INSTITUTO POLITECNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD PROFESIONAL "ADOLFO LOPEZ MATEOS"

INGENIERIA EN COMUNICACIONES Y ELECTRÓNICA

"Transición de Ipv4 a Ipv6"

PROYECTO TERMINAL

QUE PARA OBTENER EL TITULO DE:
INGENIERO EN COMUNICACIONES Y ELECTRONICA

PRESENTAN:

Cristian Joshue Delgado Ponce
José Eduardo Lara Alvarado

ASESORES:

Ing. Guillermo Santillán Guevara
Ing. Pedro Morales

MEXICO, D.F. a 28 de Febrero de 2016

INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD PROFESIONAL "ADOLFO LÓPEZ MATEOS"

T E M A D E T E S I S

QUE PARA OBTENER EL TÍTULO DE — **INGENIERO EN COMUNICACIONES Y ELECTRONICA**

POR LA OPCIÓN DE TITULACIÓN — **TESIS COLECTIVA Y EXAMEN ORAL INDIVIDUAL**

DEBERA (N) DESARROLLAR — **C. DELGADO PONCE CRISTIAN JOSHUE**

C. LARA ALVARADO JOSÉ EDUARDO

"TRANSICIÓN DE IPV4 A IPV6"

ANALIZAR ALGUNAS TÉCNICAS DE TRANSICIÓN DE IPV4 A IPV6 QUE ESTABLECEN UNA COMUNICACIÓN DE EXTREMO A EXTREMO BAJO DIFERENTES POSIBILIDADES.

- **ANTECEDENTES DEL PROTOCOLO IP.**
- **CARACTERÍSTICAS Y CONCEPTOS DE IPV6.**
- **PROTOCOLOS IPV6.**
- **TÉCNICAS DE TRANSICIÓN DE IPV4 A IPV6.**

MÉXICO D. F., A 28 DE ENERO DE 2016.

A S E S O R

ING. GUILLERMO SANTILLÁN GUEVARA

ING. PEDRO MARTÍN MORALES BECERRA

RAMIREZ LORENA

ING. PATRICIA LORENA RAMÍREZ RANGEL
JEFE DEL DEPARTAMENTO ACADÉMICO DE
INGENIERÍA EN COMUNICACIONES Y ELECTRÓNICA

“Transición de Ipv4 a Ipv6”.

INDICE

INTRODUCCION.

PLANTEAMIENTO DEL PROBLEMA.

Debido al exponencial crecimiento de la internet surge la necesidad de tomar decisiones para continuar con el buen funcionamiento de esta, así es como llegamos a IPv6 (Internet Protocol version 6) el cual es el sucesor del actual IPv4 (Internet Protocol version 4), fue definido por la IETF (Internet Engineering Tak Force).

IPv6, también llamado IPng (Internet Protocol next generation) en sus inicios fue diseñado para cubrir las ineficiencias de IPv4.

Entonces podemos clasificar el problema de IPv4 desde dos puntos de vista:

1.- Técnico: Donde el direccionamiento es insuficiente debido a la gran demanda y que a futuro incrementa considerablemente. Los routers son los encargados de almacenar las tablas de enrutamiento, dichas tablas son empleadas para saber hacia dónde se debe encaminar un datagrama, las tablas son excesivamente grandes debido a la enorme cantidad de direcciones que existen actualmente y al protocolo de enrutamiento utilizado, lo que obliga a los routers a mantener grandes cantidades de direcciones IP (Internet Protocol) para conocer hacia donde deben re direccionar los datagramas.

2.- Social: Las necesidades de los usuarios del servicio de la internet han aumentado de manera exponencial, exigiendo nuevas capacidades tales como: seguridad, privacidad, velocidad, etc., que la versión IPv4 no puede proporcionar como lo proporcionaría el protocolo IPv6.

El trabajo de investigación consiste en mostrar las diferentes técnicas o mecanismos para llevar a cabo una transición de IPv4 a IPv6, dar una vista hacia el problema o limitación de IPv4 y dar un paso hacia la nueva generación.

OBJETIVO GENERAL.

Analizar algunas técnicas de transición de IPv4 a IPv6 que establecen una comunicación de extremo a extremo bajo diferentes posibilidades.

OBJETIVOS PARTICULARES.

Describir los antecedentes del protocolo IPv4, el porqué de su deterioro y por qué se debe hacer una transición.

Mostrar el funcionamiento del protocolo IPv6 describiendo la cabecera del mismo y sus características.

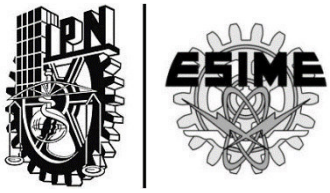
Mostrar la relación del protocolo IPv6 con los protocolos más importantes para tener una comunicación.

Analizar los mecanismos de transición y aplicar las técnicas configurándolas en una red para obtener el cambio del protocolo IPv4 al protocolo IPv6.

JUSTIFICACIÓN.

En consecuencia al gran crecimiento que existe del uso de la tecnología en el mundo, surge el amplio desarrollo de dispositivos electrónicos que ayuden a resolver problemas de la vida diaria o alguna otras necesidades, esto trae consigo mismo el uso del servicio de la red de internet, en la actualidad se utiliza IPv4 que es parte fundamental sustentado por el sistema TCP/IP (Transmision Control Protocol/ Internet Protocol) para el funcionamiento de la internet , pero en dicho protocolo anterior surge un gran problema, principalmente el agotamiento de las direcciones, IPv4 consta de direcciones IP de 32 bits, dicho número de direcciones se ha convertido en una limitante para el gran crecimiento del uso de la internet en el mundo, ya que estadísticas revelan que para el año pasado dichas direcciones habrían llegado a su fin y aunque se han creado algunos métodos para mantener el espacio de direcciones como lo es el CIDR (Classless Inter-Domain Router),que consiste básicamente en dividir rangos de direcciones IP en redes separadas, permitiendo un uso más eficiente de las escasas direcciones IPv4. Pero esto no resolvió el problema del todo, si no que solamente retraso la transición hacia un nuevo protocolo.

Para poder llegar a una solución de dicho problema se busca una transición al protocolo IPv6, el cual cuenta con un número de direcciones IP de 128 bits, este campo es lo suficientemente grande para manejar el crecimiento continuo de la internet mundial por varias décadas, pues el número de direcciones que ofrece dicho protocolo es alrededor de $3.40x10^{38}$ direcciones aproximadamente.



CAPÍTULO 1:
“Antecedentes del Protocolo IP.”

CAPITULO 1: "ANTECEDENTES DEL PROTOCOLO IP".

1.1 Situación Actual.

Nos encontramos con la actual versión del protocolo IP, la cual es Ipv4, es conocido que en dicho protocolo el espacio de sus direcciones está llegando a su fin, en América Latina y el Caribe llegará a su fin ya que la RIR (Registro Regional de Internet) de la internet en América Latina y el Caribe LACNIC (Latin America & Caribean Network Information Centre) anunció que después de llegar a la cuota de 4,194,302 direcciones IPv4, estas van llegando a su fin. El pasado 10 de junio LACNIC anunció que contaba con 4,194,302 direcciones IPv4 en su stock esto implico las asignaciones de direcciones demasiado pequeñas e insuficientes para nuestra región, esta organización desde sus inicios (2002) de operación lleva 182 millones de direcciones entregadas. Dicha situación solo es en América Latina y el Caribe. Los demás registros de la internet del mundo están mostradas por la RIR, en la siguiente tabla:

RIR	Proyección de fechas de agotamiento	Direcciones restantes en RIR pool (/8)
APNIC	19-ABR-2011	0.8359
RIPE NCC	14-SEP-2012	0.9781
LACNIC	10-JUN-2014	0.2220
ARIN	07-MAR-2015	0.7470
AFRINIC	16-JUN2019	3.0465

Tabla 1. Proyección RIR de direcciones de fechas de agotamiento del pool.

En la Figura 1 se muestran las direcciones de la RIR en el pool contra los años de su agotamiento:

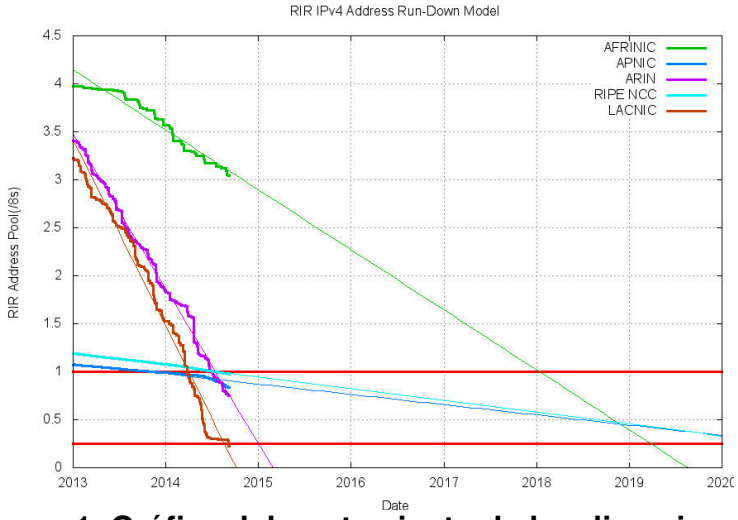


Figura 1. Gráfica del agotamiento de las direcciones

1.1.1 Asignaciones IPv4 e IPv6 en Latinoamérica.

La asignación de direcciones de IPv4 para México, dentro del top 10 en Latinoamérica nos encontramos en el 7MO puesto, en cambio en IPv6 ocupamos el 4to lugar debido a que México lidera las conexiones móviles en Latinoamérica, esto hizo que la IANA (Internet Assigned Numbers Authority) otorgara más direcciones IPv6 para México.

Figura 2. Asignación de direcciones en Latinoamérica.

1.2 Antecedentes del protocolo IPv4.

El funcionamiento del protocolo de internet IP es a través del intercambio de paquetes entre hosts. Todas las redes tienes hosts que tienen direcciones IP únicas esto es para que exista comunicación entre ellos. Dicho protocolo es de la capa de red (capa3) como se pude observar en la Figura 3 del modelo OSI (Open Systmes Interconnection) diseñado en el año 1981 (RFC 791).

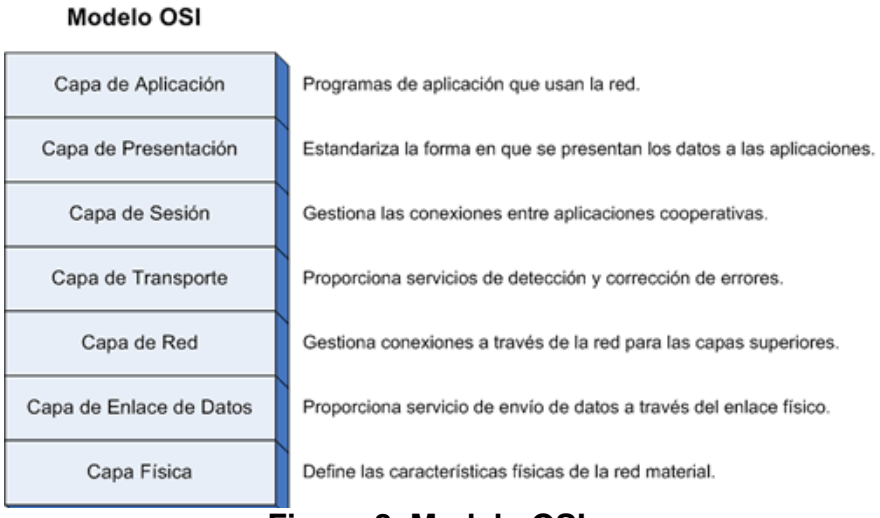


Figura 3. Modelo OSI.

IPv4 es de los principales protocolos en la capa de internet del modelo TCP/IP, este modelo es formado en conjunto con el protocolo TCP. El modelo TCP/IP es la base de la internet y su función principal es comunicar todos los dispositivos, ya que se utilizan diferentes tipos de sistemas operativos, fue desarrollado en el año 1972 por el departamento de defensa de los Estados Unidos utilizado en la red ARPANET (Advanced Research Projecs Agency Network), este modelo está compuesto por 4 capas como se puede ver en la Figura 4:

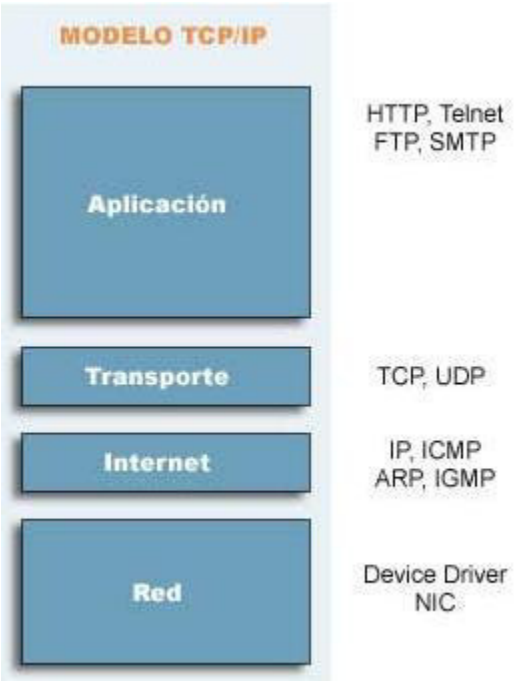


Figura 4. Modelo TCP/IP.

El protocolo IP como se puede ver en la Figura 4 se encuentra en la capa de internet, como hemos mencionado el protocolo IP es el más significativo del modelo TCP/IP encargado de diseñar el esquema de direcciones introduciendo las direcciones IPv4.
Las dos funciones principales del protocolo son entregar los paquetes a través de la red en la forma de máximo esfuerzo y el reensamblado de paquetes. Se le llama de máximo esfuerzo porque no garantiza que los paquetes sean recibidos de la misma forma en que fueron enviados.

1.3 Protocolo IPv4.

El protocolo IPv4 se encarga de dos funciones básicas: direccionamiento y fragmentación.

1.3.1 Direccionamiento.

Una distinción es creada entre nombres, direcciones y rutas; el direccionamiento se encarga de asignar una dirección IP a cada dispositivo dentro de una red para poder ser identificado por los demás hosts o routers que estén dentro de una misma red.

Las direcciones tienen un máximo de 32 bits es decir tienen una longitud fija de 4 octetos conformada por un número de red y una dirección local, tenemos 3 principales clases. (Figura 5) dividas por red y host ya que en las direcciones de clase A el primer byte es red y los 3 restantes hosts a diferencia de la clase B donde los primeros dos bytes son red y los dos restantes hosts y en clase C los 3 primeros bytes son red y el último byte es host.

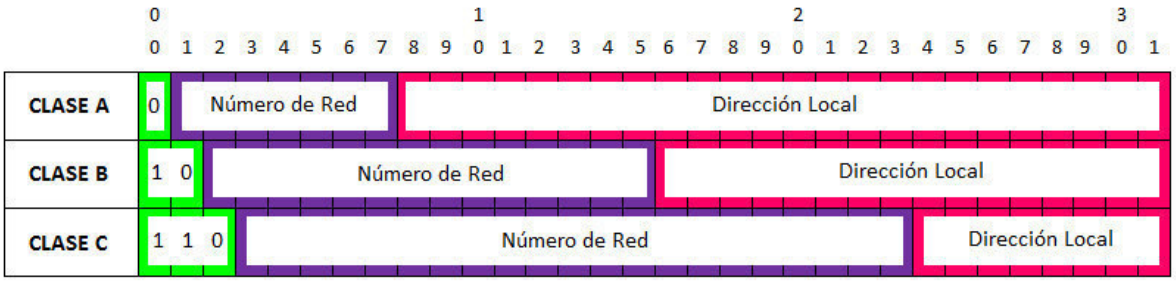


Figura 5. Clases de direcciones de internet.

En total se cuenta con 5 tipos de clases (A, B, C, D y E) pero de estas utilizamos solo las clases A, B y C puesto que la clase E es reservada para organizaciones y utilizadas internamente mientras la clase D es para Multicast. Las diferentes direcciones son otorgadas jerárquicamente gracias a la organización IANA actualmente existen varios rangos de direcciones que no son utilizadas porque están reservadas para redes privadas. Al volver a utilizar el mismo rango de direcciones se ha podido conseguir suficientes redes públicas.

Rangos reservados para redes privadas:

- 1 rango clase A: 10.x.x.x
- 16 rangos clase B: 172.16.x.x-172.31.x.x
- 256 rangos clase C: 192.168.0.x-192.168.255.x
- 1 rango clase B para enlace local: 169.254.x.x (Este sistema configura automáticamente una NIC (Network Interface Card) asignando una IP aleatoria en el rango de enlace local tras verificar mediante la ARP (Address Resolution Protocol) que está disponible. No configura routers ni servidores DNS (Domain Network Systems) por eso enlace local. Llamado por Microsoft APIPA (Automatic Private IP Addressing).

1.3.2. Fragmentación.

La fragmentación de los paquetes de internet es necesaria cuando una red local permite un paquete de tamaño largo y necesita atravesar una red local de menor tamaño y esto limita los paquetes a su destino.

El proceso de fragmentación y reensamblaje tiene que ser capaz de que los paquetes puedan ser divididos en pequeñas piezas que después puedan ser reensambladas.

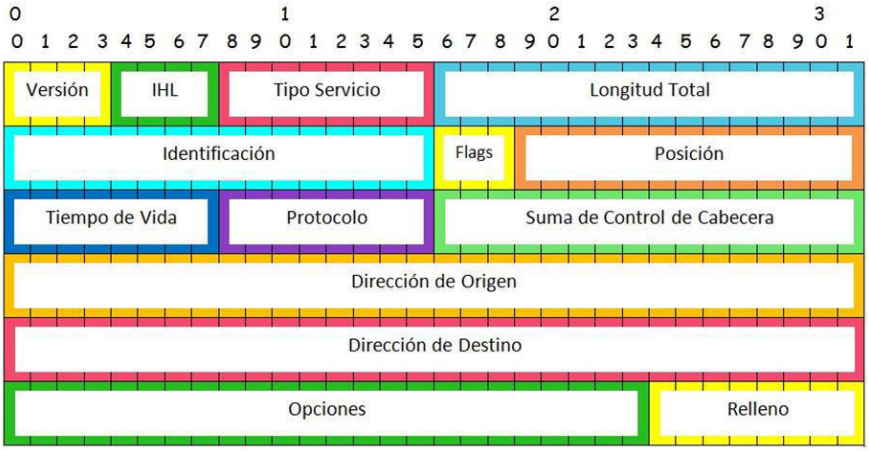


Figura 6. Cabecera de internet.

1.4 Mecanismos utilizados para alargar la vida de IPv4.

Debido al uso ineficiente de las direcciones IP se crearon nuevos mecanismos para poder solventar estos problemas, a continuación describiremos estos mecanismos:

1.4.1. Direcciones privadas.

Las direcciones privadas se empezaron a utilizar dentro de los mismos organismos o empresas, estas empresas u organizaciones solo necesitaban conectarse internamente a través de direcciones privadas es por eso que se empezaron a utilizarse estas direcciones, a continuación en la Tabla 2 se muestran los rangos de las direcciones privadas:

Nombre	Rango de Direcciones	Clase
Bloque de 24 bits	10.0.0.0 – 10.255.255.255	red simple clase A
Bloque de 20 bits	172.16.0.0 – 172.31.255.255	16 redes clase B continuas
Bloque de 16 bits	192.168.0.0 – 192.168.255.255	256 redes clase C continuas
Bloque de 8 bits	169.254.0.0 – 169.254.255.255	red simple clase B

Tabla 2. Rango de direcciones privadas.

1.4.2. VLSM (RFC 1519) y CIDR (RFC 4632).

VLSM (Mascara de Subred de Longitud Variable), el mecanismo consiste en dividir una red o subred y hacer subredes más pequeñas a su vez obteniendo mascaras de acuerdo a las necesidades de los hosts de cada una de las subredes. Al obtener mascaras diferentes por cada subred se permite no desaprovechar un gran número de direcciones, así que podemos decir que VLSM es la división de una subred en subredes.

CIDR es un mecanismo que asigna y específica las direcciones en una forma más flexible, es decir permite que las rutas se resuman en una sola ruta permitiendo que una subred se siga dividiendo en subredes, fue introducido en el año de 1993. CIDR hace una sumarización de rutas, es decir; las rutas se resumen en mascaras menores a las de las clases de direcciones (A/8, B/16 y C/24). La asignación de los prefijos está destinado a seguir la topología de red, esta agregación es utilizada para facilitar el escalamiento del enrutamiento global de la red. Una consecuencia del mismo es que la asignación de prefijo y la agregación son realizadas de acuerdo al proveedor-abonado ya que es la forma de la topología de la internet.

El cambio de los números de red de las clases A/B/C a prefijos sin clase es hacer más explícito cuales bits de una dirección de 32 bits son interpretados como el número de red (prefijo) asociados para el número de host. Un prefijo en CIDR esta denotado por 4 octetos igual que una dirección IPv4 seguida por el carácter “/” seguido de un valor decimal de 0 a 32 que describe los bits significativos.

1.4.3. Traducción de direcciones de red NAT (RFC 1631).

NAT (Network Adress Translation) es una función del router que permite utilizar las direcciones en paquetes, es decir que las direcciones dentro de un dominio puedan ser utilizadas por cualquier otro dominio. Por ejemplo una dirección de clase A puede ser usada por varios dominios. El funcionamiento de NAT es cambiar las direcciones IP de origen a cada paquete de salida, estas traducciones de direcciones son almacenadas en una tabla para poder identificar qué dirección y puerto es de cada dispositivo. NAT permite poder utilizar direcciones privadas y proveer conectividad con el resto de la internet. NAT esta instalado en cada punto de salida entre el “stub domain” y el “backbone”.

1.5. ¿Por qué el agotamiento de direcciones IPv4?

El increíble crecimiento ha hecho que las direcciones IPv4 hayan llegado prácticamente a su fin y eso se debe desde que fue creada la versión 4 de IP, no se pensó que la internet creciera de esta forma y que el tamaño de 32 bits sería más que suficiente, este hecho se ha tratado desde los 80s, los recursos de la internet empiezan a agotarse desde el momento de usarlos. Las mayores causas del agotamiento de la internet fueron las siguientes:

1.5.1. Dispositivos móviles.

Debido al crecimiento de los dispositivos móviles y que IPv4 es el protocolo para la transmisión de datos, cada dispositivo móvil cuenta con su IPv4 y este enorme crecimiento ha hecho que se agoten las direcciones ya que cada dispositivo móvil no deberán de cambiar su dirección IP.

1.5.2. Conexiones Always-On (permanente).

Cuando esto ocurrió hizo que el acceso de banda ancha creciera el 50% ocurrido esto en el 2007 y aunque las direcciones son dinámicas estas necesitan un IP permanente para poder ofrecer los servicios de comunicación.

1.5.3. Demografía de la internet.

Se pensó erróneamente, ya que en los años 90s pocos hogares tenían una conexión a internet años más tarde casi la mitad de los hogares cuentan con una conexión esto significo más direcciones IP.

