UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

CENTRO UNIVERSITARIO UAEM ECATEPEC

INTRODUCCIÓN Y CONFIGURACIÓN DEL PROTOCOLO IPV6

TESIS

PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

PRESENTA:

DAVID TORRES SÁNCHEZ

ASESORA:

M. EN I.S.C. ALEJANDRA MORALES RAMÍREZ

REVISORES:

M. EN I.S.C. CUAUHTÉMOC HIDALGO CORTÉS

ING. MARCOS HERNÁNDEZ FRAGOSO

ECATEPEC DE MORELOS, ESTADO DE MÉXICO, JUNIO DEL 2017

CARTA DE CESIÓN DE DERECHOS DE AUTOR

El (la) que suscribe ***DAVID TORRES SANCHEZ*** Autor del trabajo escrito de evaluación profesional en la opción de **TESIS** con el título **"INTRODUCCION Y CONFIGURACION DEL PROTOCOLO IPV6"** por medio de la presente con fundamento en lo dispuesto en los artículos 5, 18, 24, 25, 27, 30, 32 y 148 de la Ley Federal de Derechos de Autor, así como los artículos 35 y 36 fracción II de la Ley de la Universidad Autónoma del Estado de México; manifiesto mi autoría y originalidad de la obra mencionada que se presentó en el Centro Universitario UAEM Ecatepec para ser evaluada con el fin de obtener el Título Profesional de **INGENIERIA EN COMPUTACION**

Así mismo expreso mi conformidad de ceder los derechos de reproducción, difusión y circulación de esta obra, en forma NO EXCLUSIVA, a la Universidad Autónoma del Estado de México; se podrá realizar a nivel nacional e internacional, de manera parcial o total a través de cualquier medio de información que sea susceptible para ello, en una o varias ocasiones, así como en cualquier soporte documental, todo ello siempre y cuando sus fines sean académicos, humanísticos, tecnológicos, históricos, artísticos, sociales, científicos u otra manifestación de la cultura.

Entendiendo que dicha cesión no genera obligación alguna para la Universidad Autónoma del Estado de México y que podrá o no ejercer los derechos cedidos.

Por lo que el autor da su consentimiento para la publicación de su trabajo escrito de evaluación profesional.

a) Texto completo ■
b) Por capítulo ☐
c) Solamente portada y tabla de contenido ☐

Se firma presente en la ciudad de Ecatepec de Morelos, Estado de México, a los 16 días del mes de Mayo de 2017.

DAVID TORRES SANCHEZ

UAEM | Universidad Autónoma del Estado de México

Ecatepec de Morelos, Edo. De Méx., a 5 de Abril de 2017
ASUNTO: VOTO APROBATORIO DE ASESOR

LIA. ADRIANA MORALES LICONA
***JEFA DEL DEPARTAMENTO DE TITULACION* DEL**
CENTRO UNIVERSITARIO U.A.E.M ECATEPEC
P R E S E N T E

Por éste conducto me permito informarle que el (la) pasante **C. DAVID TORRES SANCHEZ** con el número de cuenta **1028667**, de la **INGENIERIA EN COMPUTACION**, ha concluido el desàrrollo de su **TESIS**, con el título:

"INTRODUCCION Y CONFIGURACION DEL PROTOCOLO IPV6"

Manifiesto que el borrador del trabajo escrito reúne las características necesarias para ser revisado por la Comisión especial nombrada para tal efecto.

M. EN I.S.C. ALEJANDRA MORALES RAMIREZ
NO. DE CÉDULA PROFESIONAL: 5782891

PATRIA, CIENCIA Y TRABAJO
"2017, Año del Centenario de la Promulgación de la Constitución Política de los Estados Unidos Mexicanos"

Av. José Revueltas no. 17 Col. Tierra Blanca, C.P. 55020, Ecatepec, Estado de México.
Tels: 5.7.87.36.26 Fax: 5.7.87.35.10

UAEM | Universidad Autónoma del Estado de México

Ecatepec de Morelos, Edo. De Méx., 16 de Mayo de 2017
ASUNTO: VOTO APROBATORIO DE REVISORES

LIA. ADRIANA MORALES LICONA
JEFA DEL DEPARTAMENTO DE TITULACION DEL
CENTRO UNIVERSITARIO UAEM ECATEPEC
P R E S E N T E

Nos es grato comunicarle que el trabajo de **TESIS** titulado:

"INTRODUCCION Y CONFIGURACION DEL PROTOCOLO IPV6"

Que para obtener el título de: ***INGENIERIA EN COMPUTACION***

Presenta la pasante: ***DAVID TORRES SANCHEZ***

Con números de cuenta: **1028667**

Cumplen con los requisitos teóricos-metodológicos suficientes para ser aprobada, pudiendo continuar con los trámites correspondientes para su impresión.

REVISORES

M. en I.S.C. CUAUHTEMOC HIDALGO CORTES
CÉDULA PROFESIONAL: 4797107

ING. MARCOS HERNANDEZ FRAGOSO
CÉDULA PROFESIONAL: 7232030

PATRIA, CIENCIA Y TRABAJO
"2017, Año del Centenario de la Promulgación de la Constitución Política de los Estados Unidos Mexicanos"

www.uaemex.mx

Av. José Revueltas no. 17 Col. Tierra Blanca, C.P. 55020, Ecatepec, Estado de México.
Tels: 5.7.87.36.26 Fax: 5.7.87.35.10

UAEM | Universidad Autónoma del Estado de México

Ecatepec de Morelos, Edo. De México., a 16 de Mayo de 2017

ASUNTO: IMPRESIÓN DE TRABAJO ESCRITO

C. DAVID TORRES SANCHEZ
PASANTE DE LA INGENIERIA EN COMPUTACION
P R E S E N T E

Por este medio le comunico a usted que al haber cubierto los trámites correspondientes al desarrollo del trabajo escrito bajo la modalidad **TESIS** con el fin de obtener el Título Profesional, se le aprueba la **IMPRESIÓN DE SU TRABAJO** con el título:

"INTRODUCCION Y CONFIGURACION DEL PROTOCOLO IPV6"

Con el objetivo de establecer la fecha de Evaluación Profesional, le recuerdo que la presentación final del trabajo escrito es de su completa responsabilidad.

Sin más por el momento, reciba un cordial saludo.

PATRIA, CIENCIA Y TRABAJO
"2017, Año del Centenario de la Promulgación de la Constitución Política de los Estados Unidos Mexicanos"

LIA. ADRIANA MORALES LICONA
JEFA DEL DEPARTAMENTO DE TITULACIÓN
DEL CENTRO UNIVERSITARIO UAEM ECATEPEC

CENTRO UNIVERSITARIO U.A.E.M
ECATEPEC
TITULACION

www.uaemex.mx

Av. José Revueltas no. 17 Col. Tierra Blanca, C.P. 55020, Ecatepec, Estado de México.
Tels: 5.7.87.36.26 Fax: 5.7.87.35.10

Dedicatorias:

A mis padres Lourdes Sánchez Mosqueda y David Torres Garnica, por creer siempre en mí, brindándome su apoyo incondicional, sus palabras de aliento, su amistad y su amor. Impulsándome a seguir siempre adelante en los momentos más difíciles de mi carrera profesional y de mi vida.

A mis hermanas, por inspirarme con su tenacidad y muestra de superación académica y laboral día con día.

A mis sobrinos, para ser un buen ejemplo para ellos, de tal manera que puedan creer en sí mismos y así alcanzar sus metas personales y académicas. Impulsándolos así a ser mejores personas para el mundo.

Agradecimientos

A mi institución:

La Universidad Autónoma del Estado de México, por brindarme la oportunidad de formarme como profesional e impulsarme a crecer académicamente. Y especialmente agradezco al Centro Universitario UAEM Ecatepec por proporcionarme las herramientas necesarias para adquirir el conocimiento necesario y así inspirarme a ser un buen estudiante autómata siempre con apetencia de nuevos aprendizajes.

A mis maestros:

Quienes para mí son uno de los principales pilares y fuente de inspiración para la formación de nuevas y mejores personas-estudiantes en la sociedad. Agradeciéndoles mucho por haberme guiado todos estos años en la carrera profesional y por ser parte de mi formación académica-personal. En especial, a mi asesora de tesis la M. en I.SC. Alejandra Morales Ramírez, quien con su experiencia, conocimiento y motivación me auxilió para la conclusión de los estudios superiores, siendo así para mí un ejemplo a seguir.

Índice

Índice de figuras

Índice de tablas

1. Introducción

Sin lugar a duda, las redes de computadoras han sido uno de los grandes acontecimientos dentro del ámbito de las telecomunicaciones. Su crecimiento exponencial desde la década de 1960 representa su gran éxito y aprobación por las personas y, aunque dicha área no sea tan antigua como la automotriz o la aeronáutica, ha progresado espectacularmente en poco tiempo.

Además, como resultado de su desarrollo, ha ayudado al surgimiento de nuevas formas de comunicación. Por ejemplo, gracias a las redes de computadoras se creó la gran y bien conocida internet, de tal manera que ahora pueden realizarse operaciones (hoy en día comunes) como los envíos de correos electrónicos, videoconferencias, VoIP, conversaciones y transacciones en línea, etc. Asimismo, simplifica numerosas tareas que optimizan el trabajo del ser humano.

Actualmente, es fundamental la coexistencia de las redes en las telecomunicaciones, puesto que sería una gran catástrofe si dejasen de funcionar, ya que como ha de suponerse es uno de los pilares que mantiene la comunicación a nivel mundial en la actualidad.

No obstante, es importante resaltar que uno de los factores más esenciales para el funcionamiento de las redes y por ende el éxito de las comunicaciones es el Protocolo de Internet (IP), específicamente en su cuarta versión o mejor conocido como IPv4. Además, a partir de su creación e implementación desde la década de 1970, se convirtió en uno de los protocolos más utilizados mundialmente.

Sin embargo, tras no haber previsto la alta demanda de su uso a escala internacional y el extenso crecimiento de los dispositivos que requieren una conexión a internet, las direcciones disponibles de IPv4 en la actualidad son prácticamente nulas (inicialmente se contaban con 4, 294, 967, 296 direcciones), y a pesar de contar con herramientas que han ofrecido alternativas distintas para reducir el consumo de estos identificadores (por ejemplo el protocolo NAT, renumeración y reasignación de espacio, etc.), es inevitable su terminación. No obstante, el Grupo de Trabajo en Ingeniería de Internet (IETF) desarrolló un nuevo protocolo que resuelve el gran problema a las escasas direcciones. Se trata del Protocolo de Internet versión 6 (IPv6).

A diferencia de la cuarta versión, IPv6 cuenta con 128 bits para su direccionamiento, proporcionando así 4 veces más la cantidad de identificadores que aportaba IPv4. Es decir, el número de direcciones es tan alto (3.4028237e+38 sextillones) que puede generarse un stock virtual ilimitado de direccionamiento suficiente para asignar identificadores a todas las personas del planeta.

Por otra parte, aunque las operaciones para el remplazo de IPv4 se han llevado lentamente, es evidente que el nuevo protocolo IPv6 será implementado a nivel mundial. Por ejemplo, Europa, Japón, Asia pacífica, México, Argentina y Brasil son solo algunos de los países que han efectuado el nuevo protocolo e incluso hay otros que ya han agotado sus direcciones asignadas IPv4. Por lo que es indudable y necesaria la ejecución de IPv6.

En este sentido, es necesario que los ingenieros especializados en administración de redes y/o desarrolladores de aplicaciones estén actualizados para contar con una capacitación necesaria y así ofrecer nuevas oportunidades de comunicación y optimización en el ámbito de las telecomunicaciones que integren IPv6. Del mismo modo, los aspirantes que ejerzan cualquier estudio o desarrollo que abarque las redes de computadoras (y comúnmente al Protocolo de Internet) deberán estar al día y así ampliar su conocimiento y habilidades.

Cabe señalar, que dicho aprendizaje para IPv6 puede iniciarse en muchas áreas que ofrezcan algún acceso a la información. Por ejemplo, las instituciones académicas son consideradas como una de las etapas clave para la iniciación del desarrollo de los futuros ingenieros e investigadores que deseen especializarse en el presente ámbito. Por tal motivo, es importante que el espacio académico proporcione la información requerida para cubrir los aspectos actuales (en este caso del Protocolo de Internet) y así notificar al estudiante de su funcionamiento actual.

Señalando particularmente al CU UAEM Ecatepec, cuenta con instalaciones y una gran variedad de herramientas capacitadas para impulsar la enseñanza-aprendizaje de los estudiantes y profesores respecto al área de las redes de computadoras. Sin embargo, se ha observado el escaso o incluso nulo manejo del protocolo IPv6. De hecho, en los programas de sus unidades de aprendizaje impartidas a las licenciaturas de informática administrativa e ingeniería en computación, como son: modelos de red, comunicación de computadoras 1 y 2, protocolos de red, etcétera su instrucción es mínima.

Es posible que una causa de ello sea la creencia de que el tema es demasiado complejo o apresurado para estudiarlo. No obstante, es conveniente que los alumnos continúen desarrollando sus habilidades, debido a que una de las situaciones más comunes que enfrenta un ingeniero en computación y/o un licenciado en informática administrativa es el desenvolverse en un entorno donde la tecnología se encuentra en un avance constante.

Por tal motivo, en la presente investigación se desarrolló una herramienta tanto de exploración teórica como práctica de la sexta versión del Protocolo de Internet, la cual tiene como finalidad el proporcionar el siguiente contenido: conceptos básicos IPv6; requerimientos de hardware y software; establecimiento de nuevas funciones de capa 3 del modelo OSI y principalmente la implementación y configuración de los protocolos de enrutamiento de nueva generación (RIPng, EIGRPv6 y OSPFv3) que podrán desarrollarse con el equipo físico que posee el laboratorio de redes de la institución académica.

2. Protocolo de Internet (IP) (RFC 791)

Se trata de un protocolo de comunicación de datos digitales clasificado funcionalmente en la capa de red, según el modelo de Interconexión de Sistemas Abiertos (OSI).

Su función es proporcionar un servicio de distribución de paquetes de información orientado a la no conexión de manera no fiable. El término "orientado a la no conexión" hace referencia a que los paquetes de información que serán enviados hacia la red pueden viajar por rutas independientes para llegar a su destino. El concepto “no fiable” significa que la entrega de los paquetes de datos no está garantizado, por tal motivo, el protocolo realiza técnicas de encaminamiento para buscar la mejor ruta entre las conocidas por el emisor que esté usando dicho protocolo (pero aún sin garantizar una entrega).

IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino, únicamente proporciona seguridad de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, tal como el Protocolo de Control de Transmisión (TCP).

Las cabeceras IP contienen las direcciones de las máquinas de origen y destino (direcciones IP), y también, las direcciones que serán usadas por los enrutadores (routers) para decidir el tramo de red por el que reenviarán los paquetes.

2.1 Versiones del Protocolo de Internet

El protocolo IP es el elemento común en el Internet de hoy. Sin embargo, con el paso del tiempo ha sufrido numerosos cambios de acuerdo a las funciones que ha ido adaptando para su optimización en las redes, por lo cual se ha visto obligado a crear distintas versiones de sí mismo.

Lo que es notable acerca del desarrollo de IP es que sus funciones eran originalmente parte del protocolo TCP. IP “nació” como un protocolo formal cuando una primera versión de TCP se desarrolló en la década de 1970; para los predecesores de la moderna Internet, TCP se dividió en la capa cuatro (capa de transporte) e IP en la capa tres (capa de red) del modelo OSI. Dicho protocolo se definió en el RFC 791 en el año 1981 y fue la versión ampliamente utilizada. Sin embargo, no es la primera versión de IP pero sí la numero cuatro. Esto, por supuesto supone la existencia de versiones anteriores del protocolo en un punto, aunque en realidad no es así, ya que como se ha mencionado anteriormente, el protocolo IP se creó cuando sus funciones se dividieron hacia una primera versión del protocolo TCP que combina ambas funciones TCP e IP.

TCP se desarrolló a través de tres versiones anteriores y se dividió en TCP e IP para llegar a la versión 4. Finalmente, ese número de versión se aplicó a ambos protocolos para mantener una consistencia. Por lo tanto, cuando se utiliza el Protocolo de Internet hoy en día significa que se utiliza IP versión cuatro (mejor conocido como IPv4). Este número de versión se realiza en el campo apropiado de todos los datagramas IP. (Kozierok, 2005).

En la actualidad, IPv4 es el más conocido protocolo de red y fue la primera versión en ser implementada a gran escala por su gran éxito. No obstante, debido a diversos problemas actuales causados por las escasas direcciones ante su demanda a nivel mundial, se ha creado una nueva versión del Protocolo de Internet que da solución a todos los problemas de IPv4. Se trata del protocolo IPv6.

IPv6 se ha desarrollado con el objetivo de resolver las dificultades existentes, además de optimizar y mejorar la comunicación entre los dispositivos a través de Internet. Esta nueva versión de IP también se denomina IP de próxima generación o IPng (IP next generation).

Una pregunta natural en este punto es ¿qué sucedió con la versión cinco de IP?, la respuesta es: no existe. De hecho, la versión cinco fue intencionalmente omitida para evitar confusiones. El problema con dicha versión es que se refiere a un protocolo experimental TCP/IP (originalmente definido en el RFC 1190). Esta versión en el encabezado identificaba paquetes que llevaban un protocolo experimental no IP de tiempo real llamado ST (Protocolo de Secuencia de Internet). En la década de 1970 el protocolo experimental ST fue creado con propósitos para transmitir voz y video. Dos décadas después, este fue sometido a revisión y se convirtió en ST2 y comenzó a implementarse en proyectos comerciales por grupos como IBM, Apple y Sun. Este nuevo protocolo garantizaba Calidad de Servicio (QoS), a diferencia de su contraparte IPv4. ST y ST2 fueron asignados con la versión cinco y, debido a que nunca fue extensamente utilizado, la nueva versión del protocolo IP tuvo que quedarse con el identificador 6 (RFC 1819). (Castro, 2009)

Dado que uno de los problemas principales que enfrenta el Protocolo de Internet son las direcciones disponibles, se realizaron las operaciones necesarias para que en la nueva versión del protocolo IP no encuentre algún inconveniente en lo que puede ser un futuro no muy lejano.

2.2 Protocolo de Internet versión 6 (IPv6)

IPv6 ofrece a todos los usuarios una gran cantidad de múltiples direcciones de distintos ámbitos que pueden ser usadas por una amplia variedad de dispositivos conocidos en la actualidad, sin mencionar las funciones que las nuevas tecnologías podrán ofrecer a causa del aumento del número de bits de dirección en el nuevo Protocolo de Internet.

En comparación con la cuarta versión en el que se usaban 32 bits de direccionamiento, IPv6 utiliza 128 bits, lo que es equivalente a 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456 direcciones (3.4028237e+38 sextillones), sin embargo, como en cualquier esquema de direccionamiento, no todas las direcciones estarán disponibles o podrán ser utilizadas.

2.2.1 Representación de las direcciones IPv6

La representación de las direcciones IPv6 se muestra en el siguiente esquema:

x : x : x : x : x : x : x : x

Imagen 2.1 “Representación de una dirección IPv6”

Como se observa en la imagen 2.1, su estructura consiste en ocho bloques, cada uno con un valor “x” que representa un valor en formato hexadecimal de 16 bits de la porción correspondiente a la dirección IPv6. Los valores se representan en dicho formato a causa del aumento de bits de dirección en el protocolo, de esa manera los valores de la dirección son más prácticos y de un mejor manejo.

Para transformar una dirección binaria de IPv6 a formato hexadecimal se deben realizar los siguientes pasos:

- Subdividir cada bloque a cuatro bits (imagen 2.2)
- Sumar los valores binarios de cada subdivisión y sustituir dicho valor de acuerdo con los valores hexadecimales de la imagen 2.3 (ejemplo de sustitución en la imagen 2.4).
- Al reacomodar los bloques en el formato hexadecimal, se deben separar mediante “:” cada cuatro valores hexadecimales (imagen 2.5)

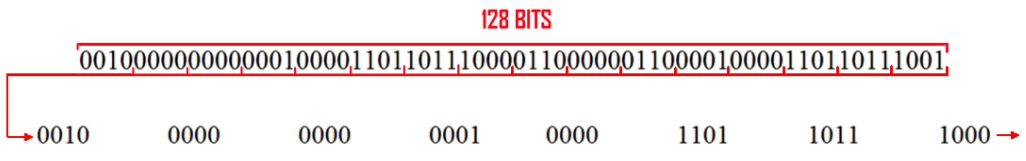


Imagen 2.2 “Bits subdivididos”

BINARIO	HEXADECIMAL	DECIMAL
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	A	10
1011	B	11
1100	C	12
1101	D	13
1110	E	14
1111	F	15

Imagen 2.3 “Valores binarios sustituidos”

Imagen 2.4 “Valores binarios sustituidos”

Imagen 2.5 “Representación final de una dirección IPv6”

Una dirección IPv6 consta de dos partes:

1.- Prefijo de subred: Es la representación de la red a la que está conectada una interfaz. Al igual que en IPv4, un prefijo de subred está asociado con un enlace.

Asimismo, se conforma de dos segmentos:

- Prefijo global
- Identificador de subred

2.- Identificador de interfaz: Su función es reconocer a los nodos como únicos dentro de una red a través de una interfaz, que a su vez es asignada a un enlace.

El identificador de interfaz normalmente es de 64 bits y puede ser creado mediante diversos métodos dinámicos o manualmente (explicados posteriormente).

64 bits	64 bits
Prefijo de subred	Identificador de Interfaz

Imagen 2.6 "Estructura básica de una dirección IPv6"

2.2.2 Simplificación de las direcciones IP versión 6

En la mayoría de los casos, las direcciones IPv6 suelen contener valores hexadecimales y/o un conjunto de bloques continuos "en blanco" que extienden considerablemente su longitud. De tal forma que algunas operaciones como su lectura y escritura llegan a ser complicadas para los operadores de redes que suelen manejar múltiples nodos. No obstante, para hacer frente a tal dificultad se cuentan con las siguientes características que facilitan y optimizan el manejo de los identificadores IPv6:

- Representación de ceros continuos
- Omitir ceros a la izquierda
- Indiferencia entre caracteres en mayúscula o minúscula

Además, existen procesos de simplificación (con base a los puntos anteriores) que especifican el uso correcto para cada operación implementada.

Los métodos son los siguientes:

2.2.2.1 Simplificación de ceros al inicio de los bloques

Conlleva a suprimir los ceros que existan al inicio (lado izquierdo) de cada bloque de la dirección IPv6. De esa manera, se reduce considerablemente el identificador. Sin embargo, si dicho bloque contiene solo ceros al menos uno debe ser mantenido (imagen 2.7).

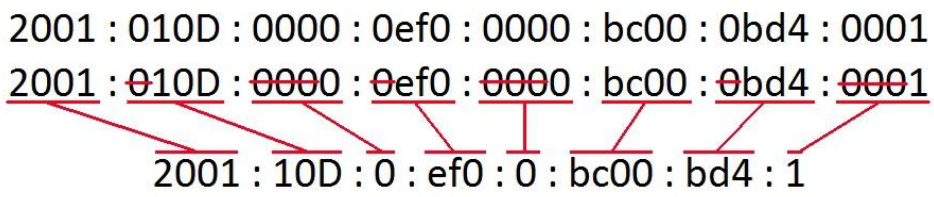


Imagen 2.7 "Ceros a la izquierda eliminados"

2.2.2.2 Simplificación de ceros continuos

Cuando existen bloques continuos únicamente con valores de ceros estos pueden representarse con "::". Estos pueden simplificarse sin importar cuántos bloques sucesivos se encuentren (imagen 2.8).

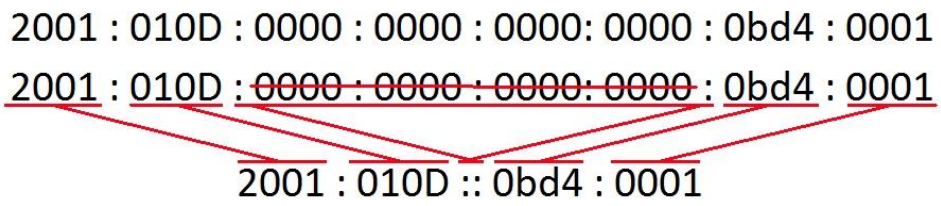


Imagen 2.8 "Ceros continuos eliminados"

No obstante, dicha simplificación solo puede realizarse una sola vez, ya que de lo contrario se generaría una ambigüedad y por lo tanto un error.

Sucede de esa manera ya que al modificar la IP más de una vez con el presente método no podrá conocerse cuantos bloques de la dirección se han simplificado al extender dicha dirección en distintas operaciones (hardware, operadores, prácticas, etc.) (imagen 2.9).

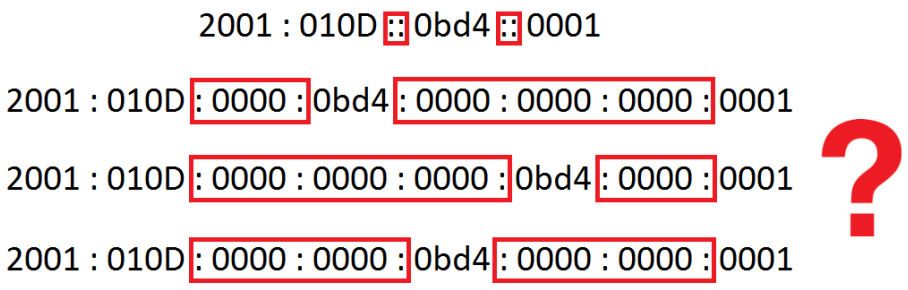


Imagen 2.9 "Error por ambigüedad"

2.2.2.3 Aplicación de ambos métodos

Ante la existencia de algunas limitaciones en cuanto a cada tipo de simplificación también es válido aplicar los dos métodos anteriores a una dirección IPv6, de tal forma que el identificador quedará en una representación definitiva pero más sencilla de leer y escribir.

En su mayoría, espacios laborales y de investigación como empresas, industrias, laboratorios de desarrollo, prácticas académicas, etc. manejan las direcciones en esta forma final (imagen 2.10).

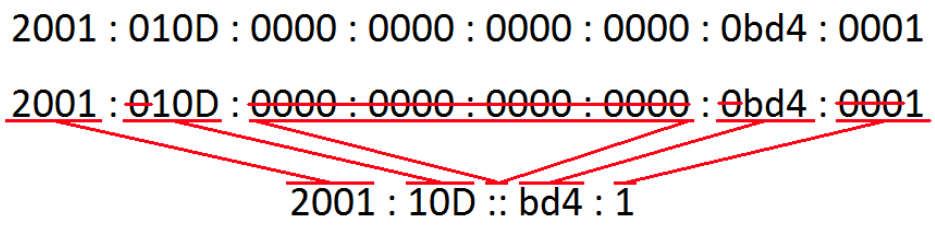


Imagen 2.10 “Dirección IPv6 simplificada en forma definitiva”

2.2.3 Tipos de direcciones IPv6 (RFC 3513 y RFC 4291)

En IPv6 se definieron distintos tipos de direcciones dependiendo del alcance de comunicación y de las necesidades de una red. Dichas direcciones son clasificadas en 3 clases:

- Unicast
- Anycast
- Multicast

Es de suma importancia conocer que las direcciones IPv6 indistintamente de su tipo son asignadas a interfaces y no a nodos. Asimismo, una única interfaz también puede tener varias direcciones IPv6 de cualquier tipo o ámbito (unicast, anycast o multicast).

En el caso de los identificadores de interfaz, deben ser únicos en un enlace ya que su función (como su nombre lo menciona) es identificar interfaces en dicho enlace. Asimismo, están obligados a ser únicos dentro de un prefijo de subred y pueden ser utilizados en múltiples interfaces en un solo nodo, siempre y cuando estén unidos a diferentes subredes.

Es indispensable tener en cuenta que la singularidad de los identificadores de interfaz es independiente de la singularidad de las direcciones IPv6. Por ejemplo, una dirección unicast global puede ser creada con un identificador de interfaz de alcance no global y una dirección local de sitio puede crearse con un identificador de interfaz de alcance global.

Nota: La independencia del alcance de una dirección IPv6 respecto a su identificador de interfaz es posible por el bit universal/local (U/L) que pertenece a la norma EUI-64 (explicado en el tema 3.1, página 85).

2.2.3.1 Unicast

Los nodos IPv6 pueden tener un mínimo o ningún conocimiento de la estructura interna de las direcciones IPv6, esto dependiendo de su misión en la red (por ejemplo, un host frente a un router). Pero como mínimo, un nodo debe considerar que las direcciones unicast no tienen estructura alguna (imagen 2.11).

128 bits
Dirección del nodo

Imagen 2.11 “Dirección unicast sin estructura”

Sin embargo, un host ligeramente sofisticado (pero aún bastante simple), puede ser consciente del prefijo de subred (es) para el enlace (s) al que está conectado, donde las diferentes direcciones pueden tener distintos valores de n:

n	n - 128 bits
Prefijo de subred	Identificador de interfaz

Imagen 2.12 “Estructura de una dirección de host”

Las direcciones unicast son identificadores para una única interfaz donde un paquete enviado a dicha dirección es entregado sólo a la interfaz identificada con tal dirección. Son el equivalente a las direcciones IPv4 actuales (imagen 2.13).

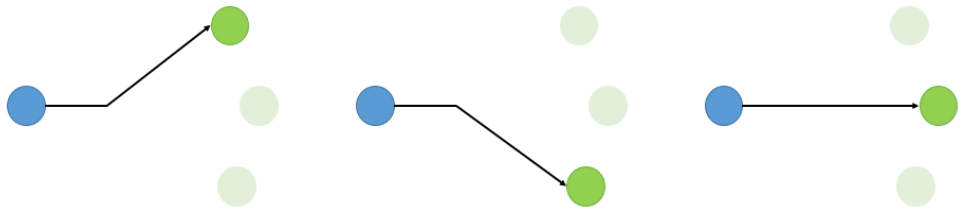


Imagen 2.13 “Representación general de transmisión de una dirección unicast”

De acuerdo a las funciones que la dirección unicast debe desempeñar, se definieron las siguientes “subclases” de direcciones unicast, para uso local y para uso global:

- Uso local:
  - Unicast de enlace local (Link-local)
  - Unicast local única (Unique-local)
  - Unicast de sitio local (Site-local)

- Uso global:
  - Unicast global agregable (mejor conocida solo como “unicast global”)

2.2.3.1.1 Unicast de enlace local (Link-local)

Las direcciones de enlace local han sido diseñadas para que los nodos puedan direccionarse en un único enlace. Además se utiliza para propósitos de autoconfiguración (mediante los identificadores de interfaz), descubrimiento de vecinos o situaciones en las que no hay routers (temas explicados posteriormente).

Son usadas por muchos protocolos de enrutamiento y pueden servir para conectar dispositivos en la misma red local. Sin embargo, no pueden usarse como direcciones globales, por lo tanto, los enrutadores no pueden retransmitir ningún paquete con direcciones fuente o destino fuera de su enlace local, es decir hacia a otros enlaces. Su alcance está limitado a la red local.

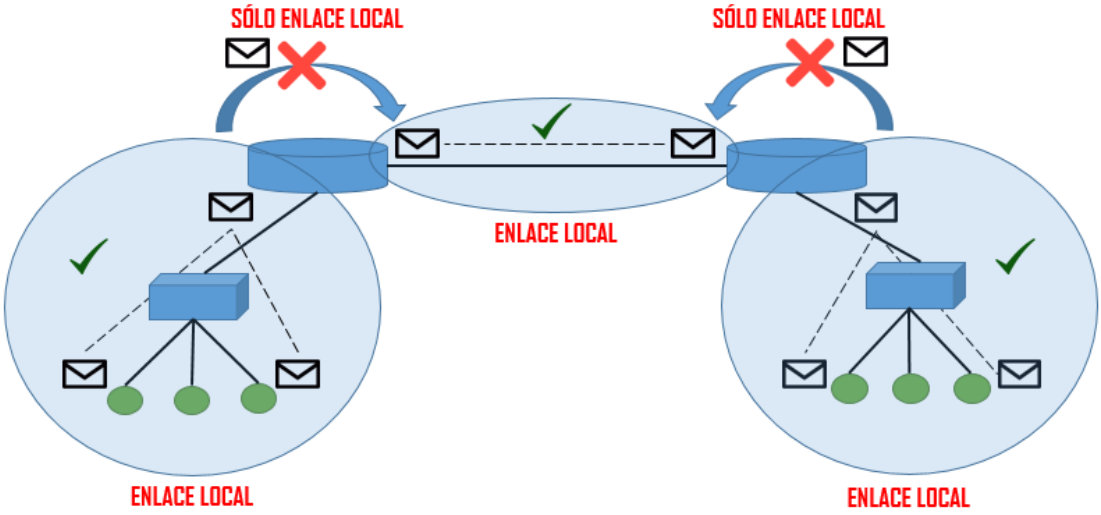


Imagen 2.14 “Límite de una dirección unicast de enlace local”

La estructura de una dirección unicast de enlace local es la siguiente:

10 bits	54 bits	64 bits
1111111010	0	Identificador de interfaz

Imagen 2.15 “Estructura de dirección de enlace local”

Son direcciones IPv6 que se identifican por el prefijo FE80::/10 donde el término /10 indica que los primeros 10 bits utilizados por la dirección son 1111 1110 10XX XXXX y el rango de direcciones es de FE80 a FEBF (imagen 2.16).

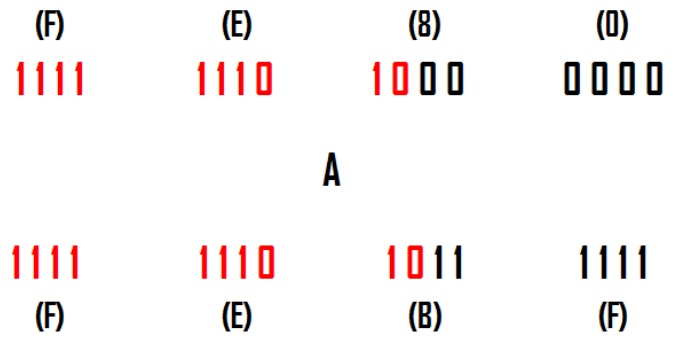


Imagen 2.16 “Limite de direcciones de enlace local”

Posteriormente, los bits del 11 hasta el 64 (es decir, los siguientes 54 bits) se configuran con valores de ceros (0000). De esa manera se forma la porción de red representada por los primeros 64 bits.

Nota: Toda dirección IPv6 que comience con los valores “FE80” es una dirección unicast de enlace local.

Cuando se comunica hacia una dirección de enlace local se especifica la interfaz de salida y por lo tanto dicha interfaz es conectada o asociada al prefijo FE80::/10.

Todas las interfaces requieren tener al menos una dirección unicast de tipo enlace local.

2.2.3.1.2 Unicast local única (Unique Local Address o ULA) (RFC 4193)

Se tratan de direcciones en un formato unicast IPv6 que son globalmente únicas pero están pensadas para comunicaciones locales. No se espera que sean enrutables en la internet global a pesar de ser irrepetibles, pero sí dentro de un área más limitada como un sitio y también pueden enrutarse entre un conjunto limitado de sitios (imagen 2.17).

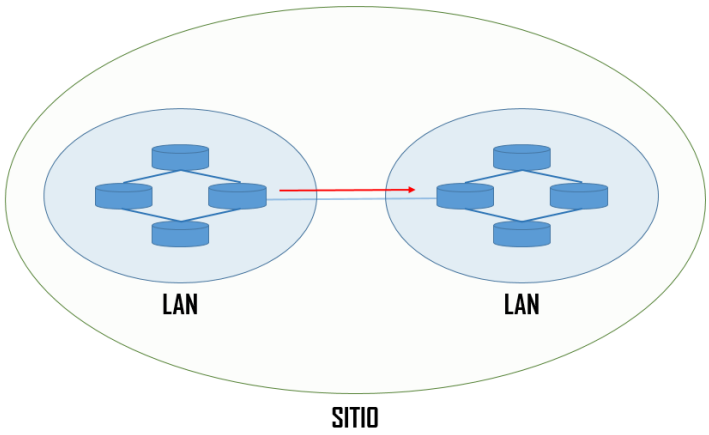


Imagen 2.17 “Limite de dirección unicast única”

Las direcciones locales únicas tienen las siguientes características:

- Prefijo global único (con alta probabilidad de originalidad).
- Prefijo conocido para permitir que sean más fáciles de filtrar en los límites del sitio.
- Permitir a los sitios combinarse o interconectarse privadamente sin crear conflictos de direcciones.
- Si accidentalmente se filtra una dirección unicast única fuera de un sitio web a través de enrutamiento o de DNS, no hay ningún conflicto con cualquier otra dirección.
- En la práctica, las aplicaciones pueden tratar estas direcciones como direcciones de alcance global.

Unicast local única sigue el siguiente formato:

7 bits	**1**	**40 bits**	**16 bits**	**64 bits**
Prefijo	L	ID global	ID subred	ID interfaz

Imagen 2.18 “Formato de dirección unicast local única”

Donde:

Tabla 2.1 “Valores de la estructura de una dirección unicast única”

Prefijo	Formado por los valores **FC00::/7** (límite hasta a FDFF::/7)
Bit L	El prefijo es local si el bit es puesto a 1
	El bit puesto a 0 podría ser definido en un futuro
ID global	Identificador global de 40 bits usado para crear un prefijo único globalmente
ID subred	Conformado por 16 bits. Es un identificador de subred dentro de un sitio
ID interfaz	Conformado de 64 bits

Dichas direcciones son creadas usando un ID global asignado de forma local (bit L=1) generado por el algoritmo aleatorio SHA-1 (Secure Hash Algorithm 1, RFC 3174).

Dichos identificadores no deben ser asignados de forma secuencial o con números conocidos. Esto es para asegurar que no exista ninguna relación entre las asignaciones dadas y para ayudar a aclarar que los prefijos de las presentes direcciones no están destinados a ser encaminados mundialmente (esto es debido a que los prefijos son concatenados con el identificador global). De hecho, estos prefijos no están diseñados para agregarse como en las direcciones unicast agregables.

Nota: Los identificadores globales asignados localmente deben ser generados por un algoritmo aleatorio consistente con los Requisitos de la Aleatoriedad para la Seguridad (RANDOM).

Nota: Es importante que todos los sitios generen un identificador global usando un algoritmo similar para tener una alta probabilidad de unicidad. Las direcciones unicast locales únicas utilizan SHA-1 por defecto.

Las asignaciones locales son autogeneradas y no necesitan ningún tipo de coordinación o asignación central. Además, poseen una muy alta probabilidad de ser únicas.

2.2.3.1.3 Unicast de sitio local (RFC 3515 y RFC 3879)

Las direcciones unicast de sitio local tienen el prefijo FEC0/10. Es decir, los primeros 10 bits son 1111 1110 11XX XXXX. Dichas direcciones pueden ser encaminadas fuera del segmento local, por ejemplo una organización o una pequeña empresa. Sin embargo, no pueden ser transmitidas hacia internet. Por tal motivo, la IETF ha declarado que estas direcciones contienen varios defectos en el direccionamiento. Dichos defectos se dividen en dos categorías:

- Ambigüedad de las direcciones
- Definición indeterminada de sitios.

En otras palabras, una dirección de sitio local puede estar presente en varios sitios y la dirección en sí no contiene ninguna indicación del lugar al que pertenece. Esto crea un dolor de cabeza para los desarrolladores de aplicaciones, para los diseñadores de routers y para los administradores de red. Este dolor se agrava por el indefinido concepto de "sitio".

Los primeros comentarios de los desarrolladores indican que las direcciones de sitios locales son difíciles de usar correctamente en una aplicación. Esto es particularmente cierto para múltiples hosts alojados que pueden estar conectados simultáneamente a múltiples sitios, y el mismo caso es para los hosts móviles. Por ejemplo, las aplicaciones podrían aprender o recordar que la dirección de algún host era "FEC0 :: 1234: 5678: 9ABC", y tratarían de agregarla en una estructura de dirección de socket y emitir una conexión. La llamada producirá un error porque no llenan la variable "identificador de sitio", como en "FEC0 :: 1234: 5678: 9ABC % 1" (se especifica el uso del carácter % como un delimitador de los identificadores de su zona en alcance). El problema se agrava por el hecho de que el identificador de sitio varía con el alojamiento del huésped (host), por ejemplo, a veces %1 y a veces %2, y por lo tanto el identificador de host no puede ser recordado en la memoria, o aprendido de un servidor de nombres.

Nota: El delimitador de zona (%) fue citado como ejemplo para generar una idea del problema de las direcciones anteriores. Los detalles acerca de los delimitadores y sus zonas de alcance se describen en el RFC 4007. Sin embargo, el propio RFC ha omitido las direcciones IPv6 de sitio local por la misma razón que describe esta sección.

En resumen, el problema es causado por la ambigüedad de las direcciones locales del sitio. Además, a consecuencias de este problema, los desarrolladores de aplicaciones tienen que gestionar los "identificadores de sitio" que califican las direcciones de los host. Esta gestión ha demostrado ser difícil de entender y de ejecutar hasta por los propios desarrolladores que ya entienden más el concepto.

2.2.3.1.4 Unicast global agregable (RFC2374)

Son direcciones unicast de modo global, es decir, no poseen ninguna restricción de alcance, de modo que se pueden enrutar mundialmente sin ningún inconveniente. Son el equivalente a las direcciones IPv4 públicas.

Este formato de dirección está diseñado para apoyar tanto a la agregación basada en los proveedores del troncal de internet y además, un nuevo tipo de agregación basado en "intercambios". La combinación de ambos permite una agregación de enrutamiento eficaz para los sitios que se conectan directamente a los proveedores y para los sitios que se conectan a los "intercambios". De igual manera, los sitios tendrán la opción de conectarse a cualquier tipo de entidad de agregación.

Dado que uno de los problemas que IPv6 resuelve es la mejor organización jerárquica de ruteo en las redes públicas (globales), es indispensable conocer el concepto de direccionamiento "agregable" en las direcciones unicast globales. (Gutiérrez, 2010)

Las direcciones unicast globales agregables se organizan en una jerarquía de tres niveles:

- **Topología Pública:** Conjunto de proveedores e "intercambiadores" que proporcionan servicios públicos de tránsito de internet.
- **Topología de Sitio:** Redes de organizaciones que no proporcionan servicios públicos de tránsito a nodos fuera de su propio "sitio".
- **Identificador de Interfaz:** Identifican interfaces de enlaces.

Como se muestra en la imagen 2.19, el formato de las direcciones agregables son diseñadas para apoyar a los proveedores de larga distancia (que se muestran como P1, P2, P3 y P4), los intercambiadores (que se muestran como X1 y X2), múltiples niveles de proveedores (probablemente ISP's que se muestran como P5 y P6), y suscriptores (usuarios finales mostradas como S "x").

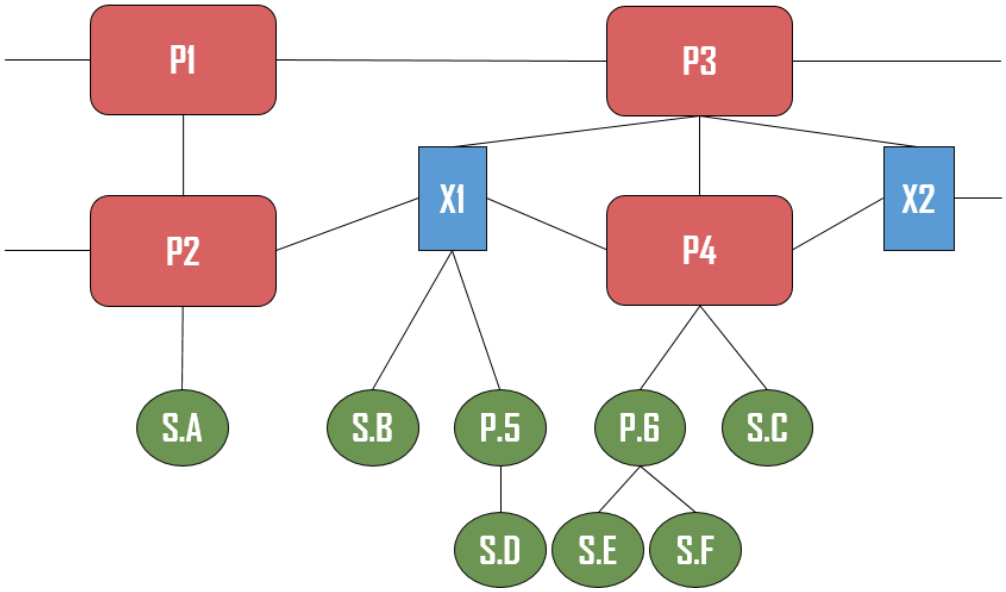


Imagen 2.19 “Multiconexión IPv6”

A diferencia de lo que ocurre actualmente, los intercambiadores también proporcionarán direcciones IPv6 públicas. Las organizaciones conectadas a dichos intercambiadores también recibirán servicios de conectividad, ya sea directamente o indirectamente a través del intercambiador de uno o varios proveedores de larga distancia. De tal forma que su direccionamiento es independiente de los proveedores de tráfico de larga distancia, y pueden, por tanto, cambiar de proveedor sin necesidad de renumerar su organización. Además, cualquier organización podrá estar suscrita a múltiples proveedores (multihoming) a través de un intercambiador sin la necesidad de tener prefijos para cada proveedor de larga distancia.

La estructura de una dirección unicast global agregable es la siguiente:

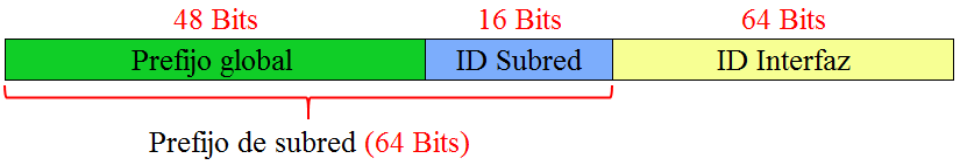


Imagen 2.20 “Estructura dirección global IPv6”

A su vez, cada segmento se compone de múltiples campos (de acuerdo con la jerarquía de tres niveles):

3	13	8	24	16	64 bits
FP	TLA ID	RES	NLA ID	SLA ID	Interfaz ID
Topología Pública				Topología de Sitio	Identificador de Interfáz

Imagen 2.21 “Estructura de una dirección global IPv6”

Donde:

Tabla 2.2 “Campos de una dirección global IPv6”

FP	Prefijo de Formato (Format Prefix)
TLA ID	Identificador de Agregación de Nivel Superior (Top Level Aggregation Identifier)
RES.	Reservado para uso futuro
NLA ID	Identificador de Agregación de Siguiente Nivel (Next Level Aggregation Identifier)
SLA ID	Identificador de Agregación de Nivel de Sitio (Site Level Aggregation Identifier)
Interfaz ID	Identificador de Interfaz

El campo “Reservado” permitirá ampliaciones organizadas del protocolo en un futuro. Por ejemplo, ampliar el número de bits de los campos TLA y NLA. Sin embargo, por el momento contiene solo ceros.

FP: El prefijo de formato se utiliza para especificar la clase de dirección IPv6. Indicado por los bits de liderazgo, es decir, los bits al inicio de la dirección.

Los primeros tres bits de unicast global agregable están compuestos por los valores 001 (notación binaria), por lo tanto, los valores hexadecimales del primer bloque serán 2000 con un prefijo de /3 teniendo como límite de direccionamiento el valor 3FFF (imágenes 2.22 y 2.23).

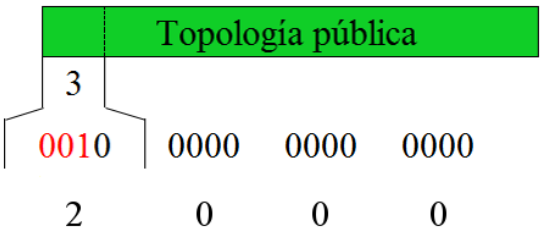


Imagen 2.22 “Prefijo global unicast agregable”

Nota: El rango para las direcciones unicast globales es de 2000 a 3FFF. Este espacio de direcciones actualmente se encuentra bajo la responsabilidad de la Internet Assigned Numbers Authority (IANA).

0010	0000	0000	0000	(2000)
		HASTA		
0011	1111	1111	1111	(3FFF)

Imagen 2.23 “Limite de direcciones global unicast agregables”

Identificador de agregación de nivel superior (TLA ID): Se trata del nivel superior en la jerarquía de enrutamiento.

Este formato de direccionamiento permite 8,192 (2^{13}) identificadores TLA ID.

Predeterminadamente en este nivel, los routers deben tener una entrada en la tabla de enrutamiento para cada “activo” TLA ID y probablemente entradas adicionales para las rutas basadas en los identificadores de agregación de nivel superior asignados a la región de enrutamiento donde están ubicados. Pueden tener otras entradas adicionales con el fin de optimizar el enrutamiento (dependiendo de su topología) pero, dichas topologías de enrutamiento en todos los niveles deben ser diseñadas para minimizar el número de entradas adicionales introducidas y así disminuir el tamaño de las tablas de enrutamiento.

Reservado para uso futuro (RES): Espacio reservado para el crecimiento en un futuro del campo TLA ID o usando esta misma estructura para prefijos de formato (FP) adicionales.

