

## **CAPÍTULO 7. ASIGNACIÓN DE DIRECCIONES IP**

### **7.1.2.1 Porciones de red y de host**

Una dirección IPv4 es una dirección jerárquica compuesta por una porción de red y una porción de host. Los bits dentro de la porción de red de la dirección deben ser idénticos para todos los dispositivos que residen en la misma red. Los bits dentro de la porción de host de la dirección deben ser únicos para identificar un host específico dentro de una red. Si dos hosts tienen el mismo patrón de bits en la porción de red especificada de la secuencia de 32 bits, esos dos hosts residen en la misma red.

### **7.1.2.3 AND lógico para identificar la dirección de red de un host IPv4**

Para identificar la dirección de red de un host IPv4, se recurre a la operación lógica AND para la dirección IPv4, bit por bit, con la máscara de subred. El uso de la operación AND entre la dirección y la máscara de subred produce la dirección de red.

Dirección IP	192	.	168	.	10	.	10
Binario	11000000		10101000		00001010		00001010
Máscara de subred	255	.	255	.	255	.	0
	11111111		11111111		11111111		00000000
Resultados de AND	11000000		10101000		00001010		00000000
Dirección de red	192	.	168	.	10	.	0

### **7.1.2.5 Longitud del prefijo**

Puede ser difícil expresar direcciones de red y de host con la dirección de la máscara de subred decimal punteada. Afortunadamente, existe un método alternativo más simple para identificar una máscara de subred que se denomina "longitud de prefijo".

Específicamente, la longitud de prefijo es el número de bits fijados en 1 en la máscara de subred. Se escribe mediante la "notación de barra diagonal", es decir, una "/" seguida por el número de bits fijados en 1. Por lo tanto, cuente el número de bits en la máscara de subred y anteponga una barra diagonal.

Máscara de subred	Dirección de 32 bits	Longitud de prefijo
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

### 7.1.2.6 Direcciones de red, de host y de difusión

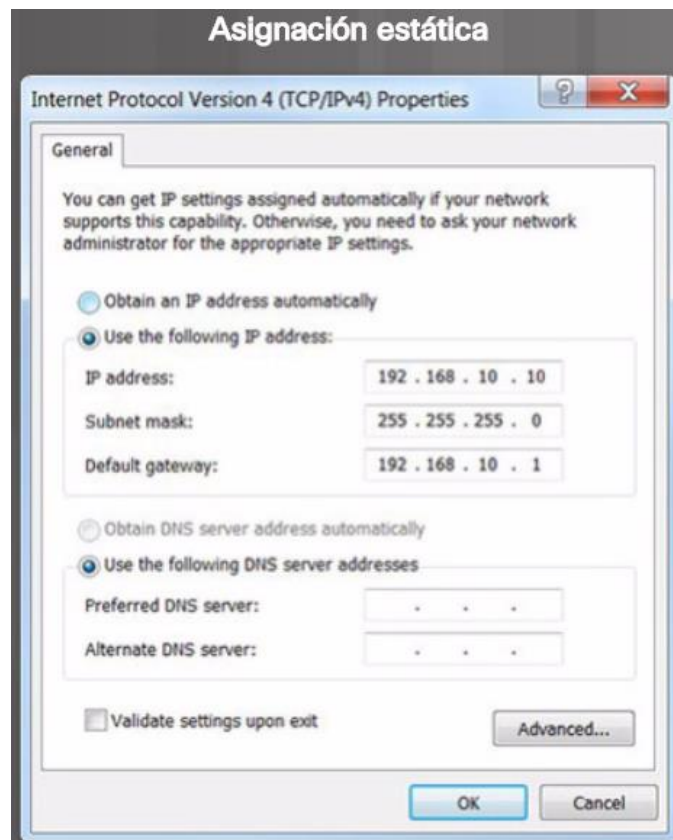
Cada dirección de red contiene (o identifica) direcciones de host y una dirección de difusión. Cada una se identifica de la siguiente forma:

- Dirección de red: la parte de host todo a 0.
- Dirección de difusión: la parte de host todo a 1.
- Dirección de host: la parte de host con 0 y 1.

### 7.1.3.1 Asignación de una dirección IPv4 estática a un host

Se pueden asignar direcciones IP a los dispositivos de manera estática o dinámica. En las redes, algunos dispositivos necesitan una dirección IP fija. Por ejemplo, las impresoras, los servidores y los dispositivos de red necesitan una dirección IP estática.

