protocolo de enrutamiento

dinámico para enrutar redes dentro de un mismo Sistema Autónomo o AS. Un enrutamiento dinámico puede clasificarse de la siguiente manera: por vector distancia (el número de saltos que toma un paquete para llegar a su destino), o bien, por estado enlace (el mejor ancho de banda de un enlace para llegar al destino), y con base en esta clasificación existen varios protocolos IGP: RIP, OSPF, IS-IS, entre otros, los cuales siguen distintos criterios de selección para seguir una ruta, y siguen las mismas directrices tanto para IPv4 como para IPv6.

- Enrutamiento RIPng

Extensión de RIPv1 y RIPv2 para soportar direcciones de 128 bits, es decir direcciones IPv6. Este protocolo es capaz de realizar el encaminamiento de prefijos IPv6: prefijo/longitud. En una topología en donde se maneja doble pila, si se utiliza RIP harán falta 2 procesos distintos: uno para IPv4 configurando RIPv2, y otro para IPv6 utilizando RIPng. Es importante destacar que RIPng solamente utiliza direcciones *link-local* como *next-hop.*

Cuando se habilita RIPng en una interfaz de un *router* se realizarán tres cosas:

  - Se enviarán actualizaciones RIP por esta interfaz
  - Se procesarán las actualizaciones RIP recibidas en esta interfaz
  - Anunciarán las rutas conectadas de esta interfaz

- Enrutamiento OSPFv3

Es un protocolo de enrutamiento OSPF para IPv6, este protocolo es una modificación de OSPFv2 y es capaz de soportar direcciones *next hop* y prefijos

de 128 bits mediante nuevos LSAs, los cuales describen el estado de una red o un *router*. Esta nueva versión para IPv6 es muy similar a OSPFv2, solamente que este no funciona sobre una subred sino sobre un enlace. Puede usarse IPsec para ofrecer autenticación, el *router* ID consta de 32 bits, permite varias instancias por interfaz y se utilizan direcciones *multicast* IPv6 para la comunicación: FF02::5 o bien FF02::6. De igual forma, si se trabaja bajo una topología de doble pila debe configurarse tanto OSPFv2 para IPv4 como OPSFv3 para IPv6.

- Enrutamiento IS-IS

IS-IS es un protocolo de encaminamiento OSI diseñado para soportar el protocolo IPv6, el cual corre sobre capa de enlace y ha sido extendido para poder soportar tanto IPv4 como IPv6.

Práctica 4 – Material 4

Enrutamiento IPv6

Con el siguiente esquema deberá configurar una ruta estática, una ruta por RIPng y una ruta por OSPFv3. Debe tener en cuenta que la PC de la red :1::/64 tendrá la dirección :10, y la que la PC de la red :3::/64 tendrá la dirección :10; la interface f0/0 del router A tendrá la :1, mientras que la interface f0/0 del router B tendrá la :2.

- Configuración de ruta estática

A>ena
A#conf t
A(config)# ipv6 unicast-routing
A(config)#int f0/1
A(config-if)#ipv6 address 2001:db8:acad:1::1/64
A(config-if)#no shutdown
A(config-if)#exit
A(config)#int f0/0
A(config-if)#ipv6 address 2001:db8:acad:2::1/64
A(config-if)#no shutdown
A(config-if)#exit
A(config)#ipv6 route 2001:db8:acad:3::/64 2001:db8:acad:1::2
A(config)#exit
A#wr

B>ena
B#conf t
B(config)# ipv6 unicast-routing
B(config)#int f0/1
B(config-if)#ipv6 address 2001:db8:acad:3::1/64
B(config-if)#no shutdown
B(config-if)#exit
B(config)#int f0/0
B(config-if)#ipv6 address 2001:db8:acad:2::2/64
B(config-if)#no shutdown
B(config-if)#exit
B(config)#ipv6 route 2001:db8:acad:1::/64 f0/0
B(config)#exit
B#wr

Por último, debe configurar las direcciones de la PC A y la PC B, y realizar pruebas de conectividad.