1.5.4. Uso ineficiente de direcciones.

La forma indebida de asignar las direcciones a las organizaciones en los años 80s y que actualmente son poco utilizadas o poco nulas. A las organizaciones que obtuvieron direcciones IP en los años 80 se les asignaron muchas más direcciones de las que realmente necesitaban. Por ejemplo, a las grandes empresas y universidades se les dieron bloques de direcciones de clase A, con 16 millones de direcciones IPv4 cada uno.

Como bien se ha mencionado la capacidad de direcciones de IPv4 es de 4.294.967.296 debido a que es de 32 bits, esta cantidad parece casi inagotable pero en la actualidad estas direcciones están por agotarse a pesar de las diferentes técnicas para poder mantener este protocolo en pie.

El portal de información LACNIC (Latin American Network Information Center) cuenta con una base de datos que nos muestra las etapas del agotamiento de IPv4 la cual cuenta con 4 etapas que mostraremos a continuación:

Fase 0.

A partir de 2011 hasta llegar al espacio equivalente a /9.

Fase 1.

Cuando se alcance el equivalente al último bloque /9, incluyendo los dos /11 reservados para la terminación gradual de IPv4 y para nuevos entrantes.

Fase 2 (Fase Actual).

Cuando se alcance el último bloque de /10.

Fase 3.
Cuando se agote el bloque /11 de terminación gradual.

1.5.5. Espacio Ipv4 disponible.

LACNIC, como uno de los 5 RIRs en el mundo, es responsable del registro y asignación de 11.16 /8s (187,254,272 direcciones IPv4) La utilización de este espacio al día es mostrada en el cuadro:

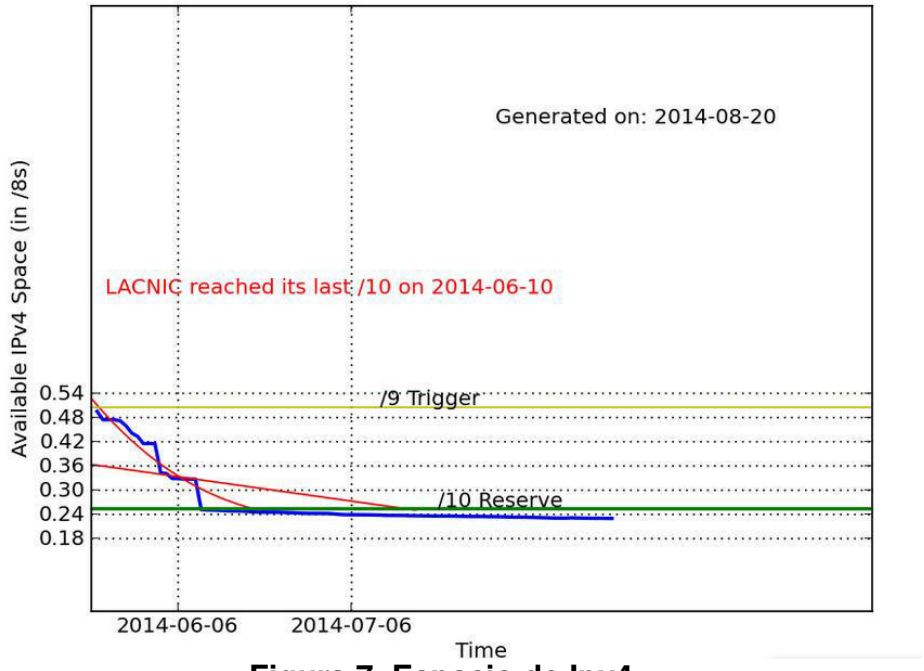


Figura 7. Espacio de Ipv4.

Esta es la última fecha de cuantificación del agotamiento de Ipv4, Cuando el espacio mostrado en la gráfica indique menos de 4,194,304 direcciones IPv4 consideraremos que el stock de LACNIC estará agotado.

1.5.6. Distribuciones de espacio IPv4 distribuido por la IANA.

Los recursos IPv4 distribuidos por la IANA a LACNIC una vez que el punto 11.2 del Manual de Políticas sea vigente solamente podrán ser distribuidos/asignados bajo los lineamientos definidos en el punto 11.1 del Manual de Políticas.

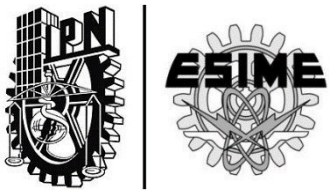
1.6 ¿Por qué la transición de versión de protocolo?

Es por eso que se necesita una transición de protocolo IP a su nueva versión Ipv6, ya que esta fue diseñada para que su uso sea más fácil y amigable con el usuario, además que es necesario tener conexiones extremo a extremo ya que con las técnicas para alargar el tiempo de vida de Ipv4 (NAT) se perdió esta característica. Ipv6 ofrece mejoras significantes en casi todos los sentidos para una conexión a internet, es por eso que debemos hacer una transición de este protocolo.
Comparando el número total de direcciones Ipv4 con Ipv6 tenemos una diferencia enorme, ya que prácticamente el espacio de direcciones Ipv6 es poco imaginable, a continuación se mostrara una comparación entre el espacio de estas dos versiones:

IPv6	340.29 x10^38 aproximadamente.
IPv4.	**4.294967296 x10^9.**
Habitantes de México (2013).	**118,397,000 habitantes.**
Habitantes del Planeta (2013).	**7,136,077,000 habitantes.**
No. de Direcciones IPv4 Faltantes.	**2,705,032,704 direcciones.**

Tabla 3. Espacio de Direcciones.

En esta tabla podemos determinar la enorme diferencia entre el espacio de IPv6 e IPv4, así podemos encontrar una gran ventaja de IPv6 ya como hemos visto en el punto 1.3 de este capítulo las direcciones IPv4 tienen una fecha de agotamiento.



CAPÍTULO 2:
“Características y conceptos de Ipv6”.

CAPÍTULO 2: "CARACTERÍSTICAS Y CONCEPTOS DE IPV6".

2.1. Antecedentes del protocolo IPV6.

El protocolo IPv6 nos otorga $3.40x10^{38}$ aproximadamente de direcciones.
El surgimiento de IPv6 empezó en el año 1993 diseñado por Steve Deering y Craig Mudge por la IETF, empezó con el nombre IPng donde se realizaron investigaciones y diferentes propuestas para el desarrollo del mismo.
IPv6 también se conoce por el nombre de "IP Next Generation", el cual está diseñado para sustituir al protocolo IPv4, siendo hasta el año de 1994 cundo se concluyó y está definido por el RFC 2460.

2.2. Características de IPv6.

Las principales cualidades que tiene IPv6 son:

- Admitir miles de millones de equipos, superando las limitaciones de espacio para las direcciones de IPv4 actuales.
- Reducir el tamaño de las tablas de enrutamiento.
- Simplificar el protocolo para permitir que los routers enruten datagramas de manera más rápida.
- Brindar mejor seguridad (autenticación y confidencialidad) que la proporcionada por el protocolo IP actual.
- Mejorar los servicios asociados con la práctica en tiempo real.
- Facilitar la difusión a destinos múltiples, permitiendo especificar el tamaño.
- Permitir la movilidad de un equipo sin cambiar su dirección.
- Permitir el futuro desarrollo del protocolo.
- Permitir la coexistencia practica de IPv4 junto con IPv6.

A continuación se mencionan las características de dicho protocolo y mismas que resuelven muchos problemas de la versión de internet 4:

- Una de las principales características de este protocolo son el número de direcciones que contiene, que es de 128 bits (16 bytes) y comparado con IPv4 es 4 veces mayor, maneja un espacio de direccionamiento de 2^{96} veces mayor a Ipv4. Para ser más precisos, IPv6 nos ofrece un espacio total de 2^{128}, es decir; $3.40x10^{38}$ direcciones posibles.

- IPv6 maneja un cabecera simplificada, que será descrita posteriormente, la cabecera consta de 40 bytes comparada con la de IPv4 que es de 20 bytes, además se mejora el campo de opciones de IPv4 denominándolo con el nombre de campo cabecera siguiente, esto simplifica el procesamiento de cada router.

- Se incorpora seguridad intrínseca, es decir que incorpora encriptación y autenticación. Esta seguridad se denomina IPSec (Internet Protocol Security) basado en un protocolo denominado con el mismo nombre, el cual está disponible tanto en IPv4 e IPv6. El IPSec es un conjunto de protocolos que operan en la capa 3 del modelo OSI y que tienen como función asegurar la comunicación sobre el protocolo de internet (IP) autentificando y/o cifrando cada paquete IP en un flujo de datos.

- Soporte en calidad de servicio QoS (Quality of Service) es todo el conjunto de técnicas para manejar una red; IPv6 proporciona soporte para seguridad basándose en sus cabeceras de extensión.

- Cuenta con servicios de red: es decir; IPv6 cuenta con un mecanismo que permite a un transmisor y a un receptor establecer una trayectoria de alta calidad por la red y asociarle los datagramas, garantizando el alto desempeño a aplicaciones de audio y video en tiempo real. IPv6 permite el etiquetado de flujo de tráfico en particular para el cual el origen solicita un manejo especial.

- La MTU (Maximun Transfer Unit) es de 1,280 bytes, siendo que la MTU de IPv4 es de 680 bytes.

- Maneja Multicast, que es él envió de un mismo paquete a un grupo de receptores y Anycast que es él envió de un paquete a un receptor que está dentro de un grupo.

- Posibilidad de paquetes con carga útil de datos de más de 65,535 bytes.

2.3 Direccionamiento de Ipv6.

La arquitectura del formato de direcciones de IPv6 se encuentra descrita en el RFC 4291.
Las direcciones IPv6 son identificadores de 128 bits para interfaces y conjunto de interfaces (donde una interfaz según el RFC 2460 es lo que acopla un nodo a un enlace).

Figura 8. Formato de dirección IPv6.

Longitud de 128 bits “prefijo de Red (64 bits) + Interface ID (64 bits)”.
8 bloques de 2 bytes conformados por 4 números hexadecimales cada uno.
Cada bloque se corresponde con dos octetos (16 bits).
Las direcciones son asignadas a las interfaces, no a los nodos.
Interface ID: se estructura por el formato EUI-64 (MAC extendida). Este proceso utiliza la dirección MAC de Ethernet de 48 bits de un cliente e introduce otros 16 bits en medio de la dirección MAC de 48 bits para crear una ID de interfaz de 64 bits, también la Interface ID se estructurar de una asignación aleatoria por el propio host de 64 bits.
Los ceros no significativos de cada grupo se pueden omitir.
Uno o más grupos de 16 bits a cero se pueden reemplazar por “::”.
No hay direcciones reservadas para red y Broadcast.

Hay tres maneras convencionales de representación de direcciones IPv6 como cadenas de texto:

1.- La primera de ellas es: X : X : X : X : X : X : X : X, donde las “X”s son de uno a cuatro dígitos hexadecimales de los 8 campos de 16 bits que conformar la dirección IPv6. Ejemplos:

ABCD : EF01 : 2345 : 6789 : ABCD : ED01 : 2345 : 6789
2001 : DB8 : 0 : 0 : 8 : 800 : 200C : 417A
2.- Debido a algunos métodos de asignación de una dirección IPv6, será común encontrar cadenas largas de 0 bits, con el fin de hacer la lectura de direcciones conformadas por varias cadenas de 0 en un mismo campo, existe una sintaxis

especial para suprimir los ceros de la izquierda y estos ser remplazados por "::", el cual indica uno o más grupos de ceros que conforman un campo de 16 bits. Por ejemplo las siguientes direcciones:
2001 : DB8 : 0 : 0 : 800 : 200C : 417A
FF01 : 0 : 0 : 0 : 0 : 0 : 0 : 101
0 : 0 : 0 : 0 : 0 : 0 : 0 : 1
0 : 0 : 0 : 0 : 0 : 0 : 0 : 0

Dichas direcciones podrán ser representadas de la siguiente manera:

2001 : DB8 :: 800 : 200C : 417A
FF01 :: 101
:: 1
::

3.- Otra de las representaciones surge debido a la interacción que existe entre el protocolo IPv4 e IPv6, por dicho punto se pueden tener direcciones mixtas representadas de la siguiente manera X : X : X : X : X : X : d : d : d : d, siendo que las "X"s son 6 campos de 4 valores hexadecimales que representan los valores de mayor orden, y las "d"s representando 4 campos decimales de menor orden, así formando 6 campos de 16 bits más 4 campos de 8 bits una direcciones de 128 bits. Ejemplos:

0 : 0 : 0 : 0 : 0 : 0 : 13 . 1.68. 3
0 : 0 : 0 : 0 : 0 : FFFF : 129 .144.52. 38

En la siguiente figura se puede observar de manera gráfica como se clasifica el direccionamiento IPv6.

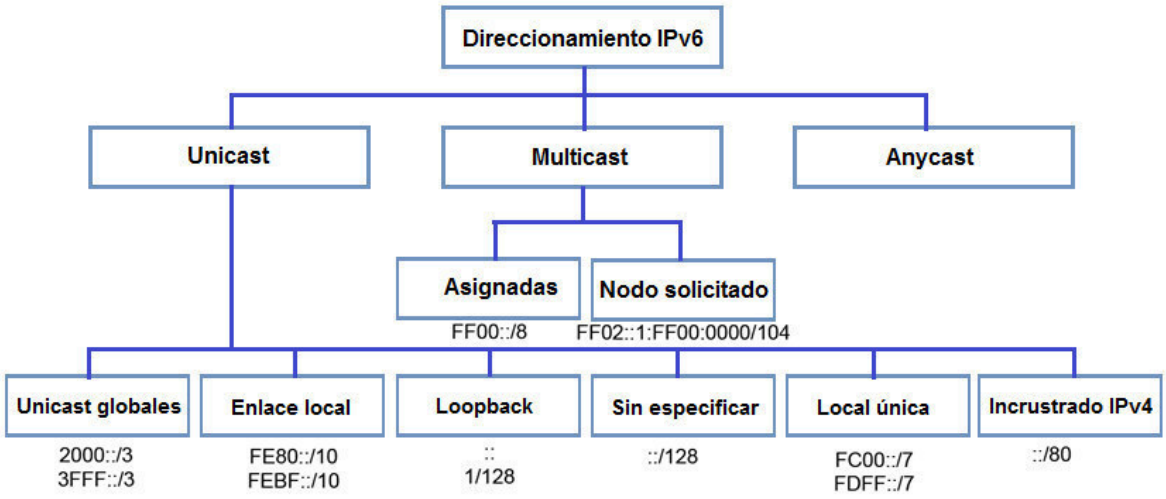


Figura 9. Direccionamiento IPv6.

A continuación se indicara que es cada tipo de dirección.

2.3.1. Unicast.

Son direcciones que tienen un identificador para cada una única interfaz. Un paquete enviado a una dirección Unicast es entregado a la interfaz identificada por esa dirección.

Las direcciones IPv6 Unicast se le agregan prefijos arbitrarios de longitud de bit, similar a las direcciones IPv4 según el protocolo CIDR.

La estructura de una dirección Unicast está representada en la Figura 10:

128 bits.
Dirección de nodo.

Figura 10. Estructura de una dirección Unicast.

Y está conformada por dos campos:

N bits.	128 – N bits.
Prefijo de subred.	Interfaz ID.

Figura 11. Campos de una dirección Unicast.

Prefijo de subred: el ID de subred o prefijo de subred es un identificador de un enlace dentro de un sitio.

Interfaz ID: es utilizado para ubicar la interfaz en un enlace, es el único prefijo en una subred, se recomienda que la misma interfaz de identificación no sea asignada a diferentes grupos es un nodo.

Hay varios tipos de direcciones Unicast:

2.3.1.1. Dirección no especificada.

La dirección “0 : 0 : 0 : 0 : 0 : 0 : 0 : 0” es la llamada dirección no especificada y esta nunca debe ser asignada a ningún nodo e indica la ausencia de una dirección.

2.3.1.2. Dirección Loopback.

La dirección Unicast “0 : 0 : 0 : 0 : 0 : 0 : 0 : 1”, se llama dirección de Loopback. Puede ser utilizada por un nodo para enviar un paquete IPv6 a si mismo, no se asigna a ninguna dirección física.

2.3.1.3. Dirección Global Unicast.

El formato general de una dirección Global Unicast IPv6 es el siguiente:

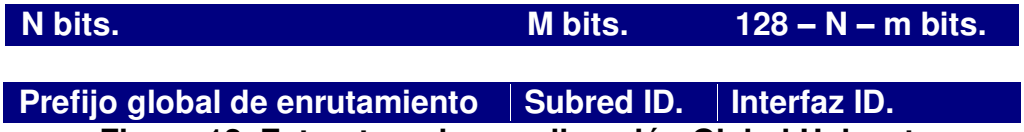


Figura 12. Estructura de una dirección Global Unicast.

Prefijo global de enrutamiento: Donde el prefijo de enrutamiento global es un valor asignado (normalmente estructurado jerárquicamente),
Subred ID: Es un identificador de un enlace.
Interfaz ID: Como ya definido anteriormente.

2.3.1.4. Direcciones Embedded.

El mecanismo de transición IPv6 incluye una técnica para que los hosts y los routers de forma dinámica coloquen en un túnel paquetes IPv6 sobre una infraestructura de enrutamiento de IPv4. Los nodos IPv6 que utilizan esta técnica tienen asignadas direcciones Unicast IPv6 especiales que llevan una dirección IPv4 global en los 32 bits menos significativos. Este tipo de direcciones se denominan "IPv4 compatible con una dirección IPv6 " y tienen el formato:

Figura 13. Dirección IPv4 compatible con IPv6.

Nota: La dirección IPv4 utilizada en "IPv4 compatible con una dirección IPv6 " debe ser una dirección Unicast IPv4 globalmente única.

Otro tipo de direcciones Embedded son las empleadas para representar las direcciones de los nodos IPv4 como direcciones IPv6 y recibe el nombre de “IPv4-mapped IPv6 address" y su formato es:

Figura 14. Dirección IPv6 mapeada IPv4.

2.3.1.5. Direcciones de Enlace Local (Link-Local).

Son para el uso de un único vínculo y tienen el siguiente formato.

10 bits.	54 bits.	64 bits.
1111111010	0	Interfaz ID.

Figura 15. Estructura de una dirección Link-local.

Están diseñadas para ser utilizadas para un único vínculo con fines tales como la configuración de la direcciones ND (Neighbor Discovery) o cuando no se presente un router.

2.3.2. Anycast.

Un identificador para un conjunto de interfaces (típicamente pertenecientes a diferentes nodos). Un paquete enviado a una dirección Anycast se entrega a una de las interfaces identificadas por esa dirección (el más cercano).

Una dirección Anycast IPv6 es una dirección que se ha asignado a más de una interfaz, con el fin de que un paquete enviado a una direccion Anycast se dirige a la interfaz más cercana.

La dirección de subred-router Anycast tiene el siguiente formato.

N bits.	128 – N bits.
Prefijo de subred.	Interfaz ID

Figura 16. Estructura de una dirección Anycast.

El prefijo de subred es una dirección Anycast que identifica un vínculo en específico, esta dirección es sintácticamente igual a una dirección Unicast con la interfaz ID puesta a 0.

2.3.3. Multicast.

Tienen una definición muy parecida a la del tipo de direcciones Anycast, es decir que también es un identificador para un conjunto de interfaces, la diferencia es que para un paquete enviado con una dirección Multicast será entregada a todas las interfaces identificadas por esa dirección.

Una direccione IPv6 Multicast, es un identificador para un grupo de interfaces (por lo general en los diferentes nodos), una interfaz puede pertenecer a cualquier

número de grupos Multicast. En la Figura 17 se muestra como se confirma una dirección Multicast:

8 bits	:	4 bits	:	4 bits	:	112 bits
11111111	:	Flags	:	Scop	:	Grupo ID

Figura 17. Estructura de una dirección Multicast.

Donde:

11111111: Grupo binario de 8 bits al comienzo que identifica la dirección como una dirección Multicast.

Flags: es un conjunto de 4 banderas.

0	P	P	T

Figura 18. Banderas.

0: Es un campo reservado y debe ser inicializado a 0.
P: Es una bandera definida por el RFC 3306.
T: Puede estar definido por dos valores.
T = 0 indica permanentemente asignado de una dirección Multicast.
T = 1 indica permanentemente no asignado de una dirección Multicast.

Scop: De 4 bits, es un valor utilizado para limitar el alcance del grupo Multicast y los valores son los siguientes:

0	Reservados.
1	Interfaz de ámbito local.
2	Enlace de ámbito local.
3	Reservados.
4	Admin. ámbito local
5	Sitio local alcance.
6	No asignado.
7	Sin asignar.
8	Organización local enlace.
9	Sin asignar.
A	Sin asignar.
B	Sin asignar.
C	No asignado.
D	No asignado.
E	Alcance mundial.
F	Reservados.

Figura 19. Valores de Scop.

Grupo ID: Identifica el grupo Multicast, ya sea definitivo o transitorio.

Jerarquización.

La escalabilidad es otro punto importante de la diferencia entre la gestión de red IPv6 y la de IPv4. El interés de los diseñadores fue que las direcciones más largas permiten una entrega jerárquica, sistemática y en definitiva mejor que las direcciones IPv4 y una eficiente agregación de rutas. Con IPv4, se desplegaron complejas técnicas CIDR para utilizar de mejor manera el pequeño espacio de direcciones como ya antes se había mencionado. El esfuerzo requerido para reasignar la numeración de una red existente con prefijos de rutas distintos es muy grande. Sin embargo, con IPv6, cambiando el prefijo anunciado por unos pocos routers es posible en principio reasignar la numeración de toda la red, ya que los identificadores de nodos (los 64 bits menos significativos de la dirección) pueden ser auto-configurados independientemente por un nodo.

Con la agregación de direcciones toda la red se vuelve completamente jerárquica a escala mundial, con los niveles que se están dictadas por la arquitectura de la dirección. Todo el sistema es a su vez, gestionado por un sistema de registro distribuido en los lugares de agregación diferentes.

Existen tres tipos de jerarquías para direcciones IPv6.

- **Topología pública (48 bits).**

Identifica a los proveedores de la conexión a internet, este nivel jerárquico contiene:

- FP (Formal Prefix): Identifica Unicast, Multicast, Anycast.
- TLA Id (Top Level Aggregation) Identifica a la autoridad de mayor nivel dentro de la jerarquía de encaminamiento
- Resv : Reservado para futuras expansiones de las direcciones
- NLA ID (Next-Level Aggregation): Identifíca el ISP (Internet Service Provider).
- Topología de la organización (16 bits).

Identifica a la organización a la que pertenece el nodo IP. El cual contiene:

- SLA Id (Site Level Aggregation) Permite a una organización crear su propia jerarquía de direcciones.
- Identificador de la interface (64 bits).

2.4 Cabecera de IPv6.

La cabecera de IPv6 tiene una longitud total de 40 bytes, a comparación de la de IPv4 que tiene una longitud de 20 bytes, en la figura 20 se muestran las diferencias entre dichas cabeceras de ambos protocolos.