Un host también se puede configurar con una dirección IPv4 estática como la que se muestra en la ilustración. En redes pequeñas, es aceptable asignar direcciones IP estáticas a los hosts. Sin embargo, en una red grande, introducir una dirección estática en cada host llevaría mucho tiempo. Es importante mantener una lista precisa de las direcciones IP estáticas asignadas a cada dispositivo.

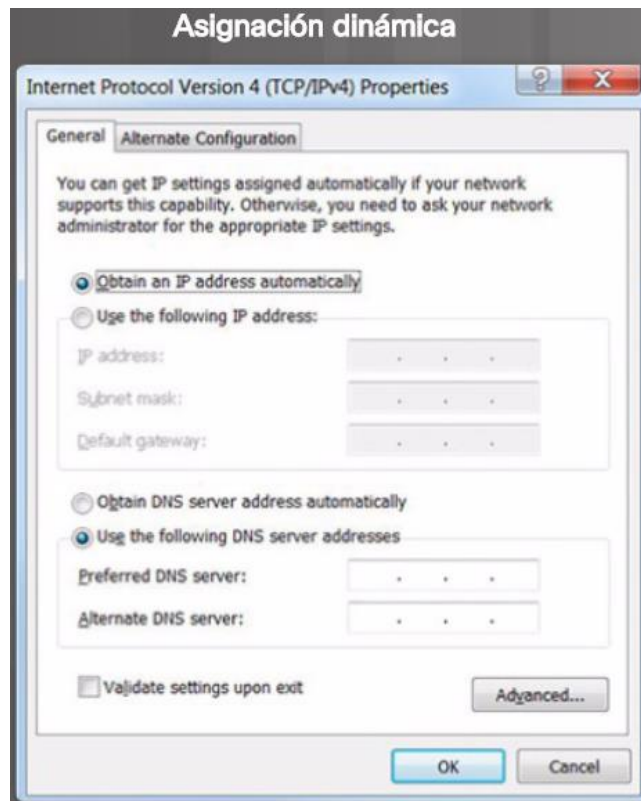


### 7.1.3.2 Asignación de una dirección IPv4 dinámica a un host

En la mayoría de las redes de datos, la mayor parte de los hosts incluyen PC, tabletas PC, teléfono inteligentes, impresoras y teléfonos IP. También suele ocurrir que la población de usuarios y los dispositivos cambian con frecuencia. No sería práctico comenzar a asignar direcciones IPv4 de manera estática a cada dispositivo. Por lo tanto, a estos dispositivos se les asignan direcciones IPv4 de manera dinámica con el protocolo DHCP.

Como se muestra en la ilustración, un host puede obtener la información de asignación de direcciones IPv4 de forma automática. El host es un cliente DHCP y solicita la información de dirección IPv4 de un servidor DHCP. El servidor DHCP proporciona una dirección IPv4, una máscara de subred, un gateway predeterminado y otra información de configuración.

En general, el protocolo DHCP es el método preferido para asignar direcciones IPv4 a los hosts en redes grandes. Un beneficio adicional de DHCP es que la dirección no se asigna permanentemente a un host, sino que solo se "presta" por un período. Si el host se apaga o se desconecta de la red, la dirección regresa al pool para volver a utilizarse. Esta característica es muy útil para los usuarios móviles que entran a una red y salen de ella.



### 7.1.3.5 Transmisión de difusión

La difusión puede ser dirigida o limitada. Una difusión dirigida se envía a todos los hosts de una red específica. Por ejemplo, un host de la red 172.16.4.0/24 envía un paquete a la dirección 172.16.4.255. Se envía una difusión limitada a 255.255.255.255. De manera predeterminada, los routers no reenvían transmisiones por difusión.

### 7.1.3.6 Transmisión de multidifusión

La transmisión de multidifusión reduce el tráfico al permitir que un host envíe un único paquete a un grupo seleccionado de hosts que estén suscritos a un grupo de multidifusión.

IPv4 reservó las direcciones de 224.0.0.0 a 239.255.255.255 como rango de multidifusión. Las direcciones IPv4 de multidifusión de 224.0.0.0 a 224.0.0.255 están reservadas para la multidifusión solo en la red local. Un router conectado a la red local reconoce que estos paquetes están dirigidos a un grupo de multidifusión de una red local y no los sigue reenviando.