- Configuración de RIPng

Para configurar RIPng, basta con el comando ipv6 rip “nombre” enable. Establecemos “nombre” como el nombre del dominio al que pertenecerán. Esto se hace en cada interfaz que se quiera publicar; como queremos publicar todas, estableceremos este comando en la interface f0/0 y f0/1 tanto en el *router* A como en el *router* B.

A>ena
A#conf t

A(config)# ipv6 unicast-routing
A(config)#int f0/1
A(config-if)#ipv6 address 2001:db8:acad:1::1/64
A(config-if)#no shutdown
A(config-if)#ipv6 rip RUTARIP1 enable
A(config-if)#exit
A(config)#int f0/0
A(config-if)#ipv6 address 2001:db8:acad:2::1/64
A(config-if)#no shutdown
A(config-if)#ipv6 rip RUTARIP1 enable
A(config-if)#exit
A(config)#exit
A#wr

B>ena
B#conf t
B(config)# ipv6 unicast-routing
B(config)#int f0/1
B(config-if)#ipv6 address 2001:db8:acad:3::1/64
B(config-if)#no shutdown
B(config-if)#ipv6 rip RUTARIP1 enable
B(config-if)#exit
B(config)#int f0/0
B(config-if)#ipv6 address 2001:db8:acad:2::2/64
B(config-if)#no shutdown
B(config-if)#ipv6 rip RUTARIP1 enable
B(config-if)#exit
B(config)#exit
B#wr

Por último, debe configurar las direcciones de la PC A y la PC B, y realizar pruebas de conectividad.

- Configuración OSPFv3

A>ena
A#conf t
A(config)# ipv6 unicast-routing
A(config)#int f0/1
A(config-if)#ipv6 address 2001:db8:acad:1::1/64
A(config-if)#no shutdown
A(config-if)#ipv6 ospf 1 area 0
A(config-if)#exit
A(config)#int f0/0
A(config-if)#ipv6 address 2001:db8:acad:2::1/64
A(config-if)#no shutdown
A(config-if)#ipv6 ospf 1 area 0
A(config-if)#exit
A(config)#ipv6 router ospf 1
A(config-ospf)# router-id 0.0.0.1
A(config-ospf)# end
A#wr

B>ena
B#conf t
B(config)# ipv6 unicast-routing
B(config)#int f0/1
B(config-if)#ipv6 address 2001:db8:acad:3::1/64

B(config-if)#no shutdown

B(config-if)#ipv6 ospf 1 area 0

B(config-if)#exit

B(config)#int f0/0

B(config-if)#ipv6 address 2001:db8:acad:2::2/64

B(config-if)#ipv6 ospf 1 area 0

B(config-if)#no shutdown

B(config-if)#exit

B(config)#ipv6 router ospf 1

B(config-ospf)#router-id 0.0.0.2

B(config-ospf)#end

B#wr

Finalmente se configuran las direcciones para la PC A y para la PC B, y se realizan pruebas de conectividad.

Tarea:

Con el mismo esquema propuesto configure la ruta utilizando IS-IS.

Material 5
Servicios con IPv6

- Introducción

Bienvenidos a este módulo de IPv6 básico para el Laboratorio de Telecomunicaciones y Redes Locales, en esta quinta y última clase se abarcarán los temas de servicios que pueden ser configurados bajo el protocolo IPv6 y amenazas que puede existir al utilizar este nuevo protocolo.

Migrar de IPv6 a IPv4 no solo conlleva la configuración de *switches* y *routers*, sino también de servicios como: servidores DNS, servidores web, NTP y la implementación de cierta seguridad para el resguardo de la información dentro de la red.

- **Servidor DNS en IPv6**

¿Qué es un servidor DNS? Un servidor DNS tiene como función ser una base de datos distribuida en donde los datos se van separando y ordenando según las etiquetas de texto separadas por un punto (nombre de dominio). Un servicio DNS tiene dos posibles resoluciones: la resolución directa, la cual resuelve de nombres a direcciones IP, y la resolución inversa, la cual resuelve de direcciones IP a nombres.

Un nombre de dominio suele estar servido por varios servidores:

- Maestro o primario: donde se hacen los cambios y se actualiza la versión del fichero de zona que contiene datos asociados al nombre de dominio.
- Esclavo o secundario: el maestro avisa de una nueva versión de datos y los esclavos solicitan actualización o transferencia de zona.