Identificador de agregación de siguiente nivel (NLA ID): Son utilizados por organizaciones a las que se les ha asignado un TLA ID para crear una jerarquía de direccionamiento, con el objetivo de administrar sus direcciones y el ruteo hacia otros ISP’s. También se utiliza para identificar los “sitios” que dependen de la misma organización. Además pueden reservar bits en la parte superior (al inicio) del NLA ID con el objetivo de crear una diferenciación de la estructura de su red, de acuerdo a sus propias necesidades (imagen 2.24).

n	24 - n bits	16 bits	64 bits
NLA1	Site ID	SLA ID	Interfaz ID

Imagen 2.24 “Espacio de direccionamiento para NLA ID”

“Dado que cada organización que recibe un TLA dispone de 24 bits de espacio NLA, permite proporcionar un servicio aproximadamente al número total de las direcciones IPv4 soportadas actualmente”. (Gutiérrez, 2010). Dichas organizaciones pueden contener varios NLA’s en su propio espacio de direccionamiento (nombrado “Site ID” en la imagen 2.24) una vez ya recibido un TLA. Esto permite que sirvan tanto a clientes directos (suscriptores) como a otras organizaciones proveedoras de servicios públicos de tránsito. Y así sucesivamente según el siguiente esquema:

a	24 - a bits			16 bits	64 bits
NLA1	Site ID			SLA ID	Interfaz ID
	b	24 - a - b bits		16 bits	64 bits
	NLA2	Site ID		SLA ID	Interfaz ID
		c	24 - a - b - c bits	16 bits	64 bits
		NLA3	Side ID	SLA ID	Interfaz ID

Imagen 2.25 “Múltiples NLA’s en Site ID”

El diseño de la disposición de bits del espacio NLA ID para un TLA ID específico se deja a la organización de ese TLA. Asimismo, el diseño de la disposición de los bits del siguiente nivel NLA ID (si es que hubiera uno) es responsabilidad del NLA de nivel inferior y así sucesivamente. Sin embargo, se recomienda seguir los procesos específicos descritos en el RFC 2050.

El diseño de un plan de asignación NLA ID es una solución de compromiso entre la eficiencia de agregación de enrutamiento y la flexibilidad. La creación de jerarquías permite una mayor cantidad de agregación y por consecuencia las tablas de enrutamiento son de menor tamaño. Por el contrario, una asignación “plana” de un NLA ID ofrece una mejor flexibilidad en la conexión (crecimientos no previstos en un determinado espacio), sin embargo, las tablas de enrutamiento son de mayor tamaño (menos eficaces).

Identificador de Agregación de Nivel de Sitio (SLA ID): El campo SLA ID es utilizado por organizaciones “finales” para crear su propia jerarquía de direccionamiento local y para identificar sus subredes. Esto es semejante al concepto de subredes en IPv4, excepto que cada organización tiene una mayor cantidad de las mismas.

El SLA ID de 16 bits soporta 65,535 subredes individuales. Del mismo modo que en el caso del NLA, se puede escoger entre una estructura “plana”, o crear varios niveles (imagen 2.26).

n	16 - n bits		64 bits
SLA1	Subred		Interfaz ID
	m	16 - n - m bits	64 bits
	SLA2	Subred	Interfaz ID

Imagen 2.26 “Espacio de direccionamiento SLA ID”

Una organización (individual) es responsable del enfoque elegido para la estructuración de su respectivo campo SLA ID.

Nota: El número de subredes apoyadas en este formato de dirección deben ser suficiente para todas las organizaciones. Sin embargo, si alguna requiere subredes adicionales existe la posibilidad de arreglarlo con la organización de quien se están obteniendo los servicios de internet y así obtener identificadores de sitios adicionales para poder crear las subredes necesarias.

2.2.3.2 Anycast (RFC 2526)

Anycast es una dirección IPv6 que se asigna a una o más interfaces de una red (normalmente pertenecientes a diferentes nodos), con la propiedad de que un paquete enviado a una dirección anycast se dirija a la interfaz (cualquiera) "más cercana", esto de acuerdo con la medida de la distancia de los protocolos de enrutamiento (métricas) y desde el punto de vista de la topología de red.

Estas direcciones son sintácticamente indistinguibles de las unicast globales. Esto es debido a que las direcciones anycast son asignadas del espacio de direccionamiento unicast global (utilizando cualquiera de sus formatos definidos). Por tal motivo, cuando una dirección unicast global es asignada a más de una interfaz, teóricamente se transforma en una dirección anycast. No obstante, los nodos que se les asignó dicha dirección deben ser explícitamente configurados para que reconozcan que se trata de una dirección anycast.

2.2.3.2.1 Dirección anycast requerida

IPv6 definió una dirección anycast que es necesaria para todos los routers dentro de un prefijo de subred que se denomina "dirección anycast del router de la subred" (subnet router anycast address). Esta dirección está diseñada para ser utilizada en aplicaciones donde un nodo necesita comunicarse con alguno del conjunto de los routers, lo que significa que dichos enrutadores deben de soportar esta dirección para las subredes a las que están conectados.

Inicialmente, dentro de cada subred, los valores del identificador de interfaz 128 más altos están reservados para la asignación de las direcciones anycast de subred. Dejando a "cero" a todos los bits del ID de interfaz (imagen 2.27).

n bits	128-n bits
Prefijo de subred	0000000000…

Imagen 2.27 "Dirección anycast requerida inicial"

Los paquetes que contengan la dirección de destino anycast mencionada, serán entregados al router de esa subred, en la cual todos sus routers deberán estar configurados para soportar dicha dirección, y de la misma forma esta será entregada al conjunto de routers que forman parte de esa "subred anycast".

La construcción de una dirección reservada anycast depende del tipo de direcciones IPv6 usadas dentro de la subred. Tal y como se indica por el prefijo de formato en cada una de ellas. Por ejemplo, las direcciones IPv6 que tienen prefijos entre 001 y 111 con excepción de las direcciones multicast (1111 1111) normalmente requieren de un ID de interfaz de una longitud de 64 bits bajo el formato EUI-64, dejando el bit U/L puesto en cero, indicando que se trata de una dirección local y por ende que no es globalmente única; para este tipo de direcciones

reservadas anycast de subred (siguiendo el algoritmo EUI-64) el formato se conforma de la siguiente manera:

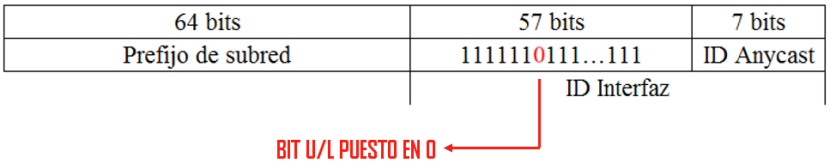


Imagen 2.28 “Dirección anycast de la subred”

Para cualquier otro tipo de dirección IPv6 (donde el prefijo sea diferente a los descritos anteriormente), el identificador de interfaz puede no contener el formato EUI-64 y tener una longitud distinta de 64 bits; para este tipo de direcciones reservadas anycast de subred se construyen de la siguiente manera:

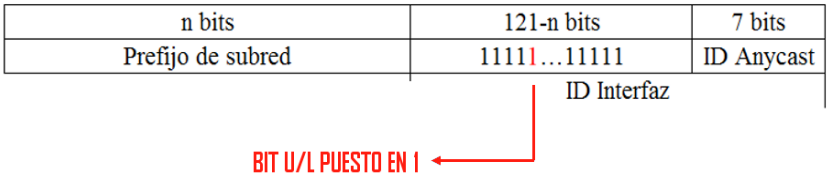


Imagen 2.29 “Dirección anycast de la subred (bit u/l puesto en 1)”

Nota: Las especificaciones por dejar el bit U/L en 0 se explican en el tema 3.1 “Bit universal/local (U/L)”, página 85.

Como se muestra en la imagen 2.29, el prefijo de subred consiste en todos los campos de la dirección IPv6, excepto el campo ID de interfaz. El identificador de interfaz en las direcciones reservadas anycast son formadas desde el identificador anycast de siete bits (“ID anycast”) con los bits restantes puestos en 1’s. Sin olvidar que para los identificadores de interfaz en formato EUI-64 el bit universal/local debe ser cero. El ID anycast identifica una dirección anycast reservada particular dentro del prefijo de subred, desde el conjunto de direcciones reservadas de las mismas. Asimismo, se reservan únicamente 128 valores (2^7) para los identificadores anycast (en lugar de quizás 256 o 2^8).

Todas las direcciones anycast de subred están reservadas en todos los enlaces, con todos los prefijos de subred. Por tal motivo, no deben ser utilizadas por el direccionamiento unicast asignadas a cualquier interfaz.

Actualmente, se han definido los siguientes identificadores de interfaz para las direcciones reservadas anycast de subred (tabla 2.3).

Tabla 2.3 “ID's de Anycast reservadas”

Decimal	Hexadecimal	Descripción
127	7F	Reservado
126	7E	Mobile IPv6 Home-Agents Anycast
0 - 125	00 - 7D	Reservado

Se espera que en un futuro se asignen identificadores anycast adicionales.

Ejemplo:

Para ilustrar la construcción de las direcciones reservadas anycast de subred, se detallará la construcción de la dirección reservada Mobile IPv6 Home-Agentes. Como se mencionó anteriormente, el identificador anycast consta de siete bits, formando en este caso el valor 126 (decimal) o 7E (hexadecimal) (imágenes 2.30 y 2.31).

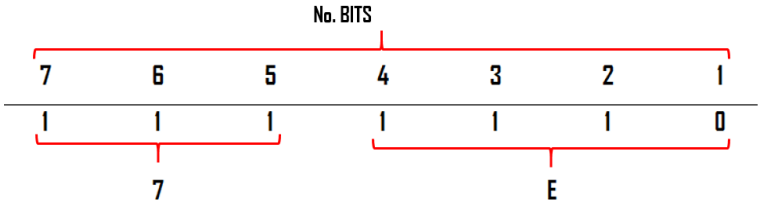


Imagen 2.30 “Formación del valor hexadecimal ID anycast”

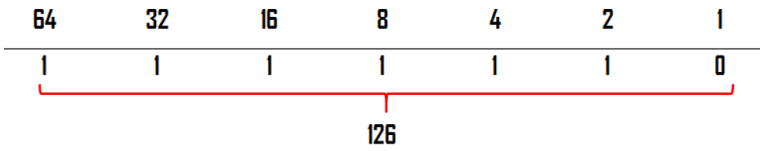


Imagen 2.31 “Formación valor decimal ID anycast”

La dirección reservada anycast de subred de Mobile Ipv6 Home-Agents consta de 64 bits de prefijo de subred, seguido por los 64 bits de identificador de interfaz como se muestra a continuación:

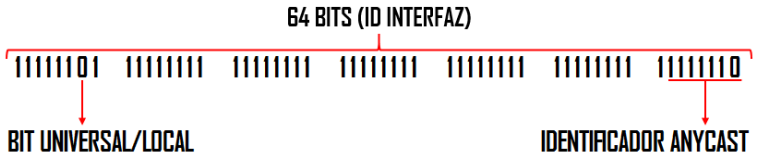


Imagen 2.32 “ID de interfaz de dirección reservada anycast Mobile IPv6 Home-Agents”

Para otros tipos de direcciones IPv6, el identificador de interfaz puede ser diferente de 64 bits de longitud y no tener el formato EUI-64. En este ejemplo, suponga que la longitud del identificador de interfaz es de 64 bits para permitir la comparación clara con el ejemplo anterior (aunque los identificadores de interfaz de longitudes distintas de 64 bits siguen la misma estructura general del identificador de interfaz que se muestra en la imagen 2.33).

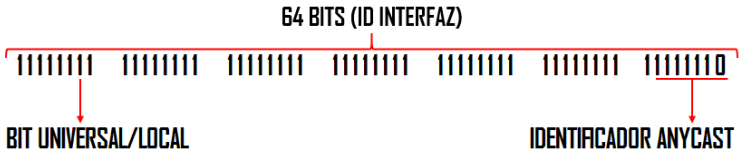


Imagen 2.33 “ID de interfaz de dirección reservada anycast Mobile IPv6 Home-Agents”

Un uso previsto de las direcciones anycast es identificar a un conjunto de routers que pertenecen a una organización que proporciona servicios de internet. Tales direcciones podrían ser utilizadas como direcciones intermedias en una cabecera de enrutamiento IPv6 para causar que un paquete sea entregado a través de un proveedor de servicio en particular o secuencia de proveedores de servicios.

Algunos otros posibles usos son identificar el conjunto de routers conectados a una subred particular, o el conjunto de routers que proporcionan la entrada en un dominio de enrutamiento particular, descubrimiento de servicios en la red (DNS, proxy HTTP, etc.).

No obstante, como se observó, existen pocas direcciones anycast asignadas actualmente. Por consecuencia, existe poca experiencia con su uso extendido y “pueden presentarse algunas complicaciones y peligros para cuando los identificadores anycast sean utilizados de manera generalizada”. (Sarria, 2004). Por tal motivo, se han impuesto las siguientes restricciones a las direcciones anycast IPv6:

- Una dirección anycast no puede ser utilizada como dirección de origen en un paquete IPv6
- Una dirección anycast no debe ser asignada a un host, es decir, solo puede ser asignada a un router IPv6

2.2.3.3 Multicast (RFC 4291)

Una dirección IPv6 multicast es un identificador para un grupo de interfaces (pertenecientes a diferentes nodos), donde una interfaz puede corresponder a cualquier número de grupos multicast.

Los paquetes de información enviados a una dirección multicast viajan a múltiples destinos al mismo tiempo. Tal dirección sigue el siguiente formato:

8	4	4	112 bits
11111111	flgs	scope	ID grupo

Imagen 2.34 “Estructura dirección multicast”

El primer campo de la estructura se conforma de ocho bits (todos puestos en 1’s), formando los valores hexadecimales “FF” (imagen 2.35), mismos que identifican que la dirección es de tipo multicast, formando así, el prefijo FF00::/8.

Imagen 2.35 “Formación de los valores del prefijo multicast”

El siguiente campo de la dirección nombrado “flags” se encarga de identificar el tipo de autenticidad de la dirección multicast. Dicho campo se conforma de cuatro bits (000T) mismos que se denominan como “banderas” (flags en inglés) donde el cuarto bit (T) puede tomar dos valores distintos para identificar el tipo de dirección multicast (tabla 2.4).

Tabla 2.4 “Valores establecidos del bit T”

T = 0	Indica que la dirección multicast es permanente y es asignada por la IANA.
T = 1	Indica que la dirección multicast asignada es temporal

Nota: Los bits previos al bit T están reservados para una implementación futura donde el objetivo es reducir el número de protocolos que deben ser desplegados para obtener la asignación dinámica de direcciones multicast e información sobre el prefijo (RFC 3356 y 3306).

Los siguientes cuatro bits que conforman el campo “scope” están reservados de forma predeterminada, por tal motivo son fijados a cero. Sin embargo, pueden llegar a tomar una serie de valores (hexadecimales) con el objetivo de identificar el nivel de alcance que pueden llegar a tener estas direcciones (tabla 2.5).

Tabla 2.5 “Valores del campo scope”

0	Reservado
1	Alcance interfaz local
2	Alcance de enlace local
3	Alcance local de subred
4	Alcance admin-local
5	Alcance local de sitio
6	Sin asignar
7	Sin asignar
8	Alcance de organización local
9	Sin asignar
A	Sin asignar
B	Sin asignar
C	Sin asignar
D	Sin asignar
E	Alcance global
F	Reservado

- **1:** Alcance de interfaz local. Abarca únicamente una interfaz en un nodo, y es útil solo para la transmisión loopback de multicast.
- **2 y 5:** Alcance de enlace local y de sitio local multicast. Abarcan las mismas regiones topológicas como los correspondientes alcances unicast.
- **3:** Alcance local de subred. Se utiliza para que las subredes puedan abarcar múltiples enlaces.
- **4:** Alcance admin-local. Es un alcance más pequeño que debe ser configurado administrativamente, es decir, no se deriva automáticamente de la conectividad física.
- **8:** Alcance local de organización. Tiene la intención de abarcar varios sitios que pertenecen a una sola organización.

Los valores marcados con el valor “Sin asignar” solo están disponibles para los administradores, con el fin de definir regiones multicast adicionales.

Por ejemplo, si una dirección multicast inicia con el prefijo FF0E::/16 significa que se trata de una dirección multicast permanente con un alcance global (internet) (imagen 2.36).

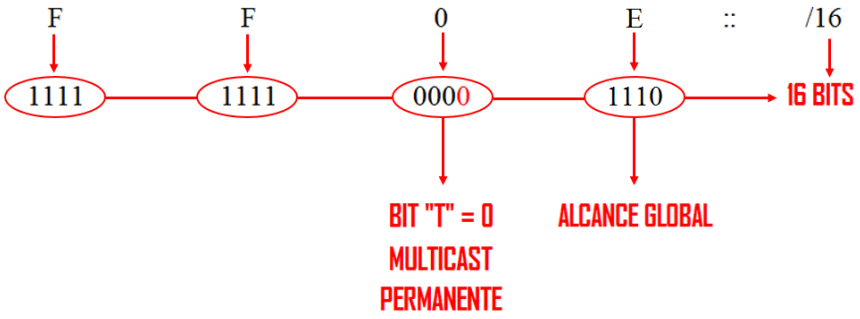


Imagen 2.36 “Ejemplo de dirección multicast”

El último campo, es decir, el bloque “identificador de grupo”, como su nombre lo menciona, identifica a un grupo multicast, ya sea de forma permanente o temporal dentro de un determinado alcance. Cabe mencionar, que el significado de una asignación permanente a una dirección multicast es independiente del valor de alcance. Por ejemplo, si a un grupo de servidores NTP (Network Time Protocol) se les asigna una dirección multicast permanente con el ID de grupo 101, entonces:

- FF01:: 101 significa: Todos los servidores NTP en su misma interfaz local.
- FF02:: 101 significa: Todos los servidores NTP con un alcance de enlace local
- FF05:: 101 significa: Todos los servidores NTP con un alcance de sitio
- FF0E:: 101 significa: Todos los servidores NTP con un alcance hacia internet

Las direcciones multicast asignadas de forma temporal sólo tienen sentido dentro de un alcance dado. Por ejemplo, un grupo identificado por la dirección multicast temporal local de sitio FF15::101 no tiene relación alguna con otro grupo que utilice la misma dirección en otro sitio, ni a un grupo temporal utilizando el mismo ID de grupo con un alcance diferente, ni a un grupo permanente con el mismo ID de grupo.

Una vez expuestos los datos anteriores respecto al manejo multicast, se deben seguir ciertas normas con base a las funciones y alcances:

- Las direcciones multicast no deben ser usadas como dirección fuente en un paquete IPv6.
- Los routers no deben presentar ningún paquete multicast más allá del alcance indicado por el campo de alcance en la dirección multicast destino.
- Los nodos no deben originar un paquete a una dirección multicast cuyo campo de alcance contenga el valor reservado cero; si se recibe tal paquete, se debe desechar.
- Los nodos no deben proceder un paquete a una dirección multicast cuyo campo de alcance contenga el valor reservado F; si tal paquete es enviado o recibido debe ser tratado igual que los paquetes destinados a un campo de alcance E (global).

Asimismo, multicast al ser un tipo de operación IPv6 para él envió de datos, brinda una considerable ventaja ante el broadcast (implementado y usado por el antiguo protocolo IP). Por tal motivo, broadcast no es usado en IPv6. Pero, ¿Por qué dejó de utilizarse broadcast en la nueva versión IP? El broadcasting en IPv4 tiene como consecuencia algunos problemas:

- Genera un número de interrupciones en cada computador de la red.
- En algunos casos, provoca malfuncionamiento que puede detener completamente una red.

Dicho evento desastroso de red se denomina como "tormenta de broadcast". Del tal manera que es reemplazado por las direcciones multicast, ya que activa la operación de la red eficientemente por el uso funcional de grupos específicos multicast para enviar solicitudes a un número limitado de computadoras en la red. Ya que un paquete enviado a una dirección multicast es enviado a todas las interfaces identificadas por esa dirección. (Gutiérrez, 2010)

Algunas aplicaciones que pueden ser utilizadas mediante estas direcciones son:

- Sistemas distribuidos
- Videos bajo demanda (VoD)
- Difusión de radio/tv
- Conferencias Multipunto
- Juegos en Red
- Funciones de nivel de red

Asimismo, existen dos tipos de direcciones multicast:

- Direcciones multicast predefinidas
- Dirección multicast de nodo solicitado

2.2.3.3.1 Direcciones multicast predefinidas

Se tratan de direcciones multicast donde sus identificadores de grupos han sido establecidos y definidos con valores de alcance explícito. Por tal motivo, no está permitido cambiar el valor de alcance ya que la bandera T es igual a cero, es decir, la dirección es permanente.

Las direcciones multicast con el prefijo "FF00::" hasta "FF0F::" están reservadas y no pueden ser asignadas a cualquier grupo. Por ejemplo:

FF01 : 0 : 0 : 0 : 0 : 0 : 0 : 1
FF02 : 0 : 0 : 0 : 0 : 0 : 0 : 1

Las direcciones anteriores identifican al grupo multicast de todos los nodos habilitados con IPv6 dentro de un alcance 1 o 2 (interfaz local y enlace local respectivamente). Tienen el mismo efecto que la dirección IPv4 de broadcast (imagen 2.37).

Comunicación IPv6 multicast de todos los nodos

Dirección IPv6 origen	Dirección IPv6 destino
2001:0db8:acad:1::1	FF02::1

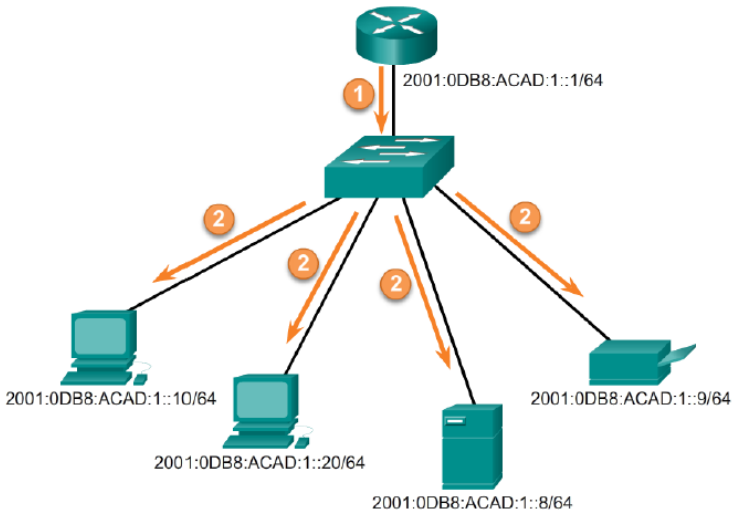


Imagen 2.37 “Multicast IPv6 de todos los nodos”

Las siguientes direcciones identifican a un grupo multicast de todos los routers IPv6 dentro de un alcance 1 (interfaz local), 2 (enlace local) o 5 (sitio local).

FF01 : 0 : 0 : 0 : 0 : 0 : 0 : 2
FF02 : 0 : 0 : 0 : 0 : 0 : 0 : 2
FF05 : 0 : 0 : 0 : 0 : 0 : 0 : 2

Un router se convierte en un miembro de un grupo multicast dependiendo de la habilitación y configuración que se realice en una interfaz del dispositivo. Sin embargo, es indispensable que previamente el comando de configuración global “ipv6 unicast-routing” (tratándose de un entorno Cisco) sea capturado para configurar correctamente cualquier interfaz.

Nota: Las especificaciones del comando “ipv6 unicast-routing” se encuentran en la práctica 6.1, página 110.

Una vez unido el enrutador a los grupos multicast mencionados, los mensajes enviados serán recibidos y procesados por el enrutador o enrutadores IPv6. No obstante, el alcance dependerá de las funciones establecidas.

2.2.3.3.2 Dirección multicast de nodo solicitado

Se trata de una dirección multicast calculada en función de las direcciones unicast global o unicast de enlace local de un nodo. Conservando sólo los 24 bits de menor peso de estas direcciones y agregando los valores hexadecimales "FF" (del bit 25 al 32), añadiéndolos finalmente al prefijo FF02 : 0 : 0 : 0 : 0 : 1 : FFXX : XXXX / 104 (donde "X" representa los valores de la dirección unicast global o de enlace local).

El rango para las direcciones multicast de nodo solicitado es:

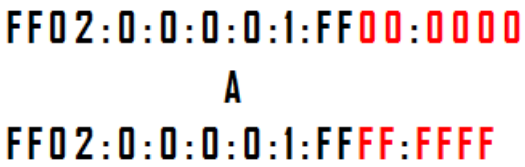


Imagen 2.38 "Rango de dirección multicast"

Estas direcciones se crean automáticamente después de haber configurado las direcciones unicast en las interfaces de un nodo.

Por ejemplo, la dirección multicast del nodo solicitado correspondiente a la dirección 4037::1:800:200E:8C6C es:

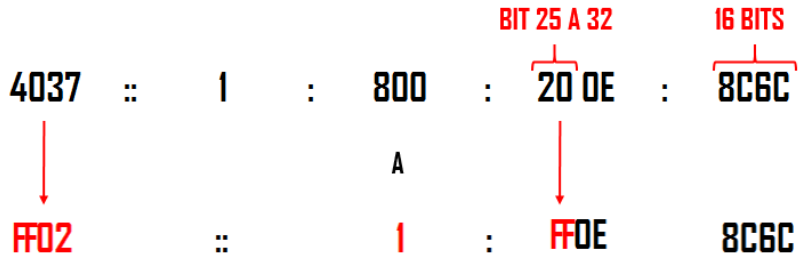


Imagen 2.39 "Transformación a la dirección multicast de nodo solicitado"

Las direcciones IPv6 que difieren sólo en los bits de orden superior (debido a múltiples prefijos asociados con diferentes agregaciones) se asignarán a la misma dirección de nodo solicitado, reduciendo con ello el número de direcciones multicast a las que un nodo debe unirse.

Esta dirección es regularmente utilizada por el Protocolo de Descubrimiento de Vecinos (Neighbor Discovery Protocol).

Por ejemplo, para conocer la dirección física de un nodo se envían peticiones a la dirección multicast de nodo solicitado, donde únicamente el dispositivo solicitado responderá a dichos paquetes (explicado con mayor detalle en el tema 2.2.9, página 54), reduciendo

considerablemente el tráfico en comparación con IPv4, donde la comunicación era de tipo broadcast.

Nota: Es poco posible que dos o más dispositivos tengan la misma dirección multicast de nodo solicitado. Si bien esto puede suceder cuando se tienen los mismos 24 bits en sus ID de interfaz. Aunque en realidad, no genera ningún problema, ya que el dispositivo aún procesa el mensaje encapsulado, el cual incluye la dirección IPv6 completa del dispositivo en cuestión. (Molinero, 2011).

2.2.4 Direcciones especiales en IPv6 (RFC 4291)

Se han definido también las direcciones para usos especiales, tales como:

- **Dirección de auto-retorno o Loopback (::1/128)**: Dirección que no es asignada a una interfaz física; se presenta como una interfaz "virtual" pues se trata de paquetes que no salen de la máquina que los emite; permite hacer un bucle para verificar la correcta inicialización del protocolo (dentro de un determinado host).

- **Dirección no especificada (::/128)**: Dirección que nunca debe ser asignada a ningún nodo, ya que se emplea para indicar la ausencia de dirección. Por ejemplo, cuando dicha dirección se halle en el campo "dirección fuente" indica que se trata de un host que está iniciándose, antes de que haya aprendido su propia dirección.

- **Túneles dinámicos/automáticos de IPv6 sobre IPv4 (::"dirección IPv4"/96)**: Se denominan direcciones IPv6 compatibles con IPv4, y permiten la retransmisión de tráfico IPv6 sobre infraestructuras IPv4. (Actualmente estas direcciones han sido despreciadas por la IANA) (imagen 2.40).

80 Bits	16 Bits	32 Bits
0000….0000	0000	Dirección IPv4

Imagen 2.40 "Formato de túneles dinámicos IPv6 sobre IPv4"

- **Representación automática de direcciones IPv4 sobre IPv6 (::FFFF:"dirección IPv4"/96)**: Permite que los nodos que sólo soportan IPv4 puedan seguir trabajando en redes IPv6. Se denominan "direcciones IPv6 mapeadas desde IPv4" (imagen 2.41).

80 Bits	16 Bits	32 Bits
0000….0000	FFFF	Dirección IPv4

Imagen 2.41 "Direcciones automáticas IPv6 sobre IPv4"

2.2.5 Direcciones requeridas para cualquier nodo

Un host requiere reconocer como mínimo las siguientes direcciones para la identificación de sí mismo al unirse a la red:

- Direcciones locales de enlace para cada interfaz
- Cualquier dirección unicast adicional que haya sido configurada manualmente o automáticamente
- Dirección loopback
- Direcciones multicast de todos los nodos
- Direcciones multicast de nodo solicitado
- Direcciones multicast de todos los grupos a los que dicho host pertenece

Además, se necesita de un router para identificar todas las direcciones que un host está obligado a reconocer y, asimismo, para reconocer las siguientes direcciones:

- Dirección reservada de subred anycast, para las interfaces en las que está configurado para actuar como router
- Dirección multicast de todos los routers
- Direcciones multicast de todos los grupos a los que el router pertenece

Al mismo tiempo, todos los dispositivos con IPv6 deben de tener predefinidos los siguientes prefijos y direcciones:

- Dirección no especificada
- Dirección de loopback
- Prefijo multicast (FF)
- Prefijos de uso local (local de enlace y local única)
- Direcciones multicast predefinidas
- Prefijos compatibles con IPv4

Se debe de asumir que todas las demás direcciones son unicast a no ser que sean específicamente configuradas (por ejemplo las direcciones anycast).

2.2.6 Diferencias con IPv4

Algunas características respecto a las direcciones IPv6 se han resaltado a lo largo del documento, tales como el tipo de formato, asignación, tipos de direcciones, etc. Esto es debido a la renovación entre las versiones del protocolo IP. Por tal motivo, las siguientes diferencias en el direccionamiento deben ser reiteradas y destacadas:

- No hay direcciones broadcast (su función es sustituida por las direcciones multicast).
- Los campos de las direcciones reciben nombres específicos; denominamos “prefijo” a la parte de la dirección hasta los bits indicados. Dicho prefijo permite conocer donde está conectada una determinada dirección, es decir, su ruta de encaminado.
- Las direcciones IPv6, indistintamente de su tipo (unicast, anycast o multicast), son asignadas a interfaces y no a nodos.
- Dado que cada interfaz pertenece a un único nodo, cualquiera de las direcciones unicast de las interfaces del nodo pueden ser empleados para referirse a dicho nodo.
- Todas las interfaces deben de tener como mínimo una dirección unicast de enlace local.
- Una única interfaz puede tener también varias direcciones IPv6 de cualquier tipo (unicast, anycast o multicast).
- Al igual que en IPv4, se asocia un prefijo de subred con un enlace, y se pueden asociar múltiples prefijos de subred a un mismo enlace. (Martínez, 2016).

2.2.7 Encabezado IPv6

Una cabecera (header en inglés) contiene la información necesaria para trasladar un paquete de datos desde un emisor hasta un receptor. En IPv6, el encabezado se conforma de 40 octetos (bytes), en contraste con la antigua versión IP que contiene solo 20. Lo cual conlleva de haber pasado de 12 campos en IPv4 a tan solo 8 en IPv6. Además, la nueva versión IP ofrece una cabecera de longitud fija, consecuencia de suprimir opciones poco utilizadas. Sin embargo, aún existe la posibilidad de especificar dichas opciones pero ya sin formar parte de la cabecera IP como sucedía anteriormente.

Esto implica muchas ventajas, por ejemplo, una mayor facilidad para su proceso en routers y conmutadores (por ende una transmisión de trafico de datagramas más veloz).

En las imágenes 2.42 y 2.43 se observa la transición de cabecera entre las dos versiones IP.

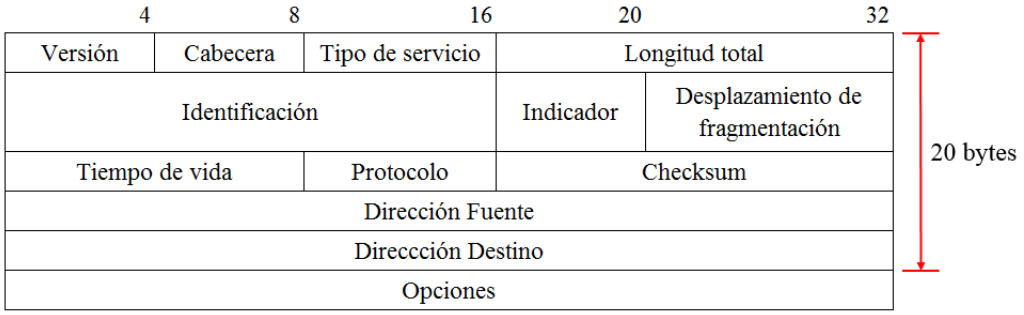


Imagen 2.42 “Campos del encabezado IPv4”

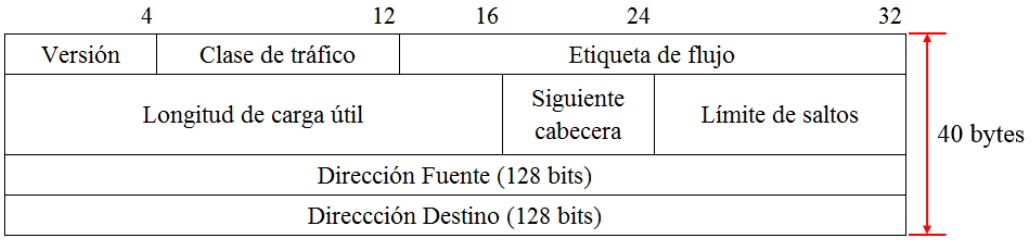


Imagen 2.43 “Campos del encabezado IPv6”

Los campos de la cabecera IPv6 son los siguientes:

Versión: Campo compuesto de 4 bits, al igual que en IPv4. Únicamente cambia el número 6 para IPv6, en lugar del 4 para IPv4.

Clase de Tráfico: Campo compuesto de 8 bits, también denominado como “Prioridad”. Este campo es similar al “tipo de servicio” (ToS) en IPv4 y se encarga de etiquetar el paquete con una clase de tráfico que se usa en servicios diferenciados.

Etiqueta de Flujo: Campo de 20 bits. Permite que una serie de datagramas reciban un mismo trato. Se utiliza para permitir tráfico con requisitos de tiempo real junto con el campo clase de tráfico.

Longitud de Carga Útil: Campo de 16 bits que es similar al campo de “longitud total” en IPv4. Este campo como su nombre lo indica, específica la longitud de carga útil, es decir, la longitud de los propios datos (pueden ser de hasta 65,535 bytes). Sin embargo, a diferencia de la antigua versión IP, el valor de este campo representa solo el tamaño de los datos que transporta sin incluir la cabecera IP.

Siguiente cabecera: Campo compuesto de 8 bits. Indica al enrutador si tras el datagrama viene algún tipo de extensión u opción. Dicho campo sustituye al campo de banderas (“indicador” en la imagen 2.42) de la versión 4 de IP. De tal manera que en lugar de complicar la cabecera IP con la interpretación de los diferentes bits de opciones, se sitúan fuera del datagrama básico.

En la versión 6 del protocolo IP se define una serie de cabeceras de extensión que se colocan justo antes de los datos en forma de cadena y que permiten al usuario personalizar el tipo de datagrama. Únicamente se establece el tipo de cabecera que vendrá a continuación en el campo “siguiente cabecera” de cada una de ellas.

Nota: La descripción detallada de las cabeceras de extensión se especifica en el tema 2.2.7.1 página 49.

Nota: En IPv4 existe un campo nombrado “protocolo” que se utiliza para identificar el siguiente nivel de protocolo, es decir, el protocolo de nivel superior que contiene encapsulado el paquete IP (normalmente TCP o UDP). En IPv6, este campo es nombrado como “siguiente cabecera”. (IANA, 2016).

Límite de Salto: Campo de 8 bits. Especifica el máximo número de saltos que un paquete IP puede atravesar. Cada salto o router disminuye este campo en uno (similar al campo de "tiempo de vida" (TTL) en IPv4).

Dirección de Origen: Campo de 16 octetos o 128 bits. Este segmento identifica el origen del paquete.

Dirección de Destino: Campo de 16 octetos o 128 bits. Identifica el destino del paquete. (Gutiérrez, 2010)

Claramente, todos los campos de la versión 4 han sufrido cambios de forma relativa e incluso algunos fueron eliminados. El único campo que conserva la misma posición y significado es el de "versión", esto debido a la interacción que experimentan actualmente ambas versiones IP. De tal forma que fueron necesarias las operaciones de transición (producto del conocimiento y experiencia con IPv4), eliminando los campos considerados redundantes y/o poco eficientes.

Por otra parte, los campos "Clase de tráfico" y "Etiqueta de Flujo" sobresalen en el nuevo encabezado, ya que "permiten algunas de las características fundamentales e intrínsecas de IPv6: Calidad de Servicio (QoS), Clase de Servicio (CoS) y en definitiva un poderoso mecanismo de control de flujo de asignación de prioridades diferenciadas, según los tipos de servicios." (Martínez, 2016).

2.2.7.1 Cabeceras de extensión de IPv6

Como se mencionó anteriormente, la nueva versión de la cabecera IP no contiene ningún tipo de opciones a diferencia de la versión 4. No obstante, en algunos casos es necesario poder especificar algunas características especiales a los enrutadores intermedios para que operen el datagrama IP de una forma determinada puesto que, no todos los datagramas son datos que circulan de un usuario a otro por internet, algunos son mensajes entre los diferentes routers.

Un ejemplo típico podría ser la necesidad de especificar los routers por los cuales debe circular un datagrama. Por lo que debe establecerse una ruta fija entre dos ordenadores, ya sea porque no se fía de las demás o simplemente para medir el rendimiento entre dos puntos. De tal manera que se necesita especificar por dónde encaminarlo, evitando que sean los routers intermedios los que tomen la decisión. La manera de hacerlo es indicar en el campo "siguiente cabecera" del paquete IPv6 el número correspondiente a la cabecera que se colocará tras el paquete. De esta forma, el router sabe que antes de encaminar el datagrama, debe de tener en cuenta esa información extra.

En la tabla 2.6 se observan algunos ejemplos conocidos de cabeceras de extensión.

Tabla 2.6 “Ejemplos típicos de cabeceras de extensión”

Valor de cabecera (decimal)	Abreviatura	Descripción
0	HBH	Opciones entre saltos
4	IP	Encapsulación en IPv4
5	ST	Stream
6	TCP	Protocolo de control de transmisión
17	UDP	Protocolo de datagrama de usuario
51	AH	Autenticación de cabecera
52	ESP	Encrypted Security Payload
58	ICMP	Protocolo de control de mensajes de internet
59	NULL	Sin siguiente cabecera
60	DO	Cabecera de opciones de destino
194	JBGR	Jumbogram

Sin embargo, antes de cualquier verificación de cabecera entre los dispositivos intermedios, debe establecerse el valor “cero” en dicho campo para realizar un examinado y proceso “salto a salto”, tal y como en la descripción del ejemplo anterior. Esto se debe a que las cabeceras sucesivas no son examinadas en cada nodo de la ruta, sino sólo en el nodo o nodos de destino final. Asimismo, múltiples cabeceras pueden ser encadenadas en un mismo datagrama, de tal forma que serán examinadas por los enrutadores de acuerdo a la posición en que se encuentren una de otra (imagen 2.44).

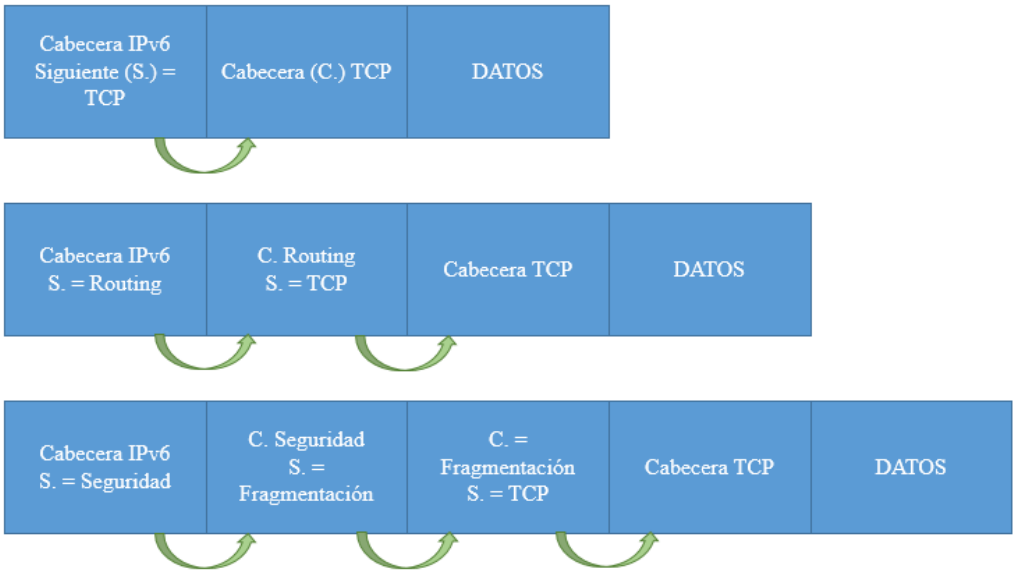


Imagen 2.44 “Representación de siguiente cabecera IPv6 concatenada”

Nota: Ante el proceso de inspección, no debería existir ningún inconveniente para los routers intermedios encaminar el datagrama hacia su destino.

Por otra parte, es importante señalar que hay diversas cabeceras con una mayor importancia que otras (esto se debe a los tipos de operaciones que emplea cada una) y pese a no existir un formato rígido para establecer dichas preferencias, hay una recomendación en cuanto al orden adecuado de estas:

1) Cabecera IP versión 6 (IPv6 Header).
2) Cabecera de opciones entre saltos (Hop-by-hop Options Header).
3) Opciones de cabecera de destino (Destination Options Header).
4) Cabecera de encaminamiento (Routing Header).
5) Cabecera de fragmentación (Fragment Header).
6) Cabecera de autenticación (Authentication Header).
7) Cabecera de protocolo de nivel superior (TCP, UDP...) (Álvarez, 2000)

2.2.8 ICMPv6 (RFC 4443)

La nueva versión IP utiliza el Protocolo de Mensajes de Control de Internet (ICMP) como se ha definido anteriormente para IPv4 en el RFC 792.

ICMPv6 es utilizado por los nodos IPv6 para informar de los errores encontrados en los paquetes de procesamiento, similar a la versión anterior (tales como algunos diagnósticos. Por ejemplo, host de destinos inaccesibles, operación "ping", límite de saltos superado, etc.). Dicho ICMPv6 es una parte integral de IPv6, por lo cual, el protocolo y la base (es decir, todos los mensajes y el comportamiento requerido por la presente especificación) deben aplicarse plenamente por todos los nodos IPv6.

Los mensajes del protocolo tienen el siguiente formato general:

8 bits	**8 bits**	**16 bits**
Tipo	Código	Checksum
Cuerpo del mensaje		

Imagen 2.45 “Estructura de mensaje ICMPv6”

El campo “Tipo” indica el tipo de mensaje. Su valor determina el formato de los datos restantes.

El campo “Código” depende del tipo de mensaje (campo anterior) y se utiliza para crear un nivel adicional para la clasificación del mensaje.

El campo de suma de comprobación o mejor conocido como “checksum”, se utiliza para detectar errores de datos en el mensaje ICMPv6 y partes de la cabecera IPv6.

Los mensajes ICMPv6 se agrupan en dos clases:

- Mensajes de error
- Mensajes informativos

Los mensajes de error son identificados como tales por tener un cero en el bit más significativo del campo “Tipo”. Por lo tanto, los mensajes de error tienen valores de mensaje del 0 al 127 (imagen 2.46) y los valores de los mensajes informativos oscilan entre 128 y 255 (imagen 2.47).

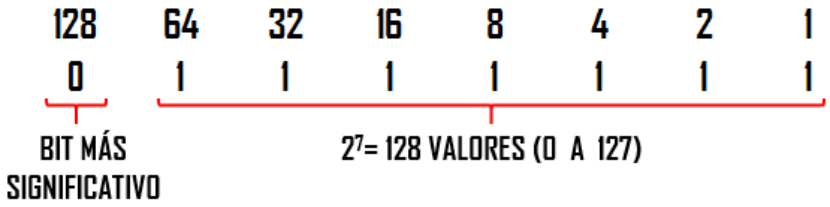


Imagen 2.46 “Rango de valores de mensajes de error”

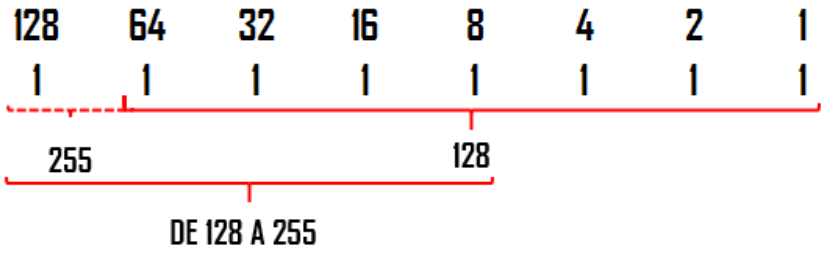


Imagen 2.47 “Rango de valores de mensajes informativos”

La definición de los formatos de mensaje ICMPv6 se describen a continuación:

Tabla 2.7 “Descripción de los mensajes ICMPv6”

MENSAJES DE ERROR ICMPv6		
Tipo "1" Destino no alcanzable	Código	Descripción
	0	Sin ruta hacia el destino
	1	Comunicación prohibida administrativamente
	2	Sin asignar
	3	Dirección no alcanzable
	4	Puerto no alcanzable
	5	Dirección de origen entrada fallida / política de egreso
	6	Rechazar ruta hacia el destino

Tipo "2" Paquete demasiado grande	0	Se establece en 0 (cero) por el emisor e ignorado por el receptor.
Tipo "3" Tiempo Excedido	0	Límite de saltos superado
	1	Tiempo de reensamblaje de fragmentos superado
Tipo "4" Problema de parámetro	0	Campo erróneo en cabecera
	1	Tipo de "cabecera siguiente" desconocida
	2	Opción IPv6 no reconocida
Tipo "100"	EXPERIMENTACIÓN PRIVADA	
Tipo "101"		
Tipo "127"	Reservado para expansión de mensajes de error ICMPv6	

MENSAJES INFORMÁTICOS ICMPv6		
Tipo	Código	Descripción
Tipo "128"	0	Petición Eco (Echo Request)
Tipo "129"	0	Respuesta Eco (Echo Reply)
Tipo "200"	EXPERIMENTACIÓN PRIVADA	
Tipo "201"		
Tipo "255"	Reservado para expansión de mensajes informáticos ICMPv6	

Los valores 100, 101, 200 y 201 están reservados para experimentación privada. No están destinados para el uso general y se espera que múltiples experimentos simultáneos se hagan con los mismos valores. Los valores 127 y 255 están reservados para una futura expansión de la gama de valores "tipo", si es que se presenta alguna escasez en el futuro.

El paquete ICMPv6 puede comenzar después de cero o más cabeceras de extensión. El valor en la última extensión de cabecera antes del encabezado ICMPv6 es 58.

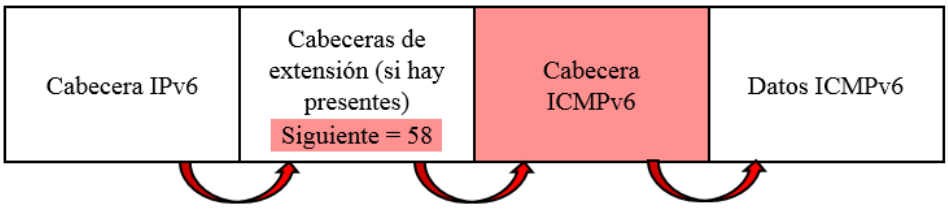


Imagen 2.48 "Valor de cabecera de extensión de ICMPv6"

2.2.9 Descubrimiento de vecinos (Neighbor Discovery) (RFC 2461)

El protocolo de Descubrimiento de Vecinos consiste en un mecanismo por el cual un nodo descubre la presencia de otros dispositivos (computadoras, enrutadores, móviles, etc.) al momento de incorporarse en una red. De manera más específica, el protocolo es utilizado con el objetivo de determinar las direcciones de la capa de enlace de los "vecinos" que se encuentran en los enlaces adjuntos. Por tal motivo, este método de identificación es el equivalente de cierto modo a ARP en IPv4. Sin embargo, en IPv6, ND (abreviatura de "Neighbor Discovery") incorpora la funcionalidad del protocolo ICMPv6 (Protocolo de Mensajes de Control de Internet para IPv6) para lograr con éxito sus operaciones. Además, realiza funciones adicionales como la detección de vecinos inaccesibles (NUD), la configuración automática con o sin estado, la adquisición de información adicional, entre otros.

Los mensajes ICMPv6 que utiliza el protocolo para llevar a cabo sus procesos son:

- Solicitud de Vecino (Neighbor Solicitation)
- Respuesta de Vecino (Neighbor Advertisement)
- Solicitud de Router (Router Solicitation)
- Anuncio de Router (Router Advertisement)
- Mensaje de redirección (Redirect Message)

Cada mensaje utilizado por el protocolo realiza funciones específicas y tienen un formato independiente de otro.

2.2.9.1 Solicitud de Vecino (Neighbor Solicitation)

Los nodos llevan a cabo la resolución de direcciones mediante el envío multidifusión de una solicitud de vecino. Por lo que el objetivo principal de este mensaje es requerir al nodo destino devolver su dirección de capa de enlace. Los paquetes de solicitud son enviados a la dirección multicast de nodo solicitado de la dirección destino. Consecuentemente, el receptor devuelve su dirección de capa de enlace en un mensaje de anuncio de vecino de forma unicast. Por lo tanto, un par de simples paquetes "solicitud-respuesta" son suficientes para que el emisor y el destino resuelvan las direcciones de capa dos de los demás nodos; el emisor incluye su dirección de capa de enlace en el mensaje enviado.