Un uso típico de una dirección de multidifusión de una red local reservada son los Routing Protocols que usan la transmisión de multidifusión para intercambiar información de routing. Por ejemplo, 224.0.0.9 es la dirección de multidifusión que usa el protocolo de información de routing (RIP) versión 2 para comunicarse con otros routers RIPv2.

Los hosts que reciben datos de multidifusión específicos se denominan “clientes de multidifusión”. Los clientes de multidifusión utilizan servicios solicitados por un programa cliente para suscribirse al grupo de multidifusión.

Cada grupo de multidifusión está representado por una sola dirección IPv4 de destino de multidifusión. Cuando un host IPv4 se suscribe a un grupo de multidifusión, el host procesa los paquetes dirigidos a esta dirección de multidifusión y los paquetes dirigidos a la dirección de unidifusión asignada exclusivamente.

#### 7.1.4.1 Direcciones IPv4 públicas y privadas

Las direcciones IPv4 públicas son direcciones que se enrutan globalmente entre los routers de los ISP (proveedores de servicios de Internet). Sin embargo, no todas las direcciones IPv4 disponibles pueden usarse en Internet. Existen bloques de direcciones denominadas *direcciones privadas* que las organizaciones usan para asignar direcciones IPv4 a los hosts internos.

Específicamente, los bloques de direcciones privadas son los siguientes:

- **10.0.0.0 /8 o 10.0.0.0 a 10.255.255.255**
- **172.16.0.0 /12 o 172.16.0.0 a 172.31.255.255**
- **192.168.0.0 /16 o 192.168.0.0 a 192.168.255.255**

Es importante saber que las direcciones dentro de estos bloques de direcciones no están permitidas en Internet y deben ser filtradas (descartadas) por los routers de Internet. Las direcciones privadas se definen en RFC 1918.

La mayoría de las organizaciones usan direcciones IPv4 privadas para los hosts internos. Sin embargo, estas direcciones RFC 1918 no se pueden enrutar en Internet y deben traducirse a direcciones IPv4 públicas. Se usa la traducción de direcciones de red (NAT) para traducir entre direcciones IPv4 privadas y públicas. En general, esto se hace en el router que conecta la red interna a la red del ISP.

#### 7.1.4.3 Direcciones IPv4 de usuarios especiales

Existen ciertas direcciones, como la dirección de red y la dirección de difusión, que no se pueden asignar a los hosts. También hay direcciones especiales que pueden asignarse a los hosts, pero con restricciones respecto de la forma en que dichos hosts pueden interactuar dentro de la red.

- **Direcciones de bucle invertido (127.0.0.0 /8 o 127.0.0.1 a 127.255.255.254):** generalmente identificadas solo como 127.0.0.1, son direcciones especiales que usa un host para dirigir el tráfico hacia sí mismo.
- **Direcciones de enlace local (169.254.0.0 /16 o 169.254.0.1 a 169.254.255.254):** más comúnmente conocidas como "direcciones IP privadas automáticas" (APIPA), un cliente DHCP Windows las usa para la autoconfiguración en caso de que no haya servidores DHCP disponibles. Son útiles en las conexiones punto a punto.
- **Direcciones TEST-NET (192.0.2.0 /24 o 192.0.2.0 a 192.0.2.255):** estas direcciones se apartan con fines de enseñanza y aprendizaje, y pueden usarse en ejemplos de documentación y de redes.

#### Ping a la interfaz de bucle invertido

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad> ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\NetAcad> ping 127.1.1.1