- **Servidor web en IPv6**

Al implementar un servidor web, se pueden encontrar dos configuraciones comunes: Apache, que trabaja sobre el sistema Linux, e IIS, que trabaja sobre el Sistema de Microsoft Windows. En cualquiera de las dos configuraciones se utiliza http o bien https, los cuales utilizan una conexión TCP, y pueden ser configurados tanto en IPv4 como en IPv6. Una vez conectados el comportamiento es muy similar en ambos protocolos.

- **Seguridad en IPv6**

¿IPv6 es más o menos seguro que IPv4? IPv6 no es ni más ni menos seguro que IPv4. Debido a esto es importante clasificar los tres tipos de categorías para las amenazas respecto a seguridad en IPv6:

- Aquellas amenazas que ya existían en IPv4 y se comportan de una manera muy similar en IPv6, como por ejemplo: *sniffing*, ataques a otras capas y *flooding.*
- Aquellas amenazas que ya existían con IPv4 y se comportan distinto con IPv6, como por ejemplo: el escaneo de la red y amplificación (*smurf*).

- Aquellas amenazas que aparecieron con la creación de IPv6, como por ejemplo: amenazas a NDP, *routing header* tipo O y cabeceras de extensión.

- Amenazas NDP

Neighbor Discovery Protocol es un protocolo vulnerable a diversos ataques, autoconfigura nodos IPv6 y permite descubrir a otros nodos del mismo enlace, así como determinar su dirección de nivel de red y mantener información de la ruta IPv6 hacia otros nodos activos. Realiza la autoconfiguración de la dirección IPv6 por medio del envío de paquetes *Router Advertisement* (RA).

Estos RA son utilizados para el ataque a NDP realizando las siguientes acciones: el atacante se hace pasar por un *router*, crea un prefijo falso en el enlace, crea un prefijo falso para la configuración de direcciones y crea parámetros falsos, y estos ataques crean lo que se denominan ataques DoS.

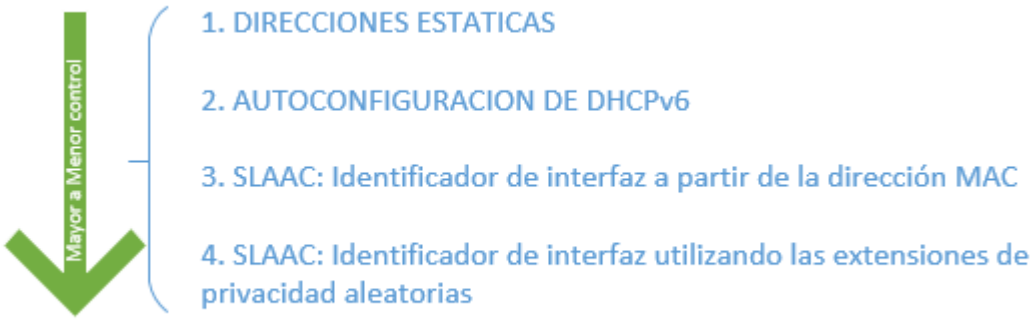
- Routing header tipo 0

El RH0 puede ser usado para acumular tráfico sobre un camino remoto con el propósito de degradar el tráfico o DoS. Es considerado una amenaza grave, por lo que se prohibió su uso en el RFC5095. Los atacantes pueden usar maliciosamente los encabezados de enrutamiento tipo 0 para eludir el filtraje de paquetes, es decir las políticas de listas de acceso de IPv6 o el enrutamiento y direccionamiento de difusión ilimitada. Este tipo de encabezados puede usarse para realizar ataques de DoS reflejados, *spoofing, spoofing* doble y ataques de ampliación, llamados también ataques *ping-pong* que causan saturación en el enlace, causando problemas de rendimiento a través del procesamiento adicional de la CPU.

- Recomendaciones de seguridad en IPv6

Una recomendación a destacar es la configuración de direcciones IPv6, de manera que se maneje un sistema jerárquico en donde lo más alto será todo aquello que puede tener un mayor control, hasta terminar por aquello de que se tenga menor control. Es importante manejar ciertos métodos de configuración y direcciones. Como ejemplo se muestra la figura 25, en que como cúspide de la pirámide se encuentran las direcciones estáticas, debido a que se configuran de manera manual, por lo que se tiene un mejor control al identificar qué dispositivo tiene configurada cierta dirección IP.