En un principio se puede observar que el campo versión no se modifica, debido a que durante un buen tiempo ambos protocolos estarán en funcionamiento al mismo tiempo, sin embargo se observan campos que fueron eliminados, tamaño de encabezado, tipo de servicio, número de identificación del datagrama, banderas, numero de byte del datagrama fragmentado y checksum, mientras que se refinaron otros campos como longitud del datagrama, tiempo de vida y tipo de protocolo.

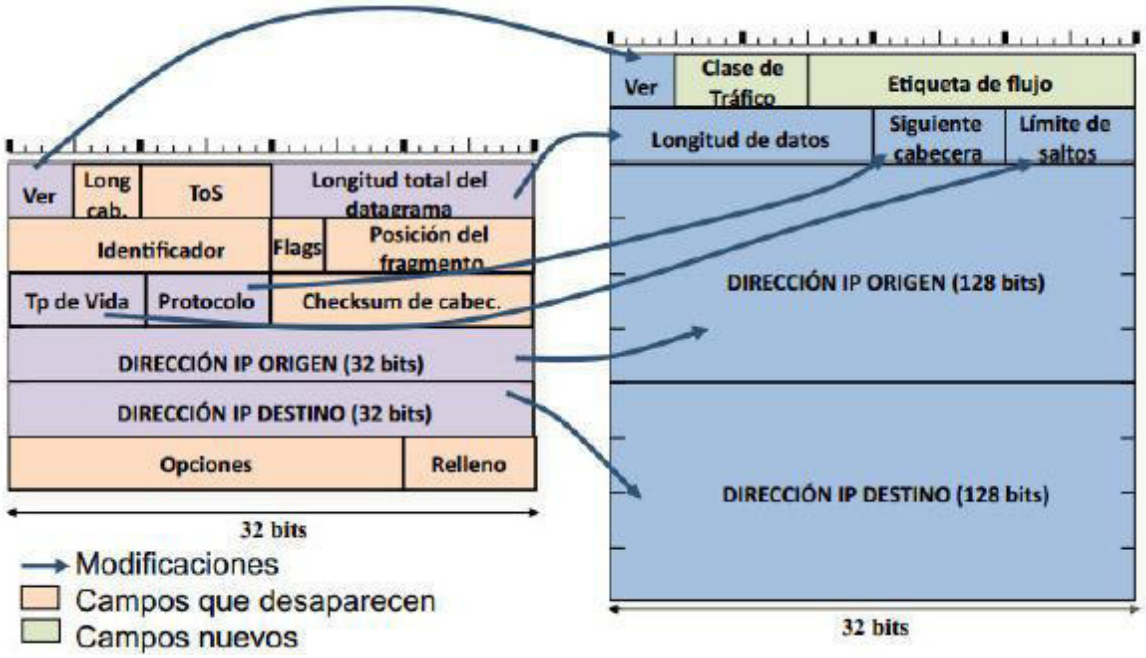


Figura 20. Comparación entre cabeceras de IPv4 con IPv6.

El motivo principal por lo que los campos son eliminados, es la innecesaria redundancia. En IPv4 se facilita la misma información en varias formas. Un caso muy evidente es el checksum o verificación de la integridad de la cabecera, ya que otros mecanismos de encapsulado ya realizan esta función (IEEE 802 MAC, capa de adaptación ATM, etc.).

En el caso de posición del fragmento, es ligeramente diferente, ya que al mecanismo por el que se realiza la fragmentación de los paquetes es totalmente modificado en IPv6, lo que implica la total inutilidad de este campo. En IPv6 los routers no fragmentan los paquetes sino que de ser preciso dicha fragmentación y desfragmentación se produce extremo a extremo.

En la Figura 21 se muestra la cabecera de IPv6 y así mismo sus campos.

Figura 21. Cabecera de Ipv6.

Tomando en cuenta la Figura 21 anterior, se describirá el tamaño de cada campo y su funcionamiento:

1.- "Versión". Consta de 4 bits, y se representa con un número, siendo el número 6 en binario "0110", claro está que se representa con el numero 6 referido al número de versión de IP (Ipv6).

2.- "Prioridad o clase de tráfico". Tiene un tamaño de 8 bits, y se utiliza para identificar y distinguir entre las prioridades del paquete IPv6. Podría ser equivalente al campo ToS de IPv4.

3.- "Etiqueta de flujo". Tiene un tamaño de 20 bits, este campo se utiliza para etiquetar secuencias de paquetes que los routers solicitan para que reciban un trato especial.

Tanto el campo de Prioridad como Etiqueta de flujo son los que permiten una de las características fundamentales e intrínsecas de IPv6 que son: QoS y CoS Clase de Servicio, y en definitiva un poderoso mecanismo de control de flujo, de asignación de prioridades diferenciadas según los tipos de servicio.

4.- "Longitud de la carga útil o longitud de datos". El tamaño de este campo es de 16 bits, está conformada por un número entero que identifica el número de octetos que están por fuera de la cabecera, incluyendo la cabecera de extensión, que en definitiva es la longitud de los propios datos y pueden ser de hasta 65,536 bytes.

5.- "Cabecera siguiente". Tiene un tamaño de 8 bits, y su función es identificar la siguiente cabecera a procesar en el des encapsulamiento del paquete, dado que en lugar de usar cabeceras de longitud variables se emplean sucesivas cabeceras

encadenadas, de ahí que desparezca el campo opciones de IPv4. En muchos casos ni siquiera es procesado por los routers, sino tan solo extremo a extremo.

6.- "Limite de saltos". Con un tamaño de 8 bits, es un numero entero que se decrementa en 1 cada vez que pasa por un router y al llegar este número a 0, se descarta dicho paquete.

7.- "Dirección origen". Este campo tiene un tamaño de 128 bits, siendo la dirección IPv6 del nodo donde se origina el paquete.

8.- "Dirección destino". Al igual que el campo de dirección origen tiene un tamaño de 128 bits, siendo la dirección IPv6 donde deberá ser entregado el paquete.

2.5 Diferencias entre IPv4 con IPv6.

	IPv4	IPv6
Direcciones.	**Las direcciones de origen y destino tienen un tamaño de 32 bits (4 bytes).**	**Las direcciones de origen y destino tienen un tamaño de 128 bits (16 bytes).**
IPSec	**La compatibilidad es opcional.**	**La compatibilidad es obligatoria.**
Identificación del número de paquetes.	**No existe ninguna identificación de flujo de paquetes para que los enrutadores controlen el QoS en el encabezado IPv4.**	**Se incluye la identificación de flujo de paquetes para que los routers controlen la QoS en el encabezado de IPv6, utilizando el campo etiqueta de flujo.**
Fragmentación .	**La llevan a cabo los routers y el host que realiza él envió.**	**No la llevan a cabo los routers, si no únicamente el host que realizo él envió.**
Encabezado.	**Incluye una suma de comprobación.**	**No incluye una suma de comprobación.**
Opciones.	**El encabezado lo incluye.**	**Todos se trasladan a los encabezados de extensión IPv6.**
Marcos de solicitud ARP.	**El protocolo de resolución de direcciones (ARP) utiliza los marcos de solicitud de difusión ARP para resolver una dirección IPv4 como una dirección de capa de vínculo.**	**Los marcos de solicitud ARP se sustituyen por mensajes de solicitud de vecinos Multicast.**
Administrar la permanencia a grupos locales de subred.	**Se utiliza el protocolo de grupos de administración de internet IGMP.**	**IGMP se sustituye por los mensajes de descubrimiento (MLD).**

Determinar la mejor puerta de enlace predeterminada.	**Se utiliza el descubrimiento de router ICMP y es opcional,**	**El descubrimiento de routers ICMP queda sustituido por los RS y RA de ICMPv6 y es obligatorio.**
Direcciones Multicast.	**Se utilizan para enviar tráfico a todos los nodos de una subred.**	**No hay direcciones de Multicast IPv6, de forma alternativa se utiliza una dirección Multicast para todos los nodos de ámbito local del vínculo.**
Configuración manual.	**Debe configurarse manualmente a través de DHCP.**	**No requiere configuración manual a través de DHCP.**
DNS.	**Utiliza recursos de registro (A) de direcciones de host en el sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv4.**	**Utiliza registros de recursos (AAA) de direcciones de host en el DNS para correlacionar nombres de host con direcciones IPv6.**
Tamaño de paquete.	**Debe admitir un tamaño de 680 bytes (posiblemente fragmentado).**	**Debe admitir un tamaño de 1280 bytes (sin fragmentación).**

Tabla 4. IPv6 vs IPv4.

1.6. IPv6 en la actualidad.

Según estudios elaborados por la ISOC (Internet Society), el crecimiento del tráfico de IPv6 desde septiembre del 2013 ha crecido del 2% al 3.57% hasta mayo de 2014.

Otro estudio estadístico de porcentaje de tráfico de usuarios IPv6, proyecta que para diciembre de 2014 el porcentaje de tráfico alcanzara hasta un 10% del total del tráfico de la red de internet.

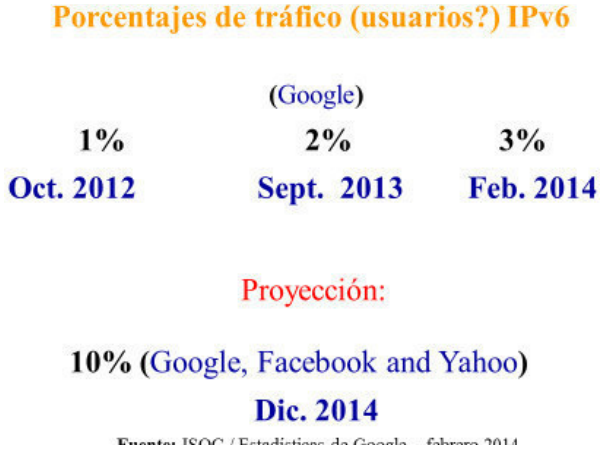


Figura 22. Porcentaje de usuarios IPv6.

En México, se aporta apenas un 0.01% de del porcentaje total estadístico hasta mayo de 2014. Aunque el porcentaje en México es muy poco, se planea que en los próximos años IPv6 sea el protocolo que rija en la red de internet, dejando atrás el IPv4, ahí entonces será cuando México y todo el mundo tendrá que adoptar este nuevo protocolo, realizando una migración o transición de sus redes a IPv6, quedando obsoleto el protocolo IPv4 que ha estado en funcionamiento por más de 20 años.

2.7. Rutas estáticas IPv6.

Las rutas estáticas IPv6 son configuradas manualmente y definen una ruta explicita entre dos dispositivos de una red. La configuración de una ruta estática es muy similar a IPv4 la diferencia recáe en el comando ipv6 route.
Antes de configurar una ruta estática IPv6 debemos verificar si:

- IPv6 unicast-routing.
- IPv6 este habilitado al menos en una interfaz.
- Una dirección IPv6 en esa interfaz IPv6.

El enrutamiento de IPv6 es descrito por el siguiente diagrama de flujo:

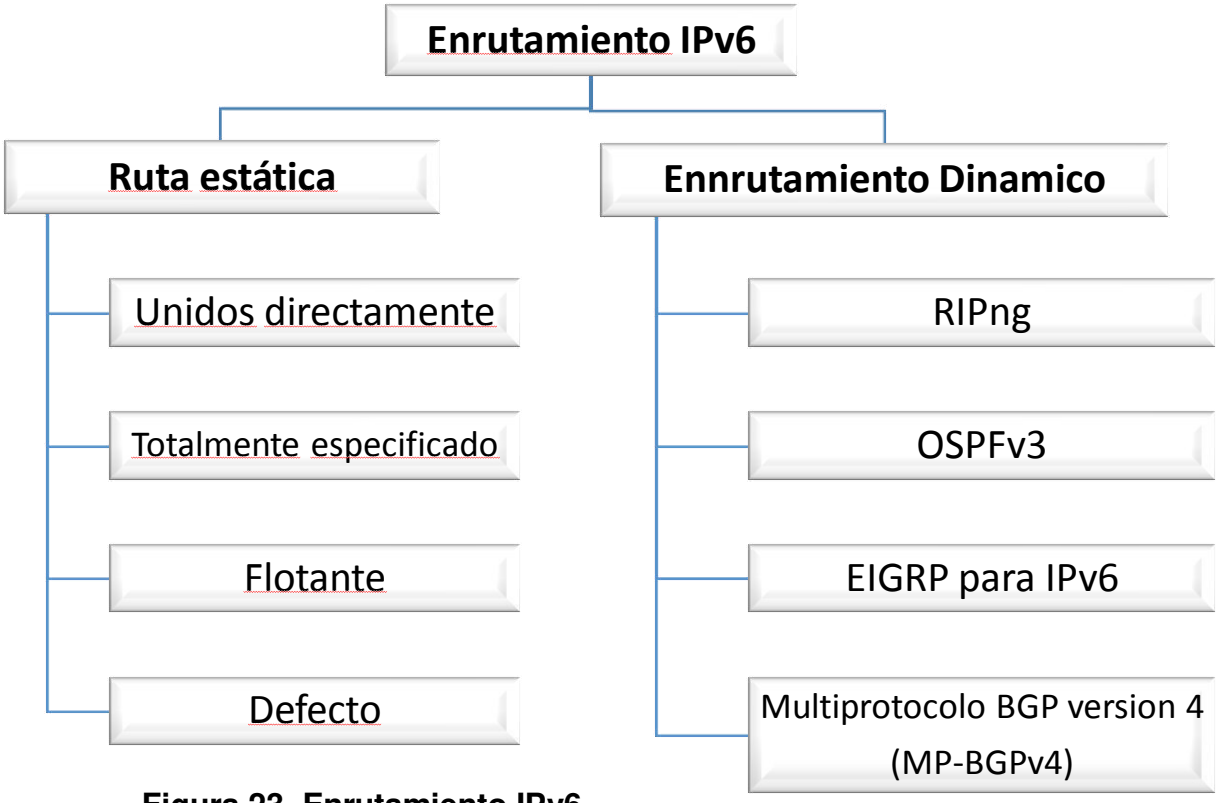


Figura 23. Enrutamiento IPv6.

Como podemos ver la Figura 23 nos muestra las formas para realizar una ruta estática.

La sintaxis de los comando IPv6 contiene más parámetros comparados con la versión IPv4.

```
ipv6 route                    ipv6-prefix/prefix-length
  {ipv6-address | interface-type interface-number [ipv6-address]}

  [administrative-distance]
```

Figura 24. Sintaxis de comandos IPv6.

Donde:

ipv6-prefix/prefix-length: Muestra el prefijo de Ipv6 y su longitud de prefijo.
interface-type interface-number: El tipo de interfaz y número de interfaz.
administrative-distance: Dos o más rutas de enrutamiento diferentes para el mismo destino.

Los comandos anteriores no son requeridos para configurar las rutas estáticas: unidos directamente, totalmente especificado, flotante y por defecto, a continuación se describirá cada uno de ellos:

- **Ruta estática unida directamente.**

```
Router(config)#
ipv6 route ipv6-prefix/prefix-length
  {ipv6-address | interface-type interface-number [ipv6-address]}
  [administrative-distance]
```

Figura 25. Comando para ruta estática directamente.

Una ruta estática unida directamente se crea al especificar solo la interfaz de salida. El parámetro *ipv6-prefix/prefix-length* identifica el destino de la red IPv6 y la longitud del mismo. El parámetro *interface-type interface-number* especifica la interfaz por la cual podemos alcanzar la red de destino.

En la siguiente red podremos mostrar un ejemplo de este tipo de ruta estática:

Figura 26. Ejemplo de ruta estática unida directamente.

En la siguiente sintaxis podemos observar los comandos subrayados nos indican que es una ruta estática unida directamente:

```
R1# config t
R1(config)# ipv6 route 13::/64 s0/0/0
R1(config)# exit
R1# show ipv6 route static
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S    13::/64 [1/0]
     via ::, Serial0/0/0
R1#
```

Figura 27. Ruta estática directamente unida a la red 13::13:1/64 configurada en el router 1.

- **Ruta estática totalmente especificada.**

  Router(config)#

```
ipv6 route ipv6-prefix/prefix-length
  {ipv6-address | interface-type interface-number [ipv6-address]}
  [administrative-distance]
```

Figura 28. Comando para una dirección estática totalmente especificada.

Una ruta estática totalmente especificada es cuando especificamos:

- La interfaz de salida.
- La dirección IP del siguiente salto.

Este método evita una búsqueda recursiva. El siguiente ejemplo de red nos muestra los comandos de este tipo de ruta:


```
R1# config t
R1(config)# ipv6 route 13::/64 s0/0/0 2001:1::2
R1(config)# exit
R1# show ipv6 route static
IPv6 Routing Table - Default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   13::/64 [1/0]
     via 2001:1::2, Serial0/0/0
R1#
```

Figura 29. Ruta estática completamente especificada a la red 13::13:1/64 en el R1.

Ruta estática flotante.

```
Router(config)#
```

```
ipv6 route ipv6-prefix/prefix-length
  {ipv6-address | interface-type interface-number [ipv6-address]}
  [administrative-distance]
```

Figura 30. Comando de una ruta estática flotante.

Una ruta estática flotante está configurada por lo general cuando hay múltiples rutas de acceso a una red de destino y una ruta de respaldo de espera que se requiere para apoyar el descubrimiento de rutas IGP.

Será solamente agregada a la tabla de enrutamiento si la entrada IGP (Interior Gateway Protocol) es eliminada.
El parámetro *administrative-distance:* La distancia administrativa es la función que utilizan los routers para seleccionar la trayectoria cuando hay dos o más rutas hacia el mismo destino desde dos protocolos de enrutamiento diferentes.
La distancia administrativa define la fiabilidad del protocolo de enrutamiento es el primer criterio que utilizan los routers para determinar que protocolo de enrutamiento se uilizara cuando hay más de dos protocolos configurados en el router que proporcionan información para el mismo destino, la elección de que protocolo será el elegido depende de un valor especificado en la Tabla 5, dependiendo de diferentes protocolos de enrutamiento de IPv6.

En la Tabla 5 se muestran los diferentes valores de distancia:

ORIGEN DE LA RUTA	VALORES DE DISTANCIA PREDETERMINADOS
Interfaz conectada	0
Ruta estática	1
Ruta de resumen del Protocolo de enrutamiento de gateway interior mejorado (EIGRP)	5
Protocolo de gateway de frontera externa (BGP)	20
EIGRP interno	90
IGRP	100
OSPF (Abrir trayecto más corto primero)	110
Sistema intermedio a sistema intermedio (IS-IS)	115
Protocolo de información de enrutamiento (RIP)	120
Protocolo de gateway interior (IGP)	130
Protocolo de gateway exterior (EGP)	140
Enrutamiento a pedido (ODR)	160
EIGRP (zona desmilitarizada) externa	170
BGP interno	200
Desconocido*	255

Tabla 5. Valores de distancia administrativa predeterminados.

El valor por defecto es 1 como se observa en la tabla 5, por lo que las rutas estáticas tienen prioridad sobre cualquier otro tipo de ruta, excepto las rutas conectadas.

En el siguiente ejemplo, R1 está configurado con una ruta estática flotante especificando una distancia administrativa de 130 a la LAN R2.

Si un IGP ya tiene una entrada en la tabla de enrutamiento IPv6 a esta LAN, entonces la ruta estática sólo aparecería en la tabla de enrutamiento si se quita la entrada IGP.


```
R1# config t
R1(config)# ipv6 route 13::/64 130
R1(config)# exit
R1#
```

Figura 31. Ejemplo ruta estática flotante.

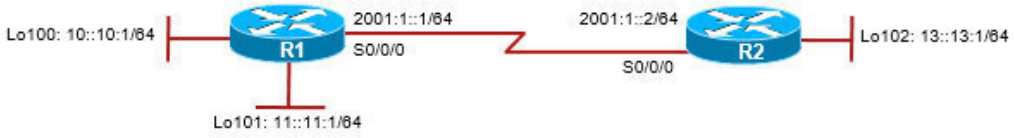
Ruta estática por default.

```
Router(config)#
ipv6 route ::/0
  {ipv6-address | interface-type interface-number [ipv6-address]}
  [administrative-distance]
```

Figura 32. Ruta estática por default.

IPv6 también tiene una ruta estática por defecto similar al cero IPv4 quad (0.0.0.0) ruta estática por defecto. En su lugar, el comando IPv6 utiliza el :: / 0 notación para especificar todas las redes.

El siguiente ejemplo, una ruta estática por defecto especificada por la entrada ":: / 0" está configurado en el router R2 para llegar a todas las otras redes conectadas a R1.




```
R2# config t
R2(config)# ipv6 route ::/0 s0/0/0
R2(config)# exit
R2# show ipv6 route static
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S    ::/0 [1/0]
     via ::, Serial0/0/0
R2#
```

Figura 33. Ruta estática por default.

2.8 Configuración de IPv6 a un host en Windows 7.

A la hora de establecer una comunicación y en este caso como en el punto anterior, para una ruta estática necesitamos que nuestro destino si es un host este configurado en IPv6, de lo contrario no podrá haber un entendimiento entre red y host. A continuación se muestran los pasos para habilitar IPv6 desde un equipo con Sistema Operativo Windows 7.

1.- Abrir centro de redes y recursos compartidos.
2.- Dar click en la opción de conexión de red inalámbrica o conexión de área local, según sea el caso.
3.- Propiedades.
4. Funciones de red.
5.- Habilitar la opción “Protocolo de internet versión 6 TCP/IPv6)”.
6.- Dar doble click en la opción anterior en donde se accederá a las propiedades del protocolo de internet versión 6 IPv6, en donde se podrá configurar la dirección y sus parámetros de manera automática o manual.

En la Figura 34 se pude observar la configuración y la habilitación de IPv6 en un host, aclarando que en un mismo host se pueden tener tanto IPv4 y/o IPv6 habilitados.

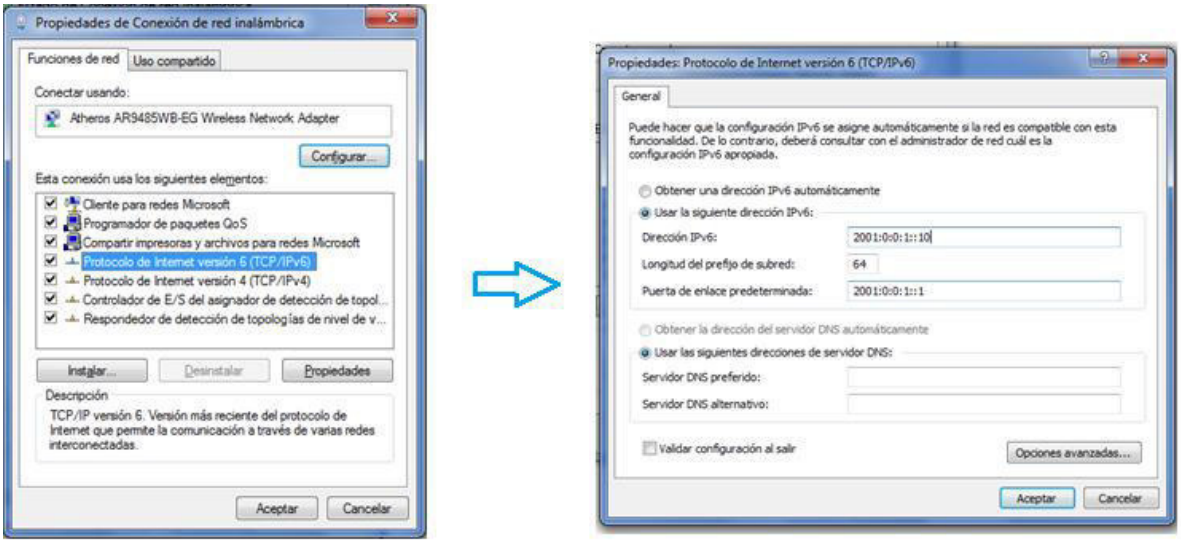


Figura 34. Habilitar IPv6 desde Windows 7.