Pinging 127.1.1.1 with 32 bytes of data:
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\NetAcad>
```

#### 7.1.4.4 Direcccionamiento con clases

(Apuntes de clase)

### 7.1.4.6 Direccionamiento sin clase

El sistema usado actualmente se conoce como *direccionamiento sin clase*. El nombre formal es “Classless Inter-Domain Routing” (CIDR, pronunciado “cider”). En 1993, el IETF creó un nuevo conjunto de estándares que permitía que los proveedores de servicios asignaran direcciones IPv4 en cualquier límite de bits de dirección (longitud de prefijo) en lugar de solo con una dirección de clase A, B o C. Se hizo para poder demorar la disminución y el agotamiento final de las direcciones IPv4.

El IETF sabía que el CIDR era solo una solución temporal y que sería necesario desarrollar un nuevo protocolo IP para admitir el rápido crecimiento de la cantidad de usuarios de Internet. En 1994, el IETF comenzó a trabajar para encontrar un sucesor de IPv4, que finalmente fue IPv6.

Entonces, ¿quién administra y asigna estas direcciones IP?

### 7.1.4.7 Asignación de direcciones IP

Para que una empresa u organización admita hosts de red, por ejemplo, servidores web a los que se accede desde Internet, esa organización debe tener asignado un bloque de direcciones públicas. Se debe tener en cuenta que las direcciones públicas deben ser únicas, y el uso de estas direcciones públicas se regula y se asigna a cada organización de forma independiente. Esto es válido para las direcciones IPv4 e IPv6.

La Autoridad de Números Asignados de Internet (IANA) administra las direcciones IPv4 e IPv6. La IANA administra y asigna bloques de direcciones IP a los Registros Regionales de Internet (RIR). Haga clic en cada uno de los RIR de la ilustración para ver más información.

Los RIR se encargan de asignar direcciones IP a los ISP, quienes a su vez proporcionan bloques de direcciones IPv4 a las organizaciones y a los ISP más pequeños. Las organizaciones pueden obtener sus direcciones directamente de un RIR, según las políticas de ese RIR.



- ARIN: direcciones IP de América del Norte.
- RIPE: direcciones IP de Europa, Oriente Medio y Asia Central.
- APNIC: direcciones IP de Asia Pacífico.
- AfriNIC: direcciones IP de África.
- LACNIC: direcciones IP de América latina y Caribe.

### 7.2.1.2 Coexistencia de IPv4 e IPv6

No hay una única fecha para realizar la transición a IPv6. En un futuro cercano, IPv4 e IPv6 coexistirán. Se espera que la transición demore años. El IETF creó diversos protocolos y herramientas para ayudar a los administradores de redes a migrar las redes a IPv6. Las técnicas de migración pueden dividirse en tres categorías:

- **Dual-stack:** como se muestra en la figura 1, la técnica dual-stack permite que IPv4 e IPv6 coexistan en el mismo segmento de red. Los dispositivos dual-stack ejecutan pilas de protocolos IPv4 e IPv6 de manera simultánea.
- **Tunelización:** como se muestra en la figura 2, el protocolo de túnel es un método para transportar un paquete IPv6 en una red IPv4. El paquete IPv6 se encapsula dentro de un paquete IPV4, de manera similar a lo que sucede con otros tipos de datos.
- **Traducción:** como se muestra en la figura 3, la traducción de direcciones de red 64 (NAT64) permite que los dispositivos habilitados para IPv6 se comuniquen con los dispositivos habilitados para IPv4 mediante una técnica de traducción similar a NAT para IPv4. Un paquete IPv6 se traduce a un paquete IPv4 y viceversa.

**Nota:** la tunelización y la traducción solo se usan cuando es necesario. El objetivo debe ser las comunicaciones IPv6 nativas de origen a destino.

### 7.2.2.1 Representación de dirección IPv6

El formato preferido para escribir una dirección IPv6 es x:x:x:x:x:x, donde cada “x” consta de cuatro valores hexadecimales. Al hacer referencia a 8 bits de una dirección IPv4, utilizamos el término “octeto”. En IPv6, un “hexteto” es el término no oficial que se utiliza para referirse a un segmento de 16 bits o cuatro valores hexadecimales. Cada “x” es un único hexteto, 16 bits o cuatro dígitos hexadecimales.

En las siguientes páginas, veremos dos reglas que permiten reducir el número de dígitos necesarios para representar una dirección IPv6.

### 7.2.2.2 Regla 1: Omitir los 0 iniciales

La primera regla para ayudar a reducir la notación de las direcciones IPv6 consiste en omitir los 0 (ceros) iniciales en cualquier sección de 16 bits o hexteto.

Recomendado	2001:0DB8:0000:1111:0000:0000:0000:0200
Sin ceros iniciales	2001: DB8: 0:1111: 0: 0: 0: 200

### 7.2.2.3 Regla 2: Omitir los segmentos de 0

La segunda regla que permite reducir la notación de direcciones IPv6 es que los dos puntos dobles (::) pueden reemplazar cualquier cadena única y contigua de uno o más segmentos de 16 bits (hexetos) compuestos solo por ceros.

Los dos puntos dobles (::) se pueden utilizar solamente una vez dentro de una dirección; de lo contrario, habría más de una dirección resultante posible. Cuando se utiliza junto con la técnica de omisión de ceros iniciales, la notación de direcciones IPv6 generalmente se puede reducir de manera considerable. Esto se suele conocer como “formato comprimido”.

Dirección incorrecta:

- 2001:0DB8::ABCD::1234

Expansiones posibles de direcciones comprimidas ambiguas:

- 2001:0DB8::ABCD:0000:0000:1234
- 2001:0DB8::ABCD:0000:0000:0000:1234

Recomendado	2 0 0 1 : 0 D B 8 : 0 0 0 0 : 1 1 1 1 : 0 0 0 0 : 0 0 0 0 : 0 0 0 0 : 0 2 0 0
Sin ceros iniciales	2 0 0 1 : D B 8 : 0 : 1 1 1 1 : 0 : 0 : 0 : 2 0 0
Comprimido	2 0 0 1 : D B 8 : 0 : 1 1 1 1 : : 2 0 0

### 7.2.3.1 Tipos de direcciones IPv6

Existen tres tipos de direcciones IPv6:

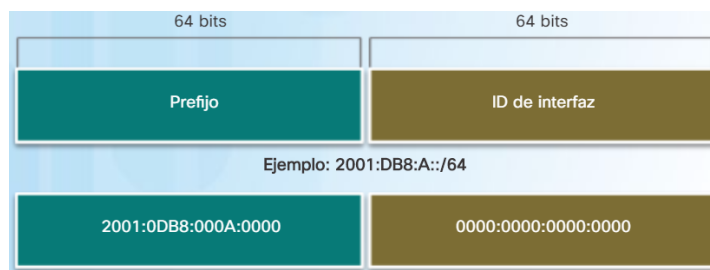
- **Unidifusión:** una dirección IPv6 de unidifusión identifica de manera única una interfaz de un dispositivo habilitado para IPv6.
- **Multidifusión:** las direcciones IPv6 de multidifusión se usan para enviar un único paquete IPv6 a varios destinos.
- **Difusión por proximidad:** una dirección IPv6 de difusión por proximidad es cualquier dirección IPv6 de unidifusión que puede asignarse a varios dispositivos. Los paquetes enviados a una dirección de difusión por proximidad se enrutan al dispositivo más cercano que tenga esa dirección. Las direcciones de difusión por proximidad exceden el ámbito de este curso.

A diferencia de IPv4, IPv6 no tiene una dirección de difusión. Sin embargo, existe una dirección IPv6 de multidifusión de todos los nodos que brinda básicamente el mismo resultado.



### 7.2.3.2 Longitud de prefijo IPv6

IPv6 no utiliza la notación decimal punteada de máscara de subred. La longitud de prefijo puede ir de 0 a 128. Una longitud de prefijo IPv6 típica para LAN y la mayoría de los demás tipos de redes es /64. Esto significa que la porción de prefijo o de red de la dirección tiene una longitud de 64 bits, lo cual deja otros 64 bits para la ID de interfaz (porción de host) de la dirección.

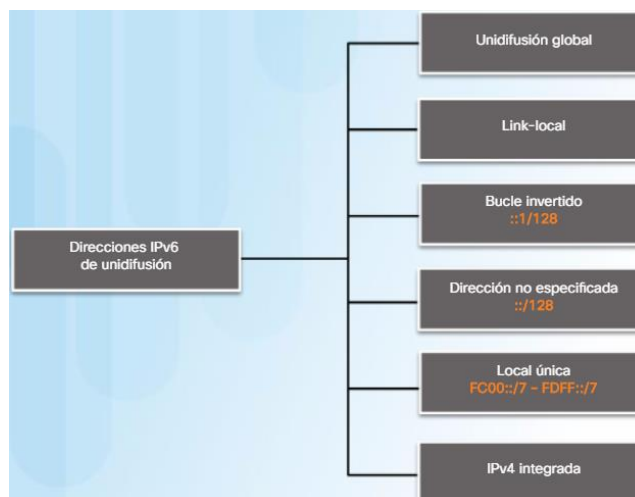


### 7.2.3.3 Direcciones IPv6 de unidifusión

Las direcciones IPv6 de unidifusión identifican de forma exclusiva una interfaz en un dispositivo con IPv6 habilitado. Como sucede con IPv4, las direcciones IPv6 de origen deben ser direcciones de unidifusión. Las direcciones IPv6 de destino pueden ser direcciones de unidifusión o de multidifusión.

- **Unidifusión global (GUA):** Las direcciones de unidifusión globales son similares a las direcciones IPv4 públicas y pueden configurarse estáticamente o asignarse de forma dinámica.
- **Link-local:** Las direcciones link-local se utilizan para comunicarse con otros dispositivos en el mismo enlace local. Con IPv6, el término “enlace” hace referencia a una subred. Las direcciones link-local se limitan a un único enlace. Su exclusividad se debe confirmar solo para ese enlace, ya que no se pueden enrutar más allá del enlace.  