El formato de cabecera para estos mensajes es el siguiente:

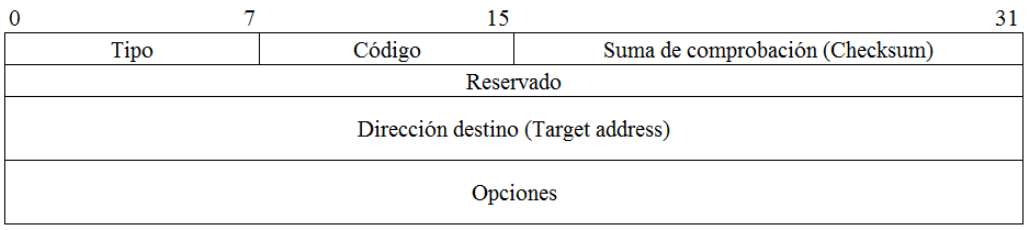


Imagen 2.49 "Formato de cabecera de una solicitud vecino"

Donde:

Tabla 2.8 “Descripción de los campos de cabecera de una solicitud vecino”

Campos IP	
Dirección fuente	Ya sea la dirección asignada a la interfaz desde la que se envía el mensaje o en caso del curso del método Detección de Direcciones Duplicadas (DAD) (tema 2.2.9.6), la dirección no especificada.
Dirección destino	Ya sea la dirección multicast de nodo solicitado que corresponde a la dirección destino (target address) o la propia dirección destino (target address). En caso de la verificación de accesibilidad de vecino (tema 2.2.9.7), la dirección unicast.
Límite de saltos	255
Campos ICMP	
Tipo	135
Código	0
Suma de comprobación	Suma de comprobación correspondiente a ICMPv6
Reservado	Campo no utilizado. Debe ser iniciado a cero por el emisor e ignorado por el receptor.
Dirección destino (Target Address)	Dirección IP a donde se enviará la solicitud. No debe ser una dirección multicast. En caso del método DAD, la dirección IP que se evalúa.
Opciones posibles	**Dirección de capa de enlace del emisor**. No debe incluirse cuando la dirección de origen no esté especificada (::). Por otro lado, esta opción debe estar incluida en las solicitudes multicast y unicast.

Notas:

- En las próximas tablas de descripción, se muestran inicialmente los campos del protocolo IP, puesto que el mensaje ICMPv6 está encapsulado dentro del paquete IPv6. Asimismo, si se examinara el campo “siguiente cabecera” del encabezado IPv6 se encontraría el valor “58”.

- La dirección destino (Target address) es un identificador sobre el que se solicita la información de resolución de direcciones o una dirección que es el nuevo primer salto al ser redirigido. Por ejemplo, si una interfaz tiene la dirección “2001:bd4:abcd:dead::3”, entonces:

  2001:bd4:abcd:dead::3 - Target address (dirección de los campos ICMP)
  FF02::1:FF00:3 - Dirección destino (dirección de los campos IP)

- Los mensajes de solicitud de vecinos también se utilizan para determinar si más de un nodo se le ha asignado la misma dirección unicast. Dicho descubrimiento se le conoce como Detección de Direcciones Duplicadas (DAD) y se describe en la sección 2.2.9.6 en la página 64.

2.2.9.2 Anuncio de Vecino (Neighbor Advertisement)

Un nodo envía anuncios de vecinos en respuesta a las solicitudes de vecino. Además, se envían anuncios no solicitados con el fin de propagar nueva información de forma rápida. Por ejemplo, información de cambio en la dirección física, cambios en el estado del enrutador, modificaciones en la autoconfiguración de host, etc.

Llevan el siguiente formato de cabecera:

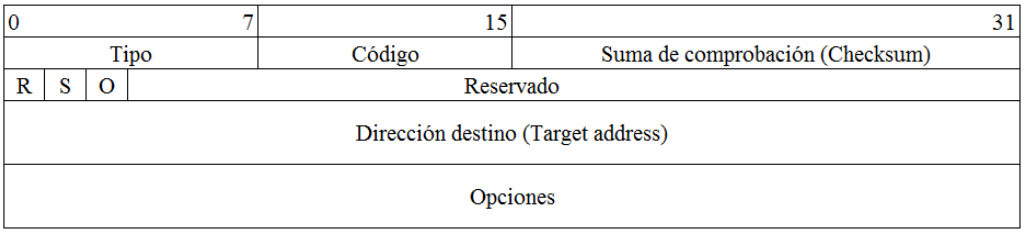


Imagen 2.50 “Formato de cabecera de un anuncio de vecino”

Donde los campos son los siguientes:

Tabla 2.9 “Descripción de los campos de cabecera de un anuncio de vecino”

Campos IP	
Dirección fuente	Dirección asignada a la interfaz desde la que se envía el anuncio.
Dirección destino	Para los anuncios solicitados, la dirección IP origen de la solicitud vecino, o en caso de que sea la dirección no especificada, la multicast de todos los nodos. Para los anuncios no solicitados, la dirección multicast de todos los nodos.
Límite de saltos	255
Campos ICMP	
Tipo	136
Código	0
Suma de comprobación	Suma de comprobación correspondiente a ICMPv6

R	Bandera de router. Cuando se establece, indica que el emisor es un router. Este parámetro es utilizado por la Detección de Inaccesibilidad de Vecino (NUD).
S	Bandera de solicitud. Al ser establecida, indica que el anuncio fue enviado en respuesta a una solicitud de vecino. También se utiliza como una confirmación de accesibilidad para NUD. No debe ser establecido en los anuncios multicast o en los anuncios no solicitados unicast.
O	Bandera inválida. Indica que el anuncio debe anular una entrada de caché existente y actualizar la dirección de capa de enlace almacenada. Cuando no se establece, el anuncio no actualiza alguna dirección.
Reservado	Campo en desuso de 20 bits. Debe ser iniciado a cero por el emisor y ser ignorado por el receptor.
Dirección destino (Target Address)	Para los anuncios solicitados, la dirección del campo "Target address" de la solicitud vecino que llevó a cabo este anuncio. Esta dirección, no debe ser multicast. Para un anuncio no solicitado, la dirección IP del nodo cuya dirección de capa de enlace ha cambiado.
Opciones posibles	**Dirección de capa de enlace**. Es decir, la dirección física del emisor del anuncio. Esta opción debe estar incluida al responder a las solicitudes multicast. También debe incluirse al responder a una solicitud de vecino unicast.

2.2.9.3 Solicitud de enrutador (Router Solicitation)

Cuando una interfaz está habilitándose, los hosts pueden enviar estos mensajes que solicitan a los routers generar anuncios de enrutador para que proporcionen los respectivos datos de configuración y prefijos de enlace asignados. Las solicitudes de enrutador se envían a la dirección IPv6 multicast de todos los enrutadores en el mismo enlace (FF02::2). Si el dispositivo aún no conoce su dirección fuente, se utilizará la dirección no especificada.

El formato que sigue es el siguiente:

0 7	15	31
Tipo	Código	Suma de comprobación (Checksum)
Reservado		
Opciones		

Imagen 2.51 “Formato de cabecera de una solicitud de enrutador”

Donde:

Tabla 2.10 “Descripción de los campos de cabecera de una solicitud de enrutador”

Campos IP	
Dirección fuente	Dirección IP de la interfaz desde donde se manda el mensaje o, la dirección sin especificar si aún no hay alguna dirección asignada.
Dirección destino	Dirección multicast de todos los enrutadores (FF02::2).
Límite de saltos	255
Campos ICMP	
Tipo	133
Código	0
Suma de comprobación	Suma de comprobación correspondiente a ICMPv6
Reservado	Este campo no se utiliza. Debe ser iniciado a cero por el emisor y ser ignorado por el receptor.
Opciones posibles	**Dirección de capa de enlace del emisor**. No debe incluirse si la dirección de origen es la dirección no especificada.

2.2.9.4 Anuncios de Enrutador (Router Advertisement)

Los anuncios de enrutador contienen una lista de prefijos utilizados para la determinación del enlace y/o la configuración automática de las direcciones IPv6. Los hosts utilizan los prefijos anunciados en el enlace para construir y mantener una lista que se utiliza para decidir cuándo un paquete de destino está en el enlace o más allá de un router. Además, estos mensajes permiten que los enrutadores informen a los hosts cómo realizar la autoconfiguración de direcciones. Por ejemplo, los routers pueden especificar si los host deben usar la configuración de DHCPv6 (configuración con estado o Stateful) y/o la configuración automática (sin estado o Stateless) de direcciones.

Nota: Las especificaciones de la configuración automática de direcciones IPv6 se describen en el capítulo 4, página 89.

Estos mensajes también contienen parámetros de internet, tales como el límite de saltos que un host debe usar en los paquetes salientes y, opcionalmente, información de enlace tales como el MTU. Esto facilita la administración centralizada de los parámetros que se pueden establecer en los routers y automáticamente propagarlos a todos los hosts conectados.

Nota: En los enlaces con capacidades multicast, cada router envía periódicamente un paquete de anuncio de enrutador informando su disponibilidad. Un host recibe los anuncios de enrutador de todos los routers (disponibles en el enlace), construyendo así una lista de enrutadores predeterminados.

Su formato el siguiente:

0 7	15			31
Tipo	Código			Suma de comprobación (Checksum)
Cur hop limit (limite de salto)	M	O	Reservado	Tiempo de vida del router
Tiempo accesible				
Tiempo de retransmisión				
Opciones				

Imagen 2.52 “Formato de cabecera de un anuncio de enrutador”

Donde:

Tabla 2.11 “Descripción de los campos de cabecera de un anuncio de enrutador”

Campos IP	
Dirección fuente	Debe ser la dirección de enlace local asignada a la interfaz desde donde se emite el mensaje.
Dirección destino	Dirección de origen de la invocación de una solicitud de router o la dirección multicast de todos los nodos.
Límite de saltos	255
Campos ICMP	
Tipo	134
Código	0
Suma de comprobación	Suma de comprobación correspondiente a ICMPv6

Límite de salto	Campo de 8 bits. Debe ser el valor predeterminado que se coloca en el campo "límite de saltos" de la cabecera IP para los paquetes IP salientes. Un valor de cero significa que no está especificado (por este router).
M	Bandera de “configuración de direcciones administradas”. Cuando se establece, indica que las direcciones están disponibles a través de DHCPv6. Si el indicador “M” se establece el indicador “O” es redundante y puede ser ignorado porque DHCPv6 devuelve toda la información de configuración disponible.
O	Bandera “otra configuración”. Cuando se establece, indica que otra información de configuración está disponible a través de DHCPv6. Es decir, es la información relacionada con DNS o datos de otros servidores de la red.

Nota: Si las banderas M u O no se establecen, indica que no hay información disponible a través de DHCPv6.

Reservado	Campo de 6 bits en desuso. Debe ser iniciado a cero por el emisor y ser ignorado por el receptor.
Tiempo de vida del router	Campo de 16 bits. Su función es anunciar a los host cuánto tiempo (dado en segundos) dicho router debe ser usado como predeterminado. El límite de tiempo de vida es de 9,000 segundos. Si el campo contiene el valor 0, indica que el router no debe ser usado por defecto.
Tiempo accesible	Campo de 32 bits. Indica el tiempo (dado en milisegundos) en que un nodo asume cuando un vecino es alcanzable después de haber recibido una confirmación de accesibilidad. El campo es utilizado por el algoritmo de Detección de Inaccesibilidad de Vecino (NUD). Un valor de cero significa que no se ha especificado (por este router).
Tiempo de retransmisión	Campo de 32 bits. Indica el tiempo (dado en milisegundos) entre los mensajes retransmitidos de solicitudes de vecino. Utilizado por la resolución de direcciones (DAD) y el algoritmo NUD. Un valor de cero significa que no se ha especificado (por este router).

Opciones posibles	**Dirección fuente de capa de enlace:** Dirección de capa de enlace de la interfaz desde la que se envía el anuncio de enrutador. **MTU:** Deben ser enviados en los enlaces que tienen una MTU variable. Puede ser enviado en otros enlaces. **Prefijo de Información:** Estas opciones especifican los prefijos que se encuentran en el enlace y/o los usados para la configuración automática de direcciones sin estado. Un router deberá incluir todos sus prefijos en el enlace (excepto el prefijo de enlace local) para que los hosts tengan la información de prefijo completa sobre los destinos de enlace para los enlaces de las que derivan.

2.2.9.5 Mensaje de redirección (Redirect Message)

La función que tiene un mensaje de redirección es bastante útil para el rendimiento y optimización de una red, ya que permite a los nodos conocer información que facilita el alcance hacía los destinos de una forma más eficiente.

Para lograr dicho objetivo, los enrutadores juegan un papel esencial, ya que son los encargados de enviar estos paquetes para informar a un host de un mejor nodo de primer-salto en el camino hacia un destino. En otras palabras, los host pueden ser redirigidos hacia un mejor router de primer salto, pero también pueden ser informados que el destino es de hecho, un vecino.

Los mensajes de redirección se utilizan en los siguientes casos:

- El host es informado que en el enlace local hay disponible un mejor enrutador que se encuentra más “próximo” hacia el destino que intenta alcanzar. La “proximidad” se utiliza en el enrutamiento para alcanzar el segmento de red de destino. Esta condición puede darse cuando existen varios enrutadores en un segmento de red y el host emisor elige un enrutador predeterminado que no resulta el más apropiado para llegar al destino.
- Un host es informado que el destino que intenta alcanzar es un vecino que está en el mismo enlace. Este caso puede darse cuando la lista de prefijos de un host no incluye el prefijo del destino. Por tal motivo, el host emisor envía el paquete a su enrutador predeterminado.

El formato para los mensajes de redirección es el siguiente:

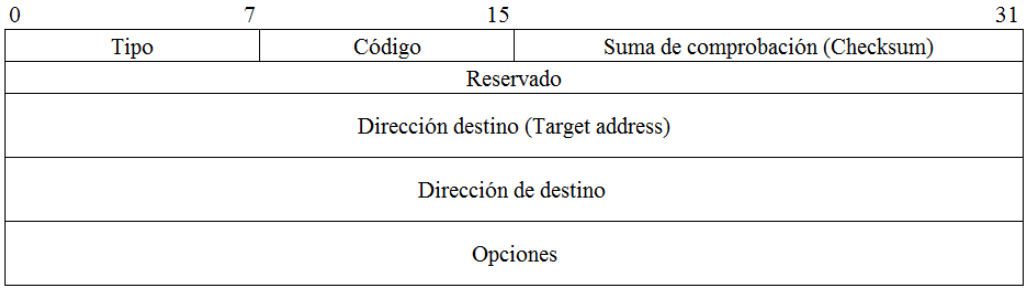


Imagen 2.53 “Formato de mensaje redirección”

Donde:

Tabla 2.12 “Descripción de los campos de un mensaje de redirección”

Campos IP	
Dirección fuente	Dirección de enlace local asignada a la interfaz desde donde se envía el mensaje.
Dirección destino	Dirección de enlace local del host que ha activado la redirección.
Límite de saltos	255
Campos ICMP	
Tipo	137
Código	0
Suma de comprobación	Suma de comprobación correspondiente a ICMPv6
Reservado	Este campo no se utiliza. Debe ser iniciado a cero por el emisor y ser ignorado por el receptor.
Dirección destino (Target Address)	Dirección IP del mejor primer salto a usarse para llegar al destino. Cuando el destino sea el actual punto final de la comunicación (por ejemplo, un vecino), este campo debe contener la misma dirección que el campo “Dirección de destino ICMP” (siguiente campo). De lo contrario, el objetivo es un router como el mejor primer salto, por lo que la dirección deberá ser la de enlace local de ese router.
Dirección de destino	Dirección IP que se redirige al destino.

Posibles opciones	**Dirección de capa de enlace:** La dirección de capa de enlace para el destino. **Cabecera de redireccionamiento.**

Para lograr un mejor entendimiento, el procedimiento de los mensajes de redirección es el siguiente:

- El host envía un paquete de forma unicast al enrutador que tiene por defecto.
- El enrutador recibe y procesa el paquete, verificando que la dirección destino del host corresponda a un vecino. Además, comprueba que la dirección destino del host y del salto siguiente se encuentren en el mismo enlace.
- El enrutador reenvía el paquete hacia la dirección de siguiente salto adecuado.
- El mismo router envía un mensaje de redirección al host, estableciendo los valores correspondientes según la descripción que se mostró en la tabla 2.12. Por ejemplo, en el campo "Target Address" se especifica la dirección de siguiente salto del nodo. Es decir, será la dirección donde el host emisor posteriormente debe enviar los paquetes dirigidos al destino.
- El host, tras recibir el mensaje de redirección, actualiza la entrada de la dirección de destino en la caché de destino con el identificador especificado en el campo "Target Address" del mensaje que recibió. Si el mensaje incluye la dirección de capa de enlace (campo "opciones"), se creará o actualizará la entrada de caché de vecino correspondiente.

Para concluir de manera general con el protocolo de resolución de direcciones para IPv6, el descubrimiento de vecinos también se emplea para mantener limpios los "caches" donde se almacena la información relativa al contexto de la red a la que está conectado un nodo (host o router), y por tanto para detectar cualquier cambio en la misma. Por ejemplo, cuando un router o una ruta hacia él fallan, el host buscará alternativas funcionales.

Asimismo, (a manera de resumen) los mecanismos que utiliza el descubrimiento de vecino se utilizan principalmente para:

- Descubrir routers
- Anunciar Prefijos y parámetros
- Autoconfiguración de direcciones
- Resolución de direcciones
- Determinación del siguiente salto
- Detección de nodos no alcanzables
- Detección de direcciones duplicadas o cambios, redirección
- Balanceo de carga entrante

2.2.9.6 Detección de Direcciones Duplicadas (DAD) (RFC 4862)

En IPv6, antes de que cualquier nodo pueda realizar sus funciones habituales de comunicación en una red, debe comprobarse que su dirección IPv6 es auténtica con la finalidad de evitar problemas de duplicidad. Por lo cual, los nodos utilizan un proceso de autenticación denominado Detección de Direcciones Duplicadas o mejor conocido por sus siglas "DAD".

Para realizar la verificación, el proceso DAD ocupa el protocolo de descubrimiento de vecinos para el envío de mensajes de solicitud y anuncios de vecinos (paquetes NS y NA respectivamente).

DAD construye inicialmente direcciones IPv6 que se denominan como "tentativas" o "provisionales". Dichos identificadores no pueden ser asignados a las interfaces hasta que hayan completado con éxito el presente algoritmo. Asimismo, el protocolo ND permite que "una interfaz descarte los paquetes recibidos dirigidos a una dirección provisional, pero acepta los paquetes de descubrimiento de vecinos relacionados con el método DAD para evaluar la dirección tentativa." (Horley, 2014).

Nota: El método DAD debe aplicarse en todas las direcciones unicast, sin importar si se obtienen a través de la configuración con estado, sin estado o manualmente (capítulo 4). Las direcciones Anycast son la única excepción al método de direcciones duplicadas establecido por el RFC 4862, debido a que son indistinguibles de las unicast.

Antes de que el host proceda con la comprobación de direcciones, su interfaz debe unirse a la dirección multicast de todos los nodos (FF02::1) y a la dirección multicast de nodo solicitado de la dirección provisional. La primera dirección asegura que el nodo recibirá los anuncios de vecino de otros nodos (recibiendo su información local) y el último asegura que dos nodos que intenten utilizar la misma dirección detecten la presencia del otro. Cabe resaltar que dentro de los mensajes vecinos que DAD utiliza, las variables "Tiempo de retransmisión" y "Transmisiones" son fundamentales para completar la operación (ambas pertenecientes a la interfaz que está bajo el presente algoritmo).

Nota: El nombre real de las variables "Tiempo de retransmisión" y "Transmisiones" son "RetransTimer" y "DupAddrDetectTransmits" respectivamente. Únicamente se simplificó su nombre para hacer más fácil su manejo en la descripción del presente algoritmo.

Su funcionamiento es simple, "Transmisiones" es el número de mensajes transmitidos para que se realice la detección de direcciones duplicadas, mientras que la variable "Tiempo de retransmisión" específica el retardo entre las transmisiones de solicitud de vecino realizados, así como el tiempo en el que un nodo debe esperar después de enviar la última solicitud de vecino antes de terminar el proceso de detección de duplicidad.

Asimismo, el mensaje de solicitud vecino establece en su campo "dirección destino" (target address) la dirección provisional de la interfaz, tal y como se describe en el campo del mensaje de solicitud de vecino (tabla 2.8).

En resumen, DAD realiza el siguiente procedimiento para evaluar las direcciones tentativas:

- Una solicitud de vecino (NS) es enviada a la dirección multicast de nodo solicitado con la dirección tentativa que DAD está verificando.
- El host espera un mensaje de respuesta, es decir, un anuncio de vecino en la interfaz.
- Si ningún mensaje de anuncio de vecino es recibido dentro de la transmisión de tiempo especificado, entonces la dirección se considera como única.
- Si un mensaje de anuncio de vecino es recibido dentro de la transmisión de tiempo especificado, entonces la dirección no se considera como única. Por lo cual el host deja el grupo multicast de nodo solicitado, emite un mensaje de consola de dirección duplicada detectada y marca la dirección como no disponible. (IBM, 2013).

Las direcciones unicast de enlace local también deben pasar por el proceso de autenticidad. Por lo tanto, una vez que un nodo determina que su dirección provisional de enlace local es única, el nodo tiene conectividad a nivel IP con nodos vecinos en su determinado enlace local.

2.2.9.7 Detección de Inaccesibilidad de vecino

El algoritmo NUD (abreviación de Neighbor Unreachability Detection) es empleado por IPv6 para tratar de resolver los problemas de accesibilidad (si se presentan) hacia o a través de los vecinos de una red. Dichos inconvenientes pueden ser causados por errores en el hardware, cortes de corriente, actualización o configuración incorrecta en la interfaz, etc.

Este proceso se utiliza para todas las rutas entre hosts y nodos vecinos, incluyendo host a host, host a enrutador y la comunicación de enrutador a host. Del mismo modo, el algoritmo se puede utilizar entre enrutadores, aunque esto no es necesario si se encuentra disponible una alternativa equivalente, por ejemplo, un mecanismo como parte de los protocolos de enrutamiento.

Asimismo, es importante resaltar que un vecino se considera accesible sólo cuando un nodo emisor recibe una confirmación de que los paquetes enviados hacia el nodo destino fueron recibidos y procesados por su capa IP. Esta confirmación se puede determinar de dos maneras:

- Mediante protocolos de capa superior indicando el progreso de la comunicación
- Mediante la recepción de un mensaje de anuncio de vecino en respuesta a una solicitud de vecino

Nota: Es importante tener en cuenta que la definición de accesibilidad no implica la entrega a un nodo remoto a través de un enrutador, sólo al enrutador vecino.

En otras palabras, cuando la confirmación no se reciba a través de los protocolos de capa superior, un nodo enviará mensajes de solicitud de vecino unicast que soliciten anuncios de vecino como confirmación de accesibilidad. Además, para reducir el tráfico innecesario en la red, los mensajes se envían sólo a los vecinos a los que el nodo esté enviando paquetes.

Nota: El RFC 4861 especifica que la Detección de Inaccesibilidad de Vecino se realiza sólo para los vecinos a los que se envían paquetes unicast; no se utiliza cuando se envían a direcciones multicast.

Por ejemplo, en TCP y UDP (ambos protocolo de capa 4) pueden existir diferentes situaciones. Para TCP, la recepción de un acuse de recibo como parte de sus funciones se utiliza como confirmación de que los datos enviados llegaron con éxito. En el caso de UDP, puede que no haya alguna validación de entrega. Por consecuencia, el nodo envía mensajes de solicitud de vecino unicast al vecino del salto siguiente para supervisar de forma continua la posibilidad de acceso al mismo.

Nota: UDP al ser un protocolo no orientado a la conexión no posee funciones de seguimiento y confiabilidad de entrega de los datos como lo efectúa TCP. Por tal motivo, requiere del proceso NUD.

No obstante, la accesibilidad es confirmada cuando el bit "S" o campo nombrado "bandera de solicitud" es establecido a uno en el anuncio de vecino (explicado en la tabla 2.9), indicando que dicho mensaje fue enviado en respuesta a la solicitud. De esta manera, el proceso NUD es capaz de identificar entre los anuncios de vecino no solicitados y el anuncio invocado para la corroboración de accesibilidad.

La recepción de otros mensajes NO solicitados de descubrimiento de vecinos como anuncios de vecino y de enrutador (es decir, con el bit "S" establecido a cero), no son prueba para la confirmación de accesibilidad en el proceso NUD. Únicamente confirma el acceso en una sola dirección, es decir, desde el emisor hasta el nodo receptor. Por el contrario, la recepción de un anuncio que fue solicitado indica que un camino está funcionando en ambas direcciones.

No obstante, el emisor del anuncio solicitado no tiene manera directa de conocer que el anuncio que envía realmente alcanzó a un vecino. Pese a este hecho, desde la perspectiva de la Detección de Inaccesibilidad de Vecino, la confirmación de acceso del nodo que emprende el proceso NUD es el de único interés.

Como último dato, el estado de la caché de vecino de un nodo cambia con base a la posibilidad de acceso hacia un nodo vecino. El RFC 4861 define los siguientes estados para una entrada de caché de vecino:

- **Incompleto:**
  En este estado se lleva a cabo la resolución de direcciones IPv6, en la que se utiliza una solicitud de vecino multicast de nodo solicitado. Dicho estado se especifica cuando se crea una nueva entrada de caché de vecino, pero el nodo aún no tiene la dirección de nivel de enlace correspondiente del nodo vecino. El número de mensajes de solicitud de vecino multicast que se envían antes de abandonar el proceso de resolución de direcciones y quitar la entrada de caché de vecino, se especifica mediante una variable que puede configurarse. El RFC 4861 utiliza el nombre de la variable como MAX_MULTICAST_SOLICIT y se recomienda un valor de 3.

- **Accesible:**
  En este estado, la posibilidad de acceso se ha confirmado al recibir un anuncio de vecino unicast solicitado. La entrada de caché de vecino permanece en estado accesible

hasta que transcurre el número de milisegundos que se indica en el campo “Tiempo accesible” (campo de la tabla 2.11) del anuncio de enrutador.

- **Obsoleto:**
  El estado se presenta cuando el tiempo de posibilidad de acceso (desde que se recibió la confirmación de acceso) ha finalizado. La entrada de caché de vecino pasa al estado obsoleto después de que se anula el valor (dado en milisegundos) del campo “Tiempo accesible” y se mantiene en ese estado hasta que se envía un paquete al vecino. El estado obsoleto también se especifica cuando se recibe un mensaje de anuncio de vecino no solicitado que actualiza una dirección a nivel de enlace.

- **Retardo:**
  Para que los protocolos de nivel superior tengan tiempo de proporcionar una confirmación de posibilidad de acceso antes de enviar mensajes de solicitud de vecinos, el estado de la caché de vecino cambia a retardo y espera durante un período de tiempo que puede ser configurado. En el RFC 4861 se utiliza el nombre de la variable DELAY_FIRST_PROBE_TIME y se recomienda un valor de 5 segundos. Si no se recibe ninguna confirmación de posibilidad de acceso durante el tiempo de retardo, la entrada pasa al estado sondeo y se envía un mensaje de solicitud de vecino unicast.

- **Sondeo:**
  En este estado, la confirmación de posibilidad de acceso está en progreso para una entrada de caché de vecino que se encuentra en los estados Obsoleto y Retardo. Los mensajes de solicitud de vecino unicast se envían a intervalos que corresponden al valor especificado en el campo “Tiempo de retransmisión” en el mensaje de anuncio de enrutador recibido. El número de mensajes de solicitud de vecino que se envían antes de abandonar el proceso de detección de posibilidad de acceso y quitar la entrada de caché de vecino se especifica mediante una variable que puede ser configurada. En el RFC 4861 se utiliza el nombre de la variable MAX_UNICAST_SOLICITS y se recomienda un valor de 3.

2.2.10 IPSec

IPSec (abreviación de IP Security) proporciona servicios de seguridad en la capa IP, permitiendo a un sistema seleccionar los protocolos de seguridad requeridos; determinar el algoritmo (s) que se utilizará para el servicio (s) y para poner en marcha cualquier clave (s) criptográfica (s) necesaria (s) para proporcionar los servicios solicitados.

El conjunto de servicios de seguridad que IPSec puede proporcionar incluye el control de acceso, integridad sin conexión, autenticación del origen de los datos, el rechazo de paquetes repetidos, cifrado y confidencialidad limitada del flujo de tráfico. Debido a que estos servicios se proporcionan en la capa IP, pueden ser utilizados por cualquier protocolo de capa superior, por ejemplo, TCP, UDP, ICMP, BGP, etc. Además, el protocolo puede ser utilizado para proteger uno o más "caminos" entre un par de hosts, entre un par de puertas de enlace de seguridad (security gateway), o entre una puerta de enlace de seguridad y un host.

Nota: El término "puerta de enlace de seguridad" se utiliza para referirse a un sistema intermedio que implementa los protocolos IPSec. Por ejemplo, un router o un firewall. (RFC 2401).

IPSec utiliza dos protocolos para proporcionar la seguridad del tráfico:

1.- Cabecera de autenticación (Authentication Header, AH). Se trata de una cabecera de extensión con un valor de siguiente cabecera igual a 51.

Se encarga de proporcionar la autenticidad de los datos y que se pueden clasificar en dos aspectos:

- Garantizar la autenticidad del origen de los datos. Es decir, los datagramas provienen de un origen específico.
- Los datagramas (y por tanto los datos que contienen) no han sido modificados.

2.- Cifrado de seguridad (Encrypted Security Payload, ESP). Cabecera de extensión con un valor de 52. Garantiza que sólo el destinatario auténtico de los datos pueda descifrar el contenido del datagrama.

Nota: Ambos protocolos se describen con más detalle en sus respectivos RFC's (KA98a, KA98b).

Es importante resaltar que la autenticidad y el cifrado de datos (o datagramas) requieren que tanto el emisor como el receptor compartan una clave, un algoritmo de cifrado/descifrado y una serie de parámetros (como el tiempo de validez de la clave) que diferencian una comunicación segura de otra. Estos parámetros conforman la asociación de seguridad (Security Association, SA) que permite unir la autenticidad y la seguridad en IPSec.

Por otra parte, para una típica sesión de usuario, se pueden llegar a tener distintas asociaciones de seguridad en cada conexión que se establezca (como mucho una por conexión). Por ejemplo, en la descarga de un fichero por FTP, en alguna transacción bancaria, consulta de un e-mail, etc.

Para poder diferenciar dichas asociaciones se utiliza un componente llamado Índice de Parámetros de Seguridad (Security Parameter Index, SPI) que permite (tras recibir un datagrama) saber a qué SA hace referencia y de esta forma poder autenticarlo y/o descifrarlo.

Nota: Al iniciar una comunicación que utilice los servicios IPSec con un único destino (direcciones unicast), este debe comunicar a que índice de parámetros de seguridad (SPI) se debe hacer referencia. De manera semejante, en una comunicación con varios destinos (direcciones multicast o anycast) todos los destinatarios deben compartir el mismo número de índice (SPI).

2.2.10.1 Cabecera de autenticación (AH)

La cabecera de autenticación IP proporciona integridad sin conexión, autenticación del origen de los datos y un servicio de anti-repetición.

Se trata de una cabecera específica de la versión 6 de IP. Normalmente situada justo antes de los datos, de forma que los proteja de posibles atacantes. No obstante, puede incluirse antes de otras cabeceras para asegurar que las opciones que acompañan al datagrama son correctas (imagen 2.54). De esta forma, la presencia de una cabecera de autenticación no modifica el funcionamiento de los protocolos de nivel superior ni el de los enrutadores intermedios, que simplemente encaminan el datagrama hacia su destino.

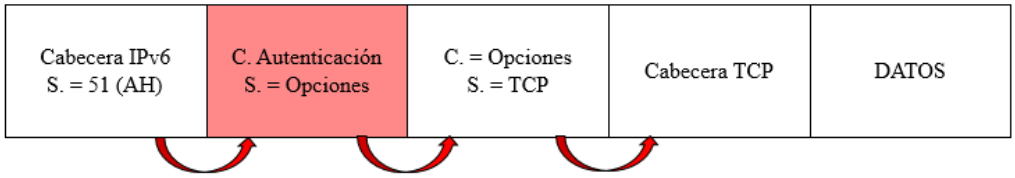


Imagen 2.54 “Ejemplo de cabecera de autenticación en un datagrama”

El formato para esta cabecera es el siguiente:

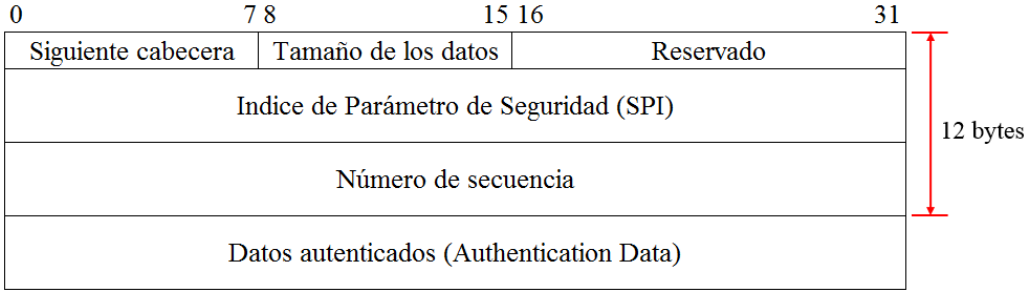


Imagen 2.55 “Formato de cabecera de autenticación (AH)”

Donde:

Tabla 2.13 “Descripción de los campos de cabecera de autenticación (AH)”

Siguiente Cabecera	Valor correspondiente a la siguiente cabecera de extensión. El valor que identifica a la presente cabecera (AH) es 51.
Tamaño de los datos	Especifica la longitud de los datos en palabras de 32 bits (4 bytes)
Reservado	Campo reservado que puede ser definido en un futuro.
Índice de Parámetros de Seguridad (SPI)	Número de 32 bits, permitiendo hasta 2^{32} conexiones de IPSec activas en un mismo ordenador.
Número de secuencia	Identifica el número del datagrama en la comunicación, estableciendo un orden y evitando problemas de entrega de datagramas fuera de secuencia o ataques externos mediante la reutilización de datagramas.
Datos autenticados	Los datos autenticados se obtienen realizando operaciones (dependiendo del algoritmo de cifrar escogido) entre algunos campos de la cabecera IP, la clave secreta que comparten emisor y receptor y los datos enviados.

Nota: El principal problema al autenticar un datagrama es que algunos campos son modificados por los routers intermedios (como el tiempo de vida (TTL) del datagrama, que se va decrementando en una unidad cada vez que pasa por un router), esto hace imposible poder autenticar todo el datagrama, ya que durante su camino por internet es modificado.

Nota: El cálculo de los datos autenticados se realiza mediante un algoritmo de Hash (actualmente se sugiere el algoritmo MD5 puesto que calcula un checksum total de 128 bits).

2.2.10.2 Cabecera de cifrado de seguridad (ESP)

La cabecera de autenticación no modifica los datos que transporta, lo que significa que circula el “texto en claro”. Simplemente añade autenticidad al origen y al contenido, de tal forma que los datos que circulan pueden ser interceptados y visualizados por un eventual atacante. Por otro lado, en caso de necesitar confidencialidad se debe utilizar la cabecera de cifrado de seguridad (ESP).

La cabecera de cifrado de seguridad es siempre la última en el sistema de cabeceras en cadena. Esto es debido a que a partir de la cabecera ESP todos los datos aparecen cifrados. Por lo tanto, los routers intermedios no podrían procesar las cabeceras posteriores (imagen 2.56).

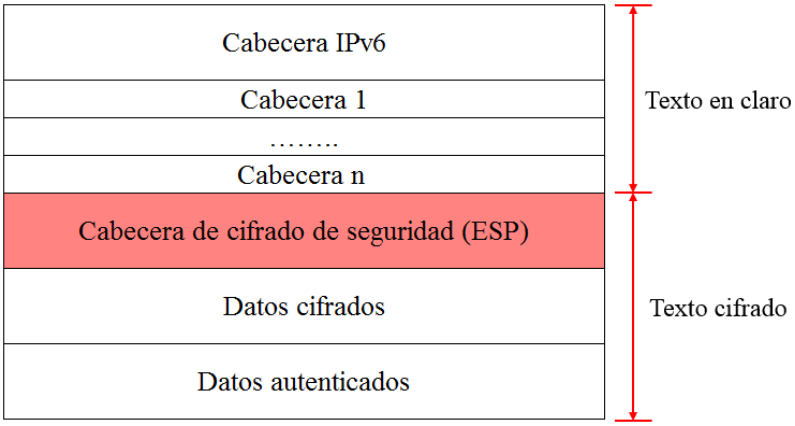


Imagen 2.56 "Ejemplo de posición de cabecera ESP y cifrado de datagrama"

Al igual que con la cabecera de autenticación, el algoritmo a utilizar se negocia con el receptor de la información antes de enviar un datagrama cifrado.

El formato de cabecera de cifrado de seguridad es el siguiente:

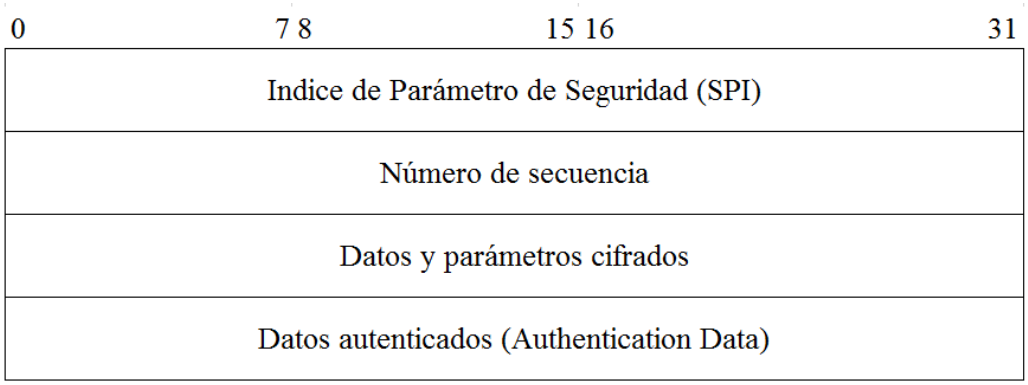


Imagen 2.57 "Formato de cabecera de cifrado de seguridad"

Nota: A diferencia de la cabecera de autenticación, en ESP no es necesario especificar el tamaño de los datos cifrados, ya que a partir de su implementación hasta el final del datagrama todo está cifrado.

El Índice de Parámetros de Seguridad (SPI) y el Número de Secuencia (Sequence Number) tienen el mismo significado que en la cabecera de autenticación (AH).

Los datos autenticados (Authentication Data) aseguran que el texto cifrado no ha sido modificado utilizando un algoritmo de Hash (dependiendo del algoritmo de cifrado escogido).

Asimismo, debido a que tanto la cabecera de autenticación (AH) como la cabecera de cifrado de seguridad (ESP) pueden ser utilizadas independientemente, se recomienda que en caso de ser necesario tanto la autenticidad como la privacidad, se incluya la cabecera de cifrado tras la de autenticación. De tal forma que se autentican los datos cifrados. (Álvares, 2000)

2.2.11 Prefijos de red IPv6

El prefijo de red es una expresión de la dirección IP en la que se conoce la cantidad de bits utilizados para identificar una red.

En IPv4 el prefijo puede expresarse en formato decimal (máscara de subred) y en formato CIDR (Enrutamiento Entre Dominios sin Clases). "La notación CIDR consiste en una barra inclinada al final de la dirección, seguida por el tamaño del prefijo de bits en formato decimal". (Oracle, s.f).

En comparación con la versión 6 del protocolo de internet, el prefijo solamente puede expresarse en la última notación descrita. Ejemplo (tabla 2.14):

Tabla 2.14 "Notación CIDR"

IPv4	
NOTACIÓN	DIRECCIÓN
DECIMAL	255.255.255.0
CIDR	192.168.12.1/24

IPv6	
NOTACIÓN	DIRECCIÓN
CIDR	2001:bd4:abcd:1111::1/64

2.2.11.1 Identificación del segmento de red y de host mediante el prefijo de red

Al igual que las direcciones IPv4 que son conformadas por un segmento de red y un segmento de host, la estructura de las IP's versión 6 utilizan la misma distribución.

Una diferencia sobresaliente entre ambas es la forma de identificación de bloques para cada segmento. Tal proceso en IPv4 es más sencillo ya que existen clases que dividen las direcciones IP en rangos y con base a esas divisiones se establecen los bits de prefijo para cada segmento.

En la tabla 2.15 se pueden visualizar específicamente los datos mencionados.

Tabla 2.15 “División de rangos IPv4”

IPv4					
Clase	Rango de direcciones IP	Mascara de Subred	Prefijo	Segmento de Red	Segmento de Host
A	1-126	255.0.0.0	/8	1er bloque IP	2°, 3er y 4° bloque IP
B	128-191	255.255.0.0	/16	1er y 2° bloque IP	3er y 4° bloque IP
C	192-223	255.255.255.0	/24	1er, 2° y 3er bloque IP	4° bloque IP
D	224-239	RESERVADO PARA MULTICAST IPv4			
E	240-254	EXPERIMENTAL. USADO PARA INVESTIGACIÓN			
DIRECCIÓN IP **127.0.0.0** RESERVADA PARA LOOPBACK					

Es decir, si el primer octeto (bloque) de una dirección IPv4 comienza dentro de un rango entre 1 y 126 (por ejemplo 25.0.0.0) entonces únicamente ese bloque pertenecerá a la porción de red y los tres restantes serán la porción de host ya que tal dirección pertenece a la clase A. De igual manera, el prefijo automáticamente será de ocho bits (/8 en notación CIDR).

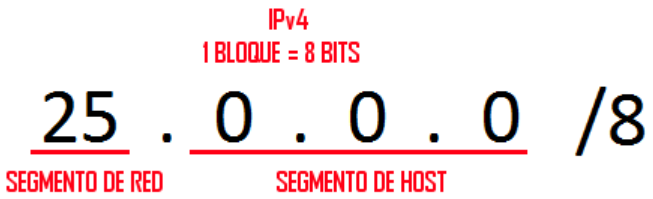


Imagen 2.58 “Notación CIDR IPv4”

Nota: En algunos casos, los prefijos en IPv4 suelen ser variables (VLSM), es decir, los bits que definen la parte de red de la dirección suelen ser de tamaño diferente al que se muestra en la tabla 2.15 a pesar de que la dirección se encuentre dentro del rango de una clase en específico. Ejemplo: Dirección IP: 25.0.0.0, CIDR: 25.0.0.0/17, Mascara de Subred: 255.255.128.0.

Por el contrario, IPv6 no posee clases que faciliten la identificación del segmento de red y de host, por lo que únicamente se determina mediante el tamaño del prefijo. Por ejemplo, si la dirección 2001 : 0bd4 : abcd : 10ef : 12df : 1111 : 01dc : 0001 posee un prefijo /64 la parte de la dirección que identifica el segmento de red será únicamente:

2001 : 0bd4 : abcd : 10ef

Ya que cada bloque que conforma una dirección IPv6 es de 16 bits y el prefijo indica la cantidad de bits que corresponden a la porción de red (imagen 2.59).

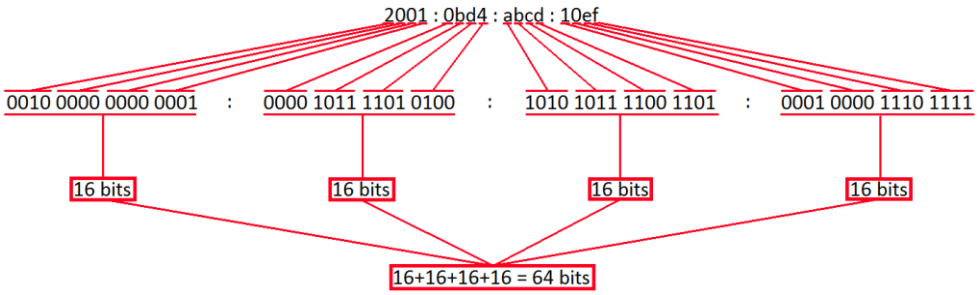


Imagen 2.59 “Conteo de bits para la porción de red”

Por consecuencia, los cuatro bloques restantes de la dirección conformarán el segmento de host. Para ello, el proceso de conteo de bits para dichos bloques se realiza de la misma forma que en la operación anterior (imagen 2.60).

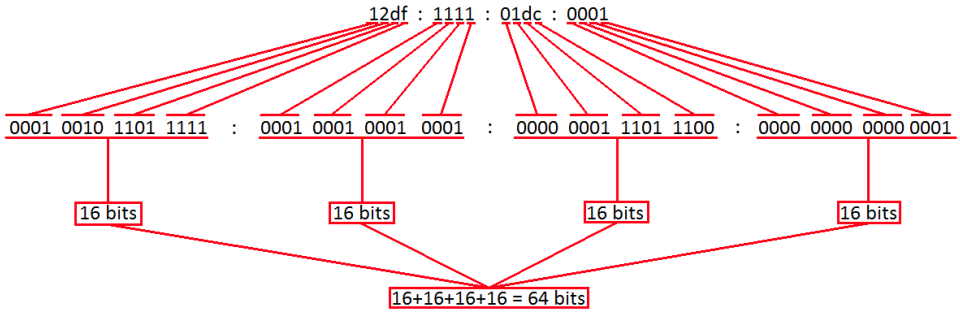


Imagen 2.60 “Conteo de bits para el segmento de host”

Por lo tanto, la identificación de ambos segmentos queda de la siguiente forma:

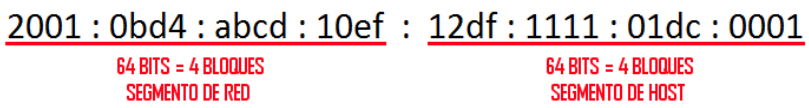


Imagen 2.61 “Segmento de red y de host”

Ejemplo 2

2001 : bd4 : abcd : dbc4 :: 1 / 80

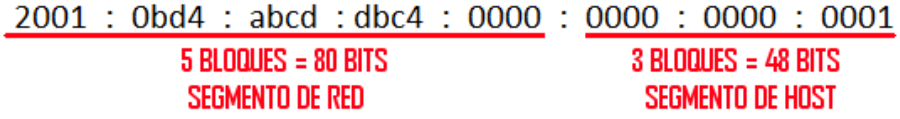


Imagen 2.62 “Identificación del segmento de red y de host mediante el prefijo”

Ejemplo 3

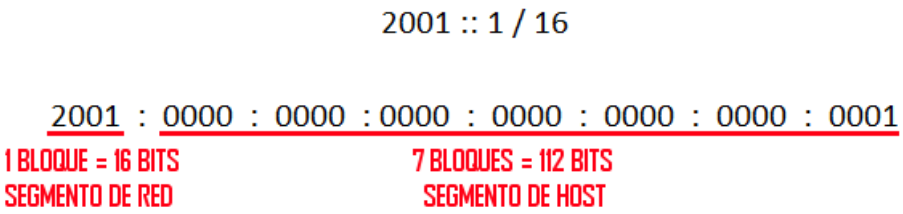


Imagen 2.63 "Identificación del segmento de red y de host mediante el prefijo"

2.2.12 Representación del identificador de red versión 6

Un identificador de red se caracteriza por ser la dirección que representa a un grupo de dispositivos dentro de un segmento de red en particular. Asimismo, al igual que en IPv4 su porción de host debe terminar en ceros.

En IPv6 la forma en que se representa el identificador debe seguir la siguiente secuencia:

1. Dirección IPv6 hasta el bloque o valor hexadecimal indicado por el prefijo de red
2. Colocar doble dos puntos (::) indicando la simplificación de la porción de host.
3. Agregar notación CIDR

Ejemplo:

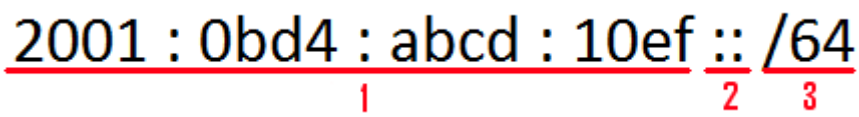


Imagen 2.64 "Dirección de red IPv6"

La dirección IPv6 completa se desglosaría de la siguiente manera:

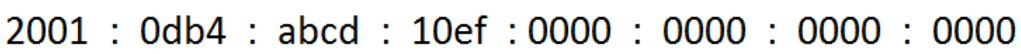


Imagen 2.65 "Dirección IPv6 desglosada"

Lo cual significa que a partir de una dirección de red se podrán asignar IP's hasta llenar los bloques que pertenecen al segmento de host. Ejemplo (imágenes 2.66 y 2.67):

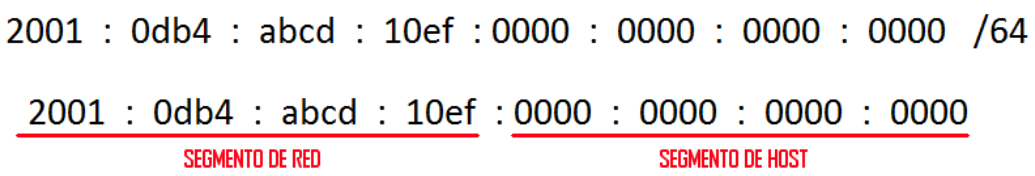


Imagen 2.66 “División de segmentos en la dirección IPv6”

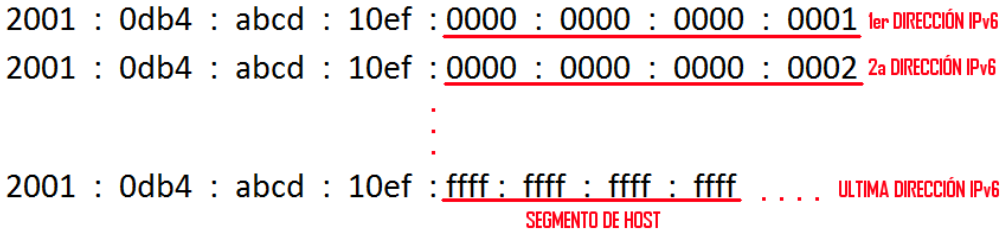


Imagen 2.67 “Direcciones IPv6 utilizables”

La dirección anterior contiene 64 bits libres (bits del segmento de host) para poder asignar direcciones a diferentes dispositivos conectados a la red 2001 : 0db4: abcd : 10ef :: / 64. Es decir, en total existen 18, 446, 744, 073, 709, 551, 616 IP’s disponibles (resultado de la operación 2^{64}). Asimismo, las direcciones asignadas a los dispositivos de la red ya mencionadas pueden escribirse directamente con el prefijo de encaminamiento mediante la notación CIDR. Ejemplo (imagen 2.68):

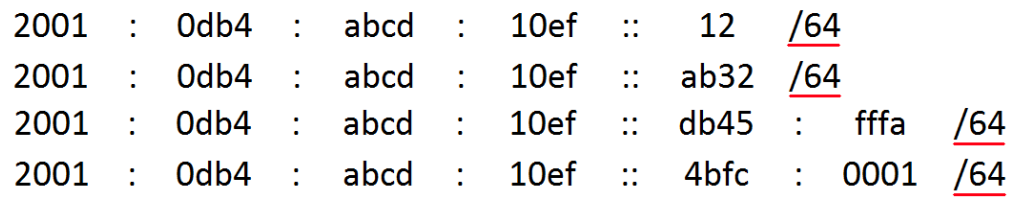


Imagen 2.68 “Direcciones IPv6 con notación CIDR”

2.2.13 Asignación de bits para el direccionamiento IPv6

A pesar de contar con un número bastante significativo de direcciones existentes en el protocolo IPv6, se han llevado acabo prevenciones y reservas con el objetivo de mantener una administración fiable en cuanto a la asignación y uso del espacio de las direcciones (dada la mala experiencia con el protocolo IPv4). Por tal motivo, la Autoridad para la Asignación de Números de Internet (IANA) ha dividido el espacio de direcciones IPv6 en octavos, con el propósito de preservar los espacios libres (actualmente más de la mitad), únicamente habilitándolos cuando las necesidades del protocolo así lo requieran (imagen 2.69).