CAPÍTULO 3: “Protocolos de Ipv6”.

CAPÍTULO 3: "PROTOCOLOS DE IPv6".

Cuando se creó la siguiente generación de protocolo IP surgió la necesidad que los protocolos que logran el enrutamiento también se actualizarán.

Existen diferentes protocolos de enrutamiento utilizados en IPv4 y en IPv6, en la Tabla 6 se podrá visualizar que protocolos se utilizan en IPv4 en comparación a los utilizados en IPv6.

	Protocolos de enrutamiento vector distancia.		Protocolos de enrutamiento de estado de enlace.		Vector Camino.
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP para IPv6	OSPFv3	IS-IS para IPv6	GGP-4 para IPv6

Tabla 6. Protocolos de enrutamiento IPv4 vs IPv6.

De los cuales se abordaran en este capítulo alguno de ellos, así como la explicación básica de dichos protocolos.

Para la configuración de IPv6 es necesario conocer también los protocolos ND, DHCPv6 (Dynamic Hosts Configuration Protocolo version 6) e ICMPv6 (Internet Control Message Protocol version 6).

3.1 RIPng (Routing Information Protocol next generation).

Como bien sabemos el protocolo RIP (Routing Information Protocol) es de la clase de algoritmos conocidos como vectores a distancia.

RIPng permite a los routers calcular rutas a través de una red IPv6 para el intercambio de información, RIPng solo es configurado en routers IPv6 ya que nos proporciona otros tipos de mecanismos para los descubrimientos de routers que los que implementa RIP en IPv4.

Características del protocolo:

Este protocolo es limitado para redes en las que la ruta de un router a otro sea mayor a 15 saltos, ya que permite redes donde no sobre pasen 15 saltos.
Puede comparar las diferentes rutas de origen-destino.
Actualizaciones cada 30 segundos.
Rutas anunciadas; se anuncia las rutas compuestas de prefijos de Ipv6.
Siguiente salto, el siguiente salto debe ser una dirección IPv6 Link-Local del router.
Usa el protocolo UDP (User Datagrama Protocol) como trasporte.

Dirección IPv6 fuente: La actualización RIP de la dirección fuente IPv6 es la dirección Link-Local de la interfaz del router fuente. Con excepción al contestar un mensaje de solicitud Unicast desde un puerto distinto al puerto RIPng, en dicho caso, la dirección fuente es una dirección global válida).
Dirección IPv6 origen: La dirección destino de la actualización RIP es FF02::9, que es la dirección multidifusión de todos los routers RIP. Únicamente los routers RIPng atienden esta dirección Multicast. Es una dirección Multicast con alcance de Link-Local, la cual no es retransmitida a otros enlaces.
El puerto UDP es 521, en lugar de 520 para RIPv1 y 2.
La autenticación RIPng se basa en la seguridad proveída por IPSec.

3.1.1 Como habilitar RIPng.

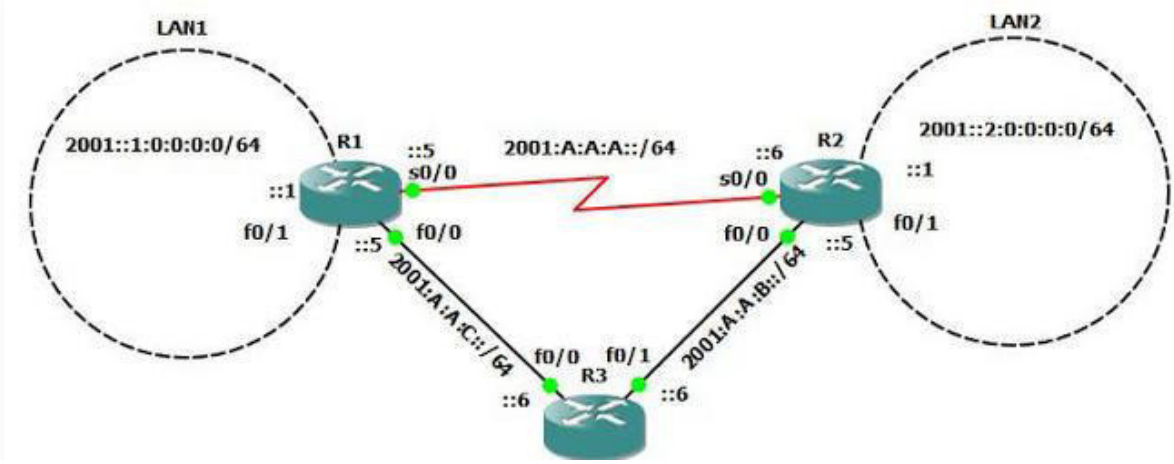


Figura 35. Ejemplo de una configuración con RIPng.

En la Figura 35, tenemos una topología de 3 routers y dos LAN que debemos unir mediante un direccionamiento IPv6. Los bloques asignados están escritos y para simplificar la configuración se han dejado todos en /64.

Configuración de las direcciones IP en cada interfaz de cada router.

R1:
R1(config)#
R1(config)#int s0/0
R1(config-if)#ipv6 address 2001:A:A:A::5/64
R1(config-if)#no shutdown
R1(config-if)#int f0/0
R1(config-if)#ipv6 address 2001:A:A:C::5/64
R1(config-if)#no shutdown
R1(config-if)#int f0/1
R1(config-if)#ipv6 address 2001:0:0:1::1/64
R1(config-if)#no shutdown

R1(config-if)#

R2:
R2(config)#
R2(config)#int s0/0
R2(config-if)#ipv6 address 2001:A:A:A::6/64
R2(config-if)#no shutdown
R2(config-if)#int f0/0
R2(config-if)#ipv6 address 2001:A:A:B::5/64
R2(config-if)#no shutdown
R2(config-if)#int f0/1
R2(config-if)#ipv6 address 2001::2:0:0:0:1/64
R2(config-if)#no shutdown
R2(config-if)#
R3:
R3(config-if)#int f0/0
R3(config-if)#ipv6 address 2001:A:A:C::6/64
R3(config-if)#no shutdown
R3(config-if)#int f0/1
R3(config-if)#ipv6 address 2001:A:A:B::6/64
R3(config-if)#no shutdown
R3(config-if)#

Después de verificar que cada router tenga comunicación entre ellos, se define que el direccionamiento IPv6 está completo, el siguiente paso es enrutar, al igual que en IPv4, los routers solo conocen los host y redes que tienen directamente conectadas. Se empleara el comando “unicast-routing” similar a “ip-routing” en IPv4.

R1:
R1(config)#ipv6 unicast-routing

R2:
R2(config)#ipv6 unicast-routing

R3:
R3(config)#ipv6 unicast-routing

Para habilitar RIPng solamente se debe ingresar a la interfaz de router que se desea publicar en el proceso RIP e ingresar el comando ipv6 rip IDENTIFICADOR enable donde “IDENTIFICADOR” es un etiqueta de proceso al estilo OSPF (Open Shortest Path First). Este valor puede ser un número o una palabra. A continuación ingresaremos en todas las interfaces de R1, R2 y R3 para ingresar este comando. Note que la interfaz f0/1 de R1 y R3 no conectan con ningún otro router, pero sin embargo en ellas también se debe habilitar RIPng para que esas redes se publiquen.

R1:
R1(config)#int f0/0
R1(config-if)#ipv6 rip IDENTIFICAR1 enable
R1(config-if)#int f0/1
R1(config-if)# ipv6 rip IDENTIFICAR1 enable
R1(config-if)#int s0/0
R1(config-if)# ipv6 rip IDENTIFICAR1 enable
R1(config-if)#end

R2:
R2(config)#int f0/0
R2(config-if)#ipv6 rip IDENTIFICAR1 enable
R2(config-if)#int f0/1
R2(config-if)# ipv6 rip IDENTIFICAR1 enable
R2(config-if)#int s0/0
R2(config-if)# ipv6 rip IDENTIFICAR1 enable
R2(config-if)#end

R3:
R3(config)#int f0/0
R3(config-if)#ipv6 rip IDENTIFICAR1 enable
R3(config-if)#int f0/1
R3(config-if)# ipv6 rip IDENTIFICAR1 enable
R3(config-if)#end

3.2. OSPF para IPv6.

OSPF es un protocolo de enrutamiento de IP de estado de enlace, en oposición a un protocolo de vector de distancia. Un protocolo de estado de enlace toma decisiones de enrutamiento basadas en los estados de los enlaces que conectan los host de origen y destino. El estado de un enlace es una descripción de esa interfaz y la relación con sus dispositivos de red vecinos. La información de interfaz incluye el prefijo IPv6 de la interfaz, la máscara de red, el tipo de red que está conectado a, los routers conectados a esa red, y así sucesivamente. Esta información se propaga en varios tipos de anuncios de estado de enlace LSA (Link State Advertisement).

OSPF para IPv6 está definido por el RFC 5340 (OSPFv3), esta última versión fue diseñada, a diferencia de la versión 2, para soportar el direccionamiento de IPv6.

Aunque la versión fue modificada para el uso en IPv6, esta contiene la mayoría de las mismas características que la versión 2, a continuación mencionaremos algunas de las características de este protocolo:

El proceso de enrutamiento no necesita ser explícitamente creado.

Cada interfaz debe ser habilitada con un comando en modo de configuración de interfaz, esto lo diferencia de la versión 2, donde las interfaces quedan automáticamente habilitadas con un comando de configuración global network router.
Al mismo tiempo se pueden configurar varios prefijos en una única interfaz.

3.2.1. Como Habilitar OSPF para IPv6.

Habilitar el ruteo IPv6 para Unicast.

Router> enable
Router# configure terminal
Router(config)# ipv6 unicast-routing

Habilitar OSPF para IPv6 en las interfaces comprometidas.

Router> enable
Router# configure terminal
Router(config)# interface<type><number>
Router(config-if)# ipv6 ospf area

Defina el rango de prefijos que utilizara en las distintas areas.

Router> enable
Router# configure terminal
Router(config)# ipv6 router ospf
Router(confing-rtr)# area <area-id> range <ipv6-prefix/prefix-length>

Donde:
<area-id>: para identificar a que red pertenece.
<process-id>: es el número que se usa internamente para identificar si existen multiples procesos OSPF en ejecución dentro del router.

Ejemplo:

```
interface Ethernet7/0
 ipv6 address 2001:DB8:0:7::1/64
 ipv6 ospf 1 area 1
!
interface Ethernet8/0
 ipv6 address 2001:DB8:0:8::1/64
 ipv6 ospf 1 area 1
!
interface Ethernet9/0
 ipv6 address 2001:DB8:0:9::1/64
 ipv6 ospf 1 area 1
!
```

```
lpv6 router ospf 1
 router-id 10.11.11.1
 area 1 range 2001:DB8::/48
```

3.3. EIGRP para IPv6.

EIGRP (Enhansed Interior Gateway Protocol Routing) es una versión mejorada del IGRP (Interior Gateway Protocol Routing) desarrollado por Cisco. EIGRP utiliza el mismo algoritmo de vector distancia como IGRP. Sin embargo, las propiedades de convergencia y la eficiencia operativa de EIGRP han mejorado sustancialmente en comparación con IGRP.

La convergencia de la tecnología se basa en una investigación realizada en el SRI Internacional (Stanford Research Institute) y emplea un algoritmo llamado el algoritmo de actualización de difusión (DUAL). Este algoritmo garantiza un funcionamiento libre de bucles en cada instante a lo largo de un cálculo de ruta y permite que todos los dispositivos que participan en un cambio de topología para sincronizar al mismo tiempo. Los dispositivos que no se ven afectados por los cambios de topología no están involucrados en nuevos cálculos. El tiempo de convergencia con DUAL compite con la de cualquier otro protocolo de enrutamiento existente.

EIGRP ofrece las siguientes características:
Aumento del ancho de la red: Con el protocolo de información de enrutamiento RIP, la mayor anchura posible de la red es de 15 saltos. Cuando EIGRP está habilitada, la mayor anchura posible es de 224 saltos. Debido a que la métrica EIGRP es lo suficientemente grande como para soportar miles de saltos, la única barrera para la expansión de la red es el contador de la capa de transporte hop. Cisco trabaja alrededor de esta limitación incrementando el campo de control de transporte sólo cuando un IPv4 o un paquete IPv6 ha atravesado 15 dispositivos y el siguiente salto hacia el destino que se ha aprendido a través de EIGRP. Cuando una ruta RIP está siendo utilizado como el siguiente salto hacia el destino, el campo de control de transporte se incrementa como de costumbre.
Convergencia rápida - El algoritmo DUAL permite que la información de encaminamiento para converger tan rápido como cualquier otro protocolo de enrutamiento.
Actualizaciones parciales - EIGRP envía actualizaciones incrementales cuando el estado de un cambio de destino, en lugar de enviar todo el contenido de la tabla de enrutamiento. Esta característica minimiza el ancho de banda requerido para los paquetes EIGRP.
Mecanismo de descubrimiento de vecinos - Este es un mecanismo de un simple hola utilizado para aprender acerca de los dispositivos vecinos. Es independiente del protocolo.
Resumen de ruta arbitraria.
Escalado - EIGRP escala a grandes redes.

Filtrado de rutas - EIGRP para IPv6 proporciona filtrado de ruta utilizando el distribute-list prefix-list de comandos. El uso del mapa de la ruta de comandos no se admite para el filtrado de ruta con una lista distribuir.
EIGRP tiene las siguientes cuatro componentes básicos:
Descubrimiento de vecinos EIGRP se logra con baja sobrecarga enviando periódicamente pequeños paquetes “hello” o de saludo. Una vez que se determina este estado, los dispositivos vecinos pueden intercambiar información de enrutamiento.
El protocolo de transporte fiable es el responsable de garantizar y ordenar la entrega de paquetes EIGRP a todos los vecinos. Es compatible con la transmisión entremezclada de paquetes de Multicast y Unicats. Algunos paquetes EIGRP deben ser enviados de forma fiable y otros no necesitan serlo. Por eficiencia, se proporciona sólo cuando sea necesario fiabilidad. Otros tipos de paquetes (tales como actualizaciones) requieren acuse de recibo, que se indica en el paquete. El transporte fiable tiene una disposición para enviar paquetes de Multicast rápidamente cuando los paquetes no reconocidos están pendientes. Esta disposición ayuda a asegurar que el tiempo de convergencia sigue siendo baja en la presencia de diferentes enlaces de velocidad.
La máquina de estados finitos DUAL realiza el proceso de decisión para todos los cálculos de ruta. Realiza un seguimiento de todas las rutas anunciadas por todos los vecinos. DUAL utiliza varias métricas, incluyendo la distancia y la información de costos, para seleccionar rutas sin bucles eficientes. Cuando existen múltiples rutas a un vecino, DUAL determina qué ruta tiene la métrica más baja (llamado la distancia factible), y entra en esta ruta en la tabla de enrutamiento. Se recibieron otras rutas posibles a este vecino con métricas más grandes, y DUAL determina la distancia notificada a esta red. La distancia notificada se define como la métrica total de publicidad por un vecino ascendente para una ruta a un destino. DUAL compara la distancia notificada con la distancia factible, y si la distancia informada es menor que la distancia factible, DUAL considera la ruta para ser un sucesor factible y entra en la ruta en la tabla de topología. La ruta del sucesor factible que se reporta con la métrica más baja se convierte en la ruta del sucesor a la ruta actual si la ruta actual falla. Para evitar bucles de enrutamiento, DUAL asegura que la distancia notificada es siempre menor que la distancia factible para un dispositivo vecino para llegar a la red de destino; de lo contrario, la ruta al bucle de mayo de vecino a través del dispositivo local.
Módulos de protocolo dependiente: Cuando no hay sucesores factibles a una ruta que ha fallado, pero hay vecinos que anuncian la ruta, debe ocurrir un recalculo. Este es el proceso en el que DUAL determina un nuevo sucesor. La cantidad de tiempo requerido para volver a calcular la ruta afecta el tiempo de convergencia. Recalculo es intensivo del procesador; es ventajoso para evitar recalculo innecesario. Cuando se produce un cambio de topología, DUAL pondrá a prueba para los sucesores factibles. Si hay sucesores factibles, DUAL utilizará con el fin de evitar recalculo innecesario

3.3.1. Como habilitar EIGRP para IPv6.

1. **Router>enable.**
2. **Router#configure terminal.**
3. **Router(config)#ipv6 unicast-routing.**
4. **Router(config)#interface *<type> <number>.***
5. **Router(config.if)#no shutdown.**
6. **Router(config-if)#ipv6 enable.**
7. **Router(config-if)# ipv6 eigrp version.**
8. **Router(config-if)# ipv6 router eigrp version.**
9. **Router(config-router)# eigrp router-id *ip-address.***
10. **Router(config)# exit.**
11. **Router#show ipv6 eigrp interfaces**

Paso	Comando	Descripcion.
Paso 1.	"enable".	Habilita EXEC el modo privilegiado.
Paso 2.	"configure terminal".	Entra al modo de configuración global.
Paso 3.	"ipv6 unicast-routing".	Permite el envió de un datagrama IPv6 Unicast.
Paso 4.	"interface *<type> <number>".*	Especifica la interfaz en la que EIGRP se va a configurar.
Paso 5.	"no shutdown".	Permite que el proceso de enrutamiento quede habilitado.
Paso 6.	"ipv6 enable".	Permite el procesamiento de IPv6 en una interfaz que no se ha configurado con una dirección IPv6 explícito.
Paso 7.	"ipv6 eigrp version".	Permite EIGRP para IPv6 en una interfaz especificada.
Paso 8.	"ipv6 router eigrp version".	Entra en el modo de configuración del Router y crea un proceso de enrutamiento EIGRP IPv6.
Paso 9.	"eigrp router-id *ip – address".*	Permite un ID de Router fijo. Introduce este comando solo si una dirección IPv4 no está especificada en el Router elegible para el Router ID.
Paso 10.	"exit".	Para salir del modo en el que se encuentra.
Paso 11.	"show ipv6 eigrp interfaces".	Muestra configuración sobre las interfaces configuradas para EIGRP para IPv6.

Tabla 7. Especificación de comandos para habilitar EIGRP para IPv6.

3.4. ICMPv6.

El Protocolo de control de mensajes Internet para IPv6 ICMPv6, es un estándar de IPv6 necesario que está definido en el documento RFC 2463, para IPv6.es utilizado para reportar errores en los nodos que se producen en el procesamiento de paquetes y para realizar otras funciones de la capa de internet, como enviar un ping. Es una parte fundamental del protocolo IPv6 ya que cada mensaje tiene una función especial, en donde cada mensaje se explicara posteriormente.

El protocolo ICMPv6 proporciona también un marco de trabajo para los protocolos siguientes:

MLD (Multicast Listener Discovery) consiste en una serie de tres mensajes ICMPv6 que reemplazan la versión 2 del Protocolo de administración del grupo Internet para IPv4 en la administración de la pertenencia a multidifusión de subred.

Descubrimiento de vecinos consiste en una serie de cinco mensajes ICMPv6 que administran la comunicación de un nodo a otro en un vínculo. Descubrimiento de vecinos reemplaza al ARP, Descubrimiento de enrutadores ICMPv4 y el mensaje de Redirección ICMPv4, además de proporcionar funciones adicionales.

Los mensajes ICMPv6 se suelen enviar automáticamente cuando un paquete IPv6 no puede llegar a su destino. Los mensajes ICMPv6 se encapsulan y envían como carga de los paquetes IPv6.

El formato de la cabecera ICMPv6 contiene 5 campos como se puede visualizar en la Figura 36.

En donde el primer campo es el campo “Tipo”, que es el tipo de mensaje, su valor determina el formato de los datos restantes.

El campo de suma de comprobación se utiliza para detectar corrupción de datos en el mensaje ICMPv6 y partes de la cabecera IPv6.

Y para el resto de los campos uno está sin utilizar y el otro es donde se tiene la cabecera IP más los 64 bits originales del datagrama.

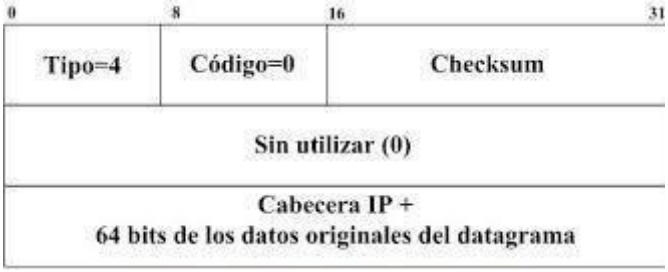


Figura 36. Cabecera ICMPv6.

Los diferentes formatos de mensajes ICMPv6 son los siguientes:
Mensaje de error IPv6, a continuación se muestra una tabla de los diferentes mensajes de error.

Mensaje	Tipo	Código	Descripción
Destino inalcanzable.	1	0	Un mensaje inalcanzable de destino debe ser generado por un router, o por la capa de IPv6 en el nodo de origen, en respuesta a un paquete que no puede ser entregado a su dirección de destino.
Paquete demasiado grande.	2	0 por el emisor e ignorado por el receptor.	Un Paquete Demasiado grande deberá ser enviado por un router en respuesta a un paquete que no puede ser enviado porque el paquete es más grande que la MTU de la enlace de salida.
Tiempo agotado.	3	0	Si un router recibe un paquete con un límite de saltos de cero, o si un router disminuye el límite de saltos de un paquete a cero saltos, se deberá desechar el paquete y originar un mensaje ICMPv6 Time Exceeded con código 0 para el origen del paquete.
Problema de parámetros.	4	0	Si un nodo IPv6 procesa un paquete y encuentra un problema en el campo en de encabezado o extensión cabeceras IPv6 no podrá realizar el procesamiento del paquete, que deberá descartar el paquete y debe originar un mensaje ICMPv6 Parameter Problem al origen del paquete, indicando el tipo y la ubicación del problema.
Experimentación privada.	100	-	-
Reservado para la expansión de los mensajes de error ICMPv6.	101 y 127	-	-

Tabla 8. Mensajes de error ICMPv6.