Las direcciones IPv6 link-local están en el rango de FE80::/10. /10 indica que los primeros 10 bits son 1111 1110 10xx xxxx. El primer hexteto tiene un rango de 1111 1110 1000 0000 (FE80) a 1111 1110 1011 1111 (FEBF).
- **Local única:** Las direcciones locales únicas se utilizan para el direccionamiento local dentro de un sitio o entre una cantidad limitada de sitios. Estas direcciones no deberían poder enrutarse en la IPv6 global, y no deberían traducirse hacia direcciones IPv6 globales. Las direcciones locales únicas están en el rango de FC00::/7 a FDFE::/7.

Con IPv4, las direcciones privadas se combinan con NAT/PAT para proporcionar una traducción de varios a uno de direcciones privadas a públicas. Se puede usar para proteger u ocultar su red de posibles riesgos de seguridad.



### 7.2.4.1 Estructura de una dirección IPv6 de unidifusión global

Actualmente, solo se asignan direcciones de unidifusión globales con los tres primeros bits 001 o 2000::/3. Es decir que el primer dígito hexadecimal de una dirección de GUA comienza con 2 o 3. Esto solo constituye un octavo del espacio total disponible de direcciones IPv6.

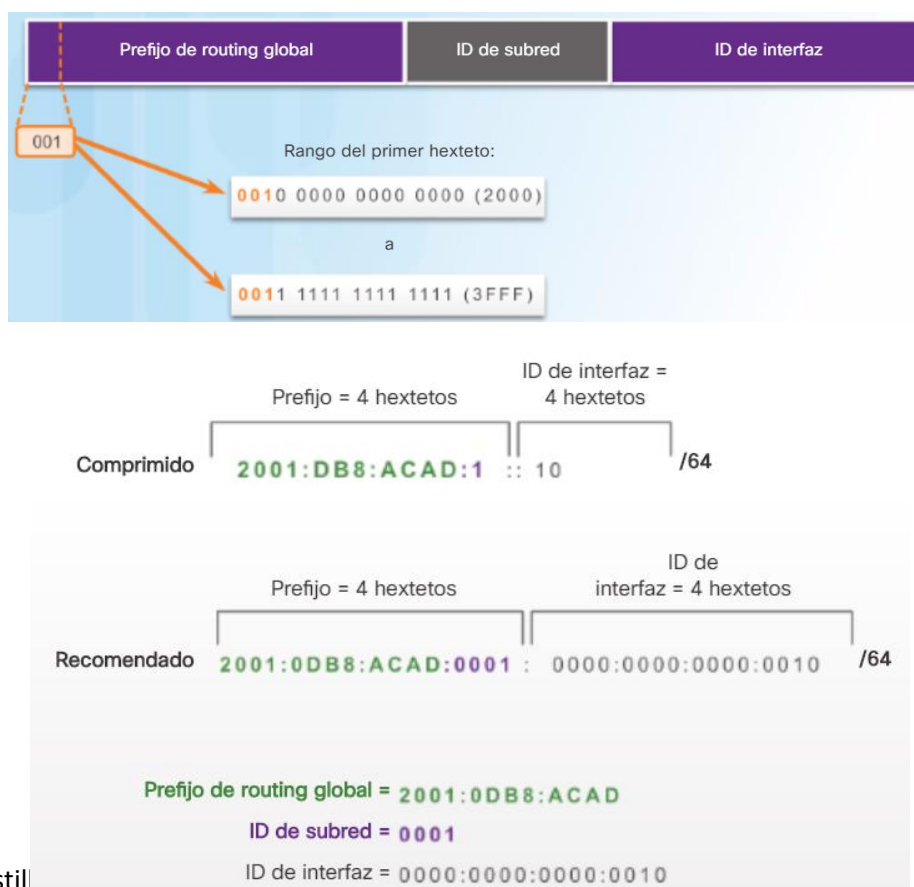
**Nota:** se reservó la dirección 2001:0DB8::/32 con fines de documentación, incluido el uso en ejemplos.

Una dirección de unidifusión global consta de tres partes:

- **Prefijo de routing global:** El prefijo de routing global es la porción de prefijo, o de red, de la dirección que asigna el proveedor (por ejemplo, un ISP) a un cliente o a un sitio.
- **ID de subred:** Las organizaciones utilizan la ID de subred para identificar subredes dentro de su ubicación. Cuanto mayor es la ID de subred, más subredes habrá disponibles.
- **ID de interfaz:** La ID de interfaz IPv6 equivale a la porción de host de una dirección IPv4. Se utiliza el término “ID de interfaz” debido a que un único host puede tener varias interfaces, cada una con una o más direcciones IPv6. Se recomienda especialmente usar subredes /64 en la mayoría de los casos.

**Nota:** a diferencia de IPv4, en IPv6, pueden asignarse a un dispositivo las direcciones de host compuestas solo por ceros y solo por unos. Se puede usar la dirección compuesta solo por unos debido al hecho de que en IPv6 no se usan las direcciones de difusión. Las direcciones compuestas solo por ceros también pueden usarse, pero se reservan como dirección de difusión por proximidad subred-router, y solo deben asignarse a los routers.

Una forma fácil de leer la mayoría de las direcciones IPv6 es contar la cantidad de hexetets. Como se muestra en la figura 2, en una dirección de unidifusión global /64, los primeros cuatro hexetets son para la porción de red de la dirección, y el cuarto hexteto indica la ID de subred. Los cuatro hexetets restantes son para la ID de interfaz.