Figura 26. **Ejemplo de jerarquía de control**



Fuente: elaboración propia.

Será común configurar varias direcciones IPv6 en una sola interfaz, y se debe seleccionar direcciones difíciles de poder ser adivinadas, debido a que los patrones de escaneo han cambiado para IPv6.

Práctica 5 – Material 5

Servicios con IPv6

- Servidor DNS – Resolución directa

    - Montar Bind 9 en un sistema operativo virtualizado Linux.
    - Configurar la dirección IPv4 al servidor: 10.0.53.50/24
    - Configurar la dirección IPv6 al servidor: 2001:db8:0:53::50/64
    - Se configurará el servidor para que esté a cargo del dominio moduloipv6.com, es decir para que responda a peticiones de dominio que terminen en moduloipv6.com.

Se añadirán las siguientes entradas:

    - ns.moduloipv6.com: tendrá como direcciones asociadas 10.0.53.50 y 2001:db8:0:53::50.
    - www.moduloipv6.com: tendrá como direcciones asociadas 10.0.80.80 y 2001:db8:0:80::80
    - ipv4.moduloipv6.com: tendrá como dirección asociada la 10.0.80.80
    - ipv6.moduloipv6.com: tendrá como dirección asociada la 2001:db8:0:80::80

- BIND contiene un fichero de configuración principal en la siguiente dirección: /etc/bind/named.conf, el cual incluye el fichero /etc/bind/named.conf.options. La opción que le indica a BIND que logre

escuchar peticiones sobre IPv6 es listen-on-v6{}; que viene por defecto configurada.

```
options {
        directory “/var/cache/bind”;
        Listen-on-v6 { any; };
};
```

- El comando *any* le indica a BIND que escuche en cualquier dirección IPv6 configurada en el sistema operativo donde se ejecuta, mientras que el parámetro *directory* indica cuál es la carpeta por defecto donde buscará los ficheros de configuración de zonas. Para visualizar si BIDN está escuchando por el puerto 53 y en qué IPs utilizar el comando netstat -tan.
- Para configurar que el servidor sepa que está a cargo del dominio moduloipv6.com debemos añadir al fichero /etc/bind/named.conf.local

```
zone “moduloipv6.com” {
        type master;
        file “moduloipv6.com.zone”;
};
```

- Crear el fichero configurado antes (/var/cache/bind/moduloipv6.com.zone), llamado fichero de zona, conteniendo toda la información relacionada con la resolución directa del dominio moduloipv6.com. Para configurar el fichero podemos utilizar el comando *sudo nano /var/cache/bid/moduloipv6.com.zone*

```
$TTL 86400
@ IN SOA ns.moduloipv6.com. admin.moduloipv6.com (
            2015091901 ; serial
            604800 ; refresh
            86400 ; retry
            2419200 ; expire
            86400 ; negative cache TTL
     )
            IN    NS    ns.moduloipv6.com.
ns          IN    A           10.0.53.50
            IN    AAAA        2001:db8:0:53::50

www         IN    A           10.0.80.80
            IN    AAAA        2001:db8:0:80:80

ipv6        IN    AAAA        2001:db8:0:80::80

ipv4        IN    A           10.0.80.80
```

- Comprobar si la configuración introducida es la correcta con el comand: *named-checkzone moduloipv6.com /var/cache/bind/moduloipv6.com.zone*
- Una vez realizada la comprobación reiniciar el servidor: *sudo service bind9 restart.*
- Comprobar si el servidor ha iniciado correctamente y cargado la zona moduloipv6.com: *sudo tail –f /var/log/syslog*
- Para probar la resolución DNS, se usará la herramienta dig, en el mismo servidor DNS, ejecutando consultas al mismo servidor local,

usando la dirección IPv6 ::1, *dig any www.moduloipv6.com @::1 +short*

Tarea:

Montar un servidor web ya sea en Linux o Windows Server, bajo el protocolo IPv6 en una máquina virtual, ya sea en virtualbox, vmware o hyper-v.

Fuente: elaboración propia