Mensajes informativos IPv6.

Mensaje.	Tipo.	Código.	
Eco request.	**128**	**0**	**Cada nodo deberá implementar una función de respuesta de eco ICMPv6 que recibe las peticiones de eco y se origina correspondientes respuestas de eco. Un nodo también DEBE implementar una interfaz de capa de aplicación para originario Eco Request y recibir respuestas de eco, para diagnóstico propósitos.**
Eco reply.	**129**	**0**	**Cada nodo debe implementar una función de respuesta de eco ICMPv6 que recibe las peticiones de eco y se origina correspondiente Eco Request. Un nodo también debe implementar una interfaz de capa de aplicación para originario Eco Request y recibir respuestas de eco, para diagnóstico propósitos.**
Experimentación privada.	**200 y 201**	**-**	**-**
Reservado para la expansión de los mensajes de información ICMPv6.	**255**	**-**	**-**

Tabla 9. Mensajes de información ICMPv6.

El siguiente protocolo por abordar es el protocolo Neighbor Discovery, el cual utiliza los siguientes mensajes de control de ICMPv6:

- **RS (Router Solicitacion).**

Son mensajes ICMPv6, utilizados para solicitar a un router local información de configuración de red, para el RS la única opción permitida es la “Source Link-Layer Address”.

- **RA (Router Advertisement).**

Son mensajes ICMPv6 utilizados para anunciar información de configuración de red.
A diferencia de los mensajes anteriores, este tipo de mensajes tiene permitido los siguientes:
Source Link-Layer Address.
Prefix Information:
MTU.

Route Information.
Recursive DNS Server.

- **NS (Neighbor Solicitacion).**

Determinan la etiqueta de enlace de un vecino, también utilizada para detectar detecciones duplicadas.
Son mensajes ICMPv6 utilizados para solicitar la capa de enlace correspondiente a una dirección IPv6.
La única opción que es permitida en este tipo de mensajes es la "Source Link-Layer Address", es la que contiene la dirección de capa de enlace correspondiente a la dirección origen del paquete IPv6.

- **NA (Neighbor Advertisement).**

De la misma manera que lo anterior, son mensajes de ICMPv6, la diferencia es que estos mensajes son utilizados para informar la dirección de capa correspondiente a una dirección IPv6.
En este tipo de mensajes la única opción admitida es la opción "Target Link-Layer Address" la cual contiene la dirección de capa de enlace.

- **Redirect.**

Utilizado por un router para informar a un conductor de un mejor ruta a un destino determinado.

3.5. SLAAC (Stataless Address Autoconfiguration).

Es un protocolo descrito por el RFC 2462, también conocido como Autoconfiguración sin Estado. En donde los host son escuchados por los RA periódicamente transmitidos por los routers. Los host también pueden enviar solicitudes al grupo Multicast de todos los routers.
Los mensajes RA vienen desde los routers en el enlace de la identificación de la subred. SLAAC permite crear al host una dirección IPv6 global desde el interfaz ID (direcciones EUI-64). Si los RA no cargan ningún de prefijo, los host no configuran (automáticamente) cualquier dirección IPv6 global (pero ellos configuran la dirección de Gateway por default).
La configuración de direcciones globales utiliza dos formatos en los cuales se muestran en la Figura 37 mostrando en qué tipo de configuración es utilizado SLAAC al igual que DHCPv6 mencionado en el punto 3.7 de este capítulo.

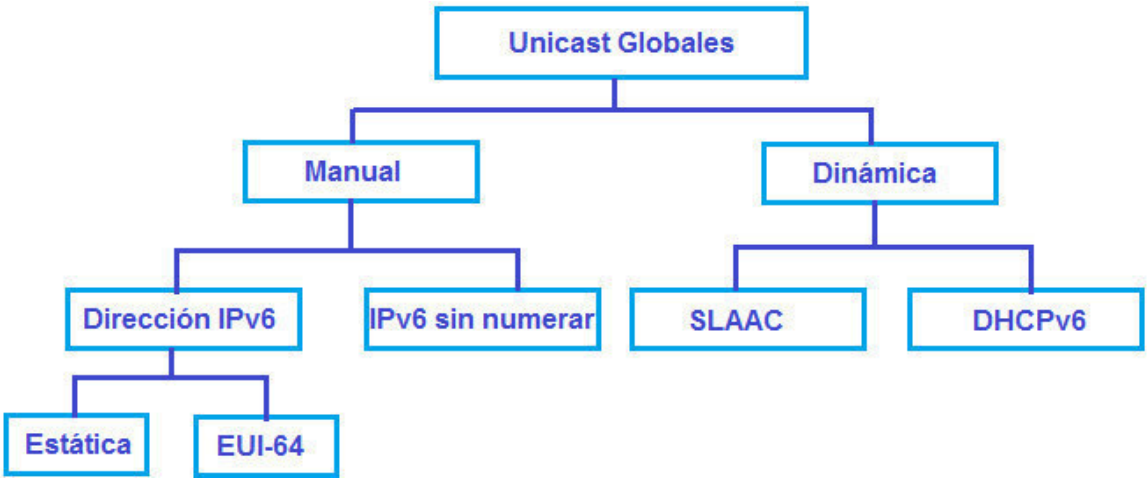


Figura 37. Unicast globales.

Como se pude observar en la Figura 37, se muestra como se clasifica SLAAC.

Configuración de una dirección dinámica usando SLAAC.

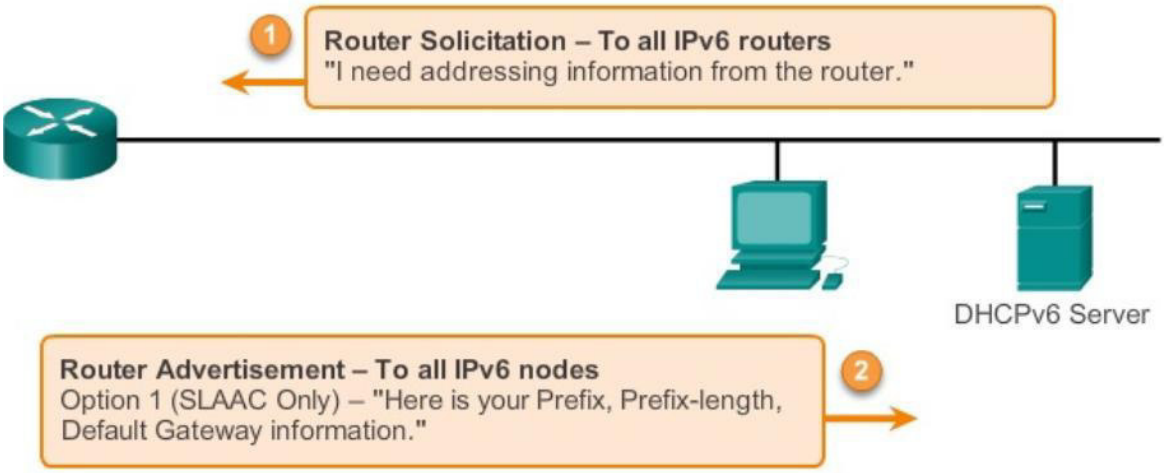


Figura 38. Ejemplo de una configuración utilizando SLAAC.

En la Figura 38 se muestra ejemplificado como se configura una dirección dinámica SLAAC:
La opción 1, implica que el host mediante un mensaje ICPMv6 RS, le solicita al router toda la información necesaria para la estructura de la dirección, donde el router debe tener lo necesario para que el host pueda configurar la dirección o elaborar la dirección, dicha información que maneja el router es necesaria, para la configuración de la dirección son tres aspectos:
1.- El prefijo, que es lo equivalente a la dirección de red en IPv4.
2.- Longitud de prefijo, que en IPv4 sería la marcara de red.
3.- Interface ID, que es el host en IPv4.
Y la opción 2, es la respuesta del router mediante un mensaje RA hacia el host, en donde le indica la información necesaria. El mensaje RA contiene los tres aspectos mencionados en la opción 1.

Ejemplo:

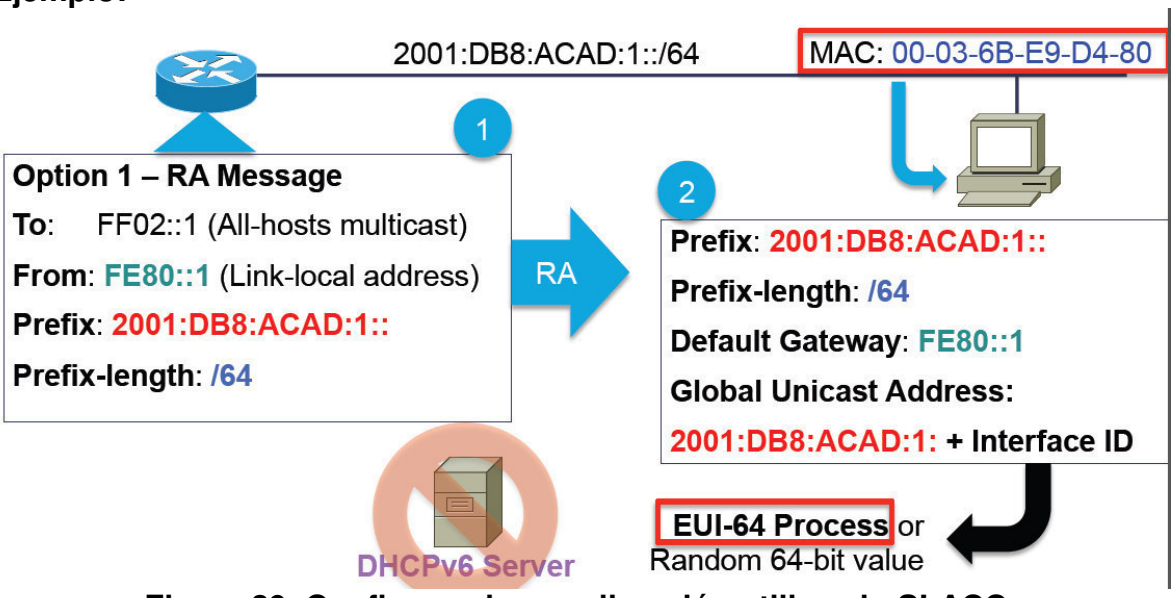


Figura 39. Configurando una dirección utilizando SLACC.

En la Figura 39 se observa un ejemplo en el cual el router le envía la información al host mediante un RA considerando que el host tendría lo necesario para la estructura de su dirección, ya que el único parámetro faltante seria la interface ID que se estructura de dos manera, mediante la norma EUI-64 mencionada en el capítulo 2 o un valor aleatorio de 64 bits.
También se puede ver que hay un servidor DCHP negado, esto implica que la dirección se pudo obtener únicamente con la ayuda del router y la información que este contiene y no fue necesario alguna otra información que haya tenido que ser requerida de un servido DCHP, y es por eso que esta manera de estructurarse la dirección en el host es tipo SLAAC,

El funcionamiento se basa en lo siguiente:

- El host configura una dirección Link-Local.
- Verifica que la dirección sea única mediante el procedimiento de DAD (Detección de Dirección Duplicada), se envía un NS para verificar si se tiene respuesta.
- El host envía un mensaje RS.
- Al recibir una respuesta se configura una dirección IPv6 tentativa.
- Se realiza de nuevo el procedimiento DAD, de la misma manera, enviando un NS para confirmar que exista una respuesta.
- Si después de lo anterior la dirección tentativa es única, se convierte en una dirección valida, si no lo es, el proceso se repite hasta encontrar una dirección valida.

3.6. ND (Neighbor Discovery).

Es un protocolo definido en el RFC 2461 con las siguientes características:
Remplaza el protocolo ARP en IPv4 a través de ICMPv6 y trafico Multicast, esto implica que los equipos pueden resolver la dirección de capa 2 basados en una dirección de capa 3.
Detecta direcciones IP duplicadas como un mecanismo de protección a los equipo determinan por si solos si la IP asignada a la interfaz está disponible.
Otro aspecto muy importante de este protocolo es la autoconfiguración, lo que quiere decir que cada equipo tiene la capacidad de descubrir la información de la red a la que perteneces y de esta forma configurar su propia dirección IP. Utiliza 3 protocolos para el proceso de autoconfiguración:
SLAAC (autoconfiguración de direcciones sin estado) especificado por el RFC 2462 como ya explicado en el subtema anterior.
DHCPv6(Protocolo de configuración dinámica de host) especificado en el RFC 3315.
Path MTU Discovery (Descubrimiento de la ruta MTU) o pMTU especificado por el RFC 1981 PS.
De igual manera que los anteriores tiene la característica del redireccionamiento con la ayuda de ICMPv6 en donde un nodo puede informar acerca de la mejor ruta de acceso hacia un vecino.

3.6.1. Resolución de direcciones.

Este proceso utiliza mensajes ICMPv6 “Neighbor Solicitation” y “Neighbor Advertisement” mediante un proceso simple denotado en los siguientes puntos:
El host 1 envía un Neighbor Solicitation, a grandes rasgos solicitando quien de entre todos los host de la red tienen la dirección IP hacia donde se enviara la información.
El host 2, responde a la solicitud del host 1 con una Neighbor Advertisement, indicando que cuenta con la dirección IP que solicita el host 1 y así mismo con la dirección MAC correspondiente.
El host 1 “cachea” la información recibida en el “Neighbor Cache” durante un tiempo.
El host 1, puede enviar ahora los paquetes o la información al host 2.

3.6.2. Ventajas del protocolo ND.

El descubrimiento es parte de la base de este protocolo, ya que no es preciso recurrir a los protocolos de encaminamiento.
La anunciación de router ya incluye las direcciones de la capa de enlace, prefijos de la capa de enlace, además dicha opción permite la autoconfiguración de direcciones.
Los routers pueden anunciar a los host del mismo enlace el MTU
Se pueden asignar múltiples prefijos al mismo enlace y por defecto los host aprenden todos los prefijos por la anunciación de router.
A diferencia de **IPv4**, en IPv6 el receptor de una redirección asume que el siguiente salto está en el mismo enlace. Se prevé una gran utilidad en el sentido

de no ser deseable o posible que los nodos conozcan todos los prefijos de los destinos en el mismo enlace.
La detección de vecinos no alcanzables es parte de la base de mejoras para la robustez en la entrega de paquetes frente a fallos en routers, particiones de enlaces, nodos que cambian sus direcciones, nodos móviles, etc.
A diferencia de ARP, en ND se puede detectar fallos de la mitad del enlace, es decir, con conectividad en un sólo sentido, evitando el tráfico hacia ellos.
A diferencia de **IPv4**, no son precisos campos de preferencia (para definir la "estabilidad" de los routers). La detección de vecinos no alcanzables sustituirá los caminos desde routers con fallos a otros activos.
El uso de *d*irecciones de enlace local para identificar routers, permite a los hosts que mantengan su asociación con los mismos, en el caso de que se realice una remuneración para usar nuevos prefijos globales.
Al realizar la resolución de direcciones en la capa **ICMP**, se independiza el protocolo del medio, permitiendo mecanismos de autenticación y seguridad normalizados.

3.6.3. PMTUD.

Es el encargado de garantizar que el paquete encaminado sea del mayor tamaño posible, todos los nodos IPv6 deben soportar (PMTUD).
Función de PMTUD:
Asume que la máxima MTU del camino es igual a la MTU del primer salto.
Los paquetes mayores que el soportado por algún router a lo largo del camino se descarta.
Se devuelve un mensaje ICMPv6 "packet too big".
Luego de recibir este mensaje el nodo de origen reduce el tamaño de los paquetes de acuerdo con la MTU indicada en el mensaje "packet too big".
El procedimiento finaliza cuando el tamaño de la MTU es igual o menor que la MTU del camino
Los paquetes enviados a un grupo Multicast utilizan un tamaño igual a la menor PMTU de todo el conjunto de destinos.

3.7. DHCPv6.

Es un protocolo cliente servidor, definido en el RFC 3315, que proporciona una configuración administrativa de dispositivos sobre IPv6.
Tipos de mensajes DHCPv6 y cómo funcionan:

Solicit: El cliente manda un mensaje para localizar los servidores.

Advertise: En respuesta al mensaje "solicit", este mensaje indica que el servidor está disponible para el servicio.

Request: Se utiliza cuando el cliente envia este mensaje para solicitar los parámetros de configuración, incluyendo la dirección IP de un cliente en específico.

Confirm: El cliente envia este mensaje a cualquier servidor disponible para confirmar si las direcciones que se asignaron siguen siendo validad.

Renew: Enviado por el cliente, se usa para extender los tiempos de vida de una dirección asigna y actualizar los parámetros de configuración.

Rebind: Cuando el cliente no obtiene respuesta del mensaje renew, se envía este mensaje a cualquier servidor disponible solicitando los mismos parámetros que en el mensaje renew.

Reply: Se envía del servidor en respuesta a los mensajes solicit, request, renew, rebind recibido del cliente, también se manda este mensaje en respuesta a la solicitud confirm, confirmando o denegando una dirección asignada al cliente.

Relase: Un cliente envía este mensaje al servidor para indicar que ya no utilizara más la o las direcciones asignadas.
En la siguiente imagen se observa un pequeño ejemplo de cómo funciona el DHCPv6.

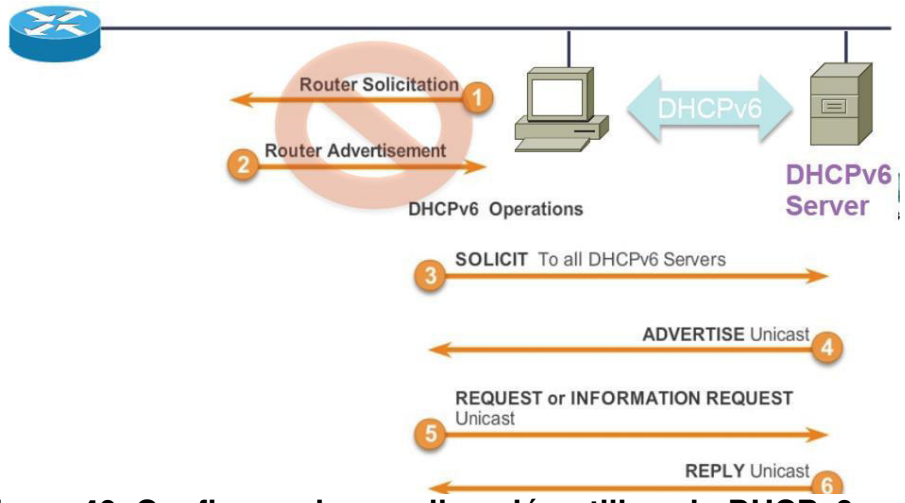


Figura 40. Configurando una dirección utilizando DHCPv6 con estado.

Como se puede ver en la imagen, en la opción 1 y 2 se observa que el host no utiliza el RS y por ende el RA debido a que requiere otro tipo de información que no puede ser brindado por el simple router, si no que necesita del servidor de DHCP.
Como se denota en la opción 3, el host solicita toda la información al servido DHCP, el cual le envía una respuesta mediante una Unicast para confirmar la información, el host le indica que la información es la correcta, lo que produce que el servidor DHCP le asigne la dirección al host. Esto se denomina como una dirección Stateful DHCPv6.

3.8. Configuración automática de direcciones IPv6.

Un aspecto muy útil de IPv6 es su capacidad para configurarse automáticamente y sin el uso de un protocolo de configuración de estado, tales como el Protocolo de configuración dinámica de host para IPv6 (DHCPv6). Por defecto, un host IPv6 puede configurar una dirección local de vínculo para cada interfaz. Mediante el uso de descubrimiento de enrutadores, un host también puede determinar las direcciones de los routers, direcciones adicionales y otros parámetros de configuración. Incluido en el mensaje de anuncio de enrutador es una indicación de si un protocolo de configuración de direcciones con estado se debe utilizar.
Autoconfiguración de dirección sólo se puede realizar en las interfaces con capacidades Multicast. Configuración automática de direcciones se describe en el RFC 2462, "sin estado Dirección IPv6 Autoconfiguración".

3.8.1. Estados de direcciones auto configuradas.

Direcciones configuradas automáticamente están en uno o más de los siguientes estados:
Tentativa. La dirección es en el proceso de ser verificado como única. La verificación ocurre a través de la detección de direcciones duplicadas.
Preferidos. Una dirección para la que se ha verificado la singularidad. Un nodo puede enviar y recibir tráfico de unidifusión hacia y desde una dirección preferida. El período de tiempo que una dirección puede permanecer en los estados provisionales y preferentes se incluye en el mensaje de anuncio de enrutador.
Deprecated. Una dirección que sigue siendo válida, pero su uso no se recomienda para la nueva comunicación. Sesiones de comunicación existentes se pueden seguir utilizando una dirección obsoleta. Un nodo puede enviar y recibir tráfico de unidifusión hacia y desde una dirección en desuso.
Válido. Una dirección en la que el tráfico Unicast puede ser enviado y recibido. El estado válido cubre tanto los estados preferidos y obsoletos. La cantidad de tiempo que una dirección se mantiene en los estados provisionales y válidos se incluye en el mensaje de anuncio de enrutador. El tiempo de vida válido debe ser mayor que o igual a la vida útil preferida.
Inválida una dirección para que un nodo ya no puede enviar o recibir tráfico de unidifusión. Una dirección entra en el estado no válido después de que expire el periodo de vida válido.

3.8.2 Tipos de autoconfiguración.

Hay tres tipos de configuración automática:

Stateless: Se basa en la recepción de mensajes de anuncio de enrutador. Estos mensajes incluyen prefijos de direcciones sin estado y requieren que los hosts no

utilizan un protocolo de configuración de direcciones con estado. Dicha configuración es la usada en SLAAC.
Stateful: Se basa en el uso de un protocolo de configuración de direcciones con estado, como DHCPv6, para obtener direcciones y otras opciones de configuración. Un host utiliza la configuración de direcciones con estado cuando recibe mensajes de anuncio de enrutador que no incluyen prefijos de dirección y requieren que el huésped utiliza un protocolo de configuración de direcciones con estado. Un host también se utiliza un protocolo de configuración de direcciones con estado cuando no hay routers presentes en el vínculo local.

Both: Se basa en la recepción de mensajes de anuncio de enrutador. Estos mensajes incluyen prefijos de direcciones sin estado y requieren que los equipos utilizan un protocolo de configuración de direcciones con estado.
Para todo tipo de autoconfiguración, una dirección de enlace local siempre está configurado.

3.9 Proceso de configuración automática.

1. El proceso de configuración automática de direcciones para un nodo IPv6 se produce como sigue:

2. Una dirección local de vínculo provisional se deriva, en función del prefijo local de vínculo de FE80 :: / 64 y el identificador de interfaz de 64 bits.

3. Detección de direcciones duplicadas se realiza para verificar la exclusividad de la dirección local de vínculo provisional.
4. Si la detección de direcciones duplicadas falla, la configuración manual debe ser realizado en el nodo.