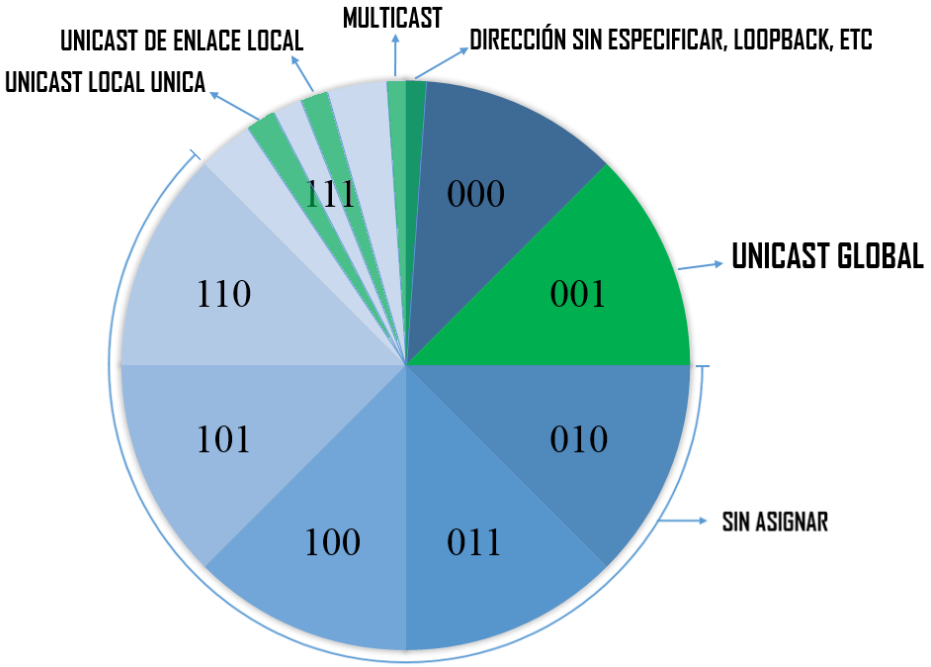


Imagen 2.69 “Espacio de direccionamiento IPv6 utilizado”

Las actuales direcciones unicast globales asignadas por la IANA utilizan el rango de direcciones que inician con el valor binario 001 (2000::/3), el cual es una octava parte del espacio total de direcciones IPv6. Hasta ahora, es el mayor bloque de las direcciones asignadas. Además, existe una gestión para designar los 128 bits de una dirección IPv6 hacia múltiples organizaciones que conforman una jerarquía de transmisión de datos por medio de internet, de manera que se impartan de acuerdo a las escalas existentes (evitando así, espacios de dirección insuficientes), hasta el punto de dejar bits libres de direccionamiento para la manipulación de usuarios finales.

La IANA ha designado a cada uno de los Registros Regionales de Internet (RIR) direcciones con un prefijo de /23. Estas organizaciones se encargan de administrar y registrar los números

de espacios de las direcciones IP dentro de una región concreta (entiéndase este último a un nivel continental).

Cada uno de los RIR's otorgan a cada ISP direcciones con un prefijo de /32 y estos a su vez conceden direcciones con un prefijo de /48 (normalmente a grandes empresas), permitiendo a organizaciones y a usuarios finales tener 16 bits libres para crear hasta 65,536 subredes (2^{16}) y terminar así con un prefijo /64 (imagen 2.70).

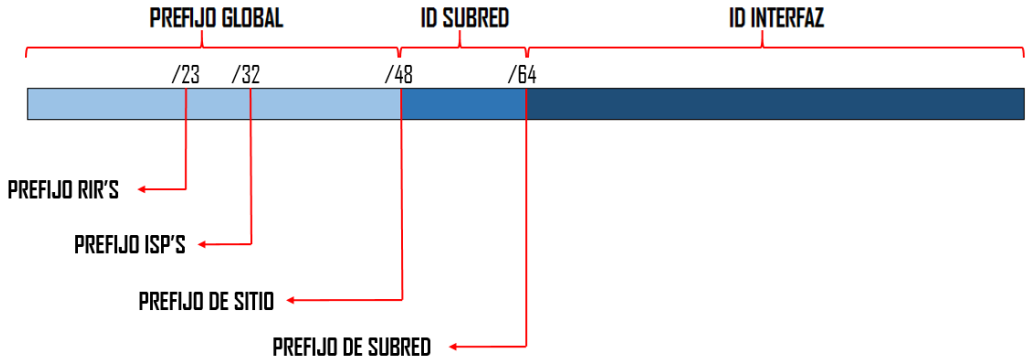


Imagen 2.70 "Asignación de bits jerárquicamente"

Actualmente, los cinco RIR's existentes son ARIN (Norteamérica), RIPE (Europa, Medio Oriente y Asia central), APNIC (Asia y la región Pacífica), AFRINIC (África) y LACNIC (América Latina).

Cabe señalar que en algunas ocasiones los ISP's otorgan a las empresas el prefijo /56, esto debido a que la propia compañía requiere "subnetear" y asignar dicho prefijo a sus sucursales distribuidas, mismas que podrán manipular nuevamente el prefijo para su sitio (teniendo así ocho bits para la operación).

2.2.14 Subredes IPv6

Dentro del ámbito de las redes y especialmente cuando se trata de mantener una administración, integridad y la intención de no desperdiciar direcciones, sin duda existe la necesidad de crear subredes. Por tal motivo, no podría pasar desapercibido ante el protocolo IPv6, siendo estos un método importante para maximizar el espacio de direcciones (reduciendo así, el tamaño de las tablas de enrutamiento) del cual el nuevo protocolo ofrece ya un número considerable.

Como se menciona previamente, el prefijo global (expuesto en la imagen 2.70) compuesto de 48 de los 128 bits de una dirección, son tomados de forma permanente por organizaciones superiores, lo cual hace que dichos bits sean prácticamente intocables. Por tal motivo, las subredes podrán establecerse y manipularse a partir del siguiente bloque de direccionamiento, conformado de 16 bits (de 48 a 64 bits) (imagen 2.71).

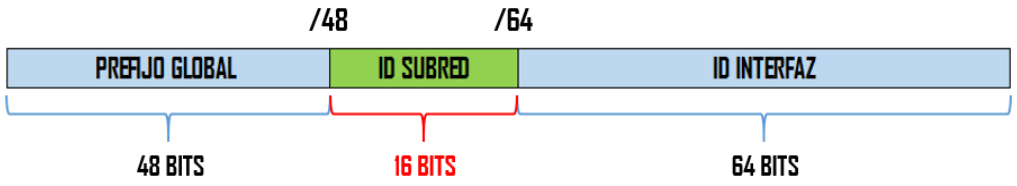


Imagen 2.71 “Bloque para subredes IPv6”

Por ejemplo, si se toma la dirección 2001 : abcd : 0bd4 :: /48, entonces se tiene el último bloque libre para poder crear subredes (imagen 2.72).

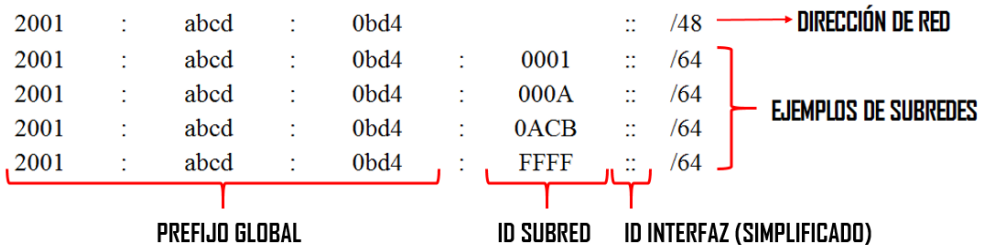


Imagen 2.72 “Ejemplos de subredes IPv6”

2.2.14.1 Subredes en el ID de interfaz (segmento de host).

Aunque se haya establecido únicamente un bloque para subredes IPv6 y este sea relativamente mínimo en comparación con el resto de los bits de la dirección, realmente es una cantidad suficiente para cubrir las necesidades de cada organización. Es decir, se tratan de 16 bits, con el cual se pueden crear 65,536 subredes. Sin embargo el prefijo de subred /48 a /64 puede prolongarse hasta llegar a los 112 bits (tomando finalmente bloques del segmento de host), esto a consecuencia de que un identificador de interfaz puede tener como mínimo 16 bits (imagen 2.73) (Graziani, 2013). Dejando en definitiva, 64 bits para la porción ID de subred (es decir, más del espacio del direccionamiento IPv4 completo).

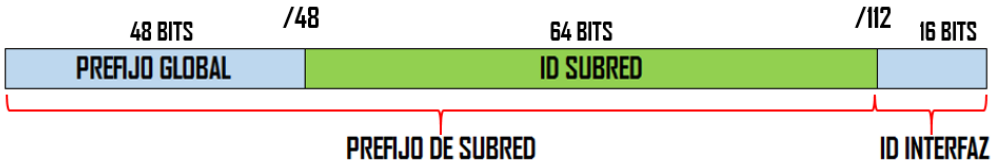


Imagen 2.73 “ID de subred extendido”

Por ejemplo, sí se toma la dirección 2001 : abcd : 0bd4 :: / 48 entonces existen 4 bloques disponibles para establecer subredes. En otras palabras, se pueden crear 18, 446, 744, 073, 709, 551, 616 subredes (2^{64}) (imagen 2.74).

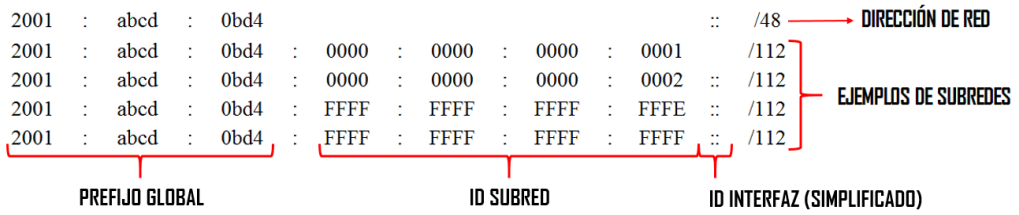


Imagen 2.74 “Ejemplos de subredes extendidas IPv6”

2.2.14.2 Subredes en la frontera de los “nibble”

Habitualmente, los prefijos en IPv6 suelen disminuir o aumentar su tamaño de bits por bloques (16 bits). Por esa razón, ya sea dentro de la WEB (prácticas de laboratorio, ejemplos en una definición, documentos, etc.) u organizaciones que ya tengan implementado el protocolo IPv6, el tamaño de prefijo de subred únicamente varía por 16 bits.

Ejemplos:

Imagen 2.75 “Aumento equivalente de bits del prefijo”

Sin embargo, no existe regla alguna que establezca que la ampliación o reducción de bits deba realizarse únicamente en bloques. La manipulación del prefijo de subred también puede efectuarse en valores hexadecimales, es decir, de cuatro en cuatro bits. A este tipo de aumento se le denomina con el nombre de “nibble”. Por ejemplo, si se encuentra una dirección IPv6 con un prefijo de subred /68, significa que sufrió un aumento de bits conformado por un bloque y finalmente por un nibble (16 + 4). Por lo tanto, serán 20 bits en total para el segmento ID de subred (imagen 2.76).

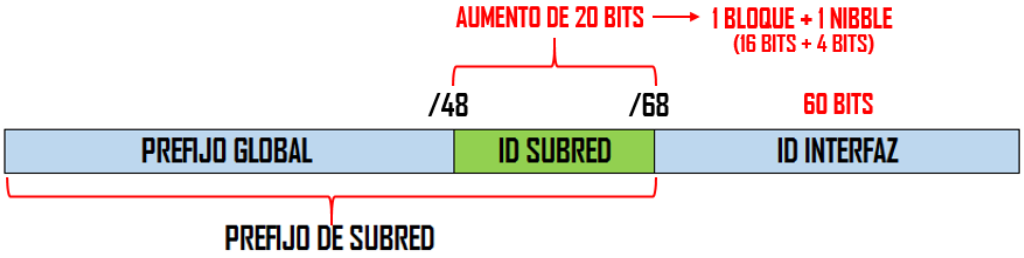


Imagen 2.76 “Aumento de prefijo por un nibble”

Tomando como ejemplo la siguiente dirección, entonces:

2001 : ABCD : 0DB4 : 10AB : 2000 :: /68

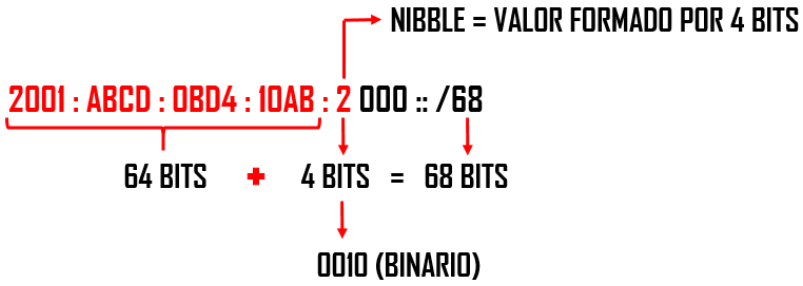


Imagen 2.77 "Dirección IPv6 con un prefijo modificado por un nibble"

Además, se puede determinar que el límite de subred en el nibble es el siguiente:

2001 : ABCD : 0BD4 : 10AB : 2 000 :: /68

HASTA

2001 : ABCD : 0BD4 : 10AB : F 000 :: /68

Imagen 2.78 "Límite de subredes en el nibble"

Por lo tanto, el prefijo límite de subred finalmente será:

2001 : ABCD : 0BD4 : 10AB : F000 :: / 68.

Otros ejemplos de prefijos de subred por aumento de nibble serían /68 /72 /76, etc. (aumento de cuatro en cuatro bits).

No obstante, la ampliación de bits para crear subredes no se limita a ser únicamente en los pares explicados anteriormente. También existen prefijos de subred con valores elevados en diferentes cantidades. El único detalle se remonta en las operaciones requeridas en los nibble para no cometer errores al momento de representar la direcciones y por ende las subredes creadas.

Por ejemplo, en una dirección IPv6 con un prefijo /70 existen un total de 22 bits para el ID de subred (70 – 48 = 22 bits). Es decir, se trata de una cantidad que no puede formarse exactamente con bloques y nibbles, de tal forma que si se deseara crear dicho prefijo con los aumentos descritos anteriormente resultaría de la siguiente manera:

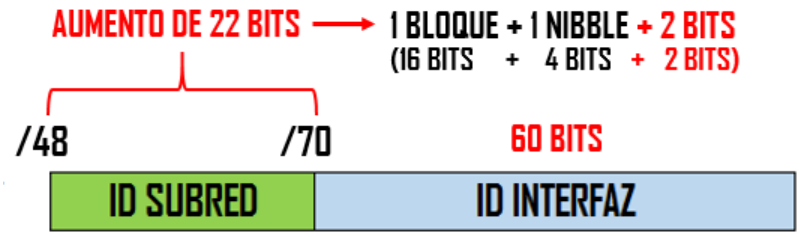


Imagen 2.79 “Formación de prefijo de subred”

Como puede apreciarse, para completar el prefijo de subred /70 se requieren de 2 bits más, por lo que la operación correspondiente será agregar un nuevo nibble pero descompuesto binariamente. Dicha descomposición binaría tiene como objetivo agregar solo los bits faltantes para completar el prefijo de subred deseado. En otras palabras, como el nibble es un valor hexadecimal compuesto de cuatro bits y solo se necesitan dos (en este caso) entonces será necesaria aplicar la operación mencionada.

Algunos ejemplos de descomposición binaria son los siguientes:

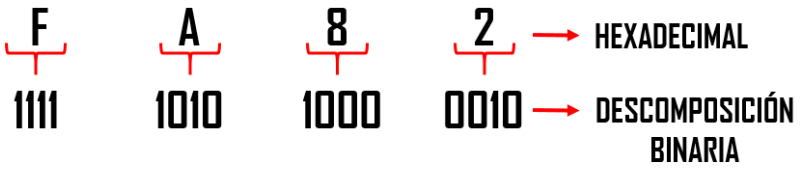


Imagen 2.80 “Valores descompuestos binariamente”

Posteriormente para la creación de las subredes, se debe ubicar el ultimo nibble utilizado (motivo por el cual se le llama límite o frontera de nibble), tomando en cuenta que al aplicarse la descomposición binaria los bits tomados para completar el prefijo de subred serán los de mayor peso y por consecuente serán los que pertenecen a la porción de subred. Por otra parte, los bits restantes del nibble serán los de menor peso y pertenecerán al segmento de host (ID interfaz).

Para finalizar, los valores binarios que pertenecen al segmento de subred en la frontera del nibble serán los únicos que podrán aumentar su valor para crear más subredes. No obstante, al final se tomarán en cuenta los cuatro bits para la representación del nibble en la dirección IPv6, transformando así el valor binario a su correspondiente valor hexadecimal.

Por ejemplo, tomando el mismo prefijo de subred /70 asignado a la dirección 2001 : ABCD : 0BD4 : 0000 : 0000 :: /70, la descomposición binaria y las subredes creadas serán las siguientes:

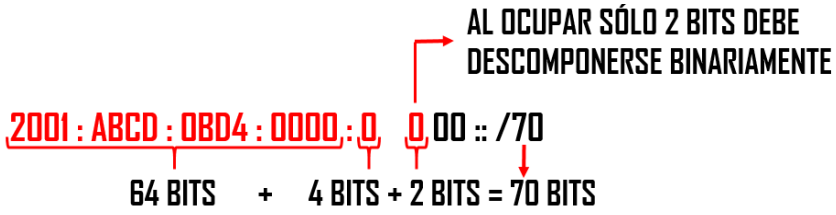


Imagen 2.81 “Identificación del ultimo nibble”

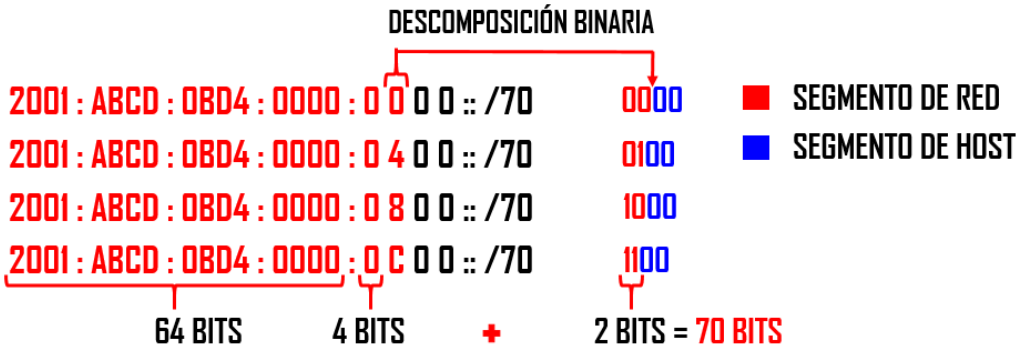


Imagen 2.82 “Subredes creadas en el último nibble”

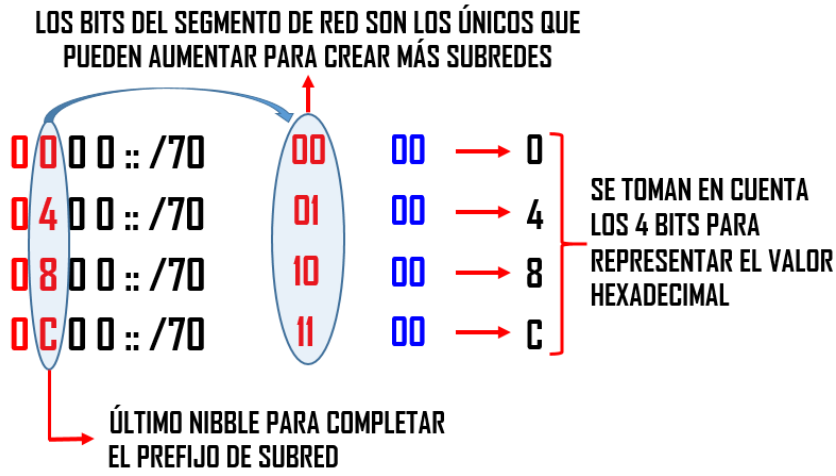


Imagen 2.83 “Representación del nibble”

3. **Norma EUI-64**

La IEEE norma EUI-64 representa un nuevo estándar en el direccionamiento de las interfaces de red. Dicho formato es tomado por el protocolo IPv6 para formar sus identificadores de interfaz (algunos de manera automática y otros manualmente). Para ello, se utiliza la dirección MAC (IEEE 802) de Ethernet de 48 bits.

Las direcciones MAC de Ethernet, por lo general, se representan en formato hexadecimal y constan de dos partes:

- Identificador único de organización (OUI): el OUI es un código de proveedor de 24 bits (seis dígitos hexadecimales) que asigna la IEEE.
- Identificador de dispositivo: el identificador de dispositivo es un valor único de 24 bits (seis dígitos hexadecimales) dentro de un OUI común.

El estándar EUI-64 explica cómo se extienden las direcciones IEEE 802 de 48 a 64 bits mediante la inserción de 16 bits (FFFE) a partir del bit 24 de la dirección MAC. Finalmente, este crea un identificador de interfaz único de 64 bits (imagen 3.1).

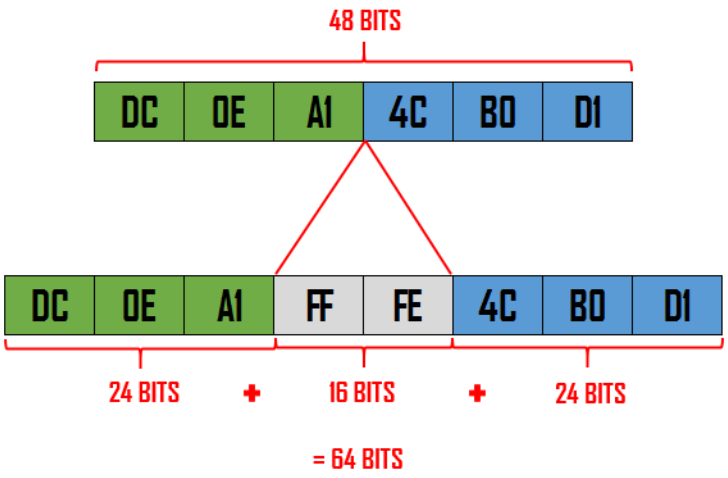


Imagen 3.1 “Inserción de los valores FFFE”

¿Por qué se asignaron los valores FFFE? Como se explica en una publicación de la IEEE para la Autoridad de Registro EUI-64; FFFE es un valor reservado que los fabricantes de equipos no pueden incluir en la asignación de direcciones EUI-64 "reales". En otras palabras, cualquier dirección EUI-64 que tenga los valores descritos seguidamente después de la porción OUI (después del bit 24) puede ser reconocida que ha sido generada a partir de una dirección EUI-48 (dirección MAC). (Stretch, 2008).

3.1 Bit universal/local (U/L)

El séptimo bit de una dirección EUI-48 se denomina como el bit universal/local (también denominado como bit "u"). Este bit identifica si el ID de interfaz es administrado universalmente o localmente.

Dicho bit, en una dirección EUI-48 puede tener alguno de los siguientes valores:

- Bit = 0 → Global
- Bit = 1 → Local

Una dirección administrada universalmente se asigna de forma única a un dispositivo por su fabricante, y una administrada localmente es asignada a un dispositivo por un administrador de red, anulando así su dirección "quemada". Las direcciones administradas localmente no contienen OUI.

Nota: Las direcciones MAC son únicas a nivel mundial, puesto que son escritas directamente en forma binaria en el hardware al momento de su fabricación. Debido a esto, las direcciones MAC son a veces llamadas " direcciones quemadas" (BIA).

Las direcciones únicas a nivel global originalmente asignadas por la IEEE tienen el bit "u" puesto a cero. Del mismo modo, las direcciones creadas localmente, tales como las utilizadas para las interfaces virtuales o una dirección MAC configurada manualmente, tendrán el séptimo bit puesto a uno. Sin embargo, el bit U/L debe invertirse una vez que la dirección EUI-48 se transforma a EUI-64 y se desee utilizar dicho segmento como un ID de interfaz para una dirección IPv6. (Stretch, 2008). Causando finalmente un cambio en el segundo valor hexadecimal y por ende, a toda la dirección (imagen 3.2).

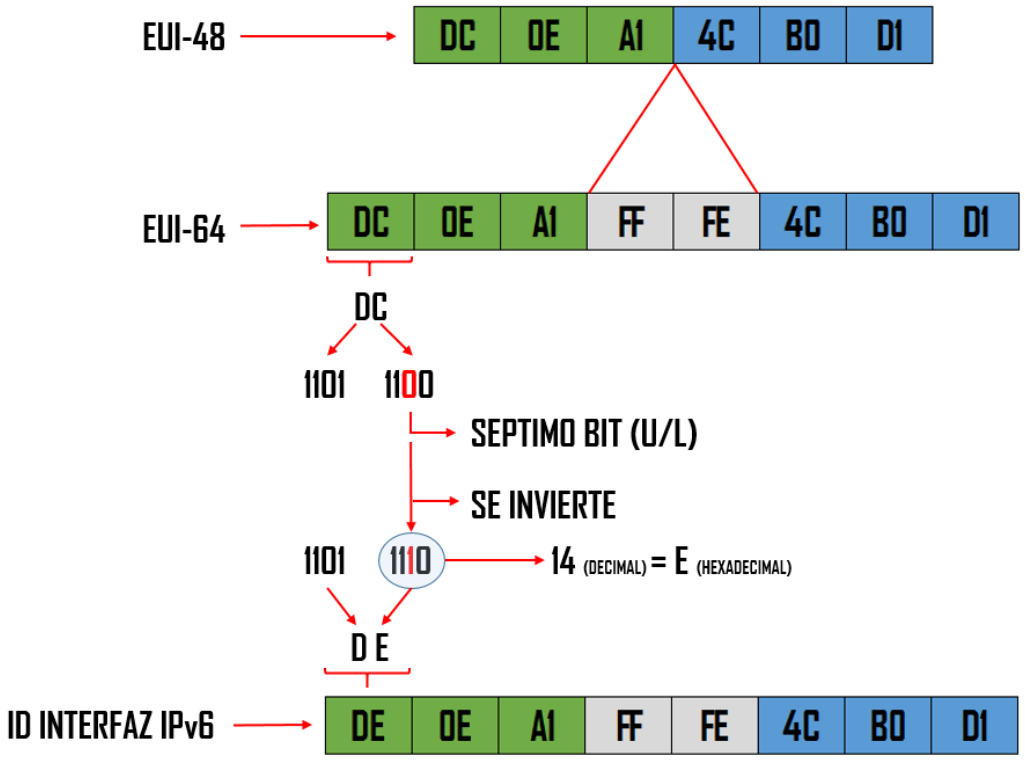


Imagen 3.2 “Inserción de los valores FFFE y transición para un ID interfaz de IPv6”

La motivación para invertir el bit “u” cuando se forma en el identificador de interfaz es para hacer más fácil a los administradores de sistemas configurar manualmente los identificadores de alcances locales cuando los tokens de hardware no están disponibles. Esto se espera que sea el caso de los enlaces seriales, túneles, puntos finales, etc. (RFC 2373).

Nota: Un identificador también puede ser llamado token.

Por ejemplo, si se tienen las siguientes direcciones:

- 0200:0:0:1
- 0200:0:0:2

Al invertir el séptimo bit los valores cambiarían y por ende podrían simplificarse de la siguiente manera:

- 0000:0:0:1 → ::1
- 0000:0:0:2 → ::2

De tal forma que los identificadores son más fáciles de manejar o aprender.

Nota: Tenga en cuenta que las direcciones simplificadas únicamente serán de alcance local.

Una característica a resaltar sobre la norma EUI-64 es que los valores que toma el bit U/L son distintos al EUI-48. Es decir:

Tabla 3.1 "Diferencia de valores entre normas"

BIT U/L	
EUI-48	EUI-64
0 = GLOBAL	0 = LOCAL
1 = LOCAL	1 = GLOBAL

La parte importante a recordar es que a causa de la alteración del séptimo bit hace que el alcance de la dirección nunca cambie. Las direcciones globales seguirán siendo globales y las direcciones locales seguirán siendo de alcance local. De manera que dicha modificación del bit U/L se invierte para mantener una correlación. Por lo tanto, tomando como ejemplo la siguiente dirección MAC:

- 00-0C-29-C2-52-FF

Y utilizando EUI-64, las normas conducen que la dirección sería:

- 00-0C-29-**FF-FE**-C2-52-FF

Si dicha dirección debe seguir siendo local, la notación IPv6 quedaría de la siguiente forma:

- 0**0**0C:29FF:FEC2:52FF → ::C:29FF:FEC2:52FF

Sin embargo, si la dirección es global, el formato correcto es:

- 0**2**0C:29FF:FEC2:52FF

La ventaja de EUI-64 es que se puede utilizar la dirección MAC de Ethernet para determinar el ID de interfaz. También permite que los administradores de red rastreen fácilmente una dirección IPv6 a un dispositivo final mediante la dirección MAC única. Sin embargo, esto generó inquietudes con respecto a la privacidad a muchos usuarios, por lo que les preocupa que los paquetes puedan ser rastreados a la PC física real. Debido a estas inquietudes, en lugar de ocupar el algoritmo EUI-64 se puede utilizar una ID de interfaz generada aleatoriamente (tema 4.1.2 página 92).

3.2 Bit individual/grupal (I/G)

El bit I/G es el bit de menor orden del primer byte de un ID de interfaz IPv6 y determina si la dirección es individual (unicast) o una dirección grupal (multicast).

Cuando se establece en 0, se trata de una dirección unicast y cuando se establece en 1 es una dirección multicast.

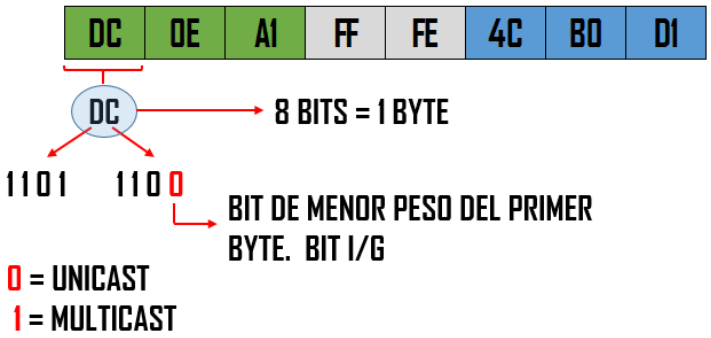


Imagen 3.3 “Identificación del bit I/G”

Para un típico adaptador de red de dirección 802.x, ambos bits U/L e I/G se establecen en 0, correspondiente a la dirección MAC unicast administrada universalmente.

4. **Autoconfiguración en IPv6 (RFC 2462)**

La autoconfiguración es el conjunto de pasos por los cuales un host decide como configurar automáticamente sus interfaces en IPv6. Entre las etapas de dicho proceso, incluye la configuración de la dirección de enlace local y la verificación de su singularidad en un enlace. Además determina qué información debe ser configurada automáticamente, como las direcciones IP, información adicional, o ambos, y en el caso de solo direcciones, si deben ser obtenidos a través de un mecanismo sin estado (también denominado "stateless", "sin intervención" o "SLAAC"), mediante un mecanismo de estado ("stateful") o ambos.

4.1 Configuración automática de direcciones sin estado (Stateless)

La configuración automática sin estado no requiere de una configuración manual de los host, de alguna configuración compleja en los routers y no requiere de servidores adicionales.

Este proceso permite que un host genere sus propias direcciones utilizando una combinación de información local e información anunciada por los routers (anuncios de enrutador o RA). Los enrutadores anuncian los prefijos que identifican a la subred (es) asociado con un enlace, mientras que los host generan un ID de interfaz de forma aleatoria (random ID) o a través de la norma EUI-64 para identificar a una interfaz en una subred. El resultado es una dirección IPv6 formada mediante la combinación de ambos. En caso de la ausencia de routers, un host sólo puede generar direcciones de enlace local. Sin embargo, estas direcciones son suficientes para permitir la comunicación entre los nodos conectados al mismo enlace.

Nota: El método de generación aleatoria de un identificador de interfaz (random ID) se describe en el tema 4.1.2 "Direcciones temporales IPv6", página 92.

Los nodos (ambos, hosts y enrutadores) comienzan el proceso de la configuración automática generando una dirección de enlace local para la interfaz. Esta dirección se forma añadiendo el identificador de interfaz a él bien conocido prefijo de la dirección unicast de enlace local (fe80::/10). Esto puede suceder a partir de cualquiera de los siguientes eventos:

- La interfaz se inicializa en el momento que inicia el sistema
- La interfaz es reiniciada después de un error de interfaz temporal o después de haber sido inhabilitada temporalmente por el administrador del sistema.
- La interfaz es conectada a un enlace por primera vez.
- La interfaz es habilitada por la administración del sistema después de haber sido inhabilitada administrativamente.

Además de esto, el protocolo realiza el procedimiento para generar las direcciones locales de sitio (unicast locales únicas o ULA) y las unicast globales. Sin embargo, como se mencionó en el tema de "Detección de Direcciones Duplicadas", antes de que cualquier interfaz pueda establecer de forma permanente cualquier dirección IPv6, debe pasar por dicho proceso.

Curiosamente, en la autoconfiguración sin estado la singularidad de una dirección está determinada principalmente por su generación a partir de un identificador de interfaz. Por tal motivo, si un nodo ya ha verificado la singularidad de su dirección de enlace local, las direcciones adicionales creadas a partir del mismo identificador de interfaz no necesitan ser verificados individualmente. No obstante, por razones de seguridad, el método DAD es aplicado a todas las direcciones sin importar que el identificador de enlace local haya sido comprobado. Únicamente, el método proporciona la opción de desactivar su operación en una interfaz (RFC 7527).

Por el contrario, todas las direcciones, obtenidas manualmente o por medio de la configuración automática de direcciones con estado (tema 4.2, página 92) deben ser verificadas para su autenticidad individualmente. En caso de que en un nodo determine que su dirección provisional de enlace local no es única, la configuración automática se detiene y requerirá de la configuración manual de la interfaz. Para simplificar la recuperación en este caso, debería ser posible para un administrador suministrar un identificador de interfaz alternativo que reemplace el predeterminado. Además, las direcciones derivadas del mismo identificador también deberán ser configuradas manualmente.

Para la generación de las direcciones unicast globales y de unicast de sitio, los host envían un mensaje RS (Router Solicitation) al router. El mensaje se envía a la dirección IPv6 multicast de todos los routers (FF02::2) y el enrutador devuelve un mensaje RA (Router Advertisement) anunciando el prefijo y su longitud correspondiente del segmento local. Este paquete es enviado a la dirección multicast IPv6 de todos los nodos (FF02::1). Posteriormente, los nodos generan automáticamente sus identificadores de interfaz utilizando el método random o la norma EUI-64. Finalmente, SLAAC combina ambos segmentos para generar las direcciones IPv6. Sin embargo, antes de que estas direcciones puedan ser establecidas en una interfaz deben pasar por el algoritmo DAD.

Nota: El proceso SLAAC que se especifica en esta sección se aplica solamente a los hosts y no a los enrutadores. Como la configuración automática de direcciones de los host utiliza la información que es anunciada por los routers, estos deben ser configurados por otro medio.

Nota: Un requisito que SLAAC necesita para poder realizar sus operaciones correctamente es que el prefijo anunciado sea /64. Es la única manera de permitir que un host genere automáticamente un ID de interfaz a través del método random o EUI -64. (Horley, 2014).

4.1.1 Tiempo de vida de una dirección IPv6

Después de que una dirección IPv6 ha sido verificada como única, ésta es cedida a una interfaz durante un tiempo predefinido. Es decir, las direcciones tienen asociado un tiempo de vida que indican durante cuánto tiempo estará vinculada dicha dirección a una determinada interfaz. Cuando el tiempo de vida expira, la vinculación se invalida y la dirección puede ser reasignada a otra interfaz en cualquier punto de internet. Por tal motivo, las direcciones IP en su versión 6 no son permanentes y comúnmente se les conoce como “alquiladas”.

Para gestionar la expiración de los enlaces, una dirección pasa a través de dos fases diferentes mientras está asignada a una interfaz. Inicialmente, una dirección es preferida o privilegiada (prefered), lo que significa que su uso no está restringido. Posteriormente, la dirección es desaprobada o en desuso (deprecated) anticipando que el vínculo actual asociado a su interfaz será anulado.

Una dirección en desuso debe continuar siendo utilizada como dirección de origen en las comunicaciones ya existentes, pero no debe ser usada en las nuevas comunicaciones si una dirección alternativa (es decir, otra que no esté en desuso) está disponible y tiene un alcance suficiente.

IP y las capas superiores (por ejemplo, TCP y UDP) deben continuar aceptando los datagramas destinados a una dirección en desuso, puesto que una dirección en este estado sigue siendo una dirección válida para la interfaz. Una implementación puede prevenir cualquier nueva comunicación con una dirección en desuso, pero la gestión del sistema debe tener la capacidad de desactivar este tipo de instalaciones y, la instalación debe ser desactivada por defecto.

Nota: Una dirección de enlace local tiene un tiempo de vida infinito preferido. Es decir, nunca expirará.

Nota: La renumeración de una interfaz consiste en pasar de una dirección a otra. Durante este proceso, no es aconsejable cambiar repentinamente de dirección, de lo contrario, todas las comunicaciones TCP que utilizan dicha dirección como identificador de conexión se cortarían inmediatamente. Esto conllevaría importantes perturbaciones a nivel de las aplicaciones.

Por ello, para facilitar la transición se implementó un mecanismo de obsolescencia que invalida gradualmente una dirección. Este mecanismo se sirve de la capacidad de la asignación de varias direcciones válidas a una misma interfaz. Para elegir la dirección a utilizar, se le asocia un estado que indica en qué fase de su tiempo de vida se encuentra con respecto a la interfaz.

A continuación se presentan los estados por los que una dirección IPv6 debe pasar:

- **Válido:** En este punto, se trata de una dirección que ha aprobado su singularidad y de la cual el tráfico puede ser enviado y recibido. Las direcciones auto configuradas tienen una duración válida asignada por el router.
- **Preferido:** En este estado, una dirección puede usarse para nuevas comunicaciones. Las direcciones auto configuradas también tienen un periodo de vida preferente asignado por el router.
- **Desuso** Una dirección en desuso aún es válida. Sin embargo no puede utilizarse para establecer nuevas comunicaciones.
- **Inválida:** Se trata de una dirección en la que el nodo ya no puede enviar o recibir tráfico. Una dirección entra en el estado inválido después de que el periodo de vida válido expira.

Imagen 4.1 “Estados de una dirección IPv6”

4.1.2 Direcciones temporales (ID de interfaz aleatorio)

Como una alternativa a las configuraciones previamente expuestas para generar los identificadores de interfaz IPv6 de forma permanente, existe la operación de las direcciones temporales.

Este método brinda un anonimato más seguro a los nodos conectados a una red. Por ejemplo, si el identificador de interfaz se basa siempre en la dirección EUI-64 (como se deriva de la dirección física IEEE 802 y por lo tanto es estática) es posible identificar el tráfico de un nodo específico independientemente del prefijo, lo que facilita el seguimiento de un usuario en particular y su uso de internet. Para solucionar dicho problema y proporcionar una mayor seguridad, se tiene la opción de utilizar el identificador de interfaz IPv6 formado de manera aleatoria y que cambia con el tiempo.

Las direcciones temporales se generan para los prefijos de direcciones públicas que utilizan la configuración automática de direcciones sin estado (SLAAC). Además, después de que expire el tiempo de vida válido de una dirección temporal, se genera un nuevo identificador de interfaz para dicha dirección IP.

Nota: Las direcciones temporales se vuelven a generar en un determinado tiempo. Esto dependiendo de los temporizadores establecidos en el mensaje RA local (RFC 3041).

Nota: Los sistemas configurados IPv6 en Windows Vista, Windows Server 2008 y versiones posteriores utilizan direcciones temporales por defecto.

4.2 Configuración automática de direcciones con estado (Stateful)

En la autoconfiguración con estado el host obtiene las direcciones de la interfaz y la configuración de información a través de un servidor (DHCPv6). Dichos servidores, mantienen una base de datos con las direcciones que han sido asignadas a cada host. Sin embargo, los dos tipos de autoconfiguración pueden complementarse entre sí. Por ejemplo, un host puede usar la autoconfiguración sin estado para configurar sus propias direcciones y usar la autoconfiguración con estado para obtener el resto de los parámetros.

Cabe resaltar que cada tipo de configuración posee algunas diferencias. Es decir, la configuración automática sin estado se emplea cuando un sitio no necesita que las direcciones

de los host sean exactas, con tal de que sean únicas y correctamente enrutables. Por otra parte, la configuración automática con estado se utiliza cuando un sitio requiere de un control más estricto sobre las asignaciones de direcciones exactas.

Tanto la configuración automática de direcciones sin estado y con estado pueden ser utilizados simultáneamente. Únicamente, el administrador del sitio debe especificar qué clase de configuración automática usar mediante el establecimiento de los campos apropiados en los mensajes de anuncios de enrutador.

Por ejemplo, un host envía una o más solicitudes de enrutador al grupo multicast de todos los enrutadores. Dichos mensajes contienen dos banderas, la primera llamada "Managed address configuration" (configuración de dirección administrada) que indica si los host deben utilizar la autoconfiguración con estado para obtener las direcciones. La segunda bandera "Other stateful configuration" (otra configuración con estado) indica si los host deben utilizar la autoconfiguración con estado para obtener información adicional. Por otro lado, los enrutadores responden con mensajes RA especificando el tipo de configuración automática que un host debe realizar.

Notas:

- Ambas banderas pueden identificarse también como el bit M para la "configuración de dirección administrada" y el bit O para "otra configuración con estado".
- **S**i el bit M se establece, el indicador O es redundante y puede ser ignorado porque DHCPv6 devolverá toda la información de configuración disponible. La información que presenta el bit O son datos relacionados con el DNS e información en otros servidores dentro de la red.
- Todas las direcciones obtenidas manualmente o por medio de la configuración automática de direcciones con estado deben ser probados para su unicidad individual (método DAD).
- El tipo de método establecido como predeterminado para generar los identificadores de interfaz variará según el tipo de S.O y su versión que el host tenga instalada.
- La configuración automática sin estado también contiene información adicional dentro de los mensajes RA. Datos como el prefijo de subred para el enlace, el límite de saltos y el tiempo de vida de la dirección.
- SLAAC es la opción de autoconfiguración de direcciones por defecto en los routers de Cisco. Tanto el indicador M como el indicador O se establecen en 0 en un mensaje RA.

La configuración automática stateless ha sido diseñada con los siguientes objetivos previstos:

- No se recomienda realizar alguna configuración manual de los dispositivos antes de conectarlos a la red. En consecuencia, se necesita un mecanismo que permita a un host obtener o crear direcciones únicas para cada una de sus interfaces. La configuración automática de direcciones asume que cada interfaz puede proporcionar un identificador único para cada interfaz.
- Los pequeños sitios que consisten en un conjunto de equipos conectados a un único enlace no requieren la presencia de un servidor (stateful) o un router como un requisito para comunicarse. Para poder obtener características de tipo "Plug & Play", se logra mediante el uso de direcciones de enlace local.

- En el caso de un sitio grande con múltiples redes y routers, tampoco debería requerir la presencia de un servidor de configuración de direcciones con estado. Con el fin de generar las direcciones locales de sitio o globales, los host deben determinar los prefijos que identifican las subredes a las que se conectan. Los enrutadores generan mensajes periódicos de que incluyen las opciones de lista del conjunto de prefijos activos en un enlace.
- La configuración de direcciones debe de facilitar la renumeración de los dispositivos. Esto se logra mediante el préstamo de las direcciones de las interfaces y el establecimiento de múltiples direcciones hacía una misma interfaz. El tiempo de vida del "préstamo" es el mecanismo por el que un sitio renuevan dichos identificadores. Al poder disponer de varias direcciones simultáneamente, permite que la transición no sea interrumpida, permitiendo que ambas, la vieja y la nueva dirección den continuidad a la comunicación durante el período de transición.
- Los administradores de sistemas necesitan la capacidad de especificar qué mecanismo (stateless, stateful, o ambos), deben ser usados. Los mensajes de anunciación de los routers (RA) incluyen unos indicadores (banderas o flags) para realizar esta función.

Los pasos básicos para la autoconfiguración una vez que la interfaz ha sido activada, son:

a) Se genera la dirección "tentativa" de enlace local, como se ha descrito previamente.
b) Verificar que dicha dirección pueda ser asignada (es decir, que no esté duplicada en el mismo enlace).
c) En caso de estar duplicada, la autoconfiguración se detiene, y se requiere un procedimiento manual (por ejemplo, usando otro identificador de interfaz).
d) En caso de no estar duplicada, la conectividad a nivel IP se logra, al asignarse definitivamente dicha dirección "tentativa" a la interfaz en cuestión.
e) Si se trata de un host, se interroga a los posibles routers para indicar al host lo que "debe de hacer a continuación".

5. IPv6 información adicional

5.1 Implementación de IPv6 en IOS Cisco System.

Los routers Cisco Sytems actualmente soportan IPv6 en la versión Cisco IOS software 12.2 (22)S y posteriores. Al igual que soportan cualquier protocolo de enrutamiento dinámico como RIPng, OSPFv3 y EIGRP para IPv6 (EIGRPv6).

Además de los routers, los switches Cisco actualmente también soportan IPv6. Cisco se centra en habilitar IPv6 en todas sus plataformas de hardware de próxima generación para permitir a los clientes y socios una transición segura a IPv6.

Dicho soporte, se lanzó en el año 2001, desde entonces, el software operativo Cisco del sistema permite el despliegue de producción de IPv6 a través de los siguientes dispositivos de Cisco:

Tabla 5.1"Dispositivos Cisco con soporte IPv6"

Sistema Operativo Cisco	Implantación de dispositivos
Cisco IOS-XR	• Cisco CRS/1 • Cisco 12000 Series
Cisco IOS-XE	• Cisco ASR 1000 Series
Cisco IOS Release 12.4M	• General production
Cisco IOS Release 12.4T	• Technology development
Cisco IOS Release 12.28x	• Cisco Catalyst switches • Cisco 7x00 and 10000 Series
Cisco NX-OS	• Nexus 7000
Cisco SAN-OS	• MDS9500

Nota: La tabla anterior no contiene la lista completa de todos los dispositivos que actualmente soportan IPv6. Para asegurar que el dispositivo maneja IPv6 únicamente se debe verificar la versión de IOS Cisco 12.2 en adelante.

5.2 ¿NAT para IPv6?

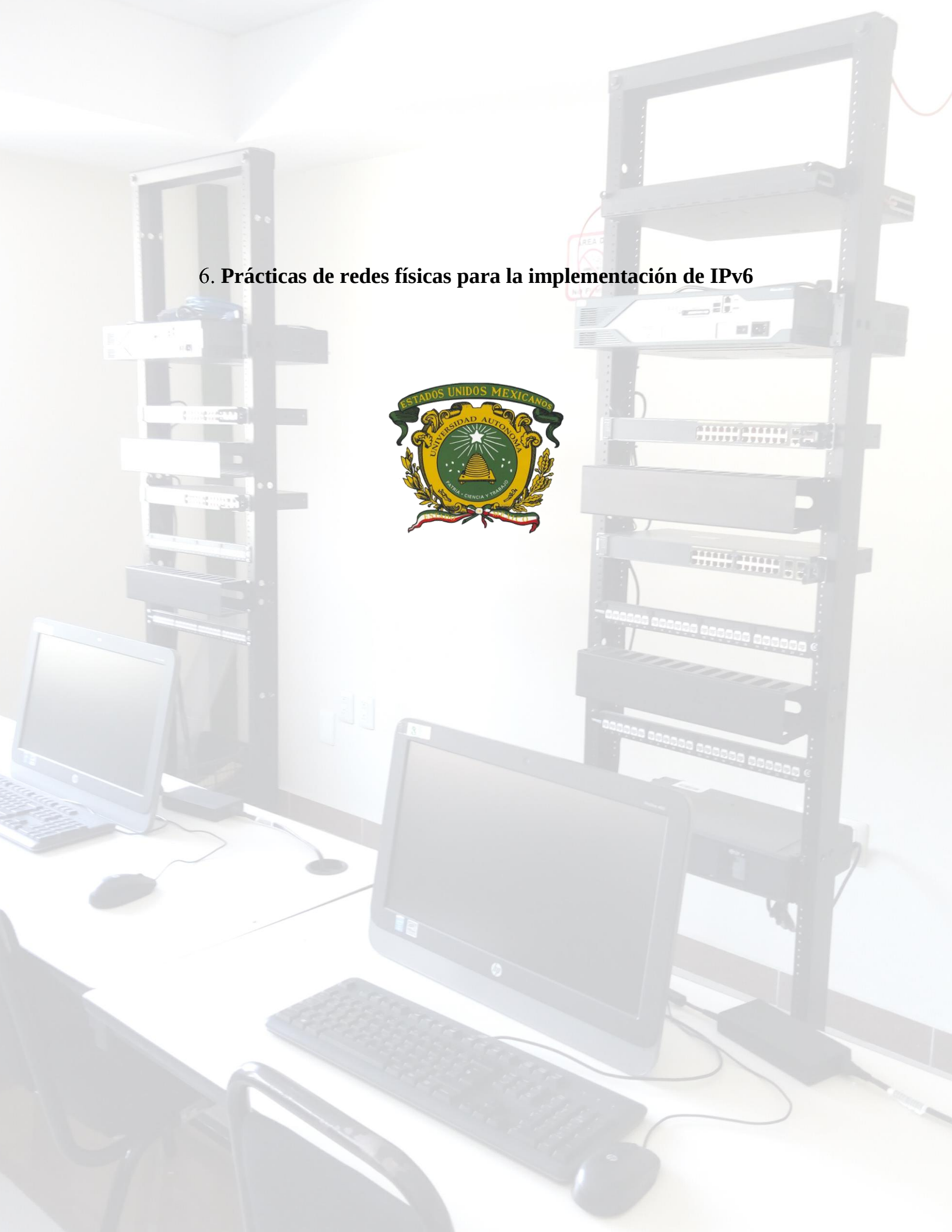
IPv6 fue desarrollado con la intención de hacer innecesario NAT para IPv4 con su traducción entre direcciones IPv4 públicas y privadas. Sin embargo, IPv6 implementa una forma de NAT.

Dicho proceso en IPv6 se usa en un contexto muy distinto al de NAT para IPv4. Las variedades de NAT para IPv6 se usan para proporcionar acceso de manera transparente entre redes de solo IPv6 a redes de solo IPv4 y viceversa. No se utiliza como forma de traducción de IPv6 privada a IPv6 global.

Lo ideal es que IPv6 se ejecute de forma nativa siempre que sea posible. Es decir, que dispositivos IPv6 se comuniquen entre sí a través de redes IPv6. No obstante, para colaborar en el cambio de IPv4 a IPv6, el IETF elaboró varias técnicas de transición que admiten una variedad de situaciones entre las dos versiones de IP, como dual-stack, tunneling y traducción.

La NAT para IPv6 no se debe usar como una estrategia a largo plazo, sino como un mecanismo temporal para contribuir a la migración de IPv4 a IPv6. Con el correr de los años, existieron varios tipos de NAT para IPv6, incluida la traducción de direcciones de red/traducción de protocolos (NAT-PT). El IETF dejó en desuso NAT-PT en favor de su reemplazo, NAT64. (Cisco System. Inc., s.f)

6. **Prácticas de redes físicas para la implementación de IPv6**



6.1 Configuración básica del protocolo IPv6 en un entorno Cisco para la implementación de una red física de área local.

Objetivo:

- Comprender y configurar los parámetros básicos del protocolo IPv6 sobre los dispositivos fundamentales que componen una red de área local.
- Implementar las operaciones básicas IPv6 para la configuración de los host con un sistema operativo Windows 8.

Nota: La realización de esta práctica también funciona sobre el S.O Windows 7. Las diferencias solo radican en las imágenes mostradas a lo largo del documento.

Para el desarrollo de la práctica es esencial contar con los siguientes dispositivos:

- 1 Router
- 2 Switch
- 4 Cables de red con configuración directa (cualquiera, T568-A o T568-B)
- 2 Computadoras (mismo S.O)
- 1 Cable de consola para la configuración remota de un enrutador

En este caso, específicamente el hardware utilizado fue el siguiente:

- 1 Router Cisco 2821 (2800 series)
- 2 Switch Cisco Catalyst 2960
- 2 Computadoras con Windows 8
- 4 Cables de red con configuración directa T568-B
- 1 Cable de consola DB9 a RJ45

La estructura que conforman los dispositivos es el mismo que se muestra en la imagen 6.1.

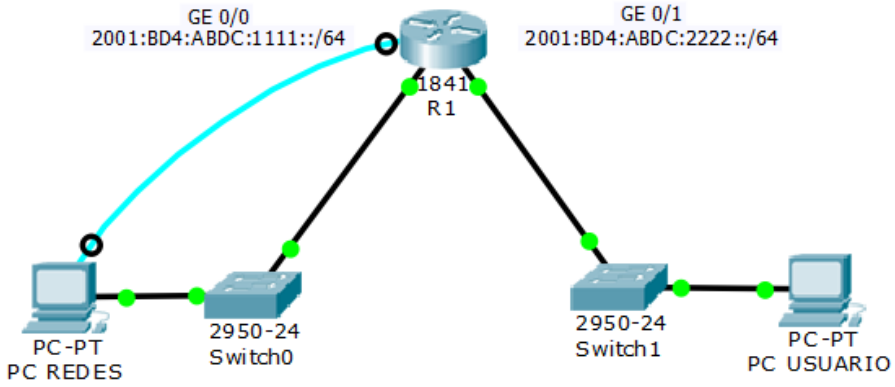


Imagen 6.1 “Diagrama de topología”

La red que se muestra en el diagrama de topología contiene una red utilizando IPv6 donde puede visualizarse el conjunto de dispositivos conectados y descritos anteriormente.

Su conexión forma dos subredes de área local (LAN) y sus respectivas direcciones son las siguientes:

Tabla 6.1 “Tabla de direccionamiento”

DISPOSITIVO	TIPO DE INTERFAZ	NÚMERO INTERFAZ	DIRECCIÓN IPv6
R1	Gigabitethernet (GE)	0/0	2001 : BD4 : ABCD : 1111 :: 1
	Gigabitethernet (GE)	0/1	2001 : BD4 : ABCD : 2222 :: 1
PC Redes	NIC	N/A	2001 : BD4 : ABCD : 1111 :: 2
PC Usuario	NIC	N/A	2001 : BD4 : ABCD : 2222 :: 2

Las conexiones físicas deberán ser idénticas a las imágenes que se muestran a lo largo de la práctica.

Los cables de red con configuración directa (cables negros en la imagen 6.1) deben ir conectados cada uno por un extremo a los puertos del router que se ubican en la parte trasera (generalmente esa es su ubicación), identificando que la placa posea un grabado como “FE0/0” y “FE0/1” (fastethernet) o los más actuales como lo es en este caso “GE0/0” y “GE0/1” (gigaethernet). Tal como se muestra en las imágenes 6.2 y 6.3.

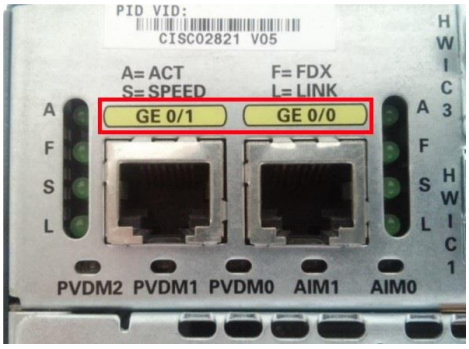


Imagen 6.2 “Puertos GE del enrutador”

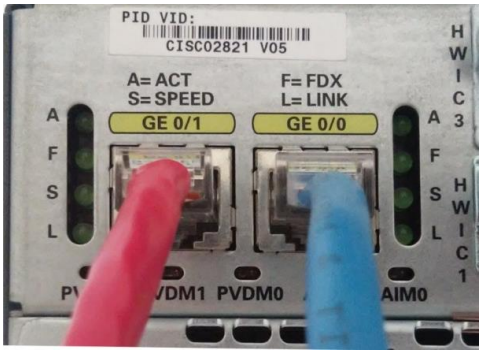


Imagen 6.3 “Cables de red conectados a los puertos”

El otro extremo de ambos cables debe ir en un puerto de cada switch ubicado en la parte frontal (imágenes 6.4 a 6.7).

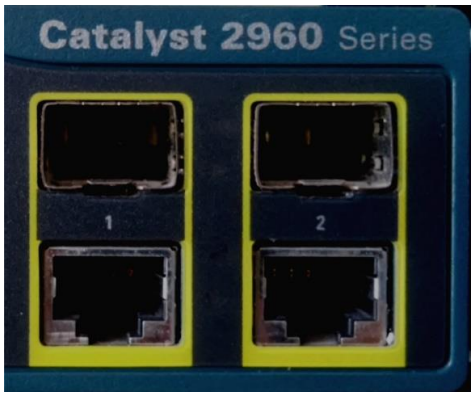


Imagen 6.4 “Puertos Switch 1”

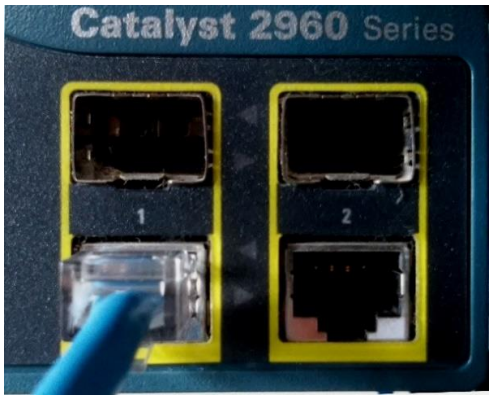


Imagen 6.5 “Cable de red conectado al Switch 1”

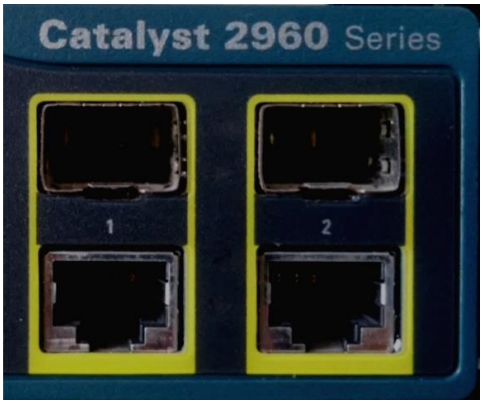


Imagen 6.6 “Puertos Switch 2”

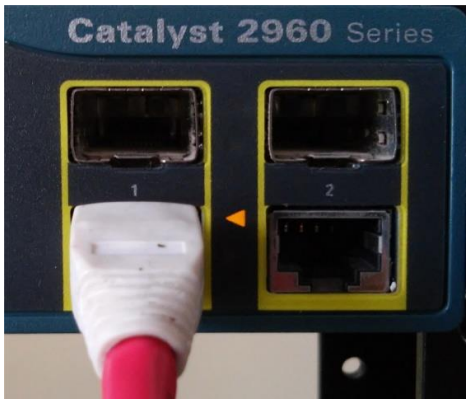


Imagen 6.7 “Cable de red conectado al Switch 2”

Los dos cables de red restantes deben ser conectados por un puerto de cada switch del panel frontal hacia una computadora (imágenes 6.8 y 6.9).

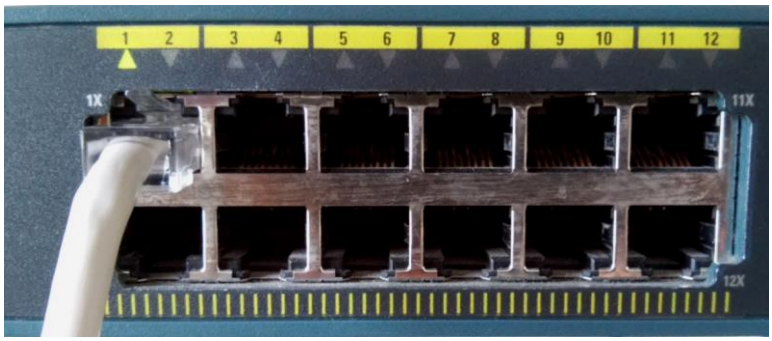


Imagen 6.8 “Puertos del switch para host”

Imagen 6.9 “Cable de red conectado al host”

Para finalizar, el cable de consola (cable azul en el diagrama de topología) debe ir conectado en el puerto RJ-45 del router (ubicado en la parte frontal), mismo que tiene grabado la palabra “CONSOLE”. Asimismo, el segundo extremo debe ir en el puerto DB9 (también conocido como COM) de la computadora que configurará el enrutador (imágenes 6.10 y 6.11).

Imagen 6.10 “Puerto de consola en el router”

Imagen 6.11 “Cable de consola al host”

En este caso, no hay relevancia en cuál de los dos host sea conectado el cable. Cualquier computadora puede realizar posteriormente la configuración.

Una vez conectados todos los dispositivos se descargará un software para hacer conexiones de tipo telnet (conexión para acceder a una computadora y manejarla de forma remota.) llamado “Hyperterminal”. Dicho programa se utiliza para conectarse a otros dispositivos independientes de una computadora por medio de la tarjeta serial (tarjeta con el puerto DB9).

Una PC con Hyperterminal proporciona un teclado y un monitor para configurar el router.

La forma más básica de acceder a un router para comprobar o modificar su configuración es conectar el puerto de consola del mismo con un cable con configuración 568-B y utilizar Hyperterminal.

Actualmente Hyperterminal no se encuentra incluido en los S.O's más recientes. Particularmente en Windows, fue instalado hasta su versión "XP" por lo que su descarga debe ser manual en la web en caso de tener un S.O más actual.

Una vez instalado el software se ejecutará y probablemente aparezca la ventana como se muestra la imagen 6.12.

Se dará clic en el botón "no" y aparecerá la ventana "Información de la ubicación" (imagen 6.13)

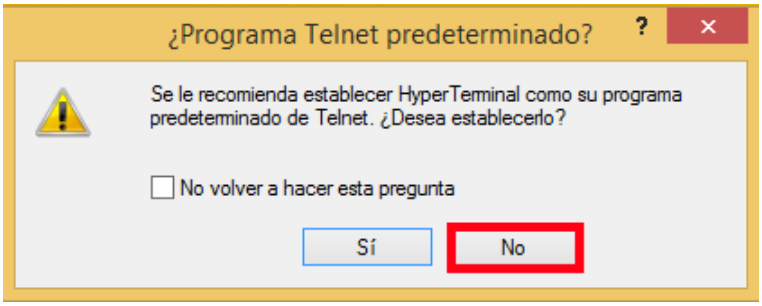


Imagen 6.12 "Conexiones Telnet"

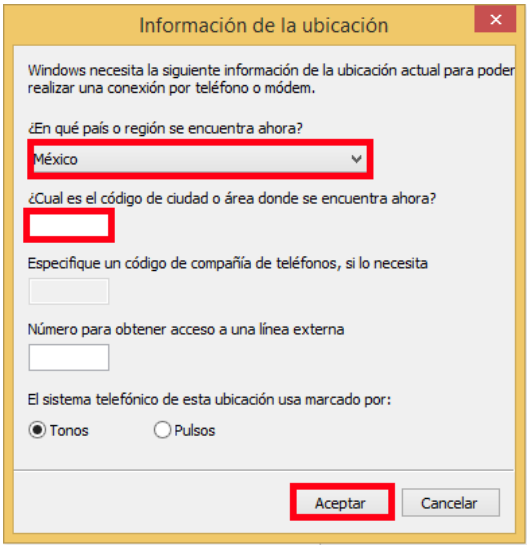


Imagen 6.13 "Información de la ubicación"

Los parámetros a colocar dependen (como su nombre lo indica) de la ubicación en el que se encuentre el operador. Sin embargo, solo es necesario colocar el país o región y el código de ciudad o área.

Posteriormente dar clic en “Aceptar”.

Nota: Los pasos parar iniciar el programa Hyperterminal pueden variar de acuerdo a ejecuciones previas o la versión instalada.

En la siguiente ventana se seleccionará “Mi ubicación” y se dará clic en “Aceptar”.

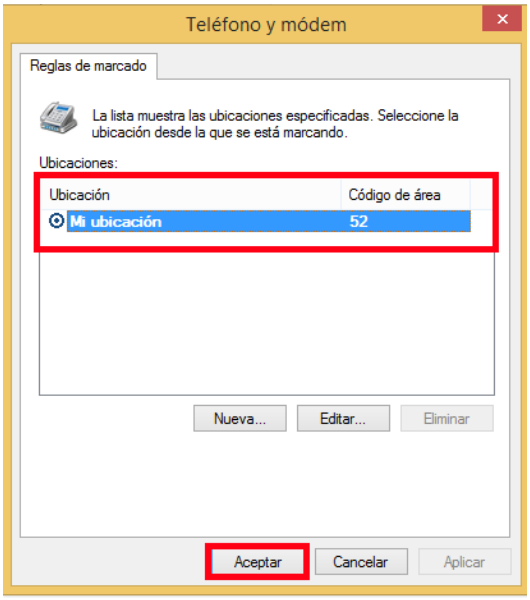


Imagen 6.14 “Mi ubicación”

Al salir la ventana sucesiva se dará clic en “no”.

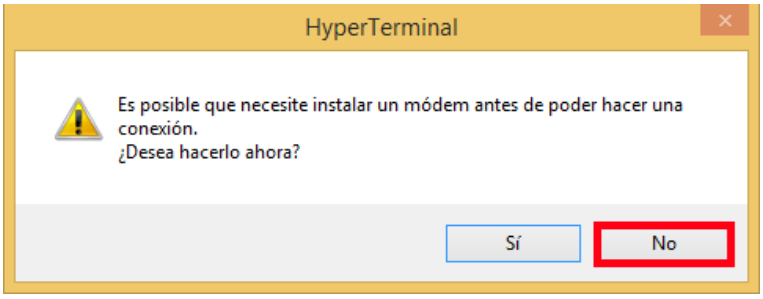


Imagen 6.15 “Requerimientos de conexión”

Posteriormente en la ventana “Descripción de la conexión” (imagen 6.16) se debe capturar un nombre y un icono (cualquiera en ambos casos) para proceder con la conexión.

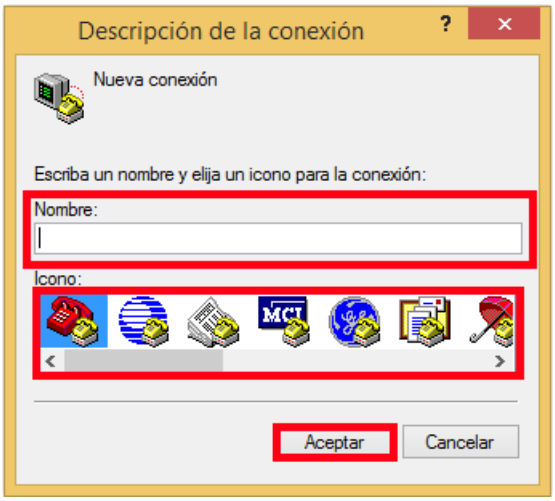


Imagen 6.16 “Nombre e icono de la conexión”

Al aparecer la ventana “conectar a” (imagen 6.17) se verificará que en la lista desplegable (habilitada) se encuentre seleccionado el parámetro “COM1” (siglas del puerto del host conectado al router).

Clic en “aceptar”.

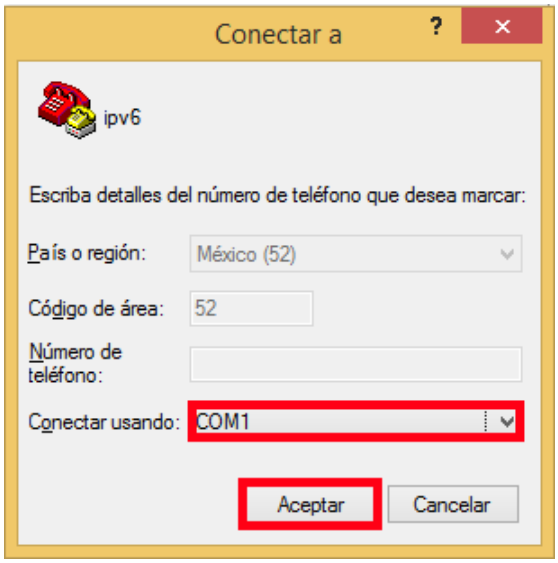


Imagen 6.17 “Conectar al puerto COM1”

Para proceder con la práctica, los valores de la ventana “Propiedades COM1” deben ser los mismos que se muestran en la imagen 6.18.

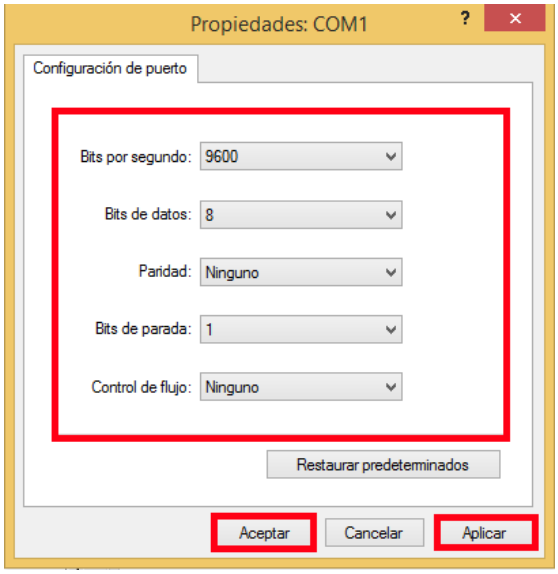


Imagen 6.18 “Parámetros del puerto COM1”

Se dará clic en “Aplicar” y posteriormente “Aceptar”.

Tras haber realizado todos los pasos anteriores, aparecerá la ventana con el nombre de la conexión que anteriormente se introdujo (imagen 6.19). Esto indica que se ha establecido la conexión al router con éxito.

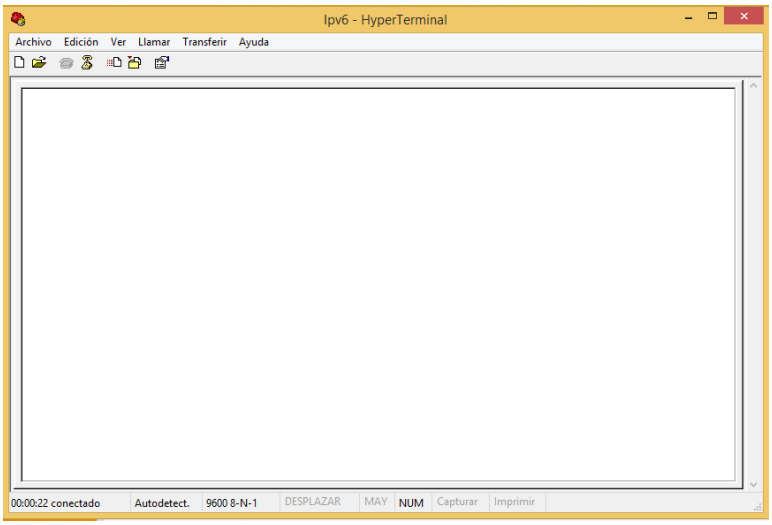


Imagen 6.19 “Conexión establecida”

Pasado unos cuantos segundos, se visualizará un código que indicará la carga del router (carga de configuración, memoria NVRAM, reconocimiento de tarjetas, etc.). En esta etapa se debe esperar unos minutos hasta que se muestre lo siguiente:

% Please answer 'yes' or 'no'.

Se escribirá ***no*** y se presionará "intro".

Nota: En adelante el texto capturado por el usuario se mostrará en ***negritas y cursiva***.

Would you like to enter the initial configuration dialog? [yes/no]: ***no***
Press RETURN to get started!

Cuando el código deje de aparecer en pantalla se pulsará nuevamente "intro" hasta que se muestre el indicador principal (imagen 6.20) lo que señala que el router está listo para configurarse.

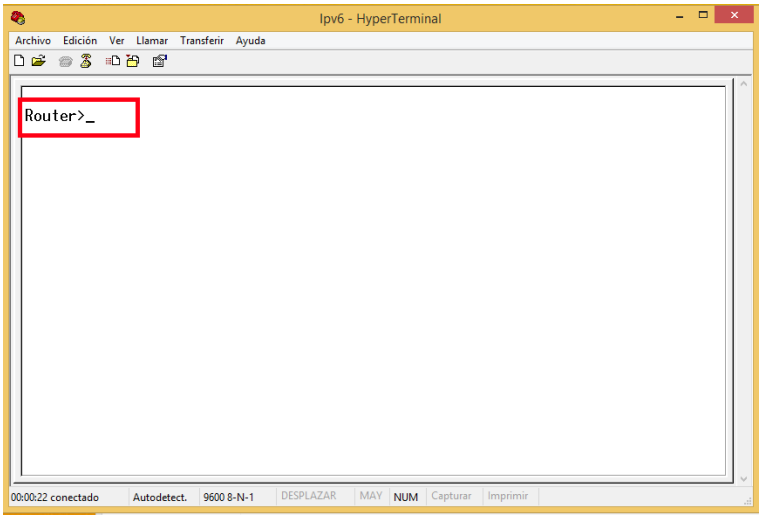


Imagen 6.20 "Comando principal. Router listo para configurarse"

Antes de llevar a cabo cualquier operación, se debe verificar que el router no contenga ninguna configuración previa a otras prácticas. Para ello, se debe ingresar a modo privilegiado mediante la captura del texto ***enable*** y posteriormente el comando ***show run***. Tal como se muestra a continuación:

*Router>**enable***
*Router#**show run***
Building configuration...
Current configuration: 926 bytes
!
version 12.4

service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
!
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
--More--

Toda la información que se muestre debe ser desplazada presionando la tecla "intro", buscando atentamente el siguiente código (resaltando a color lo más importante):

interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/3/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/3/1

no ip address
shutdown
!
ip forward-protocol nd
no ip http server

Nota: En adelante de la presente y posteriores prácticas, el código mostrado mediante el comando "***show run***" se reducirá únicamente a las interfaces ocupadas.

El código anterior muestra los parámetros que existen dentro de las interfaces del router, tal como el tipo (serial, fastethernet o gigaethernet), numero de interfaz, IP asignada, etc.

Para concluir que no existe alguna configuración previa dentro del dispositivo, se debe corroborar principalmente la nula asignación de direcciones en las interfaces mediante la línea de código "*no ip address*" ubicada después del nombre de cada interfaz del enrutador. No obstante, el resto del código debe verse igual que en la forma anterior, de lo contrario el router debe ser reiniciado. (Si no existe configuración previa saltar a la hoja 110).

Para realizar dicho reinicio en el router, se debe acceder a modo privilegiado y escribir los comandos siguientes:

Router# ***erase startup-config***
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

Presionar "intro" para confirmar

[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Ahora capturar lo siguiente:

Router# ***reload***
Proceed with reload? [confirm]

Presionar "intro" para confirmar la operación de reinicio y esperar a que el router restaure sus valores predeterminados.

El proceso habrá finalizado cuando en pantalla se muestre el indicador principal "***Router>***".

Posteriormente, se configura el nombre del enrutador y se asignan las direcciones IPv6 a sus respectivas interfaces (véase la tabla 6.1). Para ello, se debe capturar lo siguiente:

Router#
*Router#**configure t***
Enter configuration commands, one per line. End with CNTL/Z.
*Router(config)#**hostname R1***
*R1(config)#**ipv6 unicast-routing***

La última línea del código anterior es de suma importancia, ya que de no introducirla antes de configurar cualquiera de las interfaces del router estas no podrán reconocer los paquetes IPv6 recibidos. Es decir, "De forma predeterminada, el tráfico de reenvío IPv6 está desactivado en un router Cisco. Por lo cual debe ser activado entre las interfaces con el comando de configuración global." (ComputerNetworkingNotes, s.f). De lo contrario no existirá comunicación mediante IPv6 aunque las computadoras estén dentro del mismo segmento del router.

Asimismo, cuando se configure algún protocolo de enrutamiento para IPv6, este comando debe introducirse antes de cualquier otra configuración.

Ahora se escribirá lo siguiente:

*R1(config)#**interface gigabitethernet 0/0***

Nota: Para corroborar que hubo acceso a la interfaz con éxito el indicador principal debe verse como "*R1(config-if)#".*

*R1(config-if)#**ipv6 address 2001:bd4:abcd:1111::1/64***
*R1(config-if)#**no shutdown***
*R1(config-if)#**exit***
R1(config)#
**Aug 27 19:37:55.107: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up*
**Aug 27 19:38:51.719: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up*

En las tablas 6.2 y 6.3 se explican el código anterior.

Tabla 6.2 "Comandos Cisco de la práctica 6.1"

Código	Descripción
interface gigabitethernet 0/0	Indica que la interfaz a configurar es de tipo gigabitethernet Número de interfaz ingresada

Es muy importante identificar qué tipo de tecnología contienen las interfaces del router, ya sea Fastethernet o Gigabitethernet, ya que de eso depende el tipo de texto que debe capturarse para entrar a la interfaz del hardware correctamente.

Tabla 6.3 "Comandos Cisco de la práctica 6.1"

Código	Descripción
ipv6 address	Indica que la dirección que se ingresará es de tipo IPv6
2001:bd4:abcd:1111::1/64	Dirección IPv6 asignada
no shutdown	Habilita la interfaz con los datos previamente ingresados
exit	Permite salir de la interfaz configurada

Tras haber escrito la última línea y después de haber pasado unos segundos, aparecerá la siguiente información:

**Aug 27 19:37:55.107: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up*
**Aug 27 19:38:51.719: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up*

Este código indica que la interfaz ha sido correctamente habilitada, y para corroborar dicho evento se visualizará físicamente en la parte posterior del router. Es decir, los leds del puerto configurado deben estar encendidos, tal como se muestra en las imágenes 6.21 y 6.22.

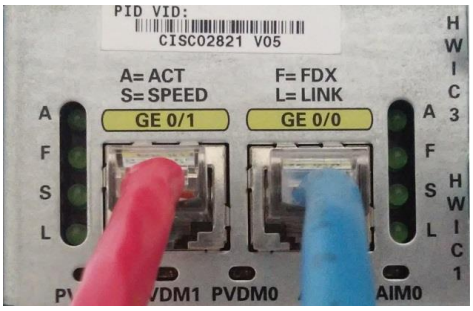


Imagen 6.21 "Interfaces desactivadas"

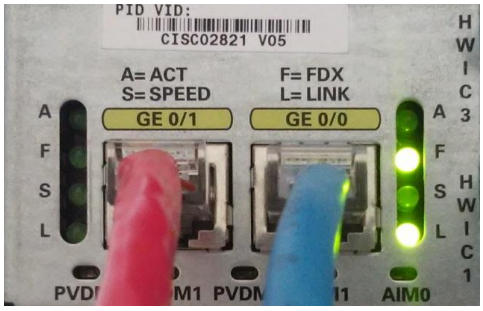


Imagen 6.22 "Interfaz GE0/0 activada"

Para configurar la siguiente interfaz, es decir la gigabitethernet 0/1, se hará de la misma forma que en la anterior, excepto que el número de puerto cambia y por ende su dirección.

*R1(config)#**interface gigabitethernet 0/1***
*R1(config-if)#**ipv6 address 2001:bd4:abcd:2222::1/64***
*R1(config-if)#**no shutdown***
R1(config-if)#
**Aug 27 19:41:04.471: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up*

**Aug 27 19:38:51.719: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up*

De igual manera, se verifica que haya sido correctamente habilitada (imagen 6.23).

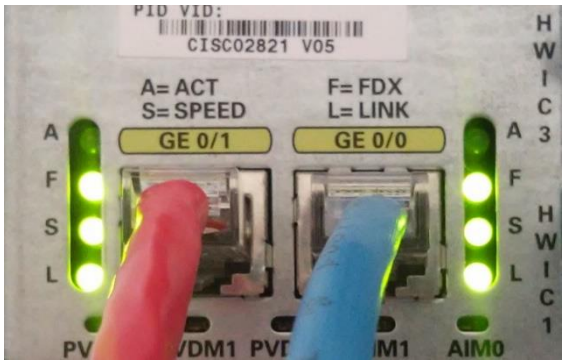


Imagen 6.23 "Interfaz GE0/1 activada"

Consecutivamente, se debe salir de la configuración de las interfaces y del modo global capturando el comando ***exit*** o de igual forma con el comando ***end*** (este último sale de cualquier nivel de configuración, dejando al operador en modo privilegiado).

*R1(config-if)#**exit***
*R1(config)#**exit***

Además, si se desea guardar los cambios realizados se captura el comando ***copy run start*** y a continuación un "enter" para confirmar, tal como se muestra en el siguiente código:

*R1#**copy run start***
Destination filename [startup-config]?
Building configuration...
[OK]
R1#

Nota: Existen otros comandos para guardar una copia de seguridad de la configuración hecha en un router. La diferencia entre ellas radica solo en la solicitud de confirmación.

Se han terminado de configurar las subredes en el router, ahora se realizará una prueba para verificar que cada PC conectado en su respectiva subred tenga comunicación con el otro. Para hacerlo posible, se hará una operación popular en el área de redes conocido como "ping".

PC Redes

Para poder completar la prueba de conexión y comunicación, es necesario configurar los host correspondientes de la presente práctica. Particularmente, en esta etapa se realizan las modificaciones en la PC denominada “Redes”.

Como primer paso, se deben conocer las direcciones IP asignadas del presente host. Para ello, se abrirá el símbolo del sistema de Windows, ya sea pulsando las teclas “Windows+R”, escribir ***cmd*** y dar clic en “aceptar” o dar clic en “inicio” y escribir en el buscador ***símbolo del sistema***. La ventana que debe aparecer es la siguiente:

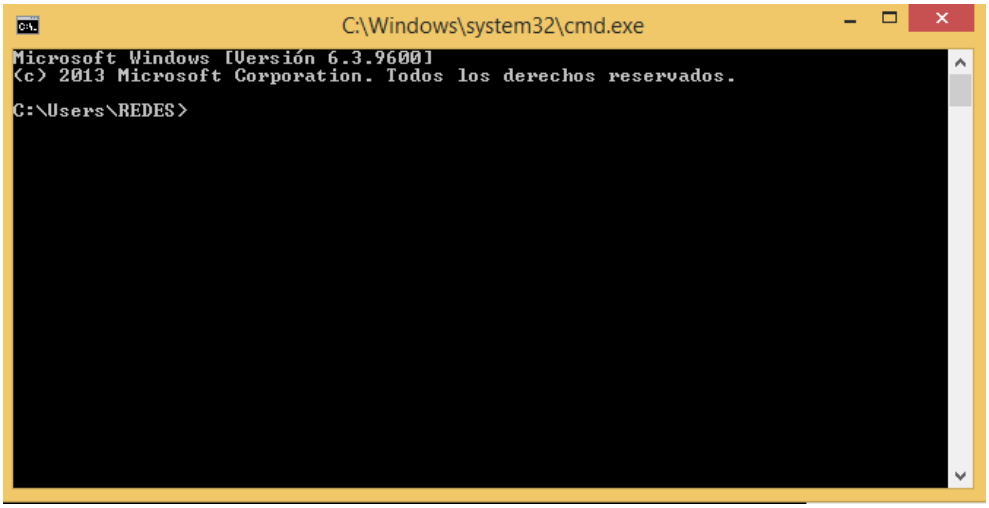


Imagen 6.24 “Ventana símbolo del sistema”

Una vez dentro la ventana, se capturará ***ipconfig***. Esto permitirá que se muestre la información acerca de los adaptadores de red de la computadora, incluyendo las direcciones que contienen cada uno.

Después se buscará el nombre del adaptador de red por donde se conectó el cable que comunica al switch. En este caso, el nombre es “Adaptador Ethernet Ethernet” (imagen 6.25).

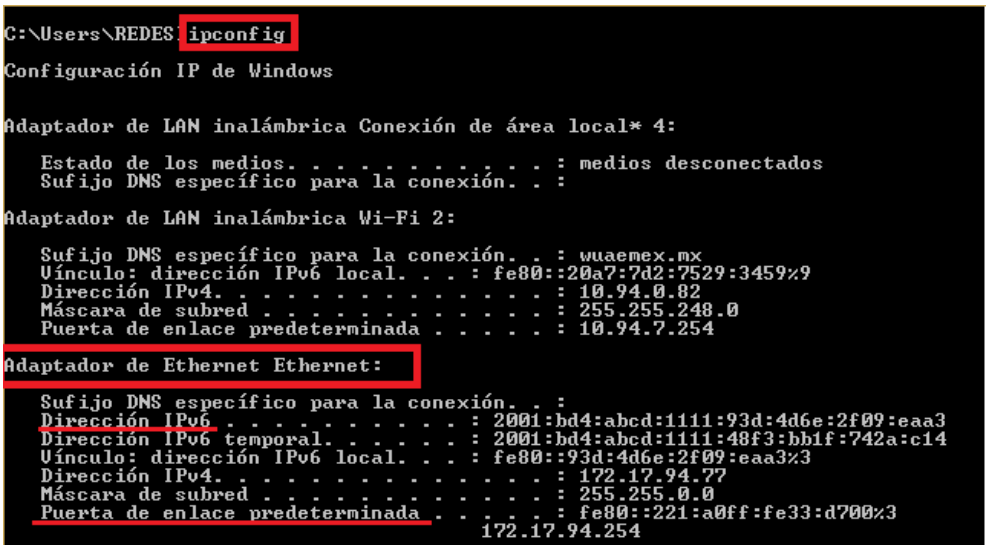


Imagen 6.25 “Identificador del adaptador ethernet”

Nota: El nombre del adaptador de red puede variar dependiendo del nombre asignado a la tarjeta de red instalada. Sin embargo, los parámetros IPv6 que se muestran al capturar “ipconfig” hacen fácil la detección del adaptador correcto.

Como puede apreciarse, existen muchos campos que poseen una dirección IPv4 e IPv6. Por ahora, las que son de interés son las de sexta versión.

El primer campo del “Adaptador Ethernet Ethernet” muestra su dirección IPv6 y contiene los valores hexadecimales “2001 : bd4 : abcd : 1111 : 93d : 4d6e : 2f09 : eaa3”. Nótese que los primeros cuatro bloques son idénticos a los de la primera subred que se configuró en el router anteriormente. Los restantes, son valores que el mismo hardware asignó automáticamente al host para identificarlo dentro de la misma subred. En otras palabras, el proceso de configuración automática sin estado de IPv6 realizó sus funciones para crear estas direcciones.

Nota: Para más información sobre la configuración automática de direcciones IPv6 consultar el capítulo 4 página 89.

Asimismo, es importante mencionar que una PC utiliza la dirección unicast de enlace local del router local como su dirección IPv6 de gateway predeterminado. Por ese motivo, puede observarse en la imagen 6.25 en la fila “puerta de enlace predeterminada” del adaptador Ethernet, la dirección unicast de enlace local de R1 (fácil de reconocer por el prefijo FE80).

La cuestión es que el host tiene una dirección IPv6 bastante extensa para memorizar, copiar o manejar, por lo que existe una alternativa más sencilla de asignar una dirección y facilitar las operaciones posteriores. Para realizarlo se debe seguir la siguiente ruta:

Inicio → Panel de control → Redes e internet → Centro de redes y recursos compartidos → Cambiar configuración del adaptador.

Una vez encontrada la ruta, se buscará la conexión de red “Ethernet”. Se dará clic derecho sobre él y se colocará en la opción “propiedades”, tal como se muestra en la imagen 6.26.

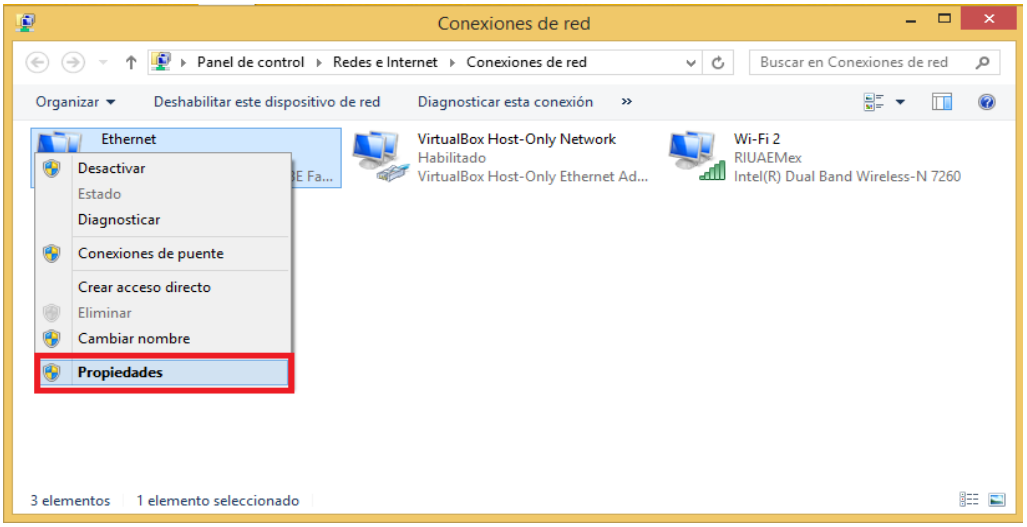


Imagen 6.26 “Propiedades”

Aparecerá la ventana “Propiedades de Ethernet” (imagen 6.27). Dentro de ella se buscará el campo “Protocolo de internet versión 6 (TCP/IPv6)”, se seleccionará y se dará clic en el botón “Propiedades”.

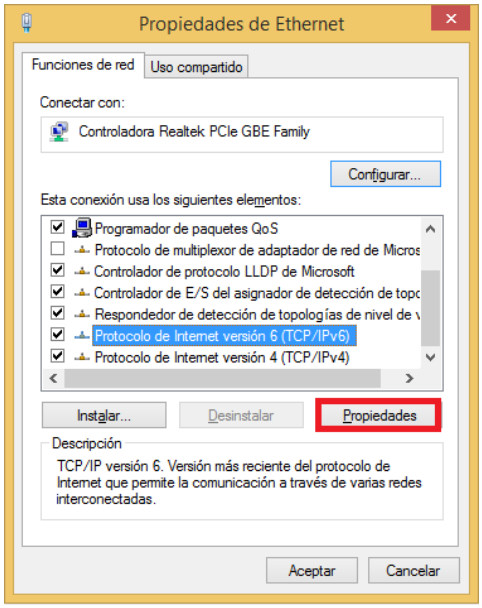


Imagen 6.27 “Propiedades de Ethernet”

La ventana que aparece tiene la opción “Obtener una dirección IPv6 automática” de forma predeterminada. Por lo tanto, se habilitará la opción “Usar la siguiente dirección IPv6” y se escribirán en los campos correspondientes los siguientes datos (tabla 6.4):

Tabla 6.4 “Dirección IPv6 estática del host Redes”

Campo	Datos
Dirección IPv6	2001:bd4:abcd:1111::2
Longitud de prefijo de subred	64
Puerta de enlace predeterminada	2001:bd4:abcd:1111::1

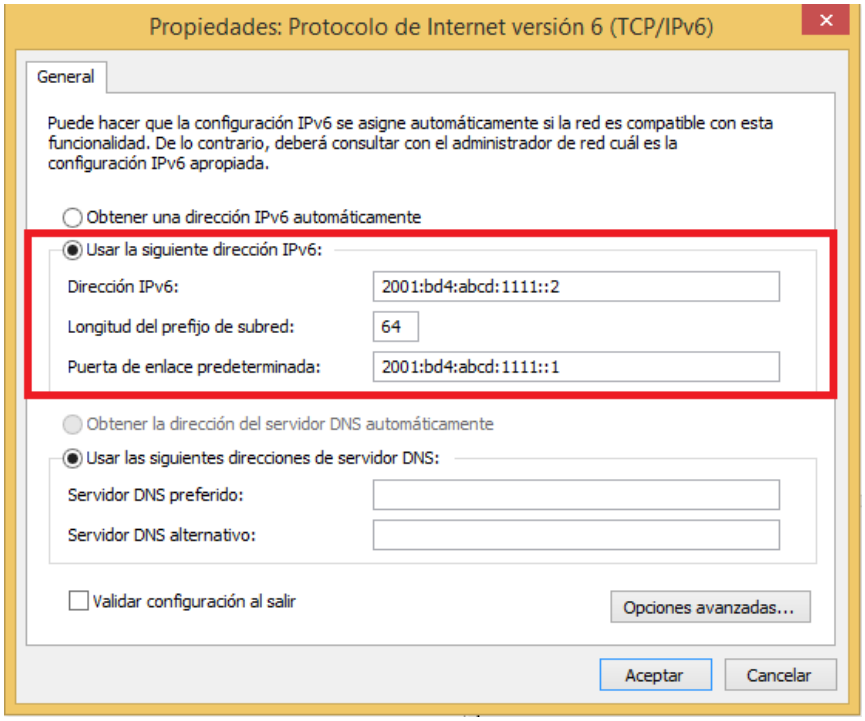


Imagen 6.28 “Captura de IPv6”

Dar clic en “aceptar” y cerrar las ventanas restantes.

Para verificar que la dirección IP ha sido modificada con éxito se abrirá (en caso de haberse cerrado) la ventana “símbolo del sistema” y nuevamente se ingresará ***ipconfig***.

En la sección “Adaptador Ethernet Ethernet” se debe visualizar la nueva IP configurada, tal como se muestra en la imagen 6.29.

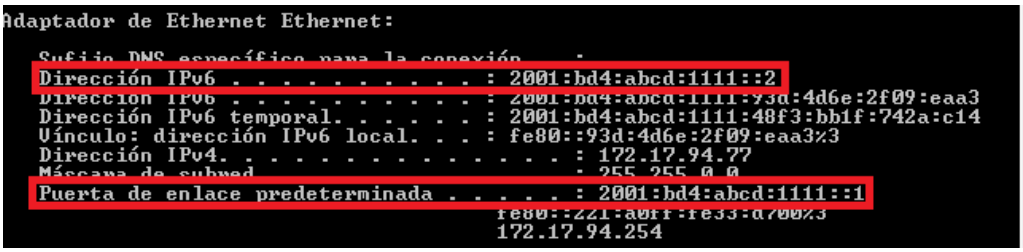


Imagen 6.29 “Verificación de IP estática”

Tras confirmar el correcto cambio de direcciones, se han completado la configuración del host Redes. No obstante, antes de realizar el ping, debe configurarse el segundo computador.

PC Usuario

En el host Usuario conectado a la segunda subred del router, deben realizarse los mismos pasos que en la PC Redes para el cambio manual de la dirección IPv6.

Los datos a capturar son los siguientes:

Tabla 6.5 “Dirección estática IPv6 del PC Usuario”

Campo	Datos
Dirección IPv6	2001:bd4:abcd:2222::2
Longitud de prefijo de subred	64
Puerta de enlace predeterminada	2001:bd4:abcd:2222::1

De igual manera, se debe verificar que la dirección haya sido correctamente modificada.

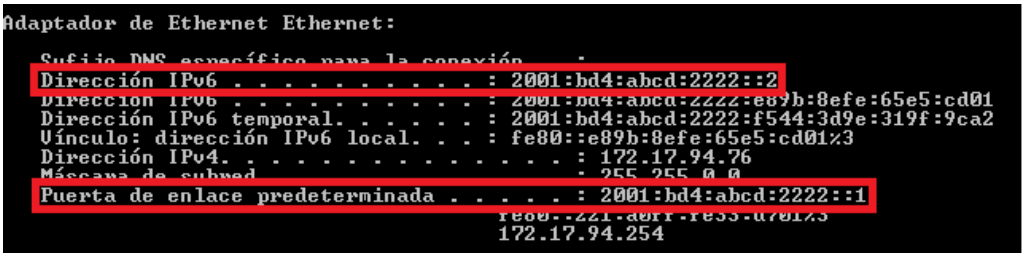


Imagen 6.30 “Verificación IP del host Usuario”

Firewall de Windows 8

Un dato importante que debe mencionarse para completar la acción "ping", es que de forma predeterminada los paquetes entrantes ICMPv6 (Protocolo de Mensajes de Control de Internet versión 6) son bloqueados por una regla del firewall en el S.O Windows 8. En otras palabras, si se intenta realizar un ping a cualquiera de las direcciones configuradas no habrá respuesta ante dicha solicitud y se obtendrá un resultado como se muestra en la imagen 6.31.

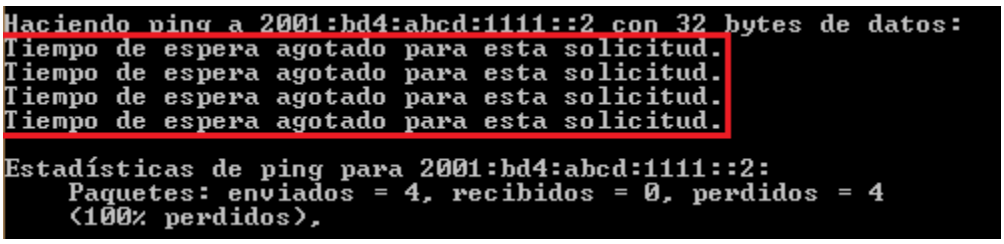


Imagen 6.31 "Mensaje de respuesta por defecto de ICMPv6"

Sucede de esta manera, dado que la función ping usa mensajes "echo request" y "echo reply" que son parte de ICMP. Sin embargo, la sexta versión de este protocolo es bloqueado por el firewall de Windows.

Por tal motivo, se deben modificar las reglas de entrada buscando la siguiente ruta:

Inicio → Panel de control → Sistema y seguridad → Firewall de Windows → Configuración avanzada.

Una vez dentro de la ventana "Firewall de Windows con seguridad avanzada", del lado izquierdo se dará clic en la opción "Reglas de entrada" y se enlistarán todas las opciones existentes que contiene esta función del S.O.