5. Si la detección de direcciones duplicadas tiene éxito, la dirección local de vínculo provisional se supone que es única y válida. La dirección de enlace local se inicializa para la interfaz. La dirección de multidifusión de capa de enlace de nodo solicitado correspondiente se ha registrado en el adaptador de red.

Para un host de IPv6, configuración automática de direcciones continúa de la siguiente manera:

1. El host envía un mensaje de solicitud de enrutador.

2. Si no se reciben mensajes de anuncio de enrutador, el host utiliza un protocolo de configuración de direcciones con estado para obtener direcciones y otros parámetros de configuración. El protocolo IPv6 para la familia Windows Server 2003 y Windows XP no admite el uso de un protocolo de configuración de direcciones con estado.

3. Si se recibe un mensaje de anuncio de enrutador, la información de configuración que se incluye en el mensaje se establece en el host.

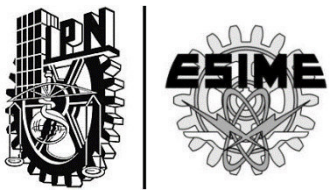
4. Para cada configuración automática sin estado prefijo de la dirección que se incluye:

   - El prefijo de la dirección y el identificador de interfaz de 64-bit apropiado se utilizan para obtener una dirección tentativa.

   - Detección de direcciones duplicadas se utiliza para verificar la exclusividad de la dirección provisional.

Si la dirección provisional está en uso, la dirección no se inicializa para la interfaz.
Si la dirección provisional no está en uso, se inicializa la dirección. Esto incluye el establecimiento de los tiempos de vida válidos y preferentes en base a la información incluida en el mensaje de anuncio de enrutador.

Si se especifica en el mensaje de anuncio de enrutador, el host utiliza un protocolo de configuración de direcciones con estado para obtener direcciones adicionales o parámetros de configuración.



CAPÍTULO 4:
Técnicas de transición de Ipv4 a Ipv6.

CAPÍTULO 4: "Técnicas de transición de IPv4 a IPv6".

Existen diferentes técnicas para la transición de IPv4 a IPv6 y cada una de estas técnicas se basa en diferentes funcionamientos incluso coexistiendo estos dos protocolos ya que en un periodo de tiempo los sistemas basados en IPv6 con la base instalada de IPv4 y es aquí donde llegamos a describir los 2 métodos de transición para el cambio de versión del protocolo IP a IPv6. Para obtener una correcta y exitosa transición de protocolo debemos de tener una inmensa compatibilidad con la base de hosts y routers de IPv4 ya que si mantenemos una compatibilidad con IPv4 mientras se despliega IPv6 permitirá la agilización de la transición de IPv6. Estos mecanismos de transición son descritos en el RFC 2893 el cual hablaremos más adelante. No necesariamente necesitamos realizar una actualización en todos los nodos ya que contamos con diferentes mecanismos de transición que nos permite una incorporación fluida de IPv4 e IPv6.

Una opción es implementar una única red IPv6

Con requerimientos específicos:

- Todos los componentes deben ser compatibles con IPv6.
- Es probable que tenga que comunicarse con sistemas IPv4.
- Entonces necesitamos una manera de traducir lo protocolos a alguna capa.

Los mecanismos de migración de IPv4 a IPv6 son los siguientes:

- **Dual Stack.**
- **Túnel.**
  - **Configuración manual.**
    - **Túnel Bróker.**
  - **Configuración automática.**
    - **Túnel 6 to 4.**
    - **Túnel 6 to 4 relay.**
    - **Túnel Teredo.**

Los cuales se describirán a detalle en este capítulo así como algunos ejemplos de cada uno de estos.

A continuación describiremos cada uno de los mecanismos de transición del protocolo.

4.1 Dual Stack (doble pila).

Este mecanismo o técnica nos proporciona soporte a los dos protocolos tanto IPv4 e IPv6 en host y routers. La forma de operación de este mecanismo es la forma más directa para hacer compatibles nodos de IPv6 con solo nodos IPv4 y es proporcionando un implementación completa a IPv4. Los nodos de IPv6 que proporcionan una completa implementación en IPv4 e IPv6 son llamados "IPv6/IPv4 nodes" estos tienen la habilidad de enviar y recibir paquetes de IPv4 e IPv6. Estos nodos pueden operar directamente con nodos IPv4 usando paquetes de IPv4 y a su vez con nodos IPv6 usando paquetes de este mismo protocolo, estos nodos tienes 3 diferentes formas de operación:

- Con la pila de IPv4 activada y la pila de IPv6 desactivada.
- Con la pila de IPv6 activada y la pila de IPv4 desactivada.
- Con ambas pilas activadas.

Como se puede observar en la Figura 41:

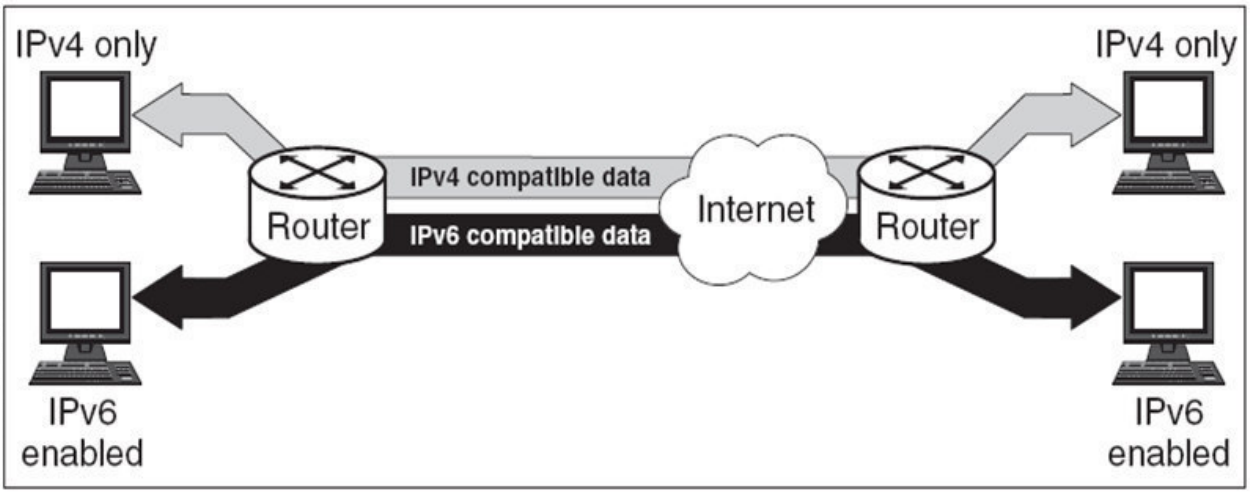


Figura 41. Dual Stack operación.

En Dual Stack ambos protocolos (IPv4 e IPv6) se encuentran en los nodos, al igual necesita plataformas de host y router. La siguiente figura muestra ambos protocolos.

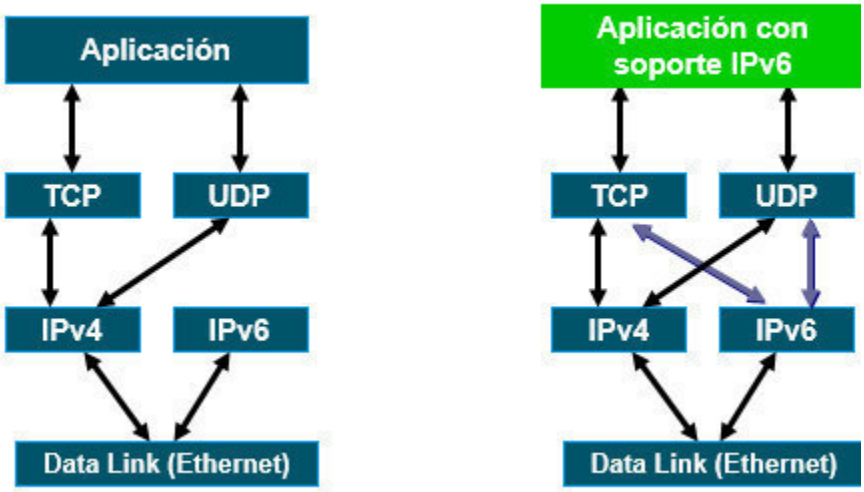


Figura 42.Soporte Dual Stack.

4.1.1. Configuración de direcciones.

Ya que los nodos IPv6/IPv4 soportan ambos protocolos pueden ser configurados con ambas direcciones tanto de IPv4 e IPv6. Los nodos IPv6/IPv4 utilizan los mecanismos de IPv4 como puede ser DHCP para obtener direcciones IPv4 y mecanismos de IPv6 como puede ser configuración automática SLAAC para adquirir direcciones nativas de Ipv6.

4.1.2. DSN (Domain Naming System).

El DNS es utilizado para ambos protocolos ya que asigna los nombres de hosts y las direcciones IP. Para IPv6 se ha definido un nuevo recurso llamado “A6” ya antes mencionado apoyándose en un recurso anterior llamado “AAA” debido a que los nodos IPv6/IPv4 deben ser capaces de interactuar con los nodos IPv4 e IPv6, es por eso que las librerías de solución de DNS en los nodos IPv6/IPv4 deben ser capaces de manejar estos recursos tanto A6/AAA y registros A. Sin embargo cuando localiza un registro A6/AAA sosteniendo una dirección IPv6, y un registro A sosteniendo una dirección IPv4 las librerías de resolución pueden ordenar los resultados devueltos a la aplicación con el fin de que en los paquetes de IP que se utilizan para comunicarse con tal nodo.

Ventajas:

- No requiere ningún mecanismo de tunelización de las redes internas
- Ipv6 e IPv4 corren independientemente entre si
- Soporte de la migración gradual de puntos finales, redes y aplicaciones
- La comunicación es posible entre todos los nodos de la red, sin necesidad de encapsulación o traducción.

- Ambas pilas IPv4 e IPv6 habilitadas.
- Las aplicaciones se comunican por IPv4 e IPv6
- Selección de la versión está basada en la resolución de nombres y la preferencia de la aplicación.

Desventajas:

- Hay que mantener dos redes.
- No reduce la demanda de direcciones IPv4.

4.2 Como configurar Dual Stack.

La configuración de Dual Stack es impresionantemente sencilla y a continuación mostraremos la sintaxis de este mecanismo:

1. **Router> enable.**
2. **Router# configure terminal.**
3. **Router(config)# ipv6 unicast-routing.**
4. **Router(config)# interface <tipo><número>.**
5. **Router(config-if)# ipv6 address <ipv6-prefijo/tamaño del prefijo> <interface>.**
6. **Router(config-if)# ip address *<dirección ip> <cascara de red>.***
7. **Router(config-if)# no shutdown.**
8. **Router(config-if)# exit.**
9. **Router(config)# exit.**
10. **Router# show run.**

En la Tabla se observa la función de cada comando.

Pasos	Comando	Acción
Paso 1	"enable"	Modo privilegiado.
Paso 2	"configure terminal"	Modo de configuración global.
Paso 3	"ipv6 unicat-routing"	Habilita el reenvió de datagramas IPv6 Unicast. .
Paso 4	"interface"	Especifica la interface a configurar, ejemplo Ethernet, FastEthernet, Seriales, etc.
Paso 5	"ipv6 address"	Especifica la dirección de red ipv6 a configurar en ese nodo.
Paso 6	"ip address"	Especifica la dirección IP de red de IPv4 que será configurada en el router.
Paso 7	"no shutdown"	
Paso 8 y 9	"exit"	Salir de cualquier modo de configuración.
Paso 10	"show run"	Comando para visualizar la configuración del router, interfaces, seriales, protocolos de enrutamiento, etc.

Tabla 10. Especificaciones de comandos para la configuración Dual Stack.

4.2.1. Implementando Dual Stack.

Ejemplo: en la siguiente imagen se puede ver una red en la que se configura Dual Stack, con el propósito de habilitar un enrutamiento IPv6, configurar las interfaces mediante un direccionamiento estático con el fin de lograr obtener comunicación de un Host origen de una red con un Host destino perteneciente a otra con ambos protocolos configurados IPv4-IPv6.

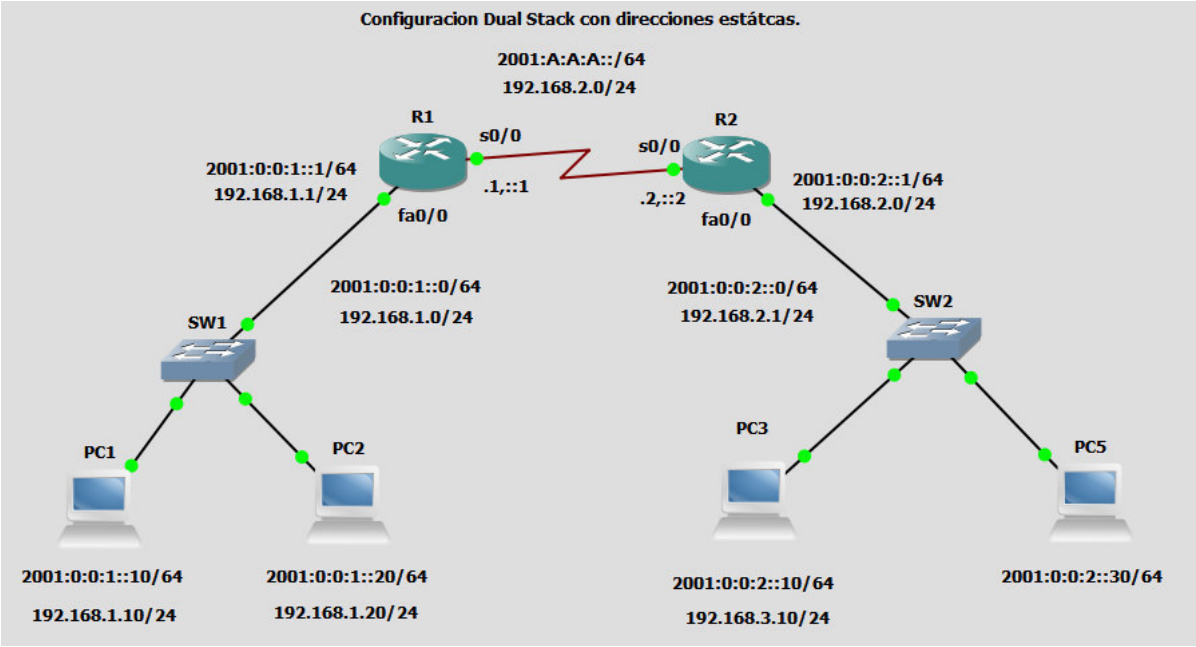


Figura 43. Red configurada con Dual Stack.

A continuación se muestra la configuración escrita del Router 1, Router 2 y en cada host habilitaremos las direcciones que se observan de manera estática:

%Configurando la FastEthernet y serial en IPv4.
Router>enable
Router#config t
Router(config)#interface f0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit

Router#config t
Router(config)#interface s0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit

%Habilitando RIPv2.
Router#config t
Router(config)#router rip
Router(config-version)#version 2
Router(config-version)#network 192.168.1.0
Router(config-version)#network 192.168.2.0

%Habilitando ahora fastehternet y serial para IPv6.
Router#config t
Router(config)#ipv6 unicast-routing
Router(config)#interface f0/0
Router(config-if)#ipv6 address 2001:0:0:1::1/64
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit

Router#config t
Router(config)#ipv6 unicast-routing
Router(config)#interface s0/0
Router(config-if)#ipv6 address 2001:A:A:A::1/64
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit

%Configurando RIPng para IPv6.
Router#config t
Router(config)#interface s0/0
Router(config-if)#ipv6 rip identificar1 enable
Router(config)#interface f0/0
Router(config-if)#ipv6 rip identificar1 enable

Router#copy running start

Para la configuración del R2 se aplica la misma configuración cambiando las correspondientes direcciones FastEthernet0/0 y la del Serial0/0 conforme a las direcciones que se ven en la imagen.

Configuración R1:

interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
ipv6 address 2001:0:0:1::1/64

```
 ipv6 rip identificar1 enable
!
interface Serial0/0
 ip address 192.168.2.1 255.255.255.0
 ipv6 address 2001:A:A:A::1/64
 clock rate 2000000
!
router rip
 version 2
 network 192.168.1.0
 network 192.168.2.0
 network 192.168.3.0
!
Configuración R2:
interface FastEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2001:0:0:2::1/64
 ipv6 rip identificar1 enable
!
interface Serial0/0
 ip address 192.168.2.2 255.255.255.0
 ipv6 address 2001:A:A:A::2/64
 clock rate 64000
!
router rip
 version 2
 network 192.168.2.0
 network 192.168.3.0
!
```

Donde se puede observar que en ambas interfaces y ambos seriales se encuentran habilitados tanto IPv4 e IPv6, en este ejemplo por los protocolos de enrutamiento RIPv2 y RIPng.

A continuación se muestra como se configuro la dirección IPv4 e IPv6 en el host1, siguiendo esta misma sintaxis para los demás hosts.

```
%Configurando las IP's en el host1:
PC1> ip 192.168.1.10/24 192.168.1.1
PC1> ip 2001:0:0:1::10/64 2001:0:0:1::1
PC1> save
```

Aplicando el comando “show ip” y el comando “show ipv6” podremos observar como quedaron almacenadas las direcciones en el host.

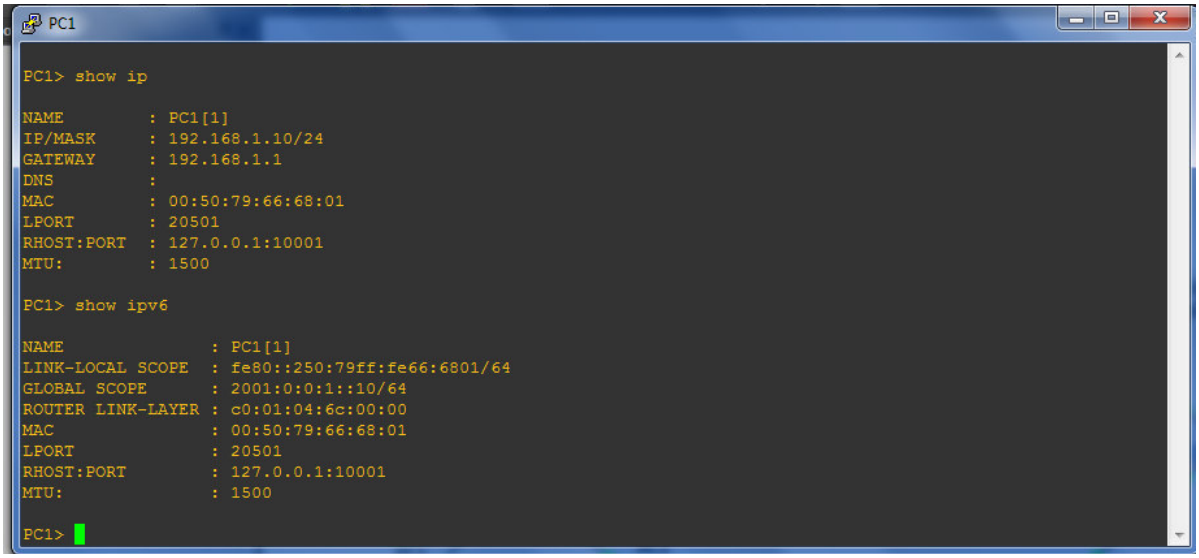


Figura 44. Muestro de configuración de IP's en el Host.

Para comprobar la conexión y que exista comunicación en cada extremo de la red se puede comprobar realizando un ping del host1 al host3, habiendo comunicación de IPv4-IPv4 y de IPv6-IPv6.

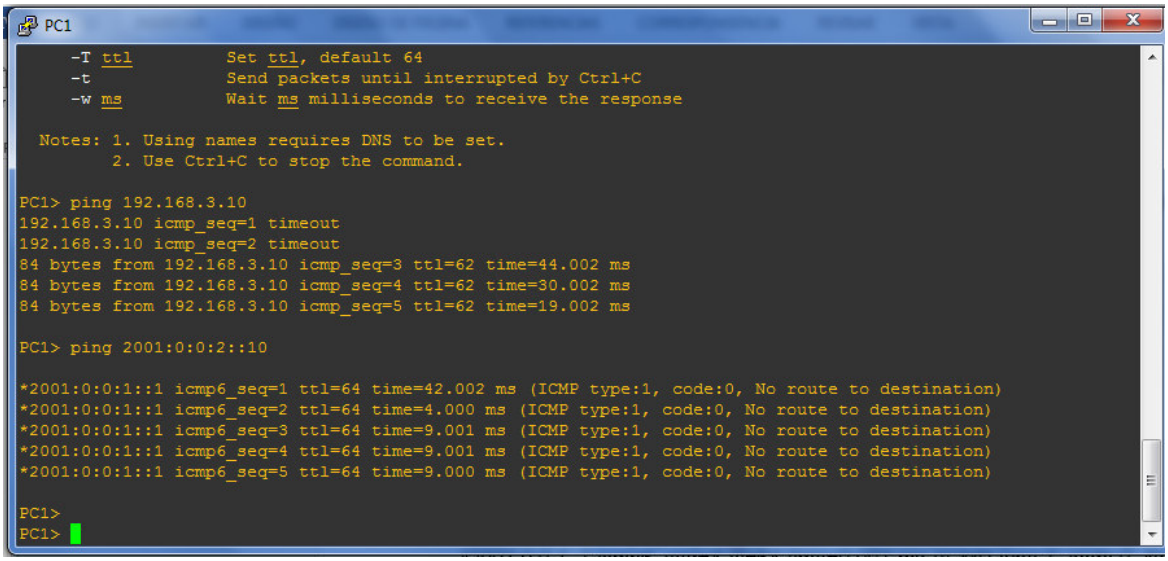


Figura 45. Haciendo ping desde el Host1 hacia el otro extremo con el Host3.

4.2 Tunelización de IPv6 (Common Tunneling Mechanisms).

La mayoría de las implementaciones de IPv6 llevan cierto periodo de tiempo ya que la infraestructura de enrutamiento de IPv6 lleva tiempo. Al igual la infraestructura de IPv4 puede ser funcional a la par que se despliega la infraestructura de IPv6 ya que utilizan la infraestructura de IPv4 para transportar el tráfico de IPv6.