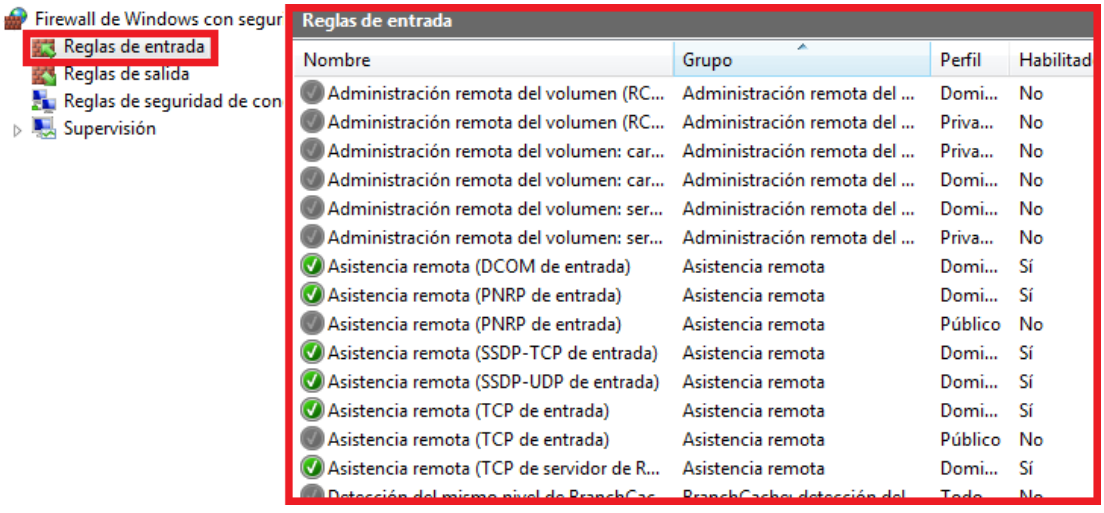


Imagen 6.32 "Lista de las reglas de entrada del Firewall de Windows 8"

Específicamente en Windows 8, la regla que debe buscarse tiene el nombre de “Supervisión de máquina virtual (solicitud de echo ICMPv6)”. A su vez, debe ser habilitada para admitir posteriormente los mensajes “echo” y así lograr hacer el ping. Para ello, se da clic derecho sobre la regla mencionada y se seleccionará “habilitar regla” (imágenes 6.33 y 6.34).

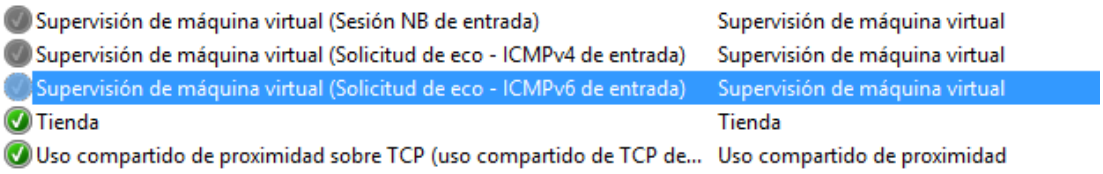


Imagen 6.33 “Regla a identificar en Firewall de Windows 8”

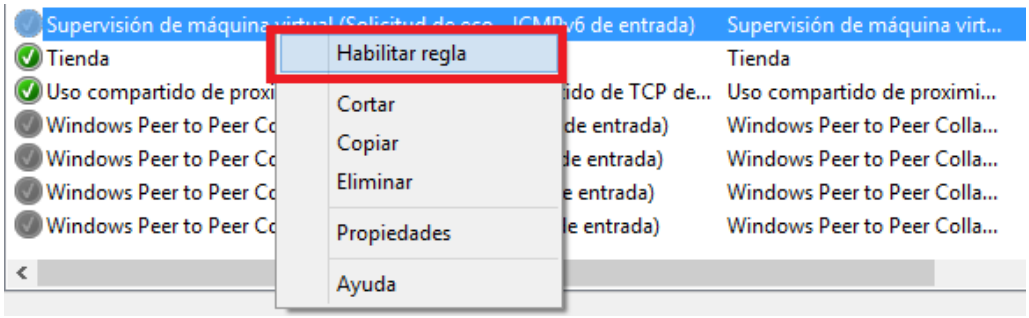


Imagen 6.34 “Habilitar regla ICMPv6”

Nota: Entre otras versiones más comunes de Windows en la actualidad (Windows XP, Windows 7, Windows 10), las reglas de entrada del firewall pueden variar. Asimismo, con el fin de evitar hacer una configuración equivocada o habilitar parámetros que se desconocen, se recomienda crear una regla de entrada especial para ICMPv6 únicamente en redes privadas y de dominio (ver anexo 6.1.1 página 122).

Nota: Otra alternativa más simple pero menos segura para la red es desactivar por completo el Firewall de Windows. Aunque si dicha acción es realizada, se recomienda su desactivación sólo hasta que se finalice la presente práctica.

Tras haber completado correctamente los pasos anteriores, el icono de la regla se verá en color verde.

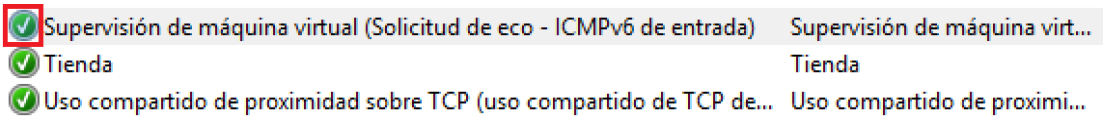


Imagen 6.35 “Corroboración de regla habilitada ICMPv6”

Es importante que esta operación se realice en ambas computadoras para proceder con la práctica y por ende obtener un resultado exitoso con el proceso ping.

PC Redes

Regresando a la ventana "símbolo del sistema" de la PC Redes se realizará un ping a las puertas de enlace (comúnmente llamado gateway) de ambas interfaces del enrutador (gigabitethernet 0/0 y 0/1), es decir, a las direcciones "2001 : bd4 : abcd : 1111 :: 1" y " 2001 : bd4 : abcd : 2222 :: 1" respectivamente. Esto es para finalmente corroborar que hay comunicación a los puertos del router y por ende a la subred conectada.

Por lo tanto, como primera operación para completar el ping, el texto a capturar es ***ping 2001:bd4:abcd:1111::1***

Si todos los pasos anteriores se hicieron correctamente la respuesta que debe aparecer será la siguiente (imagen 6.36).

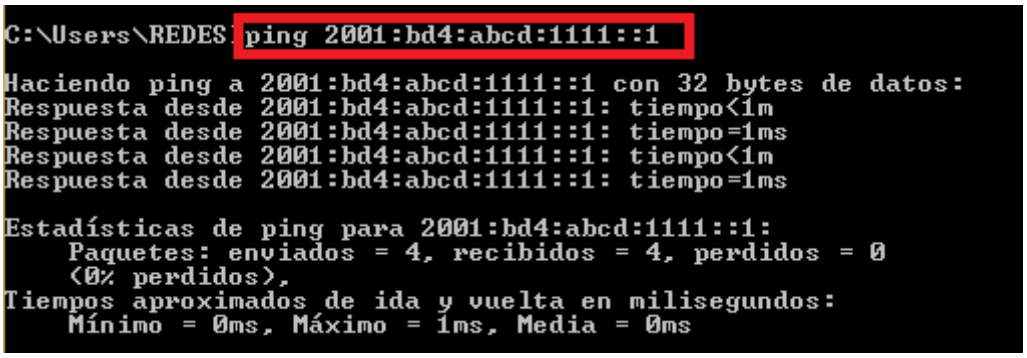


Imagen 6.36 "Ping a la interfaz gigabitethernet 0/0"

El texto "Respuesta desde" que es devuelto por el sistema, indica que sí existe comunicación entre el host que se opera y la interfaz que contiene la dirección que se ingresó junto con el comando "ping". Si por alguna razón el resultado mostrado no es igual al de la imagen 6.36 se deben verificar los pasos anteriores y corregir los errores.

Ahora se hará ping a la interfaz gigabitethernet 0/1 (imagen 6.37).

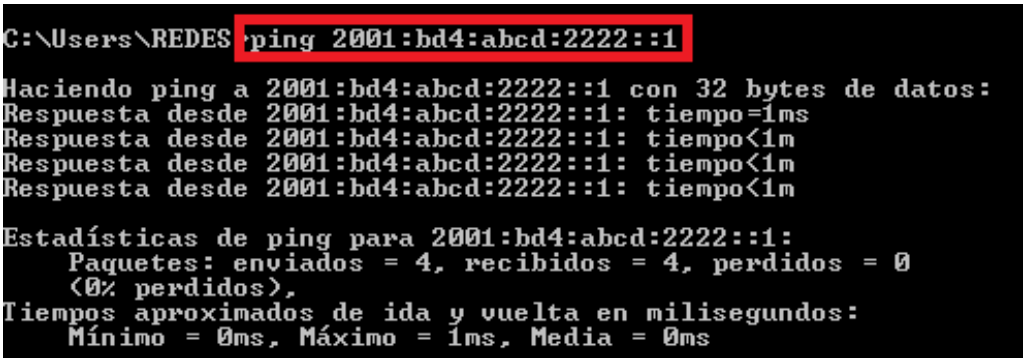


Imagen 6.37 "Ping a la interfaz gigabitethernet 0/1"

Para finalizar las pruebas en el host actual, se realizará un último ping a la dirección IP de la computadora de la segunda subred, es decir, hacia al PC Usuario. Por tal motivo, se debe capturar ***ping 2001:bd4:abcd:2222::2*** (imagen 6.38).

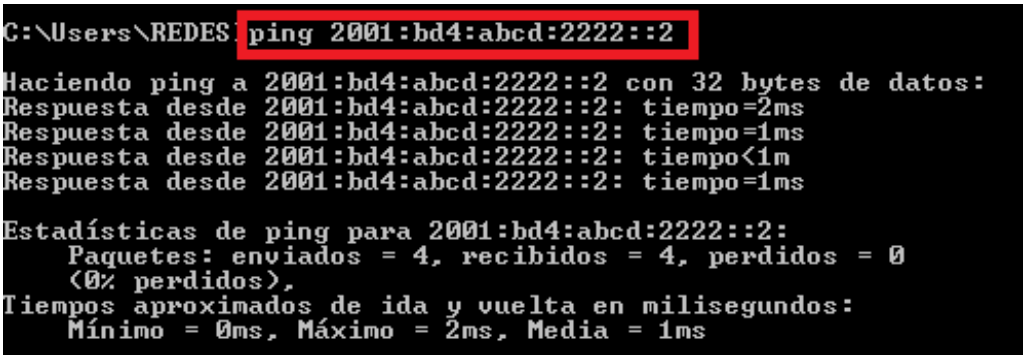


Imagen 6.38 "Ping al PC Usuario"

PC Usuario

Tras haber configurado las reglas del firewall en el presente host y de tener lista la ventana MS-DOS de Windows se hará ping al PC Redes (imagen 6.39).

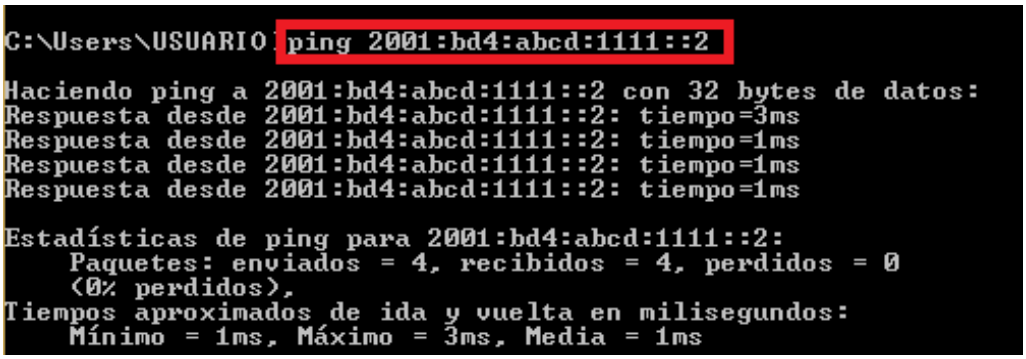


Imagen 6.39 "Ping al PC Redes"

Una vez obtenido una respuesta exitosa, se ha finalizado la implementación, configuración y pruebas de comunicación de IPv6 sin enrutamiento.

6.1.1 Anexo: Creación de una regla de entrada en firewall de Windows 8 para la aprobación de mensajes “echo” del protocolo ICMPv6

Para crear una nueva regla en el firewall de Windows 8, primero debe seguirse la siguiente ruta:

Inicio → Panel de control → Sistema y seguridad → Firewall de Windows → Configuración avanzada.

Una vez situado en la ventana de "Configuración avanzada de firewall" debe hallarse la opción "Reglas de entrada" (imagen 6.40), seguidamente se buscará la acción "Nueva regla" ubicada en el lado superior derecho de la ventana actual (imagen 6.41).

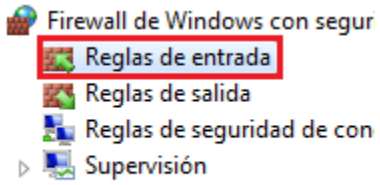


Imagen 6.40 "Opción reglas de entrada"

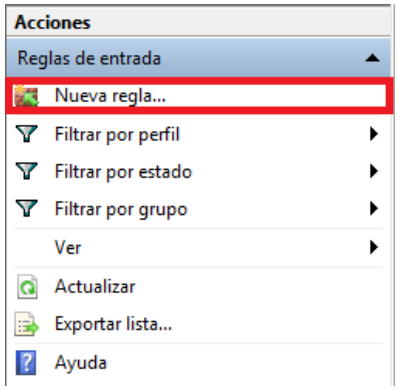


Imagen 6.41 "Opción nueva regla de firewall"

Posteriormente se abrirá el asistente de Windows para la configuración de la nueva regla. En este paso se elige la opción "Personalizada" y se da clic en "siguiente" (imagen 6.42).

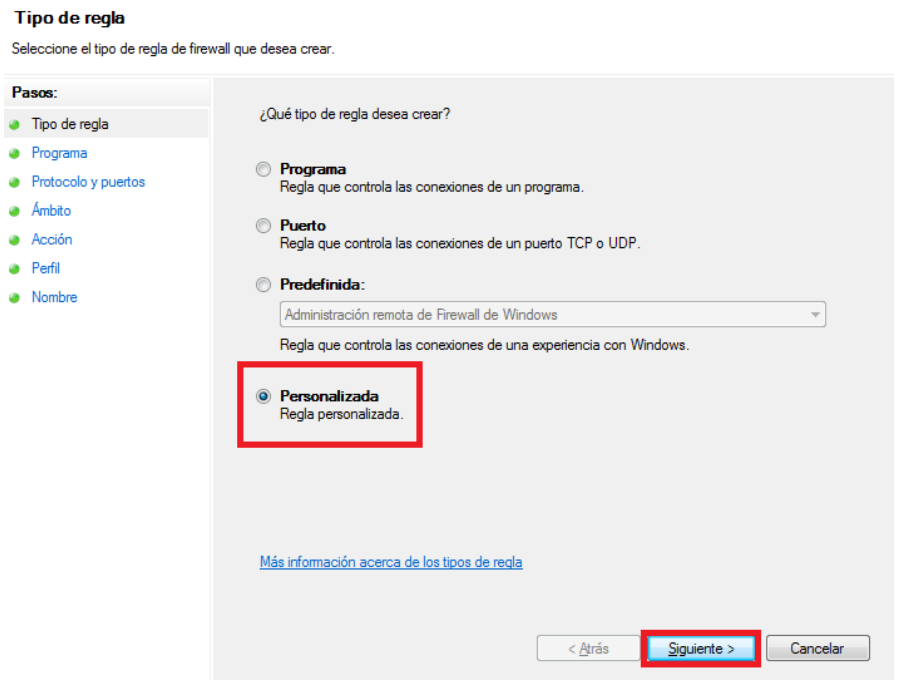


Imagen 6.42 "Opción para personalizar la regla de firewall"

En esta etapa, la configuración brinda la opción de elegir un programa específico para que la regla configurada sólo tenga efecto en este. En esta ocasión, se elige el apartado "todos los programas" dado que es de interés que la regla tenga efecto en el S.O en general (imagen 6.43).

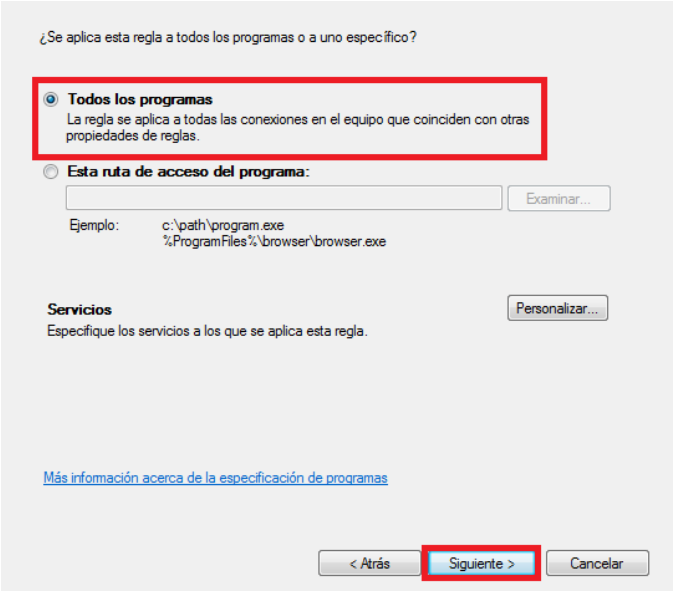


Imagen 6.43 "Opción de regla para todos los programas"

En el siguiente paso, donde se establecen los protocolos y los puertos se elige la opción "ICMPv6", tal y como se muestra en la imagen 6.44.

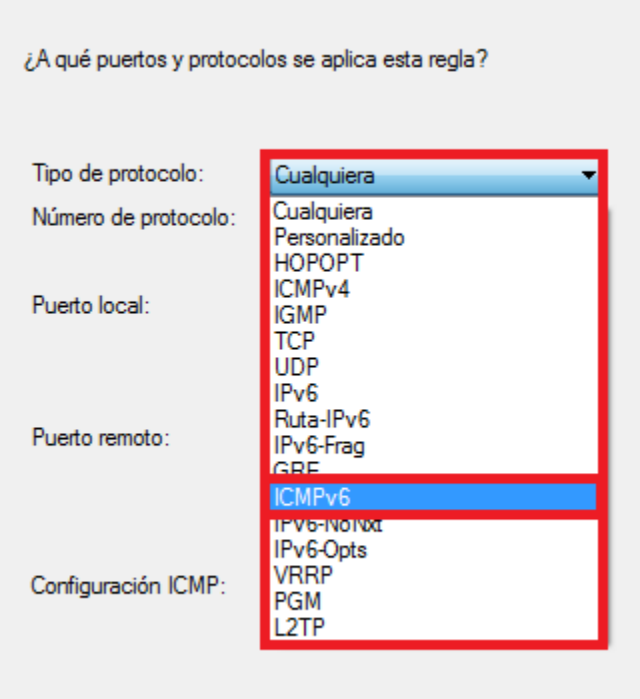


Imagen 6.44 "Protocolo especificado para la regla actual"

No obstante, antes de pasar a la siguiente etapa se debe limitar el uso de ICMPv6 a únicamente la aprobación de mensajes "peticiones eco" (echo request) por lo que se da clic en el botón "Personalizar" de la opción "Configuración de ICMP" (imagen 6.45).

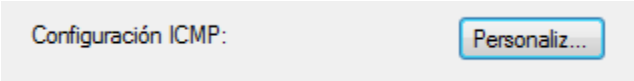


Imagen 6.45 "Opción para la limitación del protocolo ICMP"

En la ventana actual, se elige "Tipos de ICMP específicos" debido a que se desea definir y por ende limitar las funciones de ICMPv6. Posteriormente se ubica y marca la opción "Petición eco" y se da clic en "aceptar" (imagen 6.46).

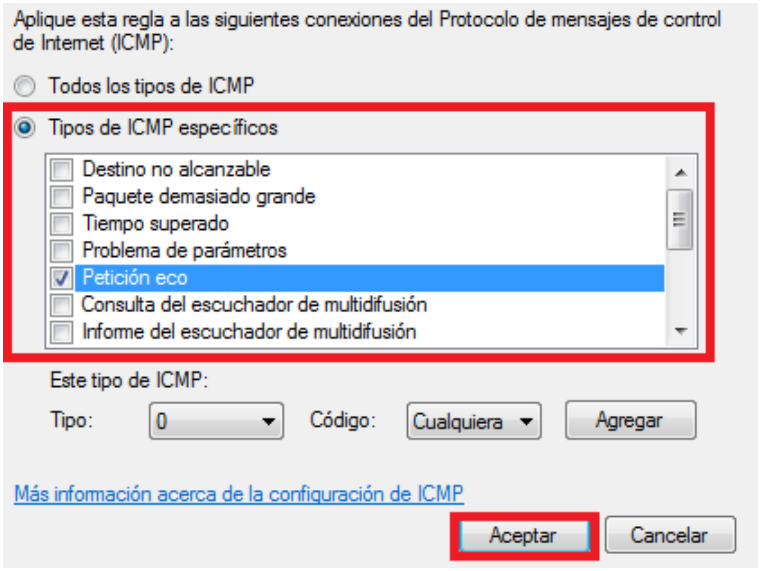


Imagen 6.46 "Tipo de ICMP especificado"

Después, en la etapa "ámbito" se dejan las opciones predeterminadas. Salvo que se desee especificar alguna dirección IP local o remota en las que únicamente se aplique la regla creada. En este caso, las opciones no son modificadas (imagen 6.47). Clic en "siguiente".

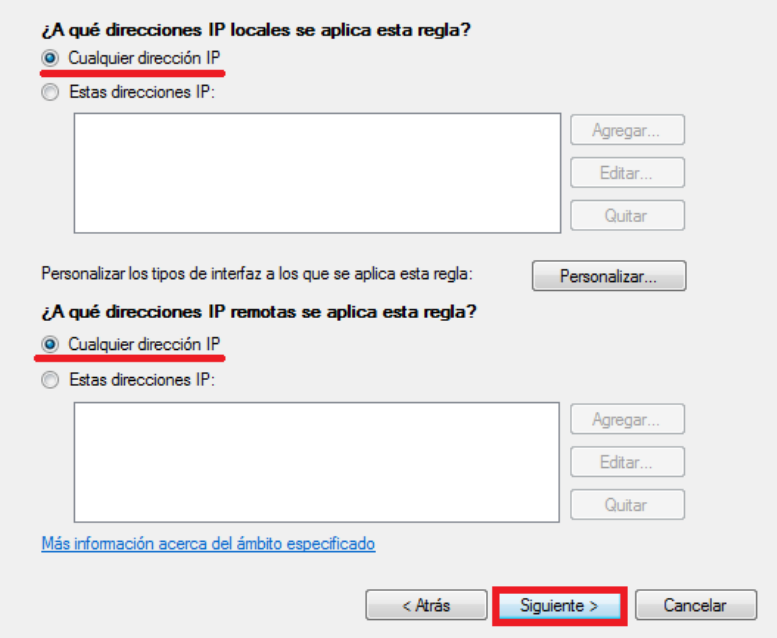


Imagen 6.47 "Opción para aplicar la regla a determinadas direcciones IP"

Posteriormente, en el paso “Acción” se deja marcado “Permitir la conexión” ya que se requiere la aprobación de las peticiones eco del proceso ping. Luego clic en “siguiente” (imagen 6.48).

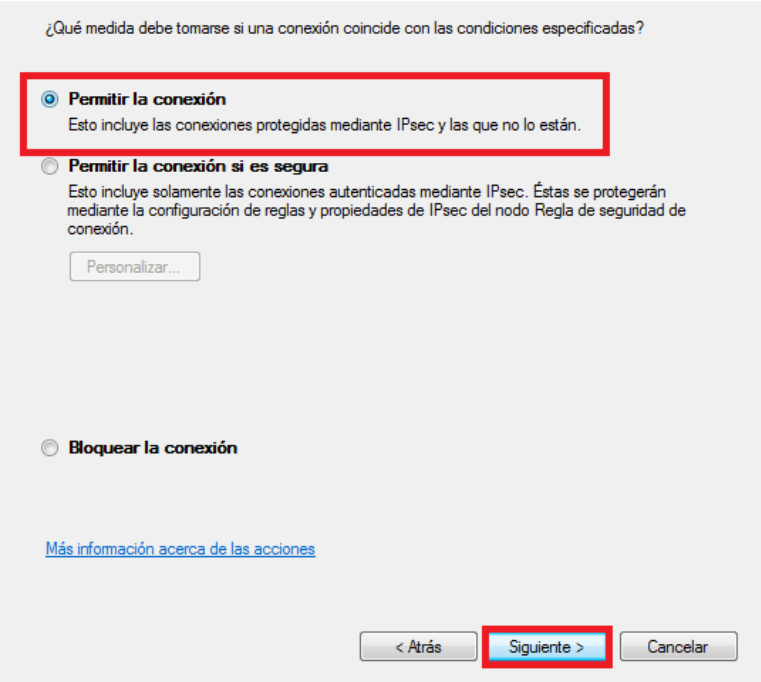


Imagen 6.48 “Opción permitir la conexión”

En la presente etapa se recomienda dejar marcadas las opciones “dominio” y “privado”, puesto que son medidas de seguridad requeridas para limitar a los nodos que podrán realizar un ping al host actual (sin tomar en cuenta si se establecieron IP’s específicas en el paso anterior). En otras palabras, esta etapa permite que los nodos que estén dentro de un determinado dominio de red puedan o no comunicarse con esta PC (imagen 6.49).

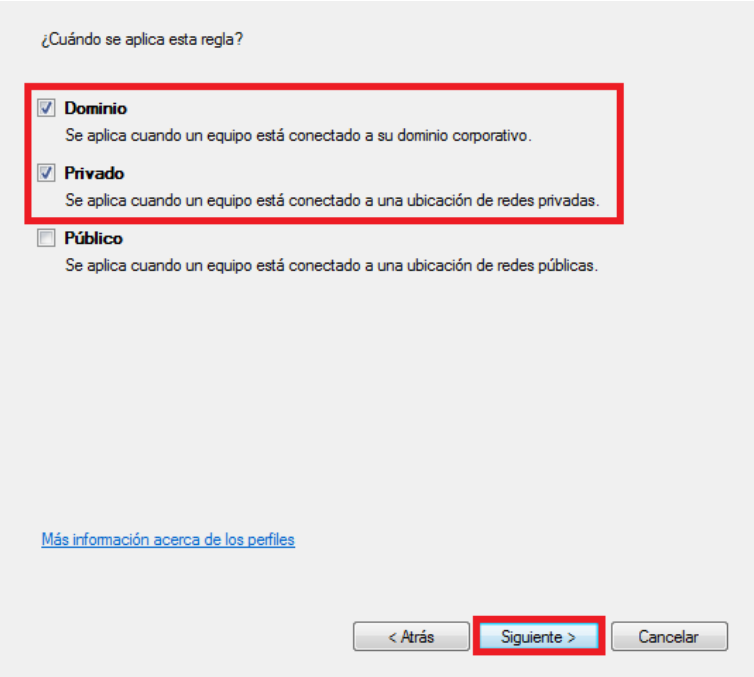


Imagen 6.49 "Opciones de comunicación de acuerdo al dominio de red"

Para concluir con la configuración, se debe nombrar la regla creada y si así se desea, agregar una descripción de la misma. Se recomienda establecer un nombre característico para identificar la regla con facilidad (imagen 6.50).

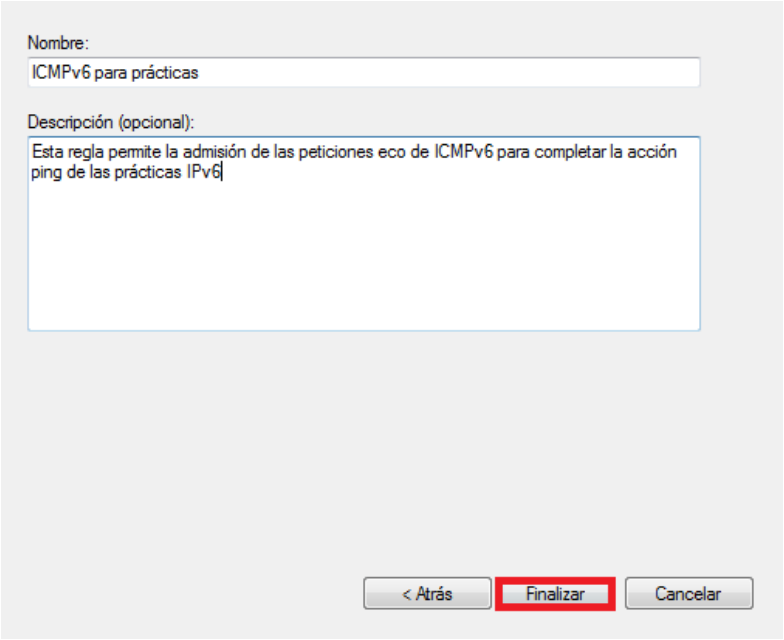


Imagen 6.50 "Nombre y descripción de la regla de firewall creada"

Como corroboración, la nueva regla debe encontrarse habilitada dentro de la lista del firewall de Windows.

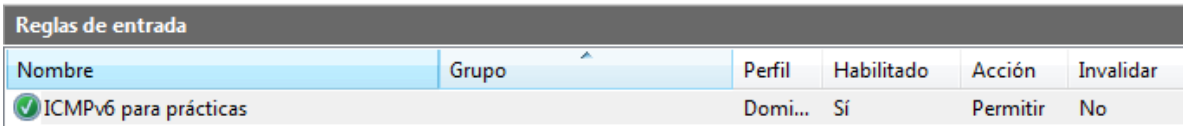


Imagen 6.51 “Regla de firewall creada correctamente”

6.2 Introducción y configuración del protocolo RIPng en un entorno Cisco para la implementación de una red física de área extensa (WAN) utilizando IPv6.

Objetivo:

- Comprender y configurar los parámetros básicos del protocolo de enrutamiento RIPng.
- Configurar el protocolo IPv6 sobre los dispositivos fundamentales que componen una red de área extensa.
- Implementar las operaciones básicas IPv6 para la configuración de los host con un sistema operativo Windows 8.

Para desarrollar la práctica es esencial contar con los siguientes dispositivos:

- 2 Routers
- 2 Switch
- 4 Cables de red con configuración directa (cualquiera, T568-A o T568-B)
- 1 Cable DCE
- 1 Cable DTE
- 1 Cable de consola para la configuración remota de un enrutador
- 2 Computadoras (mismo S.O)

En este caso, el hardware específicamente utilizado fue el siguiente:

- 2 Router Cisco 2821 (2800 series)
- 2 Switch Cisco Catalyst 2960
- 2 Computadoras con el mismo S.O (Windows 8)
- 4 Cables de red con configuración directa T568-B
- 1 Cable de consola DB9 a RJ45
- 1 Cable smart serial DTE a V.35 macho
- 1 Cable smart serial DCE a V.35 hembra

La estructura de red que conforman los dispositivos en la práctica es la que se muestra en la imagen 6.52.

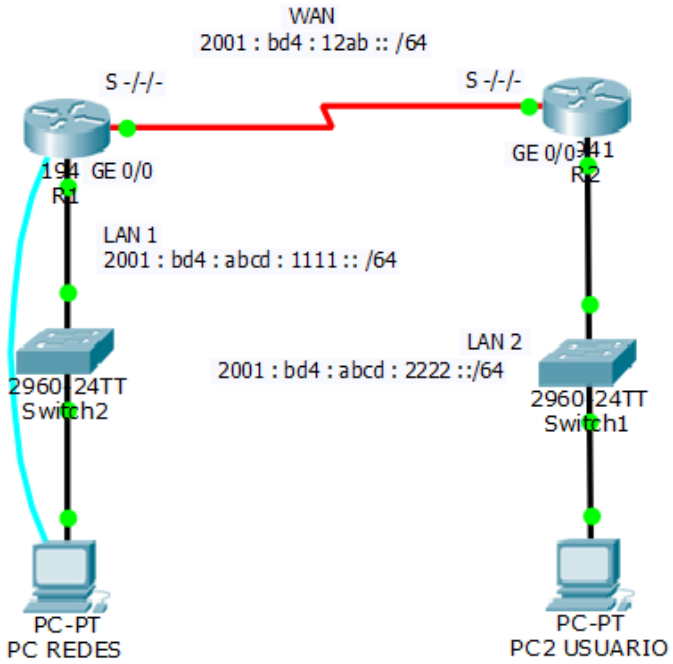


Imagen 6.52 “Diagrama de topología”

La red que se muestra en el diagrama de topología contiene una red WAN. A su vez, cada router sujeta una red LAN con sus respectivos dispositivos conectados y especificados anteriormente. Dicho esquema de red, es configurado bajo el protocolo IPv6, donde la comunicación entre routers es establecida mediante el protocolo enrutamiento más sencillo de tipo "vector-distancia", es decir, el protocolo RIP de siguiente generación (denominado como RIPng por usar IPv6).

Las direcciones para cada interfaz se muestran en la tabla 6.6.

Tabla 6.6 "Tabla de direccionamiento"

DISPOSITIVO	TIPO DE INTERFAZ	NÚMERO INTERFAZ	DIRECCIÓN IPv6
R1	Serial	-/-/-	2001 : BD4 : 12AB :: 1
	Gigabitethernet (GE)	0/0	2001 : BD4 : ABCD : 1111 :: 1
PC Redes	NIC	N/A	2001 : BD4 : ABCD : 1111 :: 2
R2	Serial	-/-/-	2001 : BD4 : 12AB :: 2
	Gigabitethernet (GE)	0/0	2001 : BD4 : ABCD : 2222 :: 1
PC Usuario	NIC	N/A	2001 : BD4 : ABCD : 2222 :: 2

Nota: El número de las interfaces seriales no se describen en la tabla anterior debido a las especificaciones de cada enrutador (explicadas posteriormente).

Las conexiones físicas deben ser idénticas a las que se mostraron en la práctica 6.1, excepto que solo un cable de red con configuración directa estará conectado a una sola interfaz gigabitethernet (en este caso la 0/0) del enrutador, es decir, un solo cable por router. Tal y como se muestra en el diagrama de topología (imagen 6.52). Teniendo de esta manera dos conjuntos de dispositivos (formado por un switch y un host) separados para cada enrutador.

Consecutivamente, el segundo extremo del cable saliente de la interfaz GE debe ser conectado al panel frontal derecho del switch, de la misma forma que en la práctica 6.1. Al igual que la conexión de la red LAN (switch a host).

Para formar la segunda red local, las conexiones serán las mismas que la primera, siendo únicamente conectados a su router correspondiente.

Posteriormente, el medio físico que permitirá la comunicación entre los enrutadores serán los cables DCE (Equipo de Comunicación de Datos) y DTE (Equipo Terminal de Datos), ya que en este caso, la manera en que dichos dispositivos se comunicarán será a través de su interfaz serial.

Nota: Es importante aprender a realizar la conexión entre los enrutadores con los cables mencionados, ya que la misma configuración es utilizada en prácticas posteriores.

Nota: Existe una distinta (aunque obsoleta) manera para comunicar a dos enrutadores, esto se realiza mediante conectores de la línea telefónica RJ11 para dial-up o conexiones de la Línea de suscriptor digital (DSL).

Ciertamente, existe una gran cantidad de modelos de cables que pueden operar como una conexión DCE y/o DTE, esto dependiendo de las necesidades de la red, del tipo de señalización y principalmente del modelo del enrutador. Ya que de este último depende el tipo de tarjetas de interfaces que pueden instalarse en él y por ende el tipo de conector del cable requerido. En este caso, para el modelo del router de la presente práctica se utiliza un conector de tipo smart serial (extremo del cable conectado al hardware), tal y como se muestra en la imagen 6.53.

Imagen 6.53 “Conector smart serial”

A su vez, por el otro extremo del cable se utiliza un conector de tipo V.35, el cual será la conexión por donde ambos cables estarán unidos. En otras palabras, por donde los enrutadores podrán estar conectados y posteriormente establecer una comunicación. Por lo cual, se necesitan de dos cables para realizar dicha conexión.

Se requiere de un cable de tipo DCE y otro de tipo DTE (ambos con conectores smart serial por el otro extremo). Físicamente cada uno se distingue por el tipo de conector V.35 que poseen. Por ejemplo, los DCE tienen un conector de tipo hembra conformado de 34 orificios (imágenes 6.54 y 6.55) y los DTE poseen un conector de tipo macho con la misma cantidad de pines (imágenes 6.56 y 6.57).

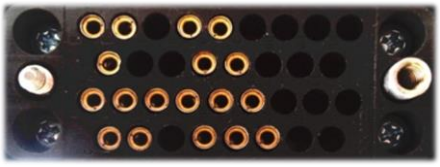


Imagen 6.54 “Vista frontal del extremo V.35 hembra (DCE)”

Imagen 6.55 “Vista superior del extremo V.35 hembra (DCE)”

Imagen 6.56 “Vista frontal del extremo V.35 macho (DTE)”

Imagen 6.57 “Vista superior del extremoV.35 macho (DTE)”

Nota: La posición y el número de pines puede variar de acuerdo con el modelo del cable V.35. En este caso el modelo específico es un CAB-SS-V35MT (Macho) y un CAB-SS-V35FT (Hembra).

El modelo del cable cambia dependiendo del tipo de conector que va enchufado al enrutador, cambiando por ende el segundo extremo V.35. (Cisco, s.f)

La conexión DCE corresponderá al router R1 y el DTE al R2. Ciertamente, cualquier enrutador de la práctica puede soportar la conexión DCE, el único detalle radica que entre estos tipos de conectores el DCE suministra la señal de reloj que establece el paso de las comunicaciones sobre el bus. Es decir, el router que se le asigne dicho extremo tendrá que utilizar el comando “*clock rate*” al momento de configurar la interfaz serial. Por el contrario, el segundo hardware con la conexión DTE no deberá realizar esta operación.

Nota: Como el laboratorio donde se realiza la presente práctica no está conectado a una línea dedicada, uno de los routers debe proporcionar la temporización para el circuito. Normalmente, el proveedor de servicios proporciona la señal de temporización a cada uno de los routers. Por tal motivo, para proporcionar dicha señal, uno de los enrutadores necesita un cable DCE en lugar del cable DTE usado en el segundo router.

Nota: En este caso, el término V.35 para los conectores de los cables de la práctica, significa la norma utilizada que define la señalización de reloj sobre el cable serial. Asimismo, también existen las normas EIA/TIA-232, X.21, **V.35**, EIA/TIA-449, EIA-530 y HSSI. Y como se mencionó, cada estándar define las señales en el cable y especifica el tipo de conector del extremo del mismo. La documentación del dispositivo conectado y/o usado debe indicar la norma de señalización utilizada para dicho dispositivo (en este caso el enrutador). (Cisco, s.f)

La asignación de cada terminal de los cables se establece como se mencionó anteriormente.

El primer extremo del cable smart serial debe ir conectado al puerto serial ubicado en la parte posterior de cada router (imágenes de 6.58 a 6.60).

En esta práctica ambos cables se conectaron al puerto serial 0.

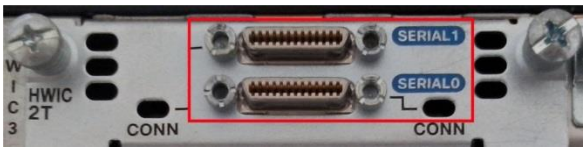


Imagen 6.58 “Puertos seriales de un enrutador”

Imagen 6.59 “Cable serial DCE R1”

Imagen 6.60 “Cable serial DTE R2”

El extremo restante (V.35) debe conectarse de manera que ambos conectores embonen sin dificultad alguna (imágenes 6.61 y 6.62).

Imagen 6.61 “Cables DCE y DTE en posición”

Imagen 6.62 “Cables DCE y DTE unidos”

Nota: Se recomienda ajustar la conexión de ambos cables girando y apretando los seguros que hay en cada uno.

Para finalizar las conexiones de la práctica, el cable de consola (cable azul en la imagen 6.52) debe ir conectado a cualquier host para configurar posteriormente ambos routers. O bien, podría cambiarse el cable de consola al segundo host y configurar el enrutador faltante. Cualquier opción descrita es válida.

Router “R1”

Al concluir las conexiones físicas requeridas, se abrirá hyperterminal, tal como se explicó en la práctica 6.1 (página 103) y se verificará que el presente router no contenga alguna configuración previa.

```
Router>
Router>enable
Router#show run
Building configuration...
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/3/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/3/1
 no ip address
 shutdown
 clock rate 2000000
!
end
Router#
```

Si al verificar que las interfaces gigabitethernet o seriales poseen direcciones, el router debe ser reiniciado a los parámetros predeterminados de fábrica (ejemplo en la página 109 de la práctica 6.1).

Una vez confirmada la nula configuración previa, se comenzarán a capturar los siguientes comandos.

```
Router#
Router#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#ipv6 unicast-routing
R1(config)#interface gigabitethernet 0/0
```

*R1(config-if)#**ipv6 address 2001:bd4:abcd:1111::1/64***
*R1(config-if)#**no shutdown***
*R1(config-if)#**exit***
R1(config)#
**Aug 27 19:37:55.107: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up*
**Aug 27 19:38:51.719: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up*

Dentro del código anterior, el comando "***ipv6 unicast-routing***" habilita el tráfico de datos de tipo IPv6 (explicado anteriormente). Posteriormente se ingresó a la interfaz gigabitethernet 0/0 y se le asignó su dirección correspondiente, dando por último la confirmación y habilitación de la interfaz con el comando "***no shutdown***". Como corroboración, los leds de la interfaz configurada estarán encendidos (imagen 6.63).

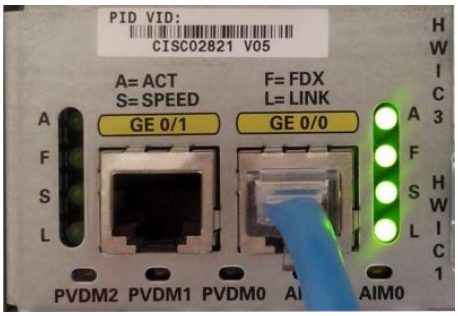


Imagen 6.63 "Interfaz GE 0/0 habilitada"

Nota: La función de los comandos capturados se describen detalladamente en la práctica 6.1 en la tabla 6.2.

Después, se captura lo siguiente:

*R1(config)#**interface serial -/-/-***

La línea anterior se explica en la tabla 6.7:

Tabla 6.7 "Comandos Cisco de la práctica 6.2"

Código	Descripción
interface serial	Indica que la interfaz a configurar es de tipo serial
-/-/-	Numero de interfaz ingresada

El número de valores que componen a una interfaz varían dependiendo de diversos factores del hardware, es decir, factores como el modelo del router, el tipo de interfaz, el puerto que la contiene, posiblemente la ubicación del puerto (chasis del enrutador), entre otros. Por tal

motivo es importante conocer la mayor cantidad de información para facilitar la identificación de la interfaz.

Como la configuración que se debe realizar en este paso tiene el objetivo de establecer una comunicación entre routers, y se sabe que para lograrlo se necesita una conexión a través de una interfaz de tipo serial (en este caso), entonces ese es el primer parámetro distinguido.

El segundo dato que debe conocerse es el tipo de tarjeta que contiene la interfaz por donde se realiza la transmisión de datos. Tomando en cuenta el primer parámetro, la interfaz es de tipo serial y esta se encuentra en la parte posterior del enrutador. Por lo tanto, se examinarán los datos de la placa del enrutador que contiene dicha interfaz (imagen 6.64).

Imagen 6.64 “Identificación del modelo de tarjeta”

El hardware que contiene la interfaz serial es una tarjeta HWIC-2T.

Para corroborar que la información es correcta se recomienda buscar las especificaciones del modelo en la web (imágenes 6.65 y 6.66).

Imagen 6.65 “Tarjeta HWIC-2T”

Imagen 6.66 “Ubicación de tarjeta HWIC-2T en el router”

Tras haber confirmado la información y al contar con la mayor cantidad de datos sobre los parámetros de la interfaz, se buscarán las especificaciones del enrutador. En este caso el modelo es Cisco 2821. Por lo tanto se designaron las siguientes características:

Tabla 7 Numeración de la interfaz de los routers de la serie Cisco 2811, Cisco 2821 y Cisco 2851 de servicios integrados

Ubicación del puerto	Esquema de numeración de interfaces	Ejemplos[1, 2]
Incorporado en el panel frontal del chasis	*Puerto de tipo de interfaz*	usb 0 usb 1
Incorporado en el panel posterior del chasis	*Tipo de interfaz* 0 / *puerto*	interfaz fa 0/x interfaz gi 0/x
En una tarjeta de interfaz (HWIC, HWIC-D, WIC, VWIC, VIC) conectada directamente a una ranura HWIC de un chasis	*Tipo de interfaz* 0 / *ranura de la tarjeta de interfaz*[3] / *puerto* **Nota** Las ranuras de tarjeta de interfaz incorporadas en el chasis están etiquetadas como HWIC *número de ranura* en los routers de la serie Cisco 2800.	interfaz serie 0/x/y interfaz asíncrona 0/x/y línea 0/x/y[4] interfaz fa 0/x/y puerto de voz 0/x/y

Imagen 6.67 “Especificaciones del enrutador Cisco 2821”

Como se puede apreciar, en la columna “Ubicación del puerto” se elige la categoría “en una tarjeta de interfaz (HWIC)” ya que coincide con la información obtenida anteriormente. Después, en la columna “Esquema de numeración de interfaces” puede visualizarse que la interfaz serial buscada se divide en 3 valores:

Tipo de interfaz 0 / ranura de la tarjeta de interfaz / puerto

Con base a este formato se conoce que el primer valor del campo “tipo de interfaz” será 0. Por lo tanto:

0 / ranura de la tarjeta de interfaz / puerto

En la siguiente sección (ranura de la tarjeta de interfaz) se debe poner atención en la nota resaltada en la imagen 6.67 (en color rojo). Básicamente describe que debe verificarse el número de ranura de la tarjeta que se pretenda utilizar.

Para realizar dicha operación, es importante conocer que el chasis posterior del enrutador posee en su placa el grabado de la nomenclatura del tipo de tarjeta y, además el número de la ranura de cada una. En este caso, la tarjeta utilizada es una HWIC-2T, por lo tanto se busca y se identifica el número de ranura (ubicado en la parte final) en donde la tarjeta está conectada (imagen 6.68).

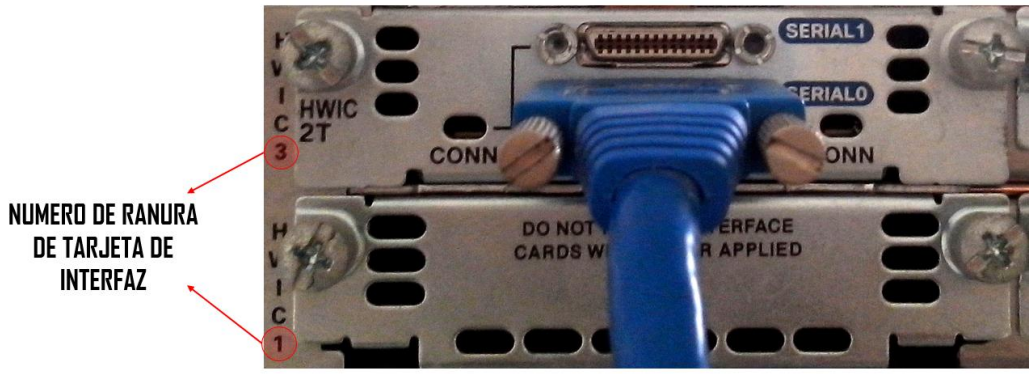


Imagen 6.68 “Identificación del número de ranura”

En este caso, la tarjeta utilizada se encuentra conectada a la ranura número 3. Por lo tanto:

0 / 3 / puerto

Para finalizar, la sección “puerto” como su nombre lo describe, es el número de puerto que está utilizándose. En este caso, es el número 0.

Imagen 6.69 “Numero de puerto utilizado”

Por tal motivo, el último dígito para completar los valores de la interfaz serial es:

0 / 3 / 0

Por lo que se reanuda el proceso de configuración en hyperterminal.

*R1(config)#**interface serial 0/3/0***
*R1(config-if)#**ipv6 address 2001:bd4:12ab::1/64***
*R1(config-if)#**clock rate ?***

A continuación, el código se detalla en la tabla 6.8:

Tabla 6.8 “Comandos Cisco de la práctica 6.2”

Código	Descripción
0/3/0	Numero de interfaz ingresada
ipv6 address	Indica que la dirección a asignarse es de tipo IPv6
2001:bd4:12ab::1/64	Dirección IPv6 asignada
clock rate	Comando para configurar la velocidad de reloj en el enlace
?	Proporciona las opciones disponibles de acuerdo al comando que lo solicita.

Es de suma importancia no olvidar configurar el clock rate (únicamente para DCE). De lo contrario, la conexión no funcionará, ya que no existiría ningún entendimiento sobre la velocidad de los datos enviados entre los dos extremos de la conexión.

Tras haber capturado el comando ***clock rate ?*** automáticamente se enlistarán las velocidades de reloj disponibles.

*R1(config-if)#**clock rate ?***
Speed (bits per second)
1200
2400
4800
9600
14400
19200
28800
32000
38400
48000
56000
57600
64000
72000
115200
125000
128000
148000
192000
250000
256000
384000
500000
512000
768000
800000
1000000
2000000
4000000

5300000
8000000

<300-8000000> Choose clockrate from list above

En este caso, la velocidad de reloj asignada es 64,000.

*R1(config-if)#**clock rate 64000***
*R1(config-if)#**no shutdown***
R1(config-if)#
**Feb 10 22:05:29.191: %LINK-3-UPDOWN: Interface Serial0/3/0, changed state to up*
**Feb 10 22:05:30.191: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up*

*R1(config-if)#**exit***
R1(config)#

Nota: Las velocidades de reloj recomendables para configurarse (o velocidades máximas) dependen del tipo de conector y por ende el tipo de señalización (explicado anteriormente), la distancia y el proveedor de tráfico de datos.

Una vez completa la configuración de la interfaz serie, se verifica físicamente en la parte posterior del router (imagen 6.70).

Imagen 6.70 "Interfaz serial habilitada"

La siguiente operación es implementar y configurar el protocolo RIPng, ya que los datos necesitan ser enrutados a través del medio físico que une a los routers para poder transmitirse correctamente.

Ciertamente las diferencias entre IPv4 e IPv6 sobre la configuración del protocolo son mínimas, por tal motivo las operaciones siguientes son sencillas.