El siguiente mecanismo nos proporciona una forma de utilizar la infraestructura ya existente para transportar el tráfico de IPv6
Hosts y routers IPv6/IPv4 pueden tunelizar paquetes IPv6 sobre regiones de topología de enrutamiento de IPv4 por medio del encapsulamiento dentro de paquetes de IPv4.la siguiente figura nos da una visión sobre este mecanismo:

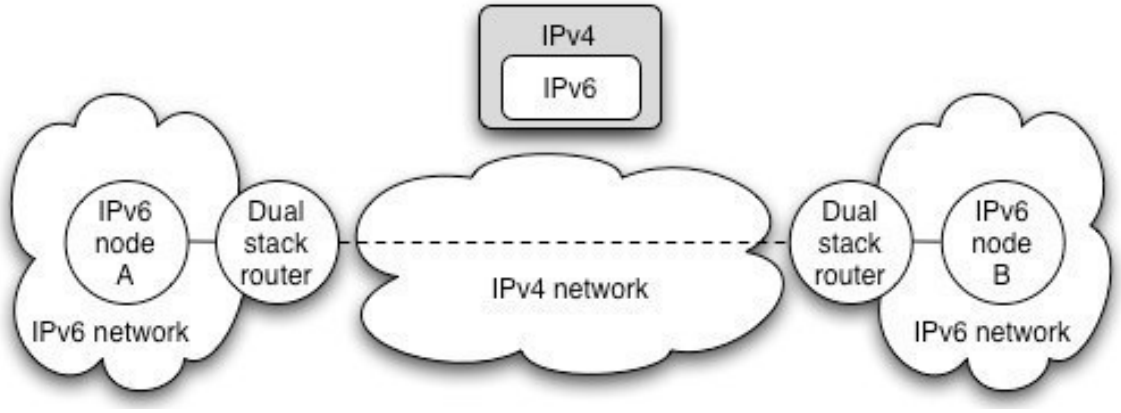


Figura 46.Tunelización

La tunelización se puede utilizar de las siguientes maneras:

Router a router.

Routers de IPv6/IPv4 son interconectados por la infraestructura de IPv4 pueden tunelizar paquetes de IPv6 entre sí. El túnel se extiende por un segmento de la ruta de extremo a extremo que el paquete IPv6 toma.

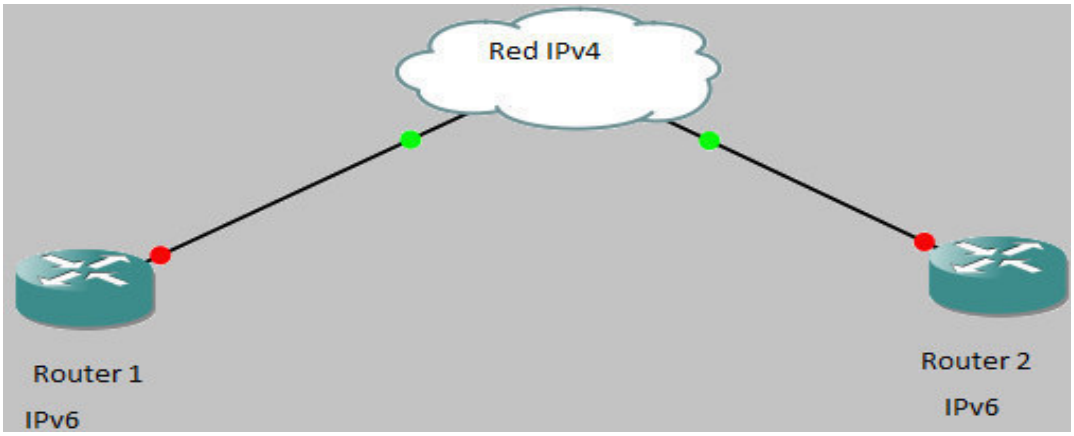


Figura 47. Túnel router a router.

Host a router.

Hosts de IPv6/IPv4 puede tunelizar paquetes de IPv6 a un router intermedio IPV6/IPv4 que es accesible a través de un infraestructura de IPv4. Este tipo de túnel se extiende al primer segmento de la trayectoria de extremo a extremo al paquete.

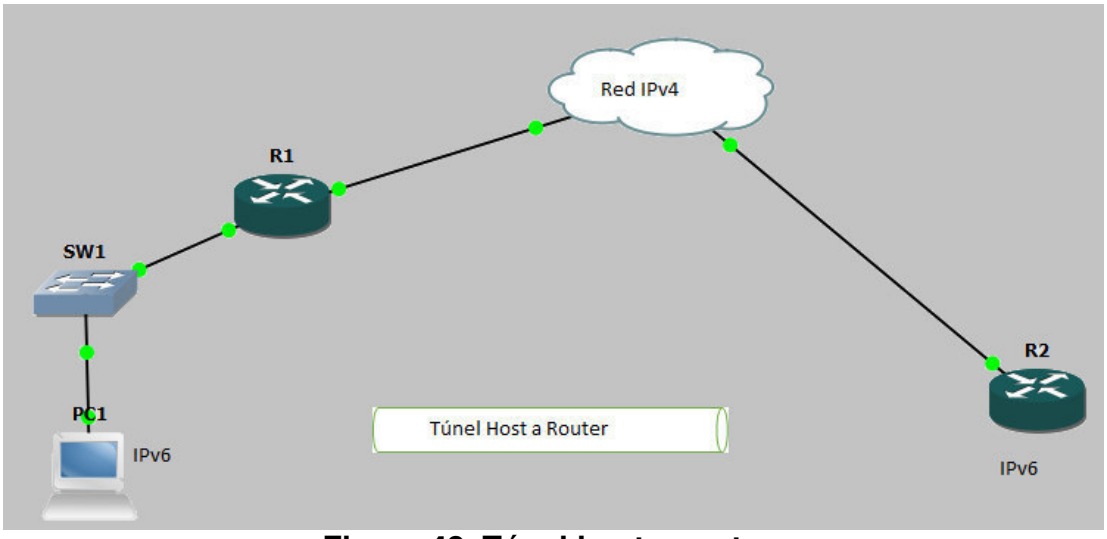


Figura 48. Túnel host a router.

Host a host.

Hosts de IPv6/IPv4 que están interconectados por una infraestructura IPv4 pueden tunelizar los paquetes entre sí, en este caso el túnel se extiende por toda la ruta de extremo a extremo del paquete.

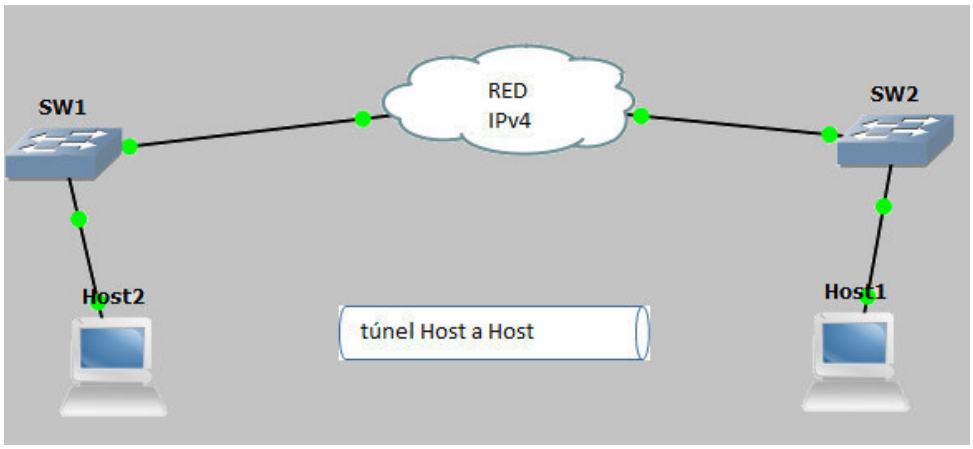


Figura 49. Túnel Host a Host.

Router a host.

Routers de IPv6/IPv4 puede tunelizar paquetes de IPv6 a su host final IPv6/IPv4. Este túnel solamente se extiende en el último segmento de la ruta de extremo a extremo.

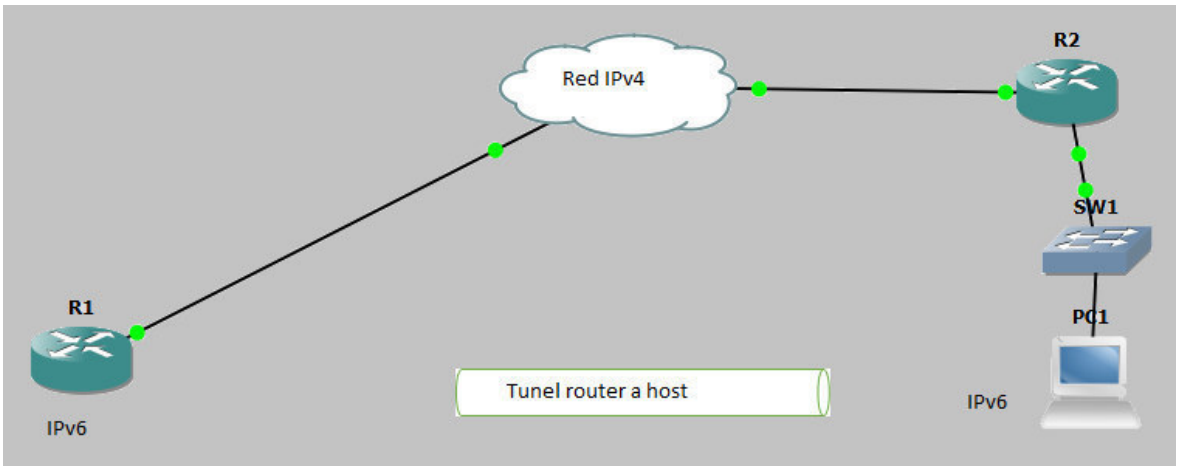


Figura 50. Túnel Router a Host.

Las técnicas de tunelización son usualmente clasificadas de acuerdo con el mecanismo por el cual el nodo de encapsulación determina la dirección del nodo en el extremo del túnel.

4.2.1. Envió de paquetes a través del túnel.

Nodo A envía un paquete IPv6 a nodo B	**El paquete es enrutado en el interior del router de frontera A**
Router de frontera A observa que la red B es accesible a través del túnel	**Encapsula los paquetes IPv6 en paquetes IPv4 (s)** **envía paquetes resultantes al router de frontera B** **se entrega sobre la infraestructura existente de internet IPv4**
Router de frontera B des encapsula el paquete IPv6 de la carga útil del paquete IPv4 recibido	**El paquete es enrutado internamente en la red B al nodo B** **El nodo B recibe el paquete IPv6**

Tabla 11. Envió de paquetes a través del túnel.

Podemos visualizar la Figura 51 con el siguiente ejemplo de un túnel:

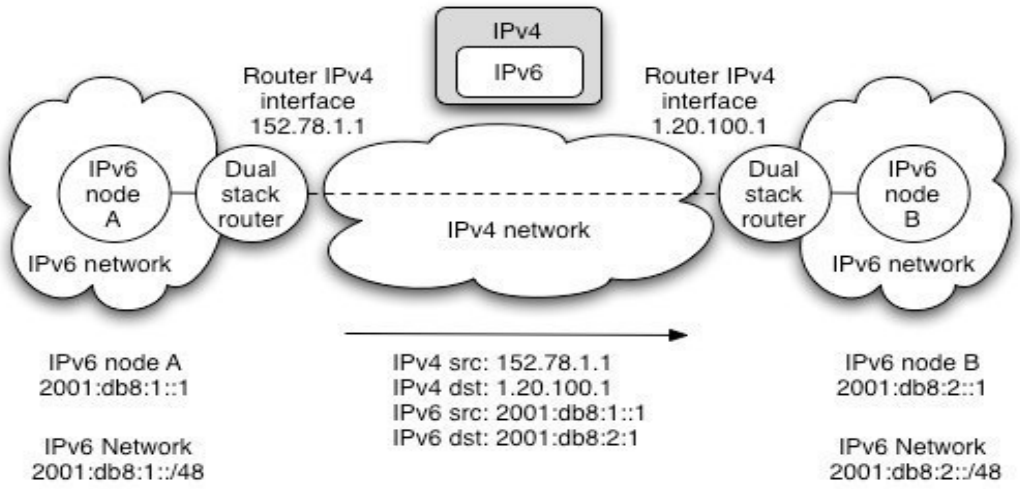


Figura 51. Ejemplo de tunelización.

4.2.2. Encapsulamiento.

La siguiente figura representa el encapsulamiento de un datagrama de IPv6 en IPv4.

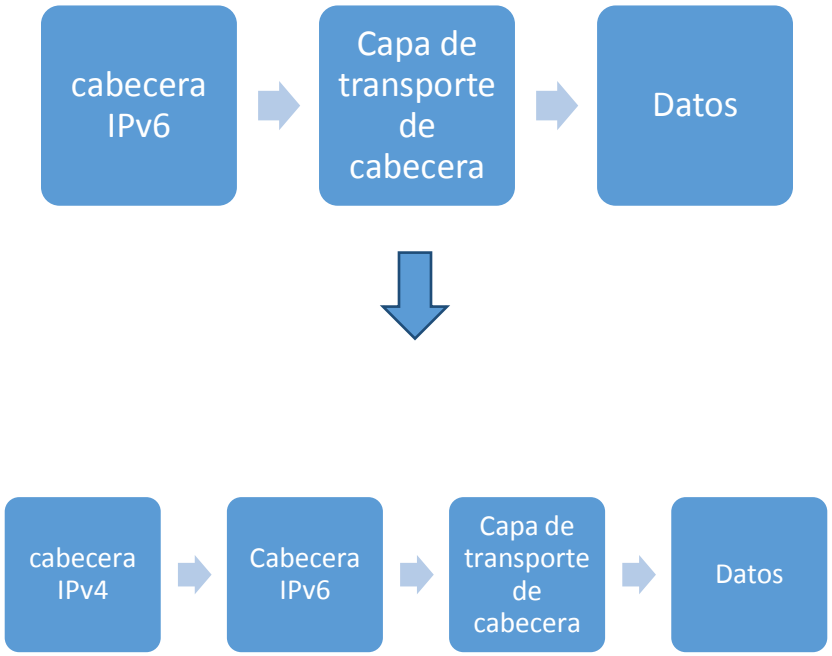


Figura 52. Encapsulamiento IPv6 en IPv4.

Al añadir un encabezado de IPv4, el nodo de encapsulamiento tiene que asumir otros problemas complejos que se mencionan a continuación:

Determinar cuándo fragmentar y cuando reportar a ICMP de un “packet too big” a la fuente.

Cómo reflejar errores IPv4 ICMP de routers a lo largo de la ruta del túnel de nuevo a la fuente como errores IPv6 ICMP

4.2.3 Des encapsulamiento.

Cuando un host IPv4/IPv6 o router recibe un datagrama Ipv4 que su destino es una dirección Ipv4 y además el valor del campo del protocolo es 41, este datagrama se vuelve a ensamblar si el paquete es fragmentado en el nivel de IPv4, entonces se elimina la cabecera de IPv4 y se envía el datagrama Ipv6 a su código de la capa de IPv6. El nodo de des encapsulación debe ser capaz de re ensamblar un paquete de Ipv4 esto es 1300 bytes (1200 bytes más la cabecera de IPv4). En la des encapsulación del paquete la cabecera de Ipv6 no es modificada.

El des encapsulamiento de mostrado en la siguiente figura:

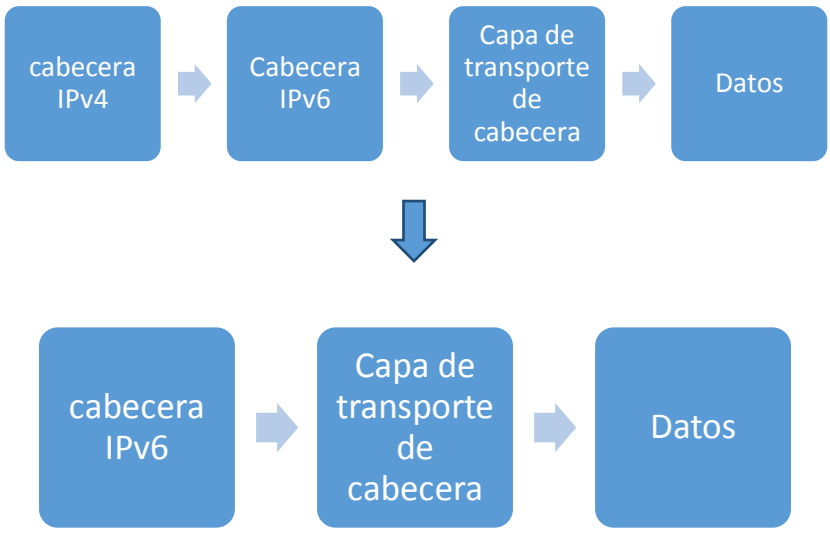


Figura 53. Des encapsulamiento IPv6 de IPv4.

4.2.4 Fragmentación.

IPv6 requiere que la fragmentación de paquetes sólo si se produce en sistemas finales, no en los routers intermedios.

Uso PMTU para elegir la MTU
Uso especial de mensajes ICMP
Mínimo MTU es 1280 bytes en IPv6

Cuando un túnel IPv6 en IPv4, los paquetes IPv4 pueden ser fragmentados
Depende del tamaño del paquete IPv4
Cabeceras adicionales IPv6 (por ejemplo, cabecera de autenticación) afectarán a este

Direcciones Link-Local.

Los túneles configurados al igual que los túneles automáticos son interface de Ipv6. Las direcciones "Link-Local" son usadas por los protocolos de enrutamiento que operan sobre los túneles.
El identificador de interfaz para una interfaz debe ser la dirección IPv4 de 32 bits de esa interfaz con el mismo orden que aparecen en la cabecera de un paquete de IPv4 rellenado desde la izquierda con ceros dando un total de 64 bits.
La dirección "Link-Local" de Ipv6 para una interface virtual de IPv4 es formado añadiendo el identificador de enlace en el prefijo "FE80::/64".

FE	80	00	00	00	00	00	00	
00	00	00	00	Dirección IPv4				Identificador de interfaz

Figura 54. Link Local.

Neighbor Discovery sobre túneles.

En este mecanismo de túneles la formación de las direcciones link-local hace uso de ND y SLAAC. Si en una implementación se proporciona túneles configurados bidireccionalmente, estos al menos deberán aceptar y responder la prueba de paquetes usados por Neighbor Unreachability Detection.

4.2.5 Configuración de túnel.

El nodo de encapsulamiento con la información de configuración es el que determina la dirección del punto final del túnel, por cada túnel el nodo de encapsulamiento debe almacenar la dirección del punto final del túnel. Cuando un paquete de IPv6 es transmitido por el túnel la dirección del final del túnel configurado por ese túnel es usado como la dirección de destino por la cabecera de IPv4 de encapsulamiento.

Configuración manualmente.

Esta es la configuración estática de un túnel, esta configuración es utilizada para comunicar dos sitios cuando en el camino no existe IPv6.

Ventajas de la configuración manualmente.

Muy sencillo de preparar y configurar.
Buen potencial de gestión.

ISP configura todos los túneles, por lo que está en control de su despliegue.
Usualmente usado para router a router y host a router.
Conveniente para permitir al usuario final registrarse (y posteriormente autenticar) para solicitar un túnel.
El IPv6 Tunnel Broker (RFC 3053) ofrece un sistema de este tipo, por lo general para la conectividad de host a router, pero a veces para router a router.

4.3 Túnel Broker.

Como hemos mencionado antes este túnel utiliza la configuración manualmente y su modelo de operación es el siguiente:

El usuario/cliente se registra en el sistema
Un túnel se pide desde una dirección IPv4
El túnel bróker establece el final del túnel solicitado en el servidor del túnel
El Broker comunica la configuración de túnel para el usuario, para la configuración del lado del cliente

La siguiente figura nos muestra la arquitectura del túnel bróker:

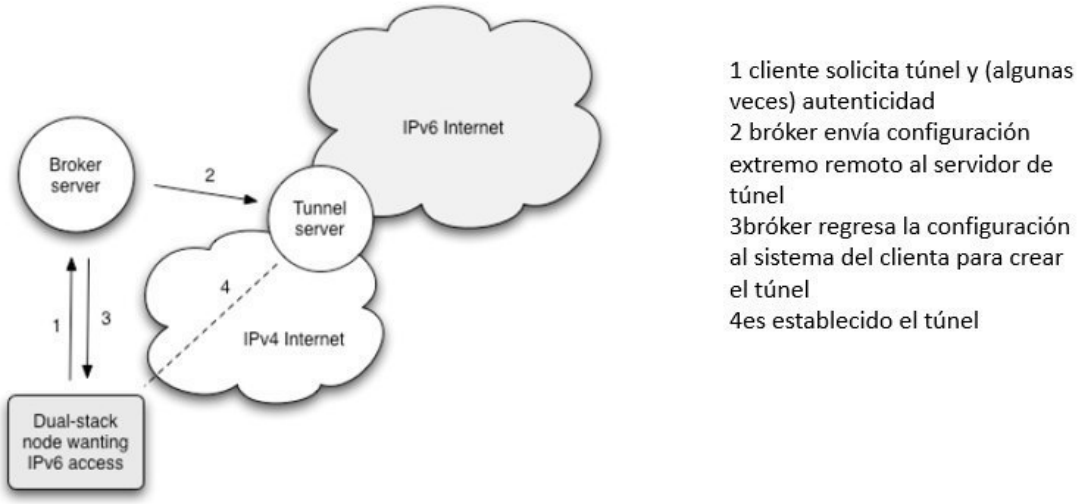


Figura 55. Arquitectura del túnel bróker.

Túnel automático.

El objetivo del túnel automático es eso, ya que se busca no se requerir un esfuerzo personal para la instalación y mantenimiento de túneles. Es generalmente utilizado de router a router, existen diferentes métodos de túneles automáticos.

4.4 6 to 4.

Es utilizado para conectar dos islas IPv6 en una red IPv4, se utiliza un truco especial para el prefijo 2002::/16 que es reservado para el uso 6 to 4 los 32 bits de este prefijo son los 32 bits de la dirección IPv4 del router 6 to 4 la siguiente figura muestra una vista básica del 6 to 4:

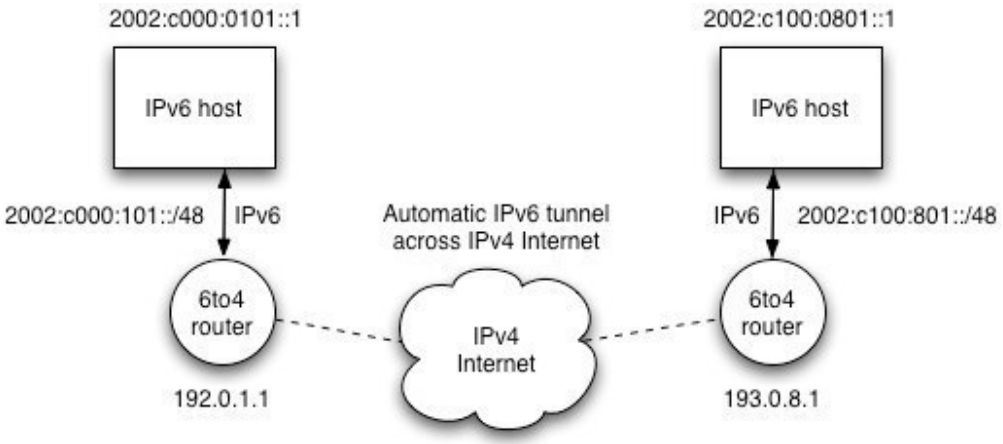


Figura 56. 6 to 4.

4.5 6 to 4 con Relay.