Como primer pasó, se debe estar dentro de la configuración global del router para capturar el siguiente comando:

***R1(config)#ipv6 router rip** "name"*

Donde el parámetro "*name*" permitirá identificar el proceso del protocolo RIPng que está configurándose a partir de un nombre, permitiendo anexar varias líneas a un mismo proceso o bien tener múltiples procesos RIP corriendo simultáneamente en el enrutador (algo que no

puede realizarse en IPv4). De hecho, cada uno de los procesos tendrá su propia tabla de enrutamiento, la cual será denominada "*Routing Information Database*" (RIB).

Nota: Si se crean distintos procesos RIP en un router, estos al final convergerán, creando una tabla general de ruteo con la cual operará el enrutador. El comando "*show ipv6 route*" desplegará dicha tabla. Sin embargo, para mostrar los detalles individuales de los procesos RIP, se captura el comando "*show ipv6 rip database*".

Posteriormente, se captura el comando anterior, eligiendo un nombre para el proceso RIPng. En este caso, se nombró "***RIP1***".

*R1(config)#**ipv6 router rip RIP1***
R1(config-rtr)#

La última línea del código muestra un nuevo nivel de configuración (fácilmente reconocible por el indicador "*config-rtr*").

En este punto, existe una diferencia con respecto a la configuración en IPv4. Para IPv6 se debe ir directamente a las interfaces e indicarles en qué proceso RIP van a participar para distribuir sus rutas. Mientras que en RIPv1 y/o RIPv2 (ambos para IPv4) se indicaba en el mismo nivel (denominado "config-router") de las interfaces a procesar. (Fuentes, 2013)

Existen otras operaciones dentro del nivel actual que pueden mostrarse con el comando de opciones disponibles ***?***. Algunas de ellas son:

*R1(config-rtr)#**?***

Tabla 6.9 "Opciones disponibles del proceso *RIP1"*

Opción	Descripción
distance	Distancia administrativa
exit	Salida del modo de configuración del protocolo de enrutamiento
no	Niega un comando o lo establece por defecto
redistribute	Redistribuye los prefijos IPv6 desde otro protocolo de enrutamiento

Por ahora, no se configurará alguna de ellas.

Para continuar, se debe salir del nivel actual con ***exit*** y acceder a la interfaz a la cual se desea asignar el proceso RIP (en este caso es la serial 0/3/0), ya que lo único que se ha elaborado hasta el momento es la creación del proceso del protocolo.

*R1(config-rtr)#**exit***
R1(config)#
*R1(config)#**interface serial 0/3/0***
R1(config-if)#

En este punto, se capturará ***ipv6 rip RIP1 ?*** donde "*RIP1*" es el nombre del proceso RIPng creado anteriormente y que se asignará a la interfaz serial 0/3/0.

*R1(config-if)# **ipv6 rip RIP1 ?***

Tabla 6.10 "Opciones disponibles del proceso *RIP1* en la interfaz serial 0/3/0"

Opción	Descripción
default-information	Configura el manejo de la ruta por defecto
enable	Habilita/Deshabilita el enrutamiento RIP

Se agregará el comando ***enable*** para finalmente habilitar el proceso "*RIP1"* a la interfaz serial 0/3/0.

*R1(config-if)# **ipv6 rip RIP1 enable***
*R1(config-if)#**exit***
R1(config)#

La misma operación se realizará para la red LAN de R1. Es decir, el proceso *"RIP1"* será asignado a la interfaz gigabitethernet 0/0.

*R1(config)#**interface gigabitethernet 0/0***
*R1(config-if)#**ipv6 rip RIP1 enable***
*R1(config-if)#**end***
R1#

Como una última operación para corroborar que las interfaces fueron correctamente configuradas, se capturará el comando ***show run*** en modo privilegiado, y entre todo el código que surja se verificarán principalmente los segmentos mostrados a continuación:

*R1#**show run***
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address 2001:BD4:ABCD:1111::1/64
ipv6 rip RIP1 enable
!
interface Serial0/3/0
no ip address
ipv6 address 2001:BD4:12AB::1/64
ipv6 rip RIP1 enable
clock rate 64000

Confirmados los parámetros en ambas interfaces, se ha terminado con la configuración del router R1. Cabe decir, que las mismas operaciones se realizarán en el segundo enrutador (R2), cambiando únicamente las direcciones correspondientes a sus respectivas interfaces mostradas en la tabla 6.6 de la presente práctica.

Router "R2"

Como se mencionó anteriormente, para configurar el segundo router, el cable de consola puede únicamente cambiarse del extremo RJ-45 hacía el puerto de consola del R2. Lo único adicional sería iniciar una nueva sesión de hyperterminal.

La segunda opción es desconectar totalmente el cable de consola y enchufarlo a una computadora más cercana al R2. Cualquiera de las dos elecciones es válida y fiable.

Una vez lista las conexiones de hardware e iniciada una nueva sesión de hyperterminal se comenzarán a configurar las interfaces:

```
Router>
Router>enable
Router#show run
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/3/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/3/1
 no ip address
 shutdown
 clock rate 2000000
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
```

En caso de NO presentar los parámetros mostrados, se deberá reiniciar el router (ejemplo en la práctica 6.1, página 109).

Router#
*Router#**configure t***
Enter configuration commands, one per line. End with CNTL/Z.
*Router(config)#**hostname R2***
*R2(config)#**ipv6 unicast-routing***
*R2(config)#**interface gigabitethernet 0/0***
*R2(config-if)#**ipv6 address 2001:bd4:abcd:2222::1/64***
*R2(config-if)#**no shutdown***
R2(config-if)#
**Feb 10 22:04:05.543: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up*
**Feb 10 22:04:07.087: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up*

Físicamente se verifica la interfaz 0/0 habilitada (imagen 6.71).

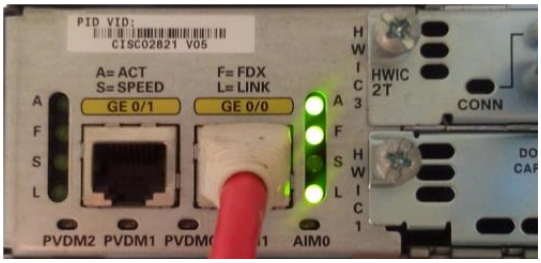


Imagen 6.71 “Interfaz Gigabitethernet 0/0 habilitada”

Confirmado esto, se procede a asignar la dirección IPv6 a su respectiva interfaz serial.

Nota: El número de la interfaz serial de R2 debe ser verificado como en R1. Esto, con el fin de evitar errores de captura y para configurar la interfaz correcta. En este caso, el número identificado es 0/3/0.

*R2(config-if)#**exit***
*R2(config)#**interface serial 0/3/0***
*R2(config-if)#**ipv6 address 2001:bd4:12ab::2/64***
R2(config-if)#
*R2(config-if)#**no shutdown***

Nota: R2 tiene asignada la conexión DTE, por lo tanto NO se debe configurar el clock rate.

*R2(config-if)#**exit***
R2(config)#

Al igual que gigabitethernet, físicamente se verificará que la interfaz serial haya sido habilitada.

Imagen 6.72 “Interfaz serial 0/3/0 habilitada”

Posteriormente se creará un nuevo proceso RIPng para ser asignado a las interfaces previamente configuradas. En este caso, el nombre será “***RIP2***”. Por lo tanto:

```
R2(config)#ipv6 router rip RIP2
R2(config-rtr)#exit
R2(config)#
R2(config)#interface serial 0/3/0
R2(config-if)#ipv6 rip RIP2 enable
R2(config-if)#exit
R2(config)#
R2(config)#interface gigabitethernet 0/0
R2(config-if)#ipv6 rip RIP2 enable
R2(config-if)#end
R2#
```

Se debe asegurar que las interfaces hayan sido correctamente configuradas con sus direcciones y su proceso RIP con el comando ***show run***:

```
R2#show run
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:BD4:ABCD:2222::1/64
 ipv6 rip RIP2 enable
!
interface Serial0/3/0
 no ip address
 ipv6 address 2001:BD4:12AB::2/64
 ipv6 rip RIP2 enable
!
```

Confirmados los parámetros en cada interfaz, se ha terminado la configuración de R2.

Para realizar una prueba de comunicación entre las redes se efectuará la operación “ping”, al igual que en la práctica 6.1. Sin embargo, el primer paso es verificar que los host contengan una dirección IPv6 estática, es decir, que se hayan agregado manualmente.

Para corroborarlo, se abre la consola de comandos de Windows, ya sea pulsando las teclas "Windows+R", escribir ***cmd*** y dar clic en "aceptar" o dar clic en "inicio" y escribir en el buscador ***símbolo del sistema***.

Una vez abierta la ventana, se escribirá ***ipconfig*** y se buscarán las direcciones correspondientes al "Adaptador Ethernet Ethernet" de ambas computadoras (imágenes 6.73 y 6.74).

Nota: La descripción detallada del comando "*ipconfig*" y la información posterior se describe en la página 113 de la práctica 6.1).

Imagen 6.73 "Dirección IPv6 del host Redes"

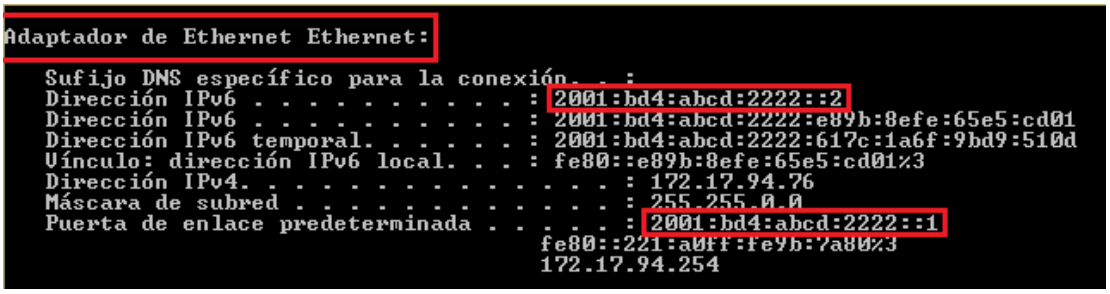


Imagen 6.74 "Dirección IPv6 del host Usuario"

Como puede apreciarse, ambas PC's ya tienen configuradas sus direcciones IPv6. Mismas que se muestran en la tabla de direccionamiento de la presente práctica (tabla 6.6, página 132).

Nota: Si los host presentan direcciones IPv6 distintas o se desconoce cómo asignar direcciones manualmente a un computador, se debe ir a la página 113 de la práctica 6.1.

Como una última operación antes de realizar el "ping", se debe verificar en ambas PC's que la regla de entrada del firewall mostrada en la imagen 6.75 se encuentre habilitada, ya que de lo contrario la comunicación no podrá ser posible.

Nota: Para más detalles acerca de las reglas de entrada y su relación con IPv6, ir a la práctica 6.1, página 118.

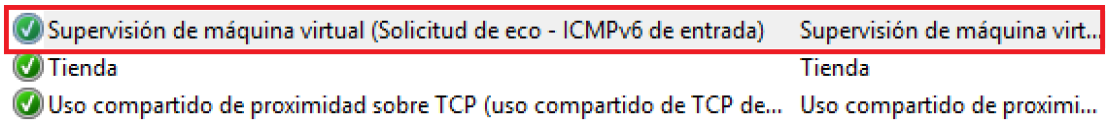


Imagen 6.75 "Regla a habilitar en Firewall de Windows 8"

Confirmados los requisitos previos, se procederá a lo siguiente.

PC Redes

Comenzando por la PC Redes, se realizará ping hacia las puertas de enlace del router R1. Posteriormente se hará la misma operación hacia el router vecino, es decir a las puertas de enlace del router R2 y finalmente a la PC Usuario.

Para un mejor entendimiento, se realizará la operación ping conforme se muestra en la siguiente lista:

- ping 2001:bd4:abcd:1111::1 - Interfaz gigabitethernet 0/0 (R1)
- ping 2001:bd4:bd4:12ab::1 - Interfaz serial 0/3/0 (R1)
- ping 2001:bd4:bd4:12ab::2 - Interfaz serial 0/3/0 (R2)
- ping 2001:bd4:abcd:2222::1 - Interfaz gigabitethernet 0/0 (R2)
- ping 2001:bd4:abcd:2222::2 - PC Usuario

Las siguientes imágenes son mostradas respectivamente a la lista anterior:

```
C:\Users\REDES>ping 2001:bd4:abcd:1111::1

Haciendo ping a 2001:bd4:abcd:1111::1 con 32 bytes de datos:
Respuesta desde 2001:bd4:abcd:1111::1: tiempo=2ms
Respuesta desde 2001:bd4:abcd:1111::1: tiempo=1ms
Respuesta desde 2001:bd4:abcd:1111::1: tiempo=1ms
Respuesta desde 2001:bd4:abcd:1111::1: tiempo=1ms

Estadísticas de ping para 2001:bd4:abcd:1111::1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 2ms, Media = 1ms

C:\Users\REDES>
```

Imagen 6.76 "Ping a la interfaz gigabitethernet 0/0, R1"

```
C:\Users\REDES ping 2001:bd4:12ab::1

Haciendo ping a 2001:bd4:12ab::1 con 32 bytes de datos:
Respuesta desde 2001:bd4:12ab::1: tiempo<1m
Respuesta desde 2001:bd4:12ab::1: tiempo=1ms
Respuesta desde 2001:bd4:12ab::1: tiempo=1ms
Respuesta desde 2001:bd4:12ab::1: tiempo=1ms

Estadísticas de ping para 2001:bd4:12ab::1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\REDES>
```

Imagen 6.77 “Ping a la interfaz serial 0/3/0, R1”

```
C:\Users\REDES ping 2001:bd4:12ab::2

Haciendo ping a 2001:bd4:12ab::2 con 32 bytes de datos:
Respuesta desde 2001:bd4:12ab::2: tiempo=24ms
Respuesta desde 2001:bd4:12ab::2: tiempo=23ms
Respuesta desde 2001:bd4:12ab::2: tiempo=23ms
Respuesta desde 2001:bd4:12ab::2: tiempo=23ms

Estadísticas de ping para 2001:bd4:12ab::2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 23ms, Máximo = 24ms, Media = 23ms

C:\Users\REDES>
```

Imagen 6.78 “Ping a la interfaz serial 0/3/0, R2”

```
C:\Users\REDES ping 2001:bd4:abcd:2222::1

Haciendo ping a 2001:bd4:abcd:2222::1 con 32 bytes de datos:
Respuesta desde 2001:bd4:abcd:2222::1: tiempo=23ms
Respuesta desde 2001:bd4:abcd:2222::1: tiempo=23ms
Respuesta desde 2001:bd4:abcd:2222::1: tiempo=23ms
Respuesta desde 2001:bd4:abcd:2222::1: tiempo=22ms

Estadísticas de ping para 2001:bd4:abcd:2222::1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 22ms, Máximo = 23ms, Media = 22ms

C:\Users\REDES>
```

Imagen 6.79 “Ping a la interfaz gigabitethernet 0/0, R2”

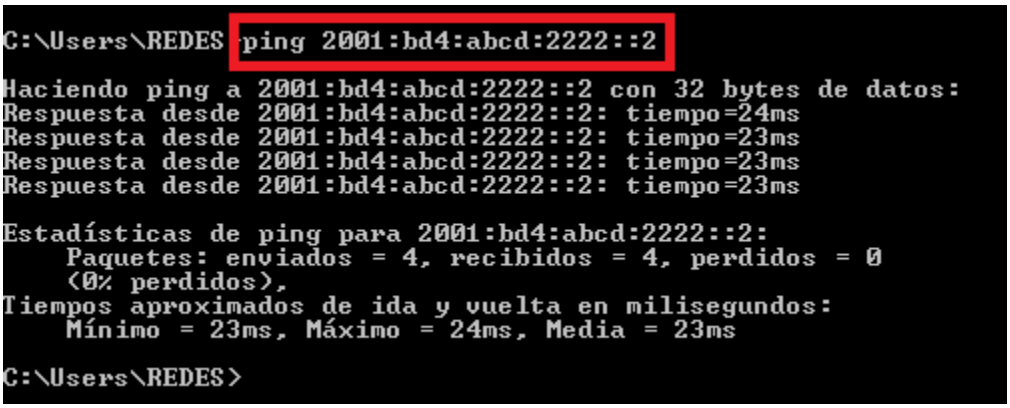


Imagen 6.80 "Ping al host Usuario"

Si la red se configuró correctamente, las respuestas del sistema debieron ser las mismas que se mostraron en las imágenes anteriores. De lo contrario, se debe verificar la configuración de los routers y corregir los errores correspondientes.

PC Usuario

De la misma manera que en el host Redes, primero se realiza un ping a las puertas de enlace del router correspondiente a la PC Usuario, es decir, hacia las interfaces del router R2. Seguidamente, se hace la misma operación a las puertas de enlace del R1 y finalmente a la PC Redes. En otras palabras, se realizará el ping conforme a la siguiente lista:

- ping 2001:bd4:abcd:2222::1 - Interfaz gigabitethernet 0/0 (R2)
- ping 2001:bd4:bd4:12ab::2 - Interfaz serial 0/3/0 (R2)
- ping 2001:bd4:bd4:12ab::1 - Interfaz serial 0/3/0 (R1)
- ping 2001:bd4:abcd:1111::1 - Interfaz gigabitethernet 0/0 (R1)
- ping 2001:bd4:abcd:1111::2 – PC Redes

Las siguientes imágenes son mostradas respectivamente a la lista anterior:

```
C:\Users\USUARIO>ping 2001:bd4:abcd:2222::1

Haciendo ping a 2001:bd4:abcd:2222::1 con 32 bytes de datos:
Respuesta desde 2001:bd4:abcd:2222::1: tiempo<1m
Respuesta desde 2001:bd4:abcd:2222::1: tiempo<1m
Respuesta desde 2001:bd4:abcd:2222::1: tiempo=1ms
Respuesta desde 2001:bd4:abcd:2222::1: tiempo=1ms

Estadísticas de ping para 2001:bd4:abcd:2222::1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\USUARIO>
```

Imagen 6.81 “Ping a la interfaz gigabitethernet 0/0, R2”

```
C:\Users\USUARIO>ping 2001:bd4:12AB::2

Haciendo ping a 2001:bd4:12ab::2 con 32 bytes de datos:
Respuesta desde 2001:bd4:12ab::2: tiempo<1m
Respuesta desde 2001:bd4:12ab::2: tiempo=1ms
Respuesta desde 2001:bd4:12ab::2: tiempo=1ms
Respuesta desde 2001:bd4:12ab::2: tiempo=1ms

Estadísticas de ping para 2001:bd4:12ab::2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\USUARIO>
```

Imagen 6.82 “Ping a la interfaz serial 0/3/0, R2”

```
C:\Users\USUARIO>ping 2001:bd4:12ab::1

Haciendo ping a 2001:bd4:12ab::1 con 32 bytes de datos:
Respuesta desde 2001:bd4:12ab::1: tiempo=23ms
Respuesta desde 2001:bd4:12ab::1: tiempo=23ms
Respuesta desde 2001:bd4:12ab::1: tiempo=23ms
Respuesta desde 2001:bd4:12ab::1: tiempo=23ms

Estadísticas de ping para 2001:bd4:12ab::1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 23ms, Máximo = 23ms, Media = 23ms

C:\Users\USUARIO>
```

Imagen 6.83 “Ping a la interfaz serial 0/3/0, R1”

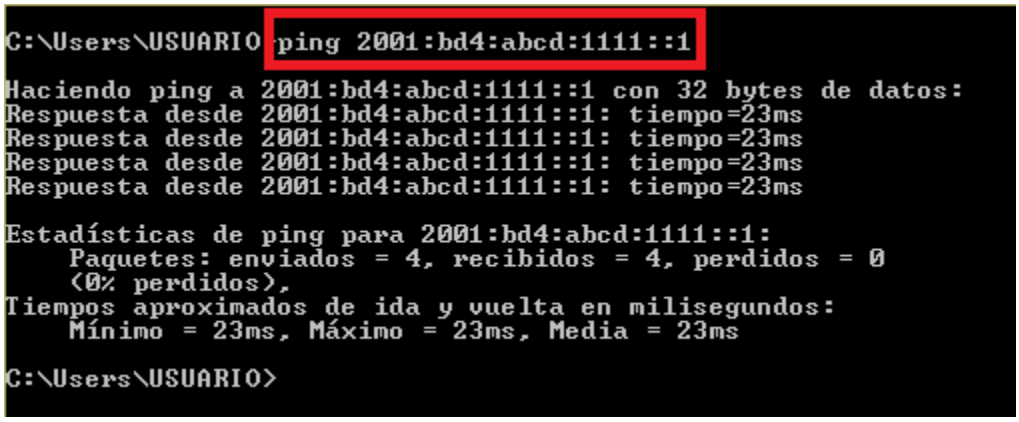


Imagen 6.84 “Ping a la interfaz gigabitethernet 0/0, R1”

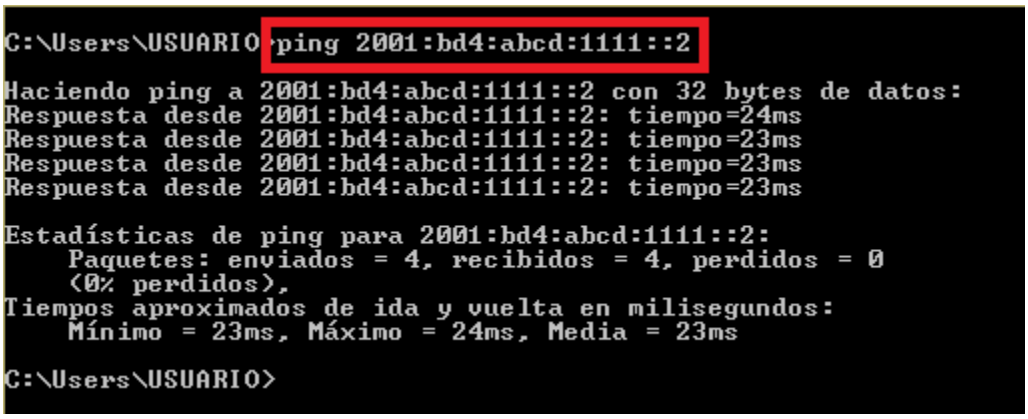


Imagen 6.85 “Ping al host Redes”

Tras haber conseguido las respuestas con éxito de cada interfaz, se ha terminado la práctica 6.2.

Durante el proceso de las prácticas 6.1 y 6.2 se utilizaron algunos comandos del entorno Cisco en su forma completa. Sin embargo, en las siguientes prácticas IPv6 serán implementados en su forma abreviada (tabla 6.11). Cabe señalar que esto no afecta sus funciones de configuración ni reduce su eficiencia, únicamente es para facilitar su captura.

Tabla 6.11 “Comandos Cisco abreviados”

Comando	Abreviación
enable	en
configure terminal	conf t
show run	sh r
interface fastethernet -/-/-	int f -/-/-
interface gigabitethernet -/-/-	int g -/-/-
interface serial	int s -/-/-
no shutdown	no sh
exit	ex
write	wr
show ipv6 route	sh ipv6 ro
show ipv6 interface brief	sh ipv6 int br

6.3 Introducción y configuración del protocolo EIGRPv6 en un entorno Cisco para la implementación de una red física de área extensa (WAN) utilizando IPv6

Objetivo:

- Comprender y configurar los parámetros básicos del protocolo de enrutamiento EIGRPv6.

Para desarrollar la práctica es esencial contar con los siguientes dispositivos:

- 2 Routers
- 2 Switch
- 4 Cables de red con configuración directa (cualquiera, T568-A o T568-B)
- 1 Cable DCE
- 1 Cable DTE
- 1 Cable de consola para la configuración remota de un enrutador
- 2 Computadoras (mismo S.O)

En este caso, el hardware específicamente utilizado fue el siguiente:

- 2 Router Cisco 2821 (2800 series)
- 2 Switch Cisco Catalyst 2960
- 2 Computadoras con el mismo S.O (Windows 8)
- 4 Cables de red con configuración directa T568-B
- 1 Cable de consola DB9 a RJ45
- 1 Cable smart serial DTE a V.35 macho
- 1 Cable smart serial DCE a V.35 hembra

La estructura que conforman los dispositivos para la práctica es la que se muestra en la siguiente imagen:

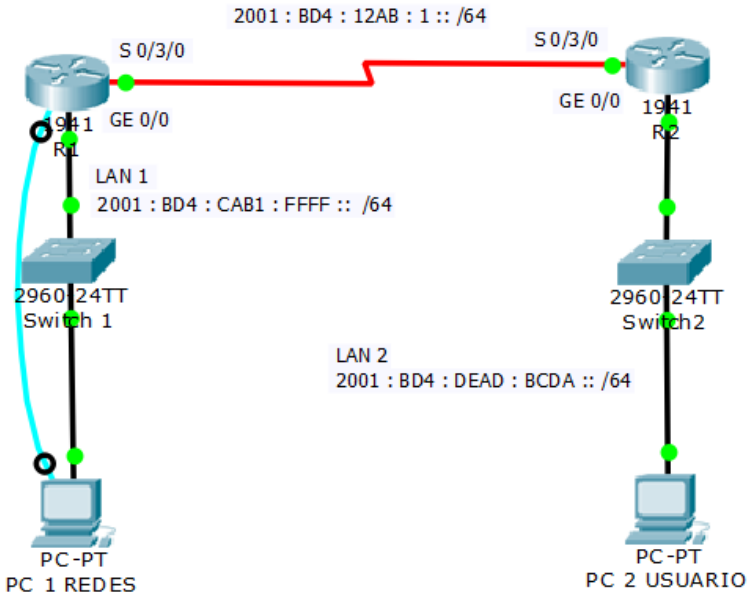


Imagen 6.86 “Diagrama de topología”

El anterior esquema de red es configurado bajo IPv6. Donde de igual manera, las redes locales (LAN) contienen sus correspondientes direcciones bajo el mismo protocolo.

La comunicación entre routers se establece mediante el enrutamiento de gateway interior mejorado (EIGRP) para IPv6, denominada EIGRPv6.

EIGRP es una versión mejorada del IGRP desarrollada por Cisco y se trata de un protocolo de enrutamiento por vector distancia mejorado que se basa en el algoritmo de actualización difusa (DUAL), para calcular la ruta más corta a un destino dentro de una red.

Las respectivas direcciones para cada interfaz se muestran en la siguiente tabla:

Tabla 6.12 "Tabla de direccionamiento"

DISPOSITIVO	TIPO DE INTERFAZ	NÚMERO INTERFAZ	DIRECCIÓN IPv6
R1	Serial	0/3/0	2001 : BD4 : 12AB : 1 :: 1
	Gigabitethernet (GE)	0/0	2001 : BD4 : CAB1 : FFFF :: 1
PC Redes	NIC	N/A	2001 : BD4 : CAB1 : FFFF :: 2
R2	Serial	0/3/0	2001 : BD4 : 12AB : 1 :: 2
	Gigabitethernet (GE)	0/0	2001 : BD4 : DEAD: BCDA :: 1
PC Usuario	NIC	N/A	2001 : BD4 : DEAD: BCDA :: 2

Las conexiones físicas deben ser idénticas a las que se mostraron en las prácticas 6.1 y 6.2, así como la conexión de los cables DCE y DTE que permiten la comunicación entre las redes (routers). Únicamente la variación existente es la configuración lógica que se introducirá a ambos enrutadores.

Nota: En esta práctica se han proporcionado los números de interfaz de tipo serial de ambos routers. Para cualquier duda de cómo identificarlos físicamente y configurarlos deberá ir a la página 132 de la práctica 6.2.

Una vez dentro del software hyperterminal y de haber corroborado que no exista alguna configuración previa en los routers (utilizar el comando ***show run***), se comienza a configurar las interfaces del primer router.

Router "R1"

*Router>**ena***
*Router#**config t***
Enter configuration commands, one per line. End with CNTL/Z.
*Router(config)#**hostname R1***
*R1(config)#**ipv6 unicast-routing***
*R1(config)#**int g0/0***
*R1(config-if)#**ipv6 address 2001:bd4:cab1:ffff::1/64***

*R1(config-if)#**no sh***
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
*R1(config-if)#**exit***
*R1(config)#**int s0/3/0***
*R1(config-if)#**ipv6 address 2001:bd4:12ab:1::1/64***
*R1(config-if)#**clock rate 64000***
*R1(config-if)#**no sh***
%LINK-5-CHANGED: Interface Serial0/3/0, changed state to down
%SYS-5-CONFIG_I: Configured from console by console

*R1(config-if)#**exit***
R1(config)#

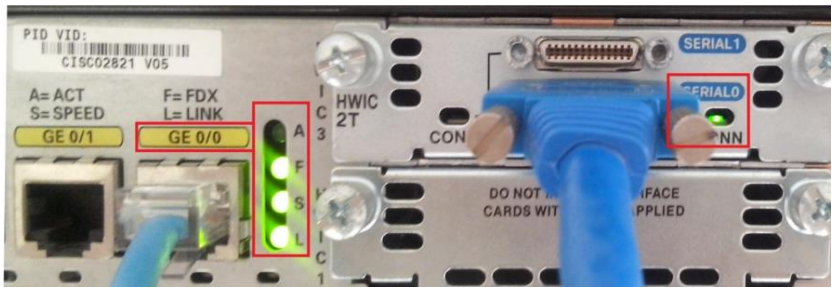


Imagen 6.87 “Interfaz GE 0/0 y Serial 0/3/0 habilitadas”

Hasta este punto únicamente se han configurado las interfaces. Lo siguiente es configurar el protocolo de enrutamiento EIGRPv6, pero, se deben conocer un par de datos útiles para entender su funcionamiento, ya que existe información adicional y algunas variaciones con respecto a la configuración de la versión 4.

Lo primero que se debe conocer es que EIGRP utiliza un factor esencial llamado ID de proceso. De hecho, EIGRP y OSPF lo utilizan para representar una instancia del protocolo de enrutamiento respectivo que se ejecuta en el router.

Por lo tanto, el próximo comando a capturar es el siguiente:

*R1(config)#**ipv6 router eigrp** “autonomous system”*

Donde el parámetro “*autonomous system*”, se traduce como un sistema autónomo.

Aunque EIGRP hace referencia a este parámetro como un número de “sistema autónomo”, en realidad funciona como el ID de proceso que se mencionó anteriormente. El número no se encuentra asociado con ningún número de sistema autónomo (analizado posteriormente) y se le puede asignar cualquier valor de 16 bits, es decir de 1 a 65,535 (2^{16}).

El motivo por el cual no puede introducirse un número de sistema autónomo (AS) es porque este representa a un conjunto de redes bajo el control administrativo de una única entidad que presenta una política de enrutamiento común para Internet.

Por tal motivo, estos números únicamente se utilizan por grandes organizaciones. Por ejemplo, ISP's, proveedores backbone de Internet y grandes instituciones que se conectan con otras entidades que también cuentan con un número de AS.

Estos ISP y las grandes instituciones utilizan el Border Gateway Protocol (BGP), del protocolo de enrutamiento de gateway exterior para propagar información de enrutamiento. BGP es el único protocolo de enrutamiento que utiliza un número de sistema autónomo real en su configuración.

La gran mayoría de las empresas e instituciones con redes IP no necesitan un número de AS porque se encuentran bajo el control de una entidad más grande, como un ISP. Estas empresas utilizan protocolos de gateway interior como RIP, EIGRP, OSPF e ISIS para realizar el enrutamiento de paquetes dentro de sus propias redes. Son una de muchas redes independientes dentro del sistema autónomo de ISP (imagen 6.88). ISP es el responsable del enrutamiento de paquetes dentro del sistema autónomo y entre otros sistemas autónomos.

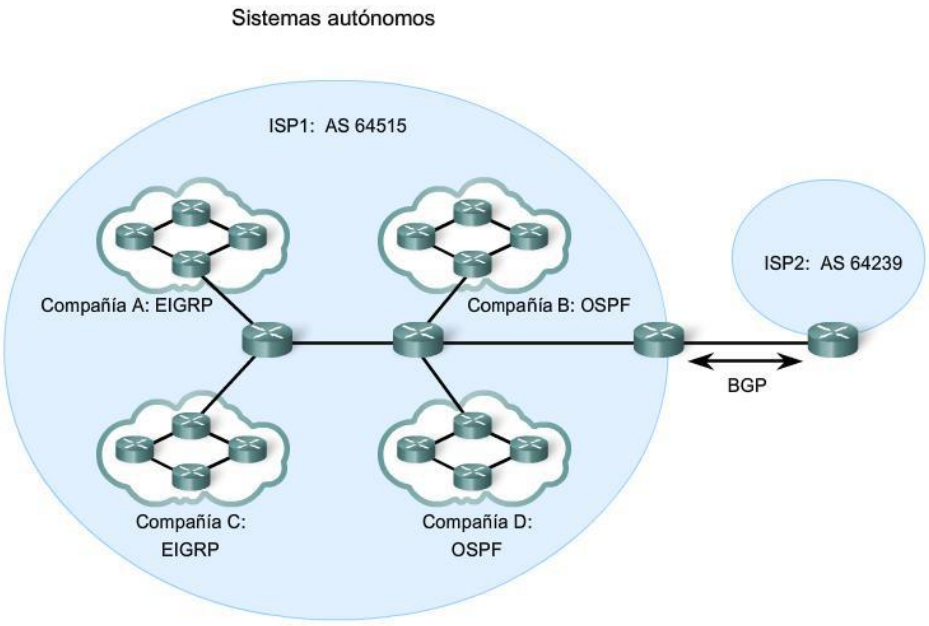


Imagen 6.88 “Escala y asignación de un AS”

Dichos números son asignados por la IANA hacia los RIR's existentes, y estos a su vez asignan otros AS de acuerdo al espacio que se les asignó.

Antes del 2007 los números de AS eran de 16 bits, que iban de 0 a 65,535. En la actualidad, se asignan números de AS de 32 bits, con lo que se aumenta el número de AS disponibles a más de 4 mil millones. (CCNA 2 Exploration, s.f)

Por lo tanto, siendo explicadas y entendidas las diferencias entre un ID de proceso y un número de sistema autónomo, las posibilidades de cometer un error disminuirán al momento de configurar cualquier red bajo un protocolo que contenga el parámetro "*autonomous system*".

Nota: Se describieron ambas diferencias ya que en la mayoría de las prácticas IPv6 implementando EIGRP u otro protocolo de enrutamiento, la representación del ID del proceso al momento de configurarlo viene similarmente o de la misma manera que en la última línea capturada ("*autonomous system"*). Generando diversas confusiones al momento de su configuración.

Posteriormente, se creará el número de proceso EIGRPv6 (entre 1 y 65,535).

*R1(config)#**ipv6 router eigrp ?***
<1-65535> Autonomous system number
*R1(config)#**ipv6 router eigrp 1***
R1(config-rtr)#

En esta práctica, el número 1 identifica el proceso particular EIGRP que se ejecuta en este router. Cabe resaltar, que para poder establecer adyacencias de vecinos, EIGRP requiere que todos los routers del mismo dominio de enrutamiento estén configurados con el mismo ID de proceso. Por lo general, sólo se configura un único ID de proceso de cualquier protocolo de enrutamiento en un router (imagen 6.89).

Imagen 6.89 "Conjunto de routers formado por un ID de proceso EIGRP"

Nota: El parámetro "sistema autónomo" es un número que el administrador de red elige entre 1 y 65535. El valor elegido es el número del ID de proceso y es importante porque todos los routers en el dominio de enrutamiento EIGRPv6 deben usar el mismo ID de proceso.

Como puede apreciarse el indicador principal cambió a un nuevo nivel de configuración:

R1(config-rtr)#

Lo anterior indica que el proceso EIGRP ha sido creado y se está dentro de él.

En este punto, debe tomarse en cuenta que EIGRP para IPv6 tiene una función de apagado administrativamente de forma predeterminada (shutdown). Por lo que debe capturarse ***no shutdown*** para comenzar a ejecutar el protocolo y continuar con la configuración. Ya que de lo contrario no existirá comunicación entre los enrutadores aunque se realice la práctica correctamente.

*R1(config-rtr)#**no sh***

Lo siguiente a configurar (una vez listo el ID de proceso) es establecer un nuevo identificador de 32 bits en formato IPv4 ("A.B.C.D") y que se denomina como "router-id" o RID.

En IPv4, EIGRP tomaba dicho RID directamente de una de sus interfaces de red. Sin embargo, si en EIGRPv6 no se cuenta con el identificador requerido, el proceso del protocolo no tendrá un router-id. En otras palabras, el protocolo estará inactivo y no existirá comunicación.

Dicho identificador es asignado basándose a las siguientes prioridades:

- Mediante la configuración manual con el comando ***eigrp router-id*** *"A.B.C.D"*
- La dirección IPv4 loopback más alta.
- La primera dirección IPv4 que se encuentra en cualquier interfaz física. (Cisco, 2014)

Nota: En la mayoría de los casos el identificador es asignado manualmente.

Nota: El router-id no puede tomar una dirección loopback en formato IPv6, ya que en los propios requerimientos del protocolo EIGRPv6 la demanda es en formato IPv4. Tal y como se muestra a continuación:

*R1(config-rtr)#**eigrp router-id ?***
A.B.C.D EIGRP Router-ID in IP address format

Nota: El router-id es obligatorio para que EIGRPv6 funcione correctamente

Dicho ID de 32 bits se utiliza para identificar en forma exclusiva a cada router en el dominio de enrutamiento EIGRP. Se recomienda que cada enrutador sea asignado con un router-id distinto (sin olvidar que el ID de proceso debe ser igual). Esto con la finalidad de facilitar la administración de los equipos y/o al realizar algún análisis de enrutamiento en un futuro.

Nota: El RID viene incluido en la información intercambiada cuando un router se une a la red EIGRP. De tal forma que identifica y se identifica con otros vecinos EIGRP.

Aclarado lo anterior, se introduce el identificador ***1.1.1.1*** y se saldrá de la configuración actual.

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

Nota: Recuerde que los 4 valores decimales formados por 8 bits (cada uno), tienen un rango entre 0 y 255.

Concluidos los pasos anteriores, finalmente el código completo quedó de la siguiente manera:

*R1(config)#**ipv6 router eigrp 1***
*R1(config-rtr)#**no sh***
*R1(config-rtr)#**eigrp router-id 1.1.1.1***
*R1(config-rtr)#**exit***
*R1(config)#**end***

Hasta esta operación, únicamente se ha creado el proceso EIGRPv6 y su correspondiente RID. Sin embargo el protocolo aún no puede enrutar paquetes a través de su enlace.

Para verificar que la configuración fue realizada correctamente, se ejecutará un ***show run*** en modo privilegiado, verificando que los dos identificadores se crearon exitosamente.

*R1#**show run***
!
!
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address 2001:BD4:CAB1:FFFF::1/64
!
interface Serial0/3/0
no ip address
ipv6 address 2001:BD4:12AB:1::1/64
clock rate 64000
!
ipv6 router eigrp 1
eigrp router-id 1.1.1.1
no shutdown
!

Nota: Los parámetros utilizados para configurar EIGRP y su funcionamiento son muy similares a los que utiliza OSPF. De hecho, EIGRP no se considera totalmente un protocolo vector distancia, dado que contiene diversas características de un protocolo de estado de enlace. Y, aunque la información intercambiada entre los enrutadores EIGRP no es tan detallada como en los datos de topología OSPF (el cual pretende describir cada router y enlace de la red), sí describe algo más que solo una distancia (métrica) y un vector (router del siguiente salto).

Nota: Un enrutador también se entera de la métrica que utiliza el router del siguiente salto. Es decir, EIGRP mantiene un registro de cada posible router del siguiente salto para las rutas alternativas y algunos detalles métricos relacionados con estas rutas. Sin embargo no hay información acerca de la topología más allá de los enrutadores del salto siguiente.

El último dato a conocer, es que en EIGRPv6 cada interfaz debe configurarse de forma independiente. Es decir, una vez que los datos anteriores hayan sido confirmados, se tiene que entrar a la configuración global del router y acceder primero a la interfaz gigabitethernet conectada; habilitar el proceso creado EIGRPv6 (activando implícitamente el RID) con el comando ***ipv6 eigrp*** "*numero de proceso*", y posteriormente realizar lo mismo con la interfaz serial. De tal forma que el código queda de la siguiente manera:

*R1#**config t***
*R1(config)# **int g0/0***
*R1(config-if)#**ipv6 eigrp 1***
*R1(config-if)# **int s0/3/0***
*R1(config-if)#**ipv6 eigrp 1***
*R1(config-if)#**end***
R1#

Nota: No hay ningún inconveniente si no se introduce el comando "exit" para salir de la interfaz actual y configurar la siguiente. Tampoco es necesario usar el comando "no shutdown" después de haber asignado el proceso EIGRPv6 a cada interfaz.

Para confirmar que ambas interfaces ahora tienen habilitado el proceso del protocolo, se realiza nuevamente un ***show run***, verificando los siguientes datos:

*R1#**show run***
!
!
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address 2001:BD4:CAB1:FFFF::1/64
ipv6 eigrp 1
!
interface Serial0/3/0
no ip address
ipv6 address 2001:BD4:12AB:1::1/64
ipv6 eigrp 1
clock rate 64000
!
!
ipv6 router eigrp 1
eigrp router-id 1.1.1.1
no shutdown
!

Una vez corroborados los datos, se procede a realizar la misma configuración al router "R2" sin olvidar configurar sus correspondientes direcciones.

Nota: En esta práctica, se recomienda no finalizar la sesión hyperterminal del router R1, ya que posteriormente se utilizará para corroborar la adyacencia entre los enrutadores. Únicamente debe desconectarse el cable de consola del host y del router sin cerrar la ventana de la sesión actual, o en caso de ocupar el mismo host, únicamente debe iniciarse una nueva sesión hyperterminal (sin cerrar la actual).

Router "R2"

*Router>**ena***
*Router#**config t***
Enter configuration commands, one per line. End with CNTL/Z.
*Router(config)#**hostname R2***
*R2(config)#**ipv6 unicast-routing***
*R2(config)#**int g0/0***
*R2(config-if)#**ipv6 address 2001:bd4:dead:bcda::1/64***
*R2(config-if)#**no sh***
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

*R2(config-if)#**exit***
*R2(config)#**int s0/3/0***
*R2(config-if)#**ipv6 address 2001:bd4:12ab:1::2/64***
*R2(config-if)#**no sh***
R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/3/0, changed state to down
%SYS-5-CONFIG_I: Configured from console by console

*R2(config-if)#**exit***

Una vez listas las interfaces, se creará el ID de proceso EIGRPv6, sin olvidar que el número de identificador debe ser el mismo que en el primer router. Seguidamente, se configurará el router-id, siendo este distinto del primer enrutador.

*R2(config)#**ipv6 router eigrp 1***
*R2(config-rtr)#**no sh***
*R2(config-rtr)#**eigrp router-id 2.2.2.2***
*R2(config-rtr)#**exit***

Nota: Como se mencionó anteriormente, el identificador de proceso EIGRPv6 debe ser el mismo que en el primer router. Esto con el objetivo de poder establecer una adyacencia (identificación y comunicación) entre los enrutadores.

*R2(config)#**int g0/0***
*R2(config-if)#**ipv6 eigrp 1***
*R2(config-if)#**int s0/3/0***
*R2(config-if)#**ipv6 eigrp 1***
R2(config-if)#

%DUAL-5-NBRCHANGE: IPv6-EIGRP 1: Neighbor FE80::221:A0FF:FE33:D700 (Serial0/3/0) is up: new adjacency

Como puede observarse en la última línea, el IOS devolvió un mensaje, indicando que dentro del protocolo EIGRPv6 se encontró un vecino (Neighbor) con la dirección "*FE80::221:A0FF:FE33:D700* " (dirección unicast de enlace local por su prefijo "FE80"). Lo cual indica que ahora existe una adyacencia entre los enrutadores.

"En IPv6, las direcciones de enlace local son usadas por EIGRP para el origen de los paquetes de saludo y establecer una adyacencia. Dicha dirección nunca se enruta y se auto asignan cuando los administradores activan una interfaz." (Cisco, 2014)

Nota: El algoritmo utilizado por EIGRP (DUAL) emplea los paquetes de saludo para que los enrutadores se reconozcan entre sí, de esa manera conocen la estructura de la red.

Las direcciones IPv6 de enlace local son ideales para el intercambio de mensajes entre vecinos. Dicha dirección permite que un dispositivo se comunique con otros dispositivos con IPv6 habilitado en el mismo enlace y solo en ese enlace (subred). Los paquetes con una dirección de enlace local de origen o de destino no se pueden enrutar más allá del enlace en el cual se originó el paquete.

Nota: Cuando debe enviarse un paquete a una dirección multidifusión se envía a la dirección IPv6 multicast FF02::A, es decir, el ámbito de todos los routers EIGRP en el enlace local. Si el paquete puede enviarse como una dirección de unicast, se envía a la dirección de enlace local del router vecino.

Si se desea corroborar este hecho se debe capturar el siguiente comando en modo privilegiado (de lo contrario, pase a la página 167):

*R2#**show ipv6 eigrp neighbors***

El comando anterior muestra la información de los vecinos reconocidos por el protocolo EIGRPv6. En este caso, la línea que se muestra después de la captura realizada, resalta que la lista expuesta es para los vecinos que pertenecen al proceso 1 (imagen 6.90). (ExamCollection, s.f).

```
R2#
R2#show ipv6 eigrp neighbors
IPv6-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   Link-local address:     Se0/3/0           11 00:02:45   29   200  0  3
    FE80::221:A0FF:FE33:D700
```

Imagen 6.90 "Adyacencia de vecinos R1 y R2"

Como puede apreciarse, en la primera fila se encuentra la dirección de enlace local del enrutador vecino y además, el número de interfaz por el cual se establece la adyacencia.

Por otro lado, en la sesión hyperterminal de R1 se capturará el siguiente comando en modo privilegiado:

*R2#**show ipv6 interface brief***

Nota: También puede simplificarse a solo ***"sh ipv6 int br"***

```
R1#
R1#show ipv6 int br
GigabitEthernet0/0         [up/up]
    FE80::221:A0FF:FE33:D700
    2001:BD4:CAB1:FFFF::1
GigabitEthernet0/1         [administratively down/down]
    unassigned
Serial0/3/0                [up/up]
    FE80::221:A0FF:FE33:D700
    2001:BD4:12AB:1::1
Serial0/3/1                [administratively down/down]
    unassigned
SSLVPN-VIF0                [up/up]
    unassigned
```

Imagen 6.91 "Dirección de enlace local de R1 para verificación de adyacencia"

Dicho comando, muestra información acerca de las direcciones IPv6 asignadas a las interfaces. Y, como puede apreciarse, en la interfaz serial 0/3/0 la dirección unicast de enlace local es la misma que el router R2 reconoce como vecino.

Nota: Si se desea verificar y/o conocer más información del actual protocolo, el comando ***show ipv6 eigrp ?*** desplegará una lista de las opciones disponibles para complementar los datos deseados.

Después de finalizar la configuración de ambos routers, se procede a configurar las direcciones IPv6 correspondientes a los host de cada subred. Con el objetivo de realizar la operación "ping" y corroborar la comunicación exitosa de ambas PC's.

La configuración de las direcciones IPv6 (mostradas en la tabla 6.12) se realiza de forma manual en los host. Por lo que en la PC Redes y la PC Usuario quedan de la siguiente forma:

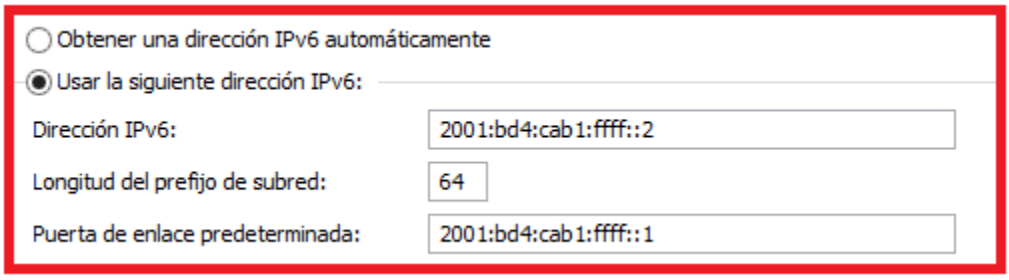


Imagen 6.92 "Configuración manual de dirección IPv6 de la PC Redes"

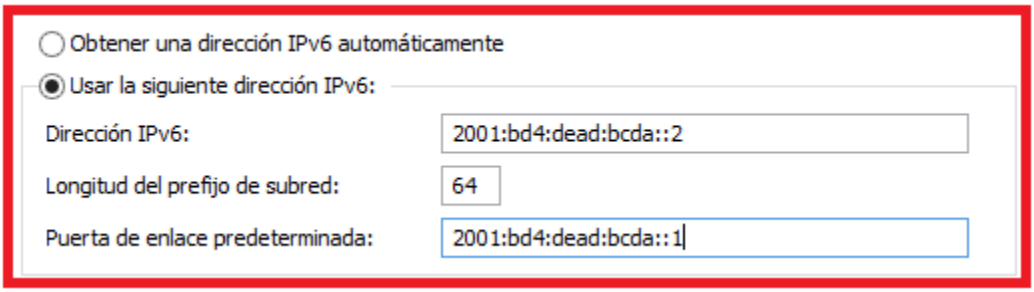


Imagen 6.93 "Configuración manual de dirección IPv6 de la PC Usuario"

Nota: Para conocer cómo configurar direcciones manualmente ir a la página 113 de la práctica 6.1.

Es conveniente asegurarse que dichas direcciones sean reconocidas por el S.O de los host. Es decir, se deben verificar en la ventana de línea de comandos de Windows (MS-DOS) capturando el comando ***ipconfig***. El resultado se debe observar como en las siguientes imágenes:

Imagen 6.94 “Direcciones IPv6 del host Redes”

Imagen 6.95 “Direcciones IPv6 del host Usuario”

Tras haber hecho los pasos anteriores y de verificar las reglas de entrada del firewall (explicado en la práctica 6.1, página 118) se procede a ejecutar la operación “ping”.