En una configuración con relay se tiene una interfaz 6 to 4 y una interfaz "real" IPv6 los paquetes enviados desde un sitio 6 to 4 con una dirección de destino exterior 2002::/16 cuando se tiene un relay los paquetes son des encapsulados en él y luego son enviados a la interfaz real IPv6. Cuando los paquetes enviados desde un sitio real IPv6 hacia una dirección utilizando el prefijo 2002::/16 son enrutados en un relay 6to 4 y después al túnel usando 6 to 4 al sitio de destino. La siguiente imagen muestra una red con túnel 6to 4 con relay:

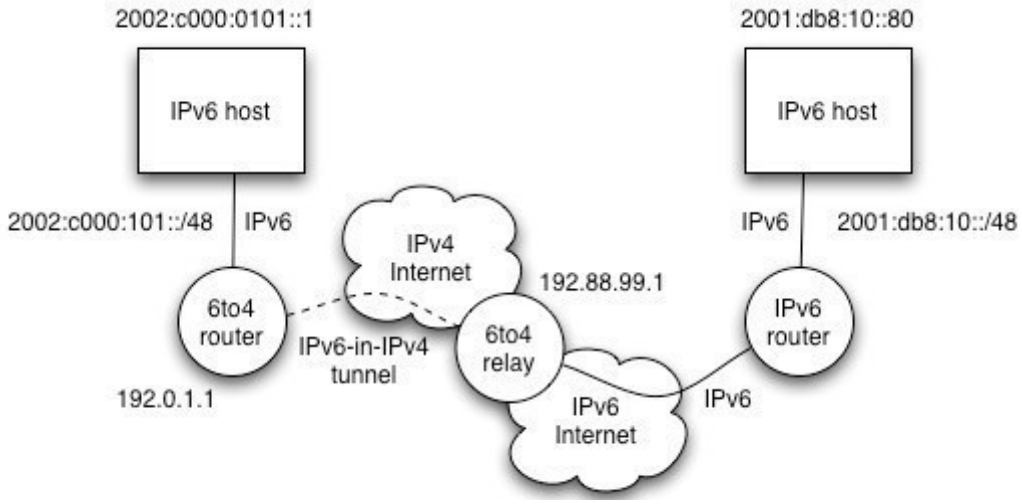


Figura 57. 6 to 4 con relay.

Así mismo utilizando dos relay podemos obtener una red asimétrica la cual puede enviar paquetes IPv4 como IPv6.

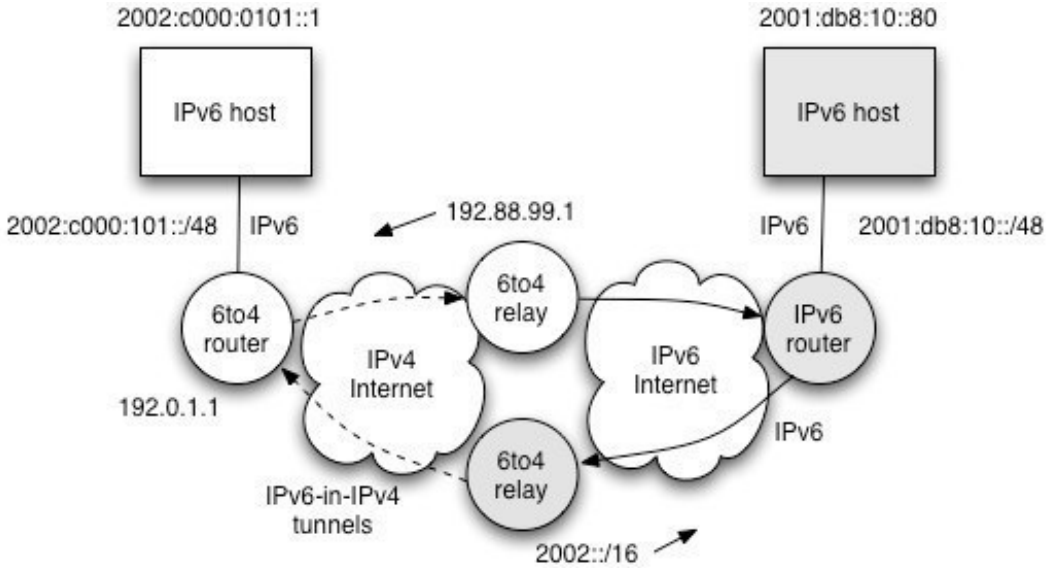


Figura 57. 6 to 4 utilizando 2 relay.

La siguiente comparación nos da las ventajas y desventajas entre si sobre una configuración manual y automática ya que se compara el túnel bróker con el túnel 6 to 4:

Característica	6 a 4	Túnel bróker
Seguridad	Potencial de abuso	Soporta auteticacion
Setup	Automático	Manual
Facilidad de gestión	Pobre (automatica)	Buena
Direcciones dinamias IPv4	Pobre	Pobre
Host o tuneles sitio	Sitio primario	Host primario
Escabilidad	Muy buena	Buena
Recorrido NAT	Difícil	Si con TSP
Descubrimiento de servicios del túnel	Automático	Configuración manual
Soporte de servicio especial	Variable	Variable
Concentración banda ancha	Solo para 6 a 4 relevador	Servidor del túnel

Tabla 12. 6 to 4 Vs túnel Broker.

4.5 Configuración de túneles automáticos (6to4).

Los siguientes pasos describen la forma en como configura un túnel automático 6to4:

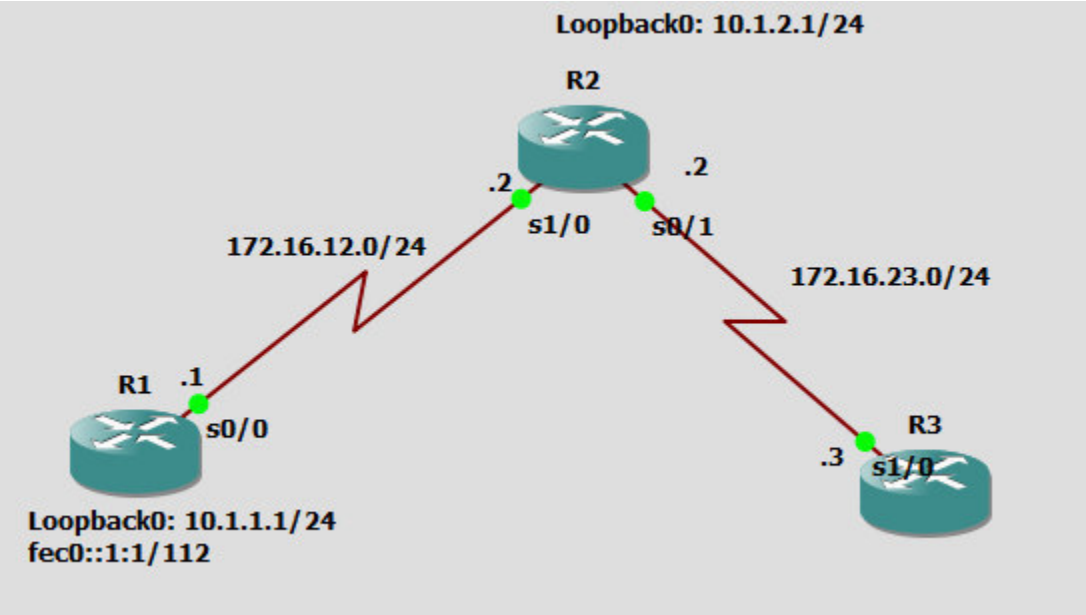
1. **Router>enable.**
2. **Router#configure terminal.**
3. **Router(config)#interface tunnel <*tunnel-number*>.**
4. **Router(config-if)#ipv6 address <*ipv6-prefix*/*prefix-length* [eui-64]>.**
5. **Router(config-if)#itunnel source <*ip-address* | *interface-type interface number*>.**
6. **Router(config-if)#itunnel mode ipv6ip 6to4.**
7. **Router(config-if)#exit.**
8. **Router(config)#iipv6 route <*ipv6-prefix*/*prefix-length* tunnel *tunnel-number*>.**

Pasos	Comando	Acción
Paso 1	"enable"	Modo privilegiado.
Paso 2	"configure terminal"	Modo de configuración global.
Paso 3	"interface tunnel"	Especifica un número e interfaz de túnel y entra al modo de configuración de la interfaz.
Paso 4	"Ipv6 address"	Especifica la dirección IPv6 asignada a la interfaz y habilita el procesamiento de IPv6 en la interfaz.
Paso 5	"tunnel source"	Especifica el tipo de interfaz de origen y el número de la interfaz de origen.
Paso 6	"tunnnel mode ipv6ip 6to4"	Especifica la incrustación de un túnel ipv6 usando direcciones 6to4.
Paso 7	"exit"	Salida de la configuración de la interfaz.
Paso 8	"ipv6 route"	Configura una ruta estática para el prefijo IPv6 6to4 2002::/16 para la interfaz del túnel especifico

Tabla 13. Tabla. Especificaciones de los comandos para la configuración de túneles automáticos.

4.6 Red con mecanismo túnel 6 to 4.

La siguiente figura muestra la red en la cual se configuro el mecanismo de transición túnel 6 to 4:



59 Figura. Red túnel 6 to 4.

En el cual configuramos en cada router direcciones Loopback para representar otras redes en cada router con direcciones ipv6 y las conexiones entre routers con direcciones IPv4. Excepto en el router 2 ya que donde haremos el túnel será entre el router 1 y el 3. A continuación los siguientes comandos son los que ingresaremos a los routers:

R1(config)#interface loopback0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# ipv6 address fec0::1:1/112
R1(config-if)# interface serial0/0
R1(config-if)# ip address 172.16.12.1 255.255.255.0
R1(config-if)# clockrate 64000
R1(config-if)# no shutdown

R2(config)# interface loopback0
R2(config-if)# ip address 10.1.2.1 255.255.255.0
R2(config-if)# interface serial1/0
R2(config-if)# ip address 172.16.12.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# interface serial0/1
R2(config-if)# ip address 172.16.23.2 255.255.255.0
R2(config-if)# clockrate 64000

R2(config-if)# no shutdown

R3(config)# interface loopback0
R3(config-if)# ip addres 10.1.3.1 255.255.255.0
R3(config-if)# ipv6 address fec0::3:1/112
R3(config-if)# interface serial1/0
R3(config-if)# ip address 172.16.23.3 255.255.255.0
R3(config-if)# no shutdown

Después de configurar cada interfaz de los routers para después configurar un protocolo de enrutamiento en este caso EIGRP en cada uno de ellos.

R1(config)# router eigrp 1
R1(config-router)# no auto-summary
R1(config-router)# network 10.0.0.0
R1(config-router)# 172.16.0.0

R2(config)# router eigrp 1
R2(config-router)# no auto-summary
R2(config-router)# network 10.0.0.0
R2(config-router)# network 172.16.0.0

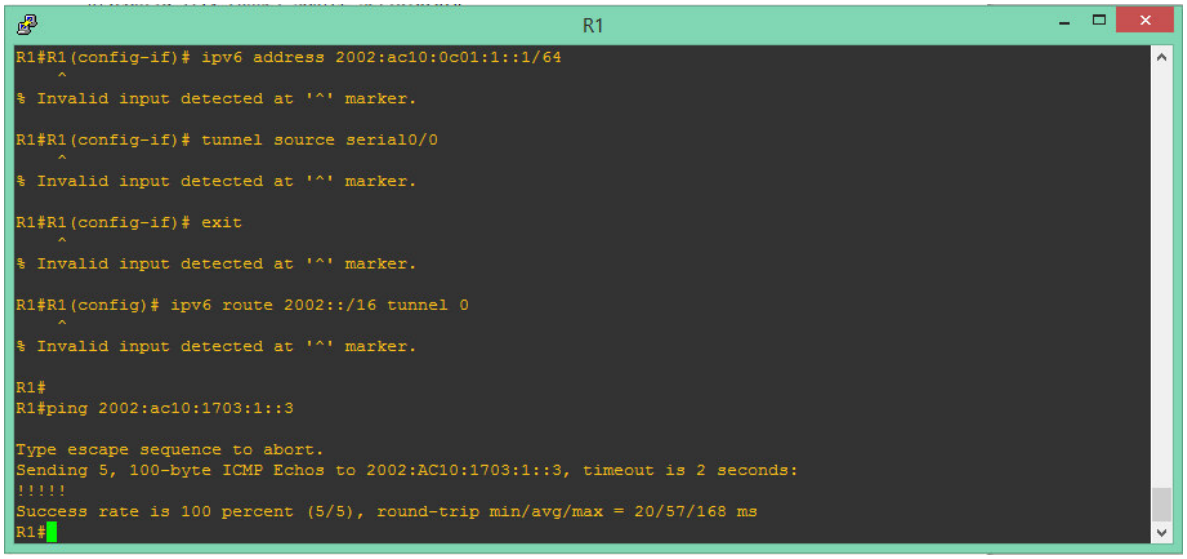
R3(config)# router eigrp 1
R3(config-router)# no auto-summary
R3(config-router)# network 10.0.0.0
R3(config-router)# network 172.16.0.0

Configuramos el túnel con los pasos antes mencionados en este capítulo en el router 1 y 3:

R1(config)# interface tunnel 0
R1(config-if)# tunnel mode ipv6ip 6to4
R1(config-if)# ipv6 address 2002:ac10:0c01:1::1/64
R1(config-if)# tunnel source serial0/0
R1(config-if)# exit
R1(config)# ipv6 route 2002::/16 tunnel 0

R3(config)# interface tunnel 0
R3(config-if)# tunnel mode ipv6ip 6to4
R3(config-if)# ipv6 address 2002:ac10:1703:1::3/64
R3(config-if)# tunnel source serial1/0
R3(config-if)# exit
R3(config)# ipv6 route 2002::/16 tunnel 0

A continuación mandamos un ping a la dirección IPv6 del túnel del router 3:



60 Figura. Ping al router 3.

Ahora mandamos un ping a la dirección IPv6 del túnel del router 1:

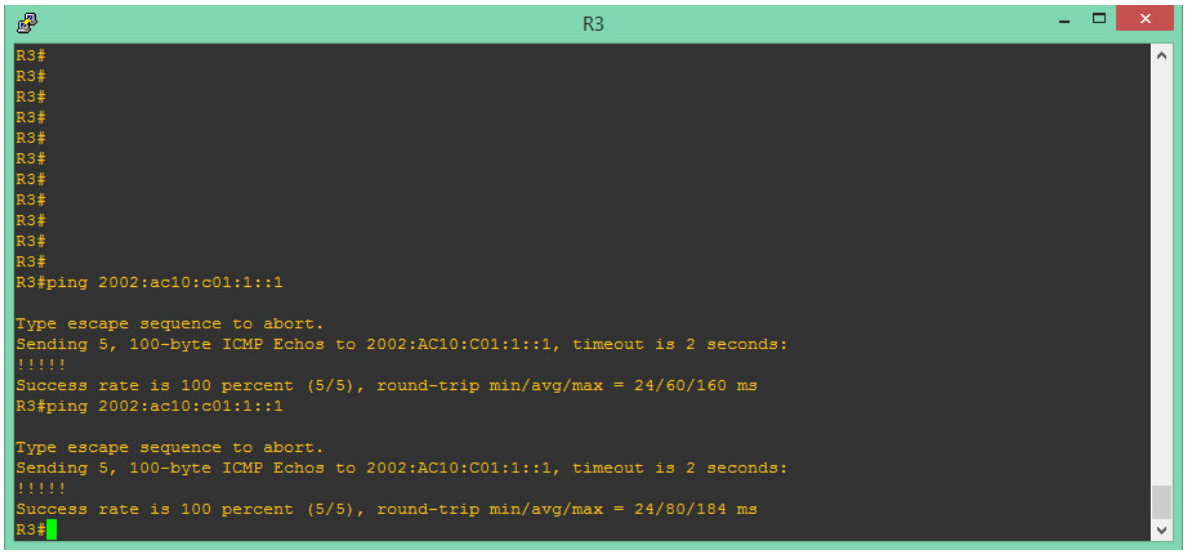


Figura 61. Ping al router 1.

Conclusión.

Como ya pudimos observar el agotamiento de IPv4 llegara tarde o temprano a su fin, con los datos que observamos, esta fecha está por llegar, es por eso que conocer el protocolo IPv6 es primordial para las redes de datos y los que se dedican a ello.

Para conocer este protocolo tuvimos que hacer uso de otros protocolos que vienen junto con el para su funcionamiento, aunque algunos de ellos venían siendo utilizados en IPv4, han sido actualizados para IPv6 e incluso otros surgieron con IPv6 como SLAAC.

En consecuencia a lo anterior llegamos al objetivo general del trabajo, que es el configurar las técnicas para una transición aplicándolas en una red en donde podemos observar que existe comunicación de extremo a extremo usando las técnicas Dual Stack y Tunel 6 to 4.

Lista de Figuras.

31	Ejemplo de una ruta estática flotante.
32	Ruta estática por default.
33	Ejemplo de una ruta estática por default.
34	Habilitar IPv6 desde Windows 7.
35	Ejemplo de configuración RIPng.
36	Cabecera ICMPv6.
37	Unicast Globales.
38	Ejemplo de una configuración utilizando SLAAC.
39	Configurando una dirección mediante SLAAC.
40	Configurando una direcciones mediante DHCPv6 con estado.
41	Dual Stack.
42	Soporte Dual Stack.
43	Red configurada con Dual Stack
44	Muestreo de configuración IP´s en el host.
45	Haciendo ping desde el host 1 hacia el otro extremo con el host 3.
46	Tunelización.
47	Router a router.
48	Túnel host a router.
49	Túnel host a host.
50	Túnel router a host
51	Ejemplo de tunelizacion.
52	Encapsulamiento IPv6 en IPv4.
53	Desencapsulamiento IPv6 en IPv4.
54	Link Local.
55	Arquitectura del Túnel Broker.
56	6 to 4.
57	6 to 4 con Relay.
58	6 ti 4 utilizando 2 Relay.
59	Red túnel 6 to 4.
60	Ping al router 3.
61	Ping al router 1.

Lista de Tablas.

Lista de Acrónimos.

Acrónimo	Significado
IPv4	Protocolo de internet versión 4.
IPv6	Protocolo de internet versión 6.
IETF	Internet Engineering Task Force (Fuerza de Tarea de Ingeniería de Internet).
IPng	Protocolo de siguiente generación.
TCP/IP	Trasnision Control Protocol /Internet Protocol (Protocolo de Control de Transmisión/Protocolo de Internet)
CIDR	*Classless Inter-Domain Routing* (Enrutamiento entre dominios sin clases).
IP	Internet Protocol (protocolo de internet).
RIR	Registro Regional de Internet.
IANA	Internet Assigned Numbers Authority (Autoridad de Números Asignados en Internet))
LACNIC	Latin America & Caribbean Network Information Centre (Registros de Direcciones de Internet para Latinoamérica y el Caribe)
OSI	Open Systems Interconnection (Interconexión de Sistemas Abiertos).
ARPANET	Advanced Research Projects Agency Network (Agencia de Investigación de Proyectos Avanzados de la Red).
DNS	Domain Name Systems (Sistemas de Nombres de Dominios)
VLSM	Variable Length Subnet Mask (Mascara de Subred de Longitud Variable).
NAT	Network Adress Traslation (Traducción de Dirección de Red).
MTU	Maximun Unit Tranfer (Unidad Máxima de Transferencia).
MAC	Media Access Control (Control de Acceso al Medio).
IEEE	*Institute of Electrical and Electronics Engineers (Instituto de Ingenieros Eléctricos y Electrónicos).*
ARP	Address Resolution Protocol (Protocol de Resolución de Direcciones).
IGMP	Internet Group Management Protocol (Protocolo de Administración de Grupos de Internet).
MLD	Multicast Listener Discovery.
ICMP	Internet Control MEssage Protocol (Protocolo de Mensajes de Control de Internet).
RA	Router Advertisement (Anuncion del Router).
RS	Router Solicitation (Solicitud del Router).
DHCP	Dynamic Host Configuration Protocol (Protocolo de

	configuración dinámica de Host).
AAA	Protocolo de seguridad que representa: Autentificación, Autorización y Auditoria.
ISOC	Internet Society.
RIPng	Routing Information Protocol next generation (Protocolo de Informacion de Enrutamiento de siguiente generación).
OSPFv3	Open Shortest Path First version 3 (El primer camino más corto versión 3).
EIGRPv6	Enhanced Interir Gateway Protocol Routing (Protocolo de Enrutamiento de Gateway Interior Mejorado).
BGP	Border Gateway Protocol.
IGP	Interior Gateway Protocol (Protocolo de pasarela externo).
IS-IS	Intermediate to System Intermediate System.
EGP	Exterior Gateway Protocol.
ODR	On Demand Routing.
LAN	Local Area Network (Red de Área Local).
UDP	User Datagrama Protocol (Protocolo de Datagrama de Sanitario).
NS	Neighbor Solucitation (Solicitud del Vecino).
NA	Neighbot Advetisement (Anuncion de Vecino).
SLAAC	Stateless Address Autodonfiguration (Congifuracion Automatica de Direcciones sin Estado).
DAD	Detención de Dirección Duplicada.
ND	Neighbot Discovery (Descubrimiento del Vecino).
APNIC	Asia Pacific Network Information Centre (Centro de Información de Red de Asia y el Pacifico)
RIP NCC	Resaux IP Europeens Network Cordination Centre (Centro de Coordinación de Redes IP Europeas)
ARIN	American Registry for Internet Numbers (Registro Regional de Internet para America)
AFRINIC	Afican Network Information Centre (Centro de Información de Redes de África)
NIC	Network Information Center (Centro de Información de Redes)
IPsec	Internet Protocol security (Protocolo de internet de seguridad)
QoS	Quality and Service (Calidad de Servicio)
ISP	Internet Service Provider (Provedor de Servicios de Internet)
RIP	Routing Information Protocol (Protocolo de Información de Enrutamiento)
LSA	Link State Advertasiment (Mensaje de Estado de Enlace)
EIGRP	Enhanced Interior Gateway Routing Protocolo (Protocolo de Enrutamiento de Gateway Interior Mejordo)
IGRP	Interior Gateway Routing Protocolo (Protocolo de Enrutamiento de Gateway Interior)
MLD	Multicast Listener Discovery.

Bibliografía.

RFC 791 IPv4
RFC 1516 VLSM
RFC 4632 CIDR
RFC 1631 NAT
RFC 2460 IPV6
RFC 3306 FLAGS
RFC 2080 RIPng
RFC 5340 OSPFv3
RFC 2463 ICMPv6
RFC 2462 SLAAC
RFC 2461 ND
RFC 3315 DHCPv6
RFC 2893Transition Mechanisms for IPv6 Hosts and Routers
RFC 2373 IP Version 6 Addressing Architecture
RFC 2374 An IPv6 Aggregatable Global Unicast Address Format
IPv6 Basics www.cisco.com/go/ipv6
Tutorial de IPv6 Ing. Azael Fernández Alcántara
IPv6 Essentials Silvia Hagen
LACNIC www.lacnic.net/
IPv6 Static Routing Cisco Networking Academy
Coexist IPv6 Ipv5 Cisco Networking Academy