PC Redes

En el primer host, la operación ping se efectuará hacía 5 direcciones:

- 2001 : bd4 : cab1 : ffff : 1 - Interfaz gigabitethernet 0/0 (R1)
- 2001 : BD4 : 12AB : 1 :: 1 - Interfaz serial 0/3/0 (R1)
- 2001 : BD4 : 12AB : 1 :: 2 - Interfaz serial 0/3/0 (R2)
- 2001 : BD4 : DEAD: BCDA :: 1 - Interfaz gigabitethernet 0/0 (R2)
- 2001 : BD4 : DEAD: BCDA :: 2 - PC Usuario

Las siguientes imágenes (6.96 a 6.100) se muestran respectivamente a la lista anterior. Corroborando que exista respuesta en cada una.

```
C:\Users\REDES>ping 2001:bd4:cab1:ffff::1

Haciendo ping a 2001:bd4:cab1:ffff::1 con 32 bytes de datos:
Respuesta desde 2001:bd4:cab1:ffff::1: tiempo=1ms
Respuesta desde 2001:bd4:cab1:ffff::1: tiempo=1ms
Respuesta desde 2001:bd4:cab1:ffff::1: tiempo=1ms
Respuesta desde 2001:bd4:cab1:ffff::1: tiempo=1ms

Estadísticas de ping para 2001:bd4:cab1:ffff::1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 1ms, Media = 1ms

C:\Users\REDES>
```

Imagen 6.96 “Ping a la interfaz gigabitethernet 0/0, R1”

```
C:\Users\REDES>ping 2001:bd4:12ab:1::1

Haciendo ping a 2001:bd4:12ab:1::1 con 32 bytes de datos:
Respuesta desde 2001:bd4:12ab:1::1: tiempo=1ms
Respuesta desde 2001:bd4:12ab:1::1: tiempo=1ms
Respuesta desde 2001:bd4:12ab:1::1: tiempo=1ms
Respuesta desde 2001:bd4:12ab:1::1: tiempo=1ms

Estadísticas de ping para 2001:bd4:12ab:1::1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 1ms, Media = 1ms

C:\Users\REDES>
```

Imagen 6.97 “Ping a la interfaz serial 0/3/0, R1”

```
C:\Users\REDES>ping 2001:bd4:12ab:1::2

Haciendo ping a 2001:bd4:12ab:1::2 con 32 bytes de datos:
Respuesta desde 2001:bd4:12ab:1::2: tiempo=23ms
Respuesta desde 2001:bd4:12ab:1::2: tiempo=23ms
Respuesta desde 2001:bd4:12ab:1::2: tiempo=23ms
Respuesta desde 2001:bd4:12ab:1::2: tiempo=23ms

Estadísticas de ping para 2001:bd4:12ab:1::2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 23ms, Máximo = 23ms, Media = 23ms

C:\Users\REDES>
```

Imagen 6.98 “Ping a la interfaz serial 0/3/0, R2”

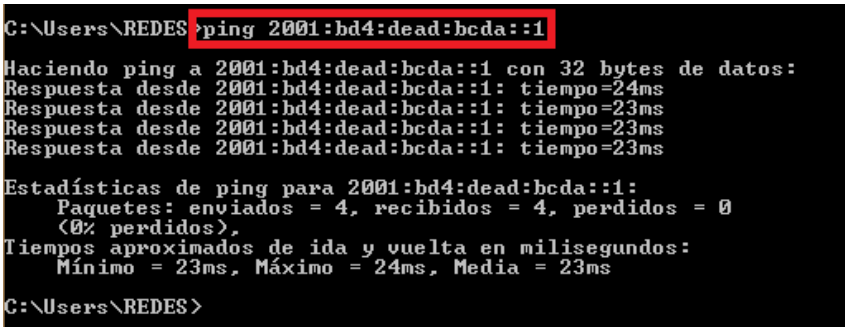


Imagen 6.99 Ping a la interfaz gigabitethernet 0/0, R2

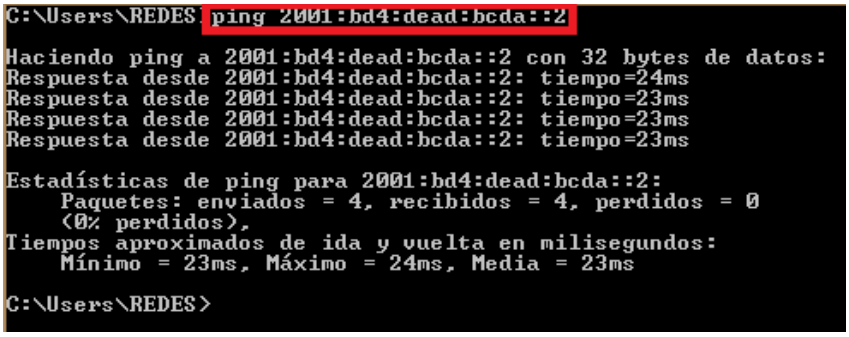


Imagen 6.100 “Ping al host Usuario”

PC Usuario

Al igual que en el host Redes, en la PC Usuario se realiza el “ping” a las siguientes direcciones:

- 2001 : BD4 : DEAD: BCDA :: 1 - Interfaz gigabitethernet 0/0 (R2)
- 2001 : BD4 : 12AB : 1 :: 2 - Interfaz serial 0/3/0 (R2)
- 2001 : BD4 : 12AB : 1 :: 1 - Interfaz serial 0/3/0 (R1)
- 2001 : bd4 : cab1 : ffff : 1 - Interfaz gigabitethernet 0/0 (R1)
- 2001 : bd4 : cab1 : ffff : 1 – PC Redes

Las siguientes imágenes (6.101 a 6.105) se muestran respectivamente a la lista anterior:

```
C:\Users\USUARIO>ping 2001:bd4:dead:bcda::1

Haciendo ping a 2001:bd4:dead:bcda::1 con 32 bytes de datos:
Respuesta desde 2001:bd4:dead:bcda::1: tiempo<1m
Respuesta desde 2001:bd4:dead:bcda::1: tiempo=1ms
Respuesta desde 2001:bd4:dead:bcda::1: tiempo=1ms
Respuesta desde 2001:bd4:dead:bcda::1: tiempo=1ms

Estadísticas de ping para 2001:bd4:dead:bcda::1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

Imagen 6.101 “Ping a la interfaz gigabitethernet 0/0, R2”

```
C:\Users\USUARIO>ping 2001:bd4:12ab:1::2

Haciendo ping a 2001:bd4:12ab:1::2 con 32 bytes de datos:
Respuesta desde 2001:bd4:12ab:1::2: tiempo<1m
Respuesta desde 2001:bd4:12ab:1::2: tiempo=1ms
Respuesta desde 2001:bd4:12ab:1::2: tiempo=1ms
Respuesta desde 2001:bd4:12ab:1::2: tiempo=1ms

Estadísticas de ping para 2001:bd4:12ab:1::2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

Imagen 6.102 “Ping a la interfaz serial 0/3/0, R2”

```
C:\Users\USUARIO>ping 2001:bd4:12ab:1::1

Haciendo ping a 2001:bd4:12ab:1::1 con 32 bytes de datos:
Respuesta desde 2001:bd4:12ab:1::1: tiempo=23ms
Respuesta desde 2001:bd4:12ab:1::1: tiempo=23ms
Respuesta desde 2001:bd4:12ab:1::1: tiempo=22ms
Respuesta desde 2001:bd4:12ab:1::1: tiempo=23ms

Estadísticas de ping para 2001:bd4:12ab:1::1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 22ms, Máximo = 23ms, Media = 22ms
```

Imagen 6.103 “Ping a la interfaz serial 0/3/0, R1”

```
C:\Users\USUARIO>ping 2001:bd4:cab1:ffff::1

Haciendo ping a 2001:bd4:cab1:ffff::1 con 32 bytes de datos:
Respuesta desde 2001:bd4:cab1:ffff::1: tiempo=24ms
Respuesta desde 2001:bd4:cab1:ffff::1: tiempo=23ms
Respuesta desde 2001:bd4:cab1:ffff::1: tiempo=23ms
Respuesta desde 2001:bd4:cab1:ffff::1: tiempo=23ms

Estadísticas de ping para 2001:bd4:cab1:ffff::1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 23ms, Máximo = 24ms, Media = 23ms
```

Imagen 6.104 “Ping a la interfaz gigabitethernet 0/0, R1”

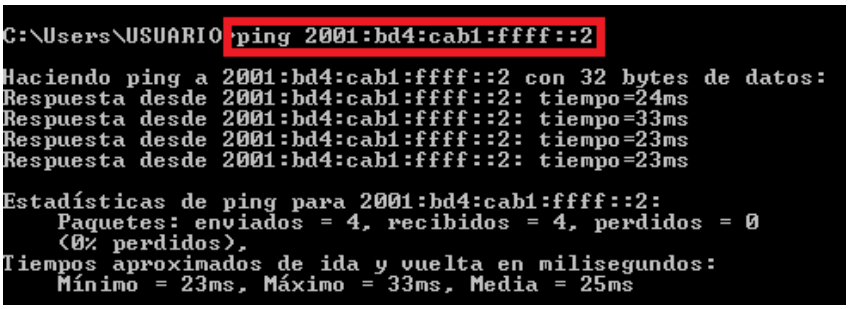


Imagen 6.105 “Ping al host Redes”

Tras haber corroborado las respuestas de las operaciones “ping” se ha finalizado con éxito la práctica 6.3.

6.4 Introducción y configuración del protocolo OSPFv3 en un entorno Cisco para la implementación de una red física de área extensa (WAN) utilizando IPv6

Objetivo:

- Comprender y configurar los parámetros básicos del protocolo de enrutamiento OSPFv3.

Para desarrollar la práctica es esencial contar con los siguientes dispositivos:

- 2 Routers
- 2 Switch
- 4 Cables de red con configuración directa (cualquiera, T568-A o T568-B)
- 1 Cable DCE
- 1 Cable DTE
- 1 Cable de consola para la configuración remota de un enrutador
- 2 Computadoras (mismo S.O)

En este caso, el hardware específicamente utilizado fue el siguiente:

- 2 Router Cisco 2821 (2800 series)
- 2 Switch Cisco Catalyst 2960
- 2 Computadoras con el mismo S.O (Windows 8)
- 4 Cables de red con configuración directa T568-B
- 1 Cable de consola DB9 a RJ45
- 1 Cable smart serial DTE a V.35 macho
- 1 Cable smart serial DCE a V.35 hembra

La estructura que conformarán los dispositivos para la práctica es la que se muestra en la imagen 6.106. (Diagrama de topología)

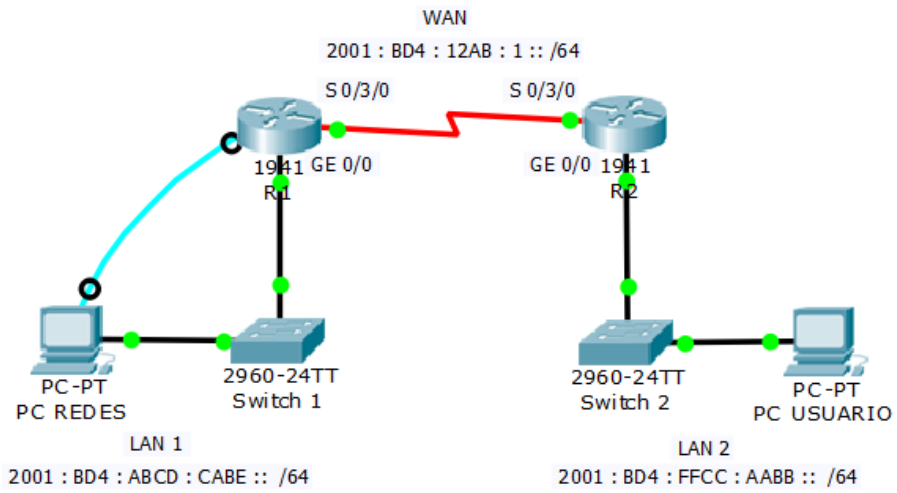


Imagen 6.106 “Diagrama de topología”

El esquema de red mostrado es configurado bajo el protocolo IPv6, donde las redes locales (LAN) de igual manera contienen sus correspondientes direcciones bajo la misma versión IP.

La comunicación entre routers se establece mediante el protocolo de estado de enlace llamado Open Shortest Path First o mejor conocido como OSPF. Sin embargo se usará en su tercera versión por utilizar IPv6.

Dicho protocolo fue diseñado por el grupo de trabajo IETF (Grupo de trabajo de ingeniería de Internet), que en la actualidad aún existe.

El desarrollo de OSPF comenzó en 1987 y actualmente hay dos versiones en uso:

- OSPFv2: OSPF para redes IPv4 (RFC 1247 y RFC 2328)
- OSPFv3: OSPF para redes IPv6 (RFC 2740)

Se trata de un protocolo de enrutamiento de estado de enlace y fue desarrollado como reemplazo del protocolo de enrutamiento por vector de distancia, RIP. RIP, constituyó un protocolo de enrutamiento aceptable en los comienzos del networking y de Internet; sin embargo, su dependencia en el conteo de saltos como la única medida para elegir el mejor camino rápidamente se volvió inaceptable en redes mayores que necesitaban una solución de enrutamiento más sólida. Por el contrario, OSPF es un protocolo de enrutamiento sin clase que utiliza el concepto de áreas para realizar la escalabilidad.

Las principales ventajas de OSPF frente a RIP son su rápida convergencia y escalabilidad a implementaciones de redes mucho mayores.

Nota: En 1989, la especificación para OSPFv1 se publicó en RFC 1131. Había dos implementaciones desarrolladas: una para ejecutar en routers y otra para ejecutar en estaciones de trabajo UNIX. La última implementación se convirtió luego en un proceso UNIX generalizado y conocido como GATED. Por tal motivo OSPFv1 fue un protocolo de enrutamiento experimental y nunca se implementó.

Continuando con la realización de la práctica, en la tabla 6.13 se muestran las respectivas direcciones para cada interfaz de los dispositivos que conforman la red.

Tabla 6.13 “Tabla de direccionamiento”

DISPOSITIVO	TIPO DE INTERFAZ	NUMERO INTERFAZ	DIRECCIÓN IPv6
R1	Serial	0/3/0	2001 : BD4 : 12AB : 1 :: 1
	Gigabitethernet (GE)	0/0	2001 : BD4 : ABCD : CABE :: 1
PC Redes	NIC	N/A	2001 : BD4 : ABCD : CABE :: 2
R2	Serial	0/3/0	2001 : BD4 : 12AB : 1 :: 2
	Gigabitethernet (GE)	0/0	2001 : BD4 : FFCC: AABB :: 1
PC Usuario	NIC	N/A	2001 : BD4 : FFCC: AABB :: 2

Las conexiones físicas deben ser idénticas a las que se mostraron en las prácticas 6.1 y 6.2. Únicamente la variación existente será la configuración lógica que se introducirá a ambos enrutadores.

Posteriormente, al contar con el software hyperterminal y de verificar que no exista alguna configuración previa (ejemplo en la práctica 6.1 página 109), se comienzan a configurar las interfaces correspondientes del primer router.

Router "R1"

*Router>**ena***
*Router#**config t***
Enter configuration commands, one per line. End with CNTL/Z.
*Router(config)#**hostname R1***
*R1(config)#**ipv6 unicast-routing***
*R1(config-if)#**int g 0/0***
*R1(config-if)#**ipv6 address 2001:bd4:abcd:cabe::1/64***
*R1(config-if)#**no sh***
*R1(config-if)#**exit***
*R1(config)#**int s 0/3/0***
*R1(config-if)#**ipv6 address 2001:bd4:12ab:1::1/64***
*R1(config-if)#**clock rate 64000***
*R1(config-if)#**no sh***
*R1(config-if)#**exit***

Hasta este punto, únicamente se han configurado las interfaces con sus correspondientes direcciones. Lo siguiente es configurar el protocolo de enrutamiento OSPFv3 pero antes de capturar los respectivos comandos se explicará su funcionamiento.

OSPF se habilita con el comando de configuración global "*router ospf process-id*". Donde "*process-id"* es un número entre 1 y 65,535 (pues se trata de un ID de 16 bits) elegido por el administrador de red. Dicho identificador "se utiliza para distinguir los procesos OSPF en caso de que existan varios ejecutados simultáneamente en el mismo router. Aunque rara vez es necesario ejecutar más de un proceso OSPF en un router". (Redes locales y globales, s.f).

Dicho comando es significativo a nivel local, lo que implica que no necesita coincidir con otros routers OSPF para establecer adyacencias con otros vecinos. Esto difiere de EIGRP, donde su ID de proceso o el número de "sistema autónomo" sí necesita coincidir con los vecinos EIGRP para volverse adyacente. (CCNA 2 Exploration, s.f)

En la versión 3 de OSPF se añade el apartado "*ipv6*" al principio del comando descrito, por lo que la próxima línea a capturar al elegir el número 1 como ID de proceso es:

*R1(config)#**ipv6 router ospf 1***
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure manually
R1(config-rtr)#

Como puede apreciarse el indicador principal cambió a un nuevo nivel de configuración:

R1(config-rtr)#

Dado que OSPF es un protocolo de enrutamiento de tipo estado de enlace es necesario que los enrutadores deban conocer a todos los demás routers vecinos (aquellos dentro del dominio de enrutamiento OSPF). Por tal motivo, el protocolo requiere de un nuevo identificador compuesto de 32 bits denominado ID de router (también conocido como router-id o RID) con el objetivo de identificarse a sí mismo en la red y reconocer a los demás vecinos. (Odom, 2013).

OSPFv3 usa las mismas reglas para la asignación del RID como lo hace en su versión anterior, incluso al conformar dicho identificador como en las direcciones IPv4 (formato "A.B.C.D") y no en las direcciones IPv6.

Los routers Cisco obtienen el ID del router conforme a los siguientes criterios y la respectiva prioridad:

- Utilizar la dirección IP configurada con el comando ***router-id*** de OSPF.
- Si el RID no está configurado, el router elige la dirección IP más alta de cualquiera de sus interfaces loopback. (CCNA 2 Exploration, s.f)

Sin embargo, debido a que los RID son altamente usados, la mayoría de los administradores de redes eligen configurar el identificador manualmente. Esto se debe a que es mucho más fácil operar una red OSPF si se lleva una secuencia organizada de dichos RID's. Por ejemplo, para el router 1 se elegiría el identificador 1.1.1.1, para el router 2 sería 2.2.2.2 o 2.1.1.1, 2.2.1.1, etc.

Por lo tanto, el siguiente comando a capturar asignando la dirección ***1.1.1.1*** como router-id de R1 es:

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

Posteriormente, se saldrá de la configuración OSPF y de la configuración global. Verificando mediante el comando ***show run*** la correcta creación de los identificadores del protocolo.

*R1(config-rtr)#**exit***
*R1(config)#**exit***
*R1#**show run***
Building configuration...
interface GigabitEthernet0/0

no ip address
duplex auto
speed auto
ipv6 address 2001:BD4:ABCD:CABE::1/64
!
interface Serial0/3/0
no ip address
ipv6 address 2001:BD4:12AB:1::1/64
clock rate 64000
!
ipv6 router ospf 1
router-id 1.1.1.1

Nota: La creación del RID es obligatoria dado que es usado para conocer la topología de la red OSPF. De lo contrario, la comunicación no funcionará correctamente.

OSPFv3 debe ser configurado de manera independiente en cada interfaz de los enrutadores, introduciendo la siguiente y última línea de captura, la cual es "***ipv6 ospf*** *process-id área-id*". Donde "*process-id"* es el número de proceso OSPF creado anteriormente y el nuevo parámetro "*área-id"* es un valor que el administrador de red elige tomando en cuenta la siguiente información:

Un área OSPF es un grupo de routers que comparte la misma información de estado de enlace de cada uno. En esta práctica, la configuración de ambos routers será de tipo OSPF de área única. Se le conoce de esa manera cuando los enrutadores poseen el mismo número de área. Por lo tanto, el esquema para representar lo descrito sería de la siguiente manera:

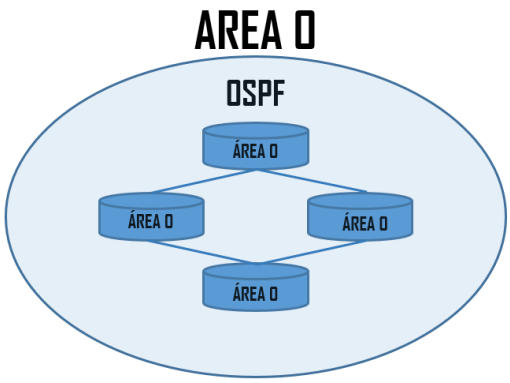


Imagen 6.107 "Representación de OSPF de área única"

Una red OSPF también puede configurarse como áreas múltiples. Existen varias ventajas en la configuración de redes de este tipo, incluidas las bases de datos de estado de enlace más pequeñas y la capacidad de aislar problemas de redes inestables dentro de un área.

Nota: Debido a la disposición del hardware existente de la práctica, únicamente se realiza un OSPF de área única.

Si bien, un dato curioso al momento de la configuración del enrutador, es que puede utilizarse un "área-id" distinto para cada uno. Sin embargo, se recomienda que el número de proceso sea el mismo entre un conjunto de routers pertenecientes a una misma área, ya que originalmente OSPF se creó con el objetivo de resolver los problemas de escalabilidad de red, por lo que es aconsejable contar con una administración y seguir una secuencia entre los ID's como prevención a la necesidad de agregar más áreas (imagen 6.108).

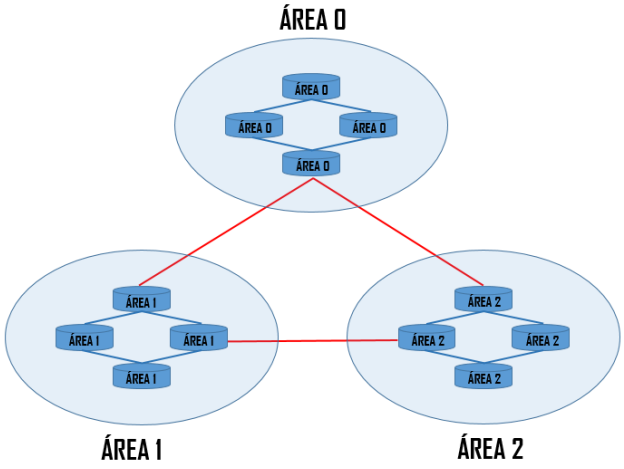


Imagen 6.108 "Representación de OSPF de múltiples áreas"

El número de área elegido para ambos enrutadores es el número 0, lo que hace que la configuración de OSPF sea de área única. Por lo tanto, el código completo para configurar el protocolo en las interfaces de R1 es el siguiente:

*R1(config)#**int g0/0***
*R1(config-if)#**ipv6 ospf 1 area 0***
*R1(config)#**int s0/3/0***
*R1(config-if)#**ipv6 ospf 1 area 0***
*R1(config-if)#**exit***
*R1(config)#**exit***
R1#

Nota: OSPFv2 funciona con wildcard pero en OSPFv3 al ser asignados desde una interfaz no requieren de este parámetro.

Nota: Cuando se configura el encaminamiento OSPF de área única, se aconseja utilizar el área-id igual a 0. Esta convención facilita la posterior configuración de la red con áreas OSPF múltiples en las que el área 0 se convierte en el área de backbone. (Redes locales y globales, s.f).

Se corroborará que dichas interfaces ahora tengan configurado OSPFv3 mediante un ***show run**:*

*R1#**show run***
Building configuration...
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address 2001:BD4:ABCD:CABE::1/64
ipv6 ospf 1 area 0
!
interface Serial0/3/0
no ip address
ipv6 address 2001:BD4:12AB:1::1/64
ipv6 ospf 1 area 0
clock rate 64000
!
ipv6 router ospf 1
router-id 1.1.1.1
log-adjacency-changes
!
ip classless
!
ip flow-export version 9

Router "R2"

La configuración del segundo router es la misma, cambiando únicamente las direcciones correspondientes y el router-id.

*Router>**ena***
*Router#**config t***
Enter configuration commands, one per line. End with CNTL/Z.
*Router(config)#**hostname R2***
*R2(config)#**ipv6 unicast-routing***
*R2(config)#**int g0/0***
*R2(config-if)#**ipv6 address 2001:bd4:ffcc:aabb::1/64***
*R2(config-if)#**int s 0/3/0***
*R2(config-if)#**ipv6 address 2001:bd4:12ab:1::2/64***
*R2(config-if)#**no sh***
*R2(config-if)#**exit***
%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up
*R2(config)#**ipv6 router ospf 1***
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure manually

Nota: Aunque el número de proceso OSPF sea el mismo que el de otro enrutador (en este caso de R1) no existe ningún error de duplicidad ni tampoco es necesario asignar el mismo número para crear alguna adyacencia entre vecinos. Sin embargo, como se mencionó anteriormente, para llevar una buena administración es recomendable asignar el mismo número de proceso a los enrutadores que pertenecen a una misma área.

*R2(config-rtr)#**router-id 2.2.2.2***

En la última línea expuesta puede apreciarse que el router-id cambia respecto al del primer router.

Es importante que todos los enrutadores tengan un RID auténtico (distinto), ya que cuando más de uno tiene la misma dirección en un protocolo OSPF es posible que el enrutamiento de dominio no funcione correctamente. Es decir, es posible que no se realice el establecimiento de vecinos.

Lo siguiente es configurar cada interfaz con el número de proceso creado y el área.

*R2(config-rtr)# **exit***
*R2(config)#**int g0/0***
*R2(config-if)# **ipv6 ospf 1 area 0***
*R2(config-if)#**int s0/3/0***
*R2(config-if)#**ipv6 ospf 1 area 0***

00:23:10: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/3/0 from LOADING to FULL, Loading Done

El último mensaje arrojado por el IOS de Cisco indica que a través de la interfaz serial 0/3/0 se detectó un vecino con el router-id 1.1.1.1, lo que es efectivamente el identificador de 32 bits de R1.

Es importante verificar que dicho mensaje sea mostrado al terminar la configuración de la interfaz que comunica con el enrutador vecino, debido que a través de ello se confirma que la conexión entre R1 y R2 se creó correctamente.

*R2(config-if)#**exit***
*R2(config)#**exit***
R2#

Nota: Si se desea verificar la configuración de R2, se debe ejecutar un ***show run*.**

Concluidas las configuraciones anteriores, se han terminado de realizar las operaciones correspondientes de ambos enrutadores.

Finalmente, se hacen pruebas de comunicación entre los host de cada subred. Para ello se requiere la asignación manual de las direcciones IPv6 (mostradas en la tabla 6.13 de la presente práctica) en cada host.

La configuración queda de la siguiente manera (imágenes 6.109 a 6.112):

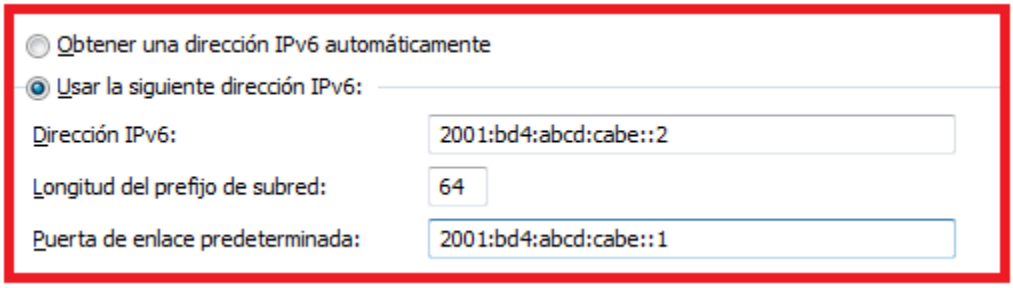


Imagen 6.109 “Configuración manual de la dirección IPv6 del host Redes”

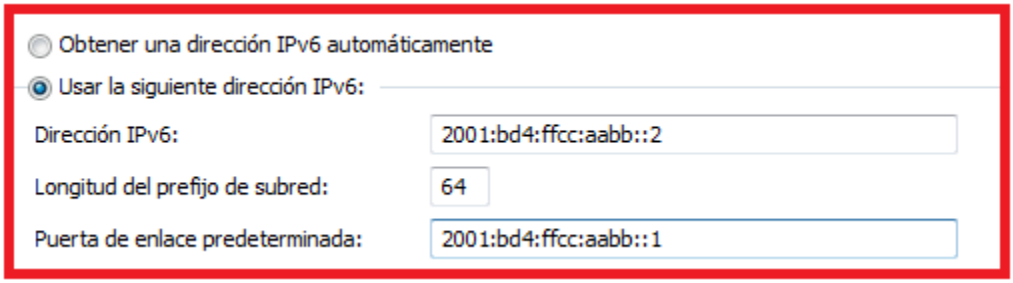


Imagen 6.110 “Configuración manual de la dirección IPv6 del host Usuario”

Imagen 6.111 “Verificación de la dirección estática IPv6 del host Redes”

Imagen 6.112 “Verificación de la dirección estática IPv6 del host Usuario”

Nota: El proceso detallado sobre la configuración manual de direcciones se explica en la práctica 6.1, página 113.

Tras haber realizado los pasos anteriores y de verificar las reglas de entrada del firewall (explicado en la práctica 6.1, página 118) se procederá a ejecutar la operación “ping”.

PC Redes

En el primer host, la operación ping se efectuará hacía 5 direcciones:

- ping 2001 : bd4 : abcd : cabe :: 1 - Interfaz gigabitethernet 0/0 (R1)
- ping 2001 : bd4 : 12ab : 1 :: 1 - Interfaz serial 0/3/0 (R1)
- ping 2001 : bd4 : 12ab : 1 :: 2 - Interfaz serial 0/3/0 (R2)
- ping 2001 : bd4 : ffcc: aabb :: 1 - Interfaz gigabitethernet 0/0 (R2)
- ping 2001 : bd4 : ffcc: aabb :: 2 – PC Usuario

Las siguientes imágenes se muestran respectivamente a la lista anterior (imágenes 6.113 a 6.117), corroborando de esta manera que existe la comunicación correcta en cada una de las interfaces.

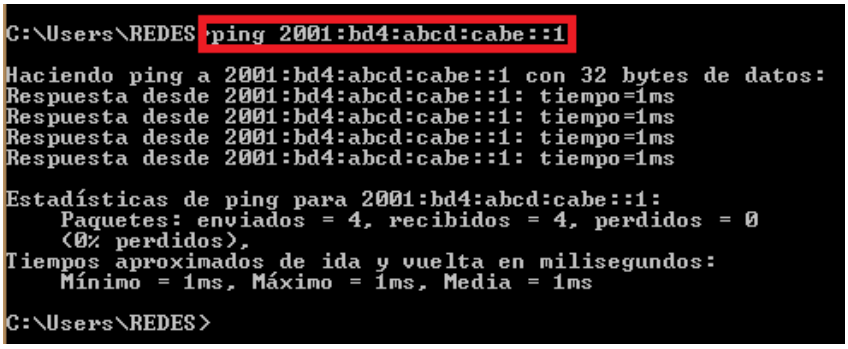


Imagen 6.113 “Ping a la interfaz gigabitethernet 0/0, R1”

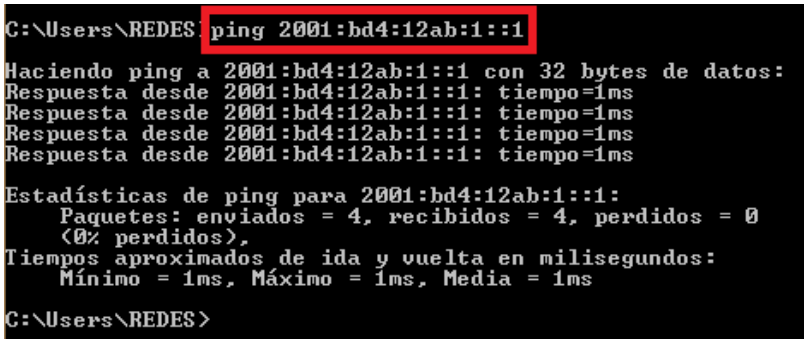


Imagen 6.114 "Ping a la interfaz serial 0/3/0, R1”

```
C:\Users\REDES>ping 2001:bd4:12ab:1::2

Haciendo ping a 2001:bd4:12ab:1::2 con 32 bytes de datos:
Respuesta desde 2001:bd4:12ab:1::2: tiempo=23ms
Respuesta desde 2001:bd4:12ab:1::2: tiempo=23ms
Respuesta desde 2001:bd4:12ab:1::2: tiempo=23ms
Respuesta desde 2001:bd4:12ab:1::2: tiempo=23ms

Estadísticas de ping para 2001:bd4:12ab:1::2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 23ms, Máximo = 23ms, Media = 23ms

C:\Users\REDES>
```

Imagen 6.115 “Ping a la interfaz serial 0/3/0, R2”

```
C:\Users\REDES>ping 2001:bd4:ffcc:aabb::1

Haciendo ping a 2001:bd4:ffcc:aabb::1 con 32 bytes de datos:
Respuesta desde 2001:bd4:ffcc:aabb::1: tiempo=24ms
Respuesta desde 2001:bd4:ffcc:aabb::1: tiempo=23ms
Respuesta desde 2001:bd4:ffcc:aabb::1: tiempo=23ms
Respuesta desde 2001:bd4:ffcc:aabb::1: tiempo=23ms

Estadísticas de ping para 2001:bd4:ffcc:aabb::1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 23ms, Máximo = 24ms, Media = 23ms

C:\Users\REDES>
```

Imagen 6.116 “Ping a la interfaz gigabitethernet 0/0, R2”

```
C:\Users\REDES>ping 2001:bd4:ffcc:aabb::2

Haciendo ping a 2001:bd4:ffcc:aabb::2 con 32 bytes de datos:
Respuesta desde 2001:bd4:ffcc:aabb::2: tiempo=24ms
Respuesta desde 2001:bd4:ffcc:aabb::2: tiempo=23ms
Respuesta desde 2001:bd4:ffcc:aabb::2: tiempo=23ms
Respuesta desde 2001:bd4:ffcc:aabb::2: tiempo=23ms

Estadísticas de ping para 2001:bd4:ffcc:aabb::2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 23ms, Máximo = 24ms, Media = 23ms

C:\Users\REDES>
```

Imagen 6.117 “Ping al host Usuario”

PC Usuario

Consecutivamente se realiza “ping” a las siguientes direcciones en el host Usuario:

- ping 2001 : bd4 : ffcc: aabb :: 1 - Interfaz gigabitethernet 0/0 (R2)
- ping 2001 : bd4 : 12ab : 1 :: 2 - Interfaz serial 0/3/0 (R2)
- ping 2001 : bd4 : 12ab : 1 :: 1 - Interfaz serial 0/3/0 (R1)
- ping 2001 : bd4 : abcd : cabe :: 1 - Interfaz gigabitethernet 0/0 (R1)
- ping 2001 : bd4 : abcd : cabe :: 2 – PC Redes

Las siguientes imágenes se muestran respectivamente a la lista anterior (imágenes 6.118 a 6.122), corroborando de esta manera la comunicación correcta en cada una de las interfaces.

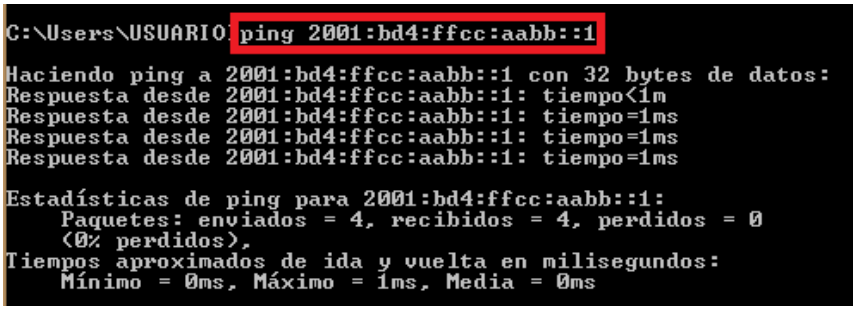


Imagen 6.118 “Ping a la interfaz gigabitethernet 0/0, R2”

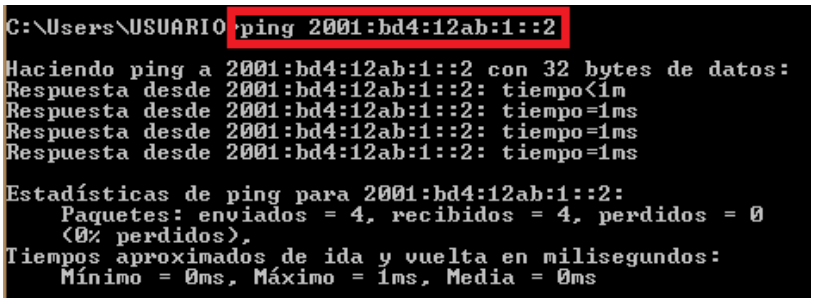


Imagen 6.119 “Ping a la interfaz serial 0/3/0, R2”

Imagen 6.120 “Ping a la interfaz serial 0/3/0, R1”

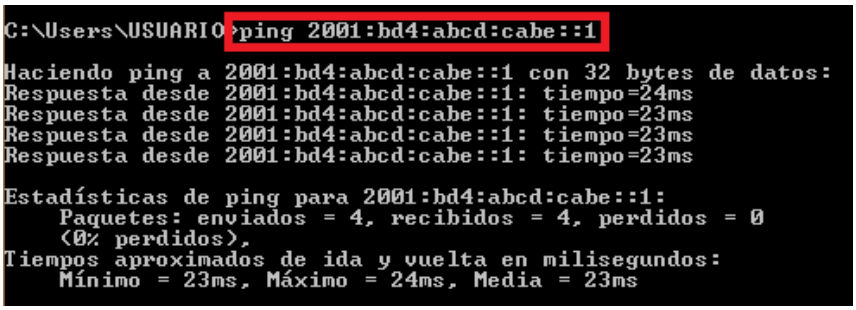


Imagen 6.121 "Ping a la interfaz gigabitethernet 0/0, R1"

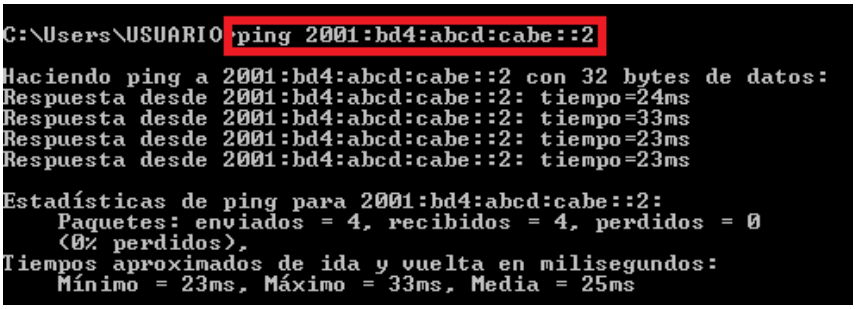


Imagen 6.122 "Ping al host Redes"

Tras haber corroborado las respuestas de las operaciones "ping", se ha finalizado con éxito la práctica 6.4.

7. Conclusiones

Al finalizar este proyecto de tesis se llegaron a las siguientes conclusiones:

- Se obtuvo como resultado final una herramienta que expone e implementa las funciones esenciales de la última versión del protocolo IP.

- El protocolo IPv6 ofrece ciertas ventajas en comparación a su antigua versión. Por ejemplo, los paquetes del nuevo IP contienen un encabezado de tamaño fijo y no poseen campos redundantes que puedan consumir ancho de banda innecesario. Asimismo, proporciona seguridad y confiabilidad al ejecutar el protocolo IPsec, el cual ofrece autenticación y cifrado a la información que viaja a través de la red. También desarrolló una nueva forma de comunicación a través de las direcciones anycast, utilizando parámetros como las métricas de enrutamiento para realizar una entrega más rápida a un grupo de nodos con una misma dirección.

- Con la utilización de esta herramienta se puede facilitar el aprendizaje del protocolo IPv6, debido a que combina la parte teórica con ejemplos prácticos. Mismos que fueron diseñados para adaptarse al área curricular de las redes computacionales para los estudiantes que cursan las carreras de informática administrativa e ingeniería en computación, cumpliendo de esta forma con el objetivo planteado.

- Con la ayuda del equipo físico del laboratorio de redes del CU UAEM Ecatepec, se lograron desarrollar e implementar los protocolos de enrutamiento de siguiente generación (llamados así por utilizar IPv6), tales como el Protocolo de Gateway Interior versión 6 (EIGRPv6), el Protocolo de Información de Enrutamiento de siguiente generación (RIPng) y el protocolo del Primer Camino más Corto en su tercera versión (OSPFv3).

- Gracias a la elaboración y comprensión que adquirí con la presente tesis, tuve la oportunidad de exponer los conceptos e ilustraciones fundamentales de IPv6 hacia diversos estudiantes y docentes en la semana de ingeniería en computación del CU UAEM Ecatepec. Describiendo de forma clara y objetiva su funcionamiento y el gran impacto de su integración en las redes. Asimismo, el conocimiento alcanzado fue de gran ventaja para presentar y aprobar un examen de certificación de fundamentos de redes de la empresa Microsoft, el cual parte de su contenido llevaba el presente protocolo IP.

- Durante el desarrollo de la investigación se pudo determinar que es esencial para un ingeniero en computación especializado en redes de computadoras, contar con los conocimientos fundamentales de este protocolo, ya que actualmente uno de los requisitos demandados para obtener cargos y/o puestos dentro de una empresa a nivel nacional e incluso internacional, es la habilidad y comprensión de IPv6.

Por ejemplo, en los entornos laborales a nivel de automatización y producción ha comenzado una nueva era llamada industria 4.0, la cual aprovecha la tecnología de los microordenadores autónomos (sistemas embebidos) y su conexión inalámbrica hacia internet con el objetivo de integrarlos dentro del ámbito del Internet de las Cosas (IoT).

Asimismo, IPv6 toma un papel importante, ya que es incorporado por el IoT en la industria 4.0 y toma la ventaja al usar su considerable número de direcciones disponibles.

Como resultado, las empresas podrán establecer redes mundiales que incorporarán a sus máquinas sistemas de almacenamiento e instalaciones de producción en forma de Sistemas Cibernéticos (CPS). En el entorno de fabricación, estos Sistemas Cibernéticos comprenden máquinas inteligentes, sistemas de almacenamiento e instalaciones de producción capaces de intercambiar de forma autónoma información, acciones desencadenantes y control mutuo de forma independiente con ayuda de las redes. Esto facilitará las mejoras fundamentales en los procesos industriales involucrados en la fabricación, la ingeniería y el uso de materiales.

8. **Anexos**

8.1 Anexo 1

Certificación “Networking Fundamentals” de Microsoft Technology Associate.

Descripción:

Parte del contenido de la información para acreditar la presente certificación se encontraban diversos conocimientos sobre IPv6.

Microsoft Technology Associate

DAVID TORRES SÁNCHEZ

has successfully completed the requirements to be recognized as a Microsoft Technology Associate for

Networking Fundamentals

Date of achievement: abril 6, 2017
verify.certiport.com rcXc-uGHw

Satya Nadella
Chief Executive Officer

Microsoft
Technology Associate

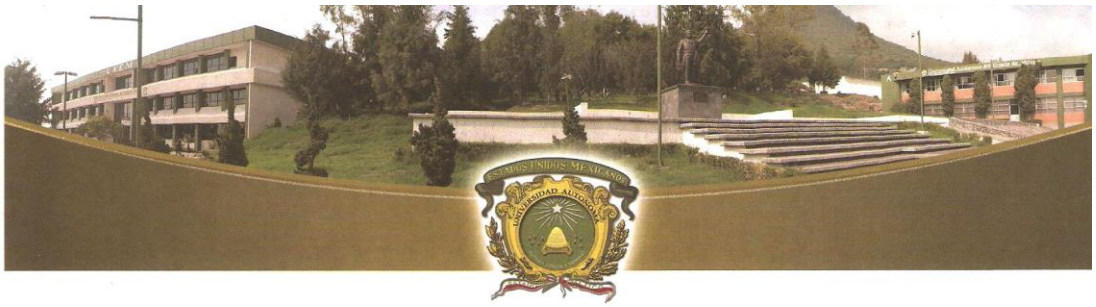
8.2 Anexo 2

Constancia por la impartición del taller titulado:

"Introducción y configuración básica del protocolo IPv6"

Descripción:

Dicho taller pudo ser impartido en el Centro Universitario UAEM Ecatepec debido a la comprensión y aplicación del protocolo IPv6 en el laboratorio de redes de la presente institución.



UAEM | Universidad Autónoma del Estado de México

Centro Universitario UAEM Ecatepec

Otorga la presente

Constancia

A: C. DAVID TORRES SÁNCHEZ

Por la Impartición del Taller Titulado:
"Introducción y configuración básica del protocolo IPv6"
en el Marco de la "Segunda Semana Multidisciplinaria"
llevada a cabo del 24 al 28 de Abril de2017
en este Centro Universitario.

Ecatepec, Estado de México a 28 de Abril de 2017.

Patria, Ciencia y Trabajo

"2017, Año del Centenario de la Promulgación de la Constitución Política de los Estados Unidos Mexicanos"

DG CUyUAP
Dirección General de Centros Universitarios y Unidades Académicas Profesionales

M. EN C. ED. MARCO ANTONIO VILLEDA ESQUIVEL
DIRECTOR DEL CENTRO UNIVERSITARIO UAEM ECATEPEC

DIRECCION

9. **Bibliografía**

Alvarez, G. V. (Febrero de 2000). *El protocolo IPv6 y sus extensiones de seguridad IPSec*. Barcelona. Recuperado de http://beta.redes-linux.com/manuales/ipv6/Memoria_del_proyecto_IPv6.pdf

Castro, A. (09 de Marzo de 2009). *IPv5*. Obtenido de http://redesandrescastro.blogspot.mx/

Cisco System Inc. (s.f). *Routing and switching essentials, CCNA.* Recuperado de: https://www.netacad.com/es/group/landing/

CCNA 2 Exploration. (s.f). *Escala y asignación de un AS*. (IMAGEN). Recuperado de: ftp://soporte.uson.mx/PUBLICO/02_ING.SISTEMAS.DE.INFORMACION/Nueva%20carpeta%20(3)/Libro%20de%20CCNA%20II%20PDF.pdf

CCNA 2 Exploration. (s.f). *Conceptos y protocolos de enrutamiento*. Recuperado de: ftp://soporte.uson.mx/PUBLICO/02_ING.SISTEMAS.DE.INFORMACION/Nueva%20carpeta%20(3)/Libro%20de%20CCNA%20II%20PDF.pdf

Cisco. (s.f). *Guia de conexión de cables seriales*. Obtenido de http://www.cisco.com/cisco/web/support/LA/102/1024/1024826_17.html

Cisco. (08 de Marzo de 2014). *Cisco Support Comunity* . Obtenido de https://supportforums.cisco.com/document/11934696/eigrp-ipv6-configuration-name-mode

Cisco Systems Inc. (2004). *Especificaciones del enrutador Cisco 2821*. (IMAGEN). Recuperado de: http://docstore.mik.ua/univercd/cc/td/doc/product/access/acs_mod/2800/qsg/qsg28esp.pdf

ComputerNetworkingNotes. (s.f). ComputerNetworkingNotes.com. Obtenido de http://computernetworkingnotes.com/computer-networking-notes/contact-us.html

Coto Cortés. (2008). *Multicast IPv6 de todos los nodos.* (IMAGEN). Recuperado de http://www.ie.itcr.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter8_Direccionamiento%20IP.pdf

ExamCollection. (s.f). Obtenido de http://www.examcollection.com/certification-training/ccnp-configure-and-verify-eigrp-for-ipv6.html

Fuentes, R. A. (Enero de 2013). Obtenido de http://cs.mty.itesm.mx/lab/redes2/ipv6/P6_IPv6_RIPng.pdf

Graziani, R. (2013). *IPv6 Fundamentals: A Straightforward Approach*. Indianapolis USA. Cisco Press.

Gutiérrez, R. B. (17 de Octubre de 2010). *Elaboración de un estado del arte sobre el protocolo IPv6*. Colombia. Obtenido de http://repository.upb.edu.co:8080/jspui/bitstream/123456789/1259/1/digital_20422.pdf

Horley, E. (2014). *Practical Windows IPv6 for Administrators*. Nueva York: Apress.

IANA. (22 de Junio de 2016). *Protocol Numbers* . Obtenido de http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

IBM. (Septiembre de 2013). *IPv6 Network and Application Design*. Carolina del Norte, USA. Obtenido de http://publibz.boulder.ibm.com/epubs/pdf/f1a2f100.pdf

Kozierok, C. M. (20 de Septiembre de 2005). *TCP/IP Guide*. Obtenido de http://www.tcpipguide.com/free/t_IPHistoryStandardsVersionsandCloselyRelatedProtoco.htm

Martínez, J. P. (14 de Agosto de 2016). *The IPv6 Company Consulintel*. Obtenido de http://www.consulintel.es/html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf

Molinero, J. C. (13 de Junio de 2011). *IPv6 de Tknika*. Obtenido de https://sites.google.com/site/tknikaipv6/2-direccionamiento/2-2-direccionamiento/2-2-7-direcciones-multicast

Odom, W. (2013). *Cisco CCNA Routing and Switching ICND2*. Indianapolis: Cisco Press.

Oracle. (s.f). *Oracle*. Obtenido de http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-170/index.html

Redes locales y globales. (s.f). Obtenido de https://sites.google.com/site/redeslocalesyglobales/system/app/pages/recentChanges

Sarria, J. A. (05 de Enero de 2004). *IPv4 to IPv6*. Obtenido de http://ipv4to6.blogspot.mx/p/tipos-de-direcciones-ipv6-unicast.html

Soultek Informática. 2010. *Ubicación de tarjeta HWIC-2T en el router*. (IMAGEN). Recuperado de: http://cisco.solutekcolombia.com/routers_cisco/HWIC-2T/

Stretch, J. (04 de Agosto de 2008). PacketLife.net. Obtenido de http://packetlife.net/blog/2008/aug/4/eui-64-ipv6/