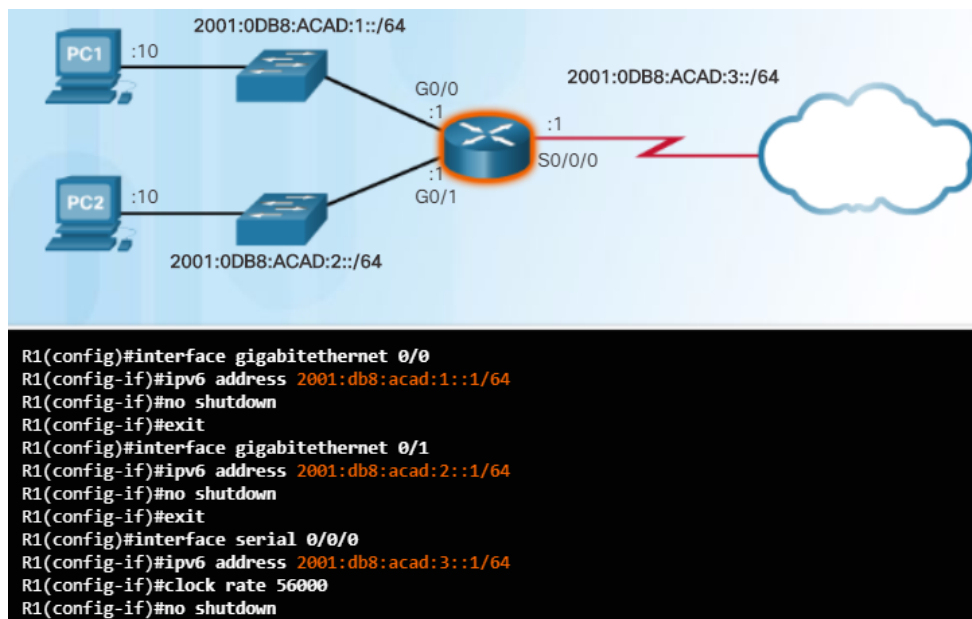


#### 7.2.4.2 Configuración estática de una dirección de unidifusión global

##### Configuración del router

La mayoría de los comandos de configuración y verificación IPv6 de Cisco IOS son similares a sus equivalentes de IPv4. En la mayoría de los casos, la única diferencia es el uso de **ipv6** en lugar de **ip** dentro de los comandos.

El comando para configurar una dirección IPv6 de unidifusión global en una interfaz es **ipv6 address ipv6-address/prefix-length**. Observe que no hay un espacio entre *ipv6-address* y *prefix-length*. En la figura, también se muestran los comandos necesarios para configurar la dirección IPv6 de unidifusión global en la interfaz GigabitEthernet 0/0, GigabitEthernet 0/1 y Serial 0/0/0 del R1.



### Configuración de host

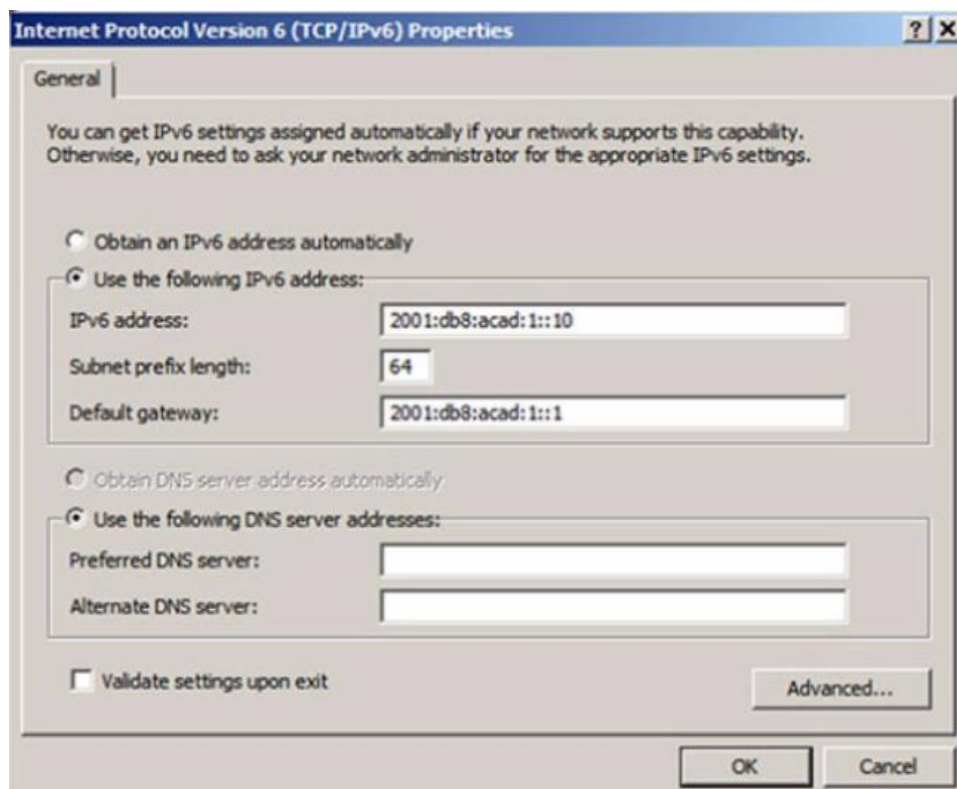
La dirección de gateway predeterminado configurada para la PC1 es 2001:DB8:ACAD:1::1. Esta es la dirección de unidifusión global de la interfaz GigabitEthernet del R1 de la misma red. De manera alternativa, la dirección de gateway predeterminado puede configurarse para que coincida con la dirección link-local de la interfaz GigabitEthernet. Cualquiera de las dos configuraciones funciona.

Al igual que con IPv4, la configuración de direcciones estáticas en clientes no se extiende a entornos más grandes. Por este motivo, la mayoría de los administradores de redes en una red IPv6 habilitan la asignación dinámica de direcciones IPv6.

Los dispositivos pueden obtener automáticamente una dirección IPv6 de unidifusión global de dos maneras:

- Configuración automática de dirección independiente del estado (SLAAC)
- Mediante DHCPv6 con estado

**Nota:** cuando se usa DHCPv6 o SLAAC, se especifica automáticamente la dirección link-local del router local como dirección de gateway predeterminado.



### 7.2.4.3 Configuración dinámica: SLAAC

La configuración automática de dirección independiente del estado (SLAAC) es un método que permite que un dispositivo obtenga su prefijo, la longitud de prefijo, la dirección de gateway predeterminado y otra información de un *router IPv6*, sin usar un servidor DHCPv6. Mediante SLAAC, los dispositivos dependen de los mensajes de anuncio de router (RA) de ICMPv6 del router local para obtener la información necesaria.

Los routers IPv6 envían mensajes RA de ICMPv6 periódicamente, cada 200 segundos, a todos los dispositivos con IPv6 habilitado en la red. También se envía un mensaje RA en respuesta a un host que envía un mensaje ICMPv6 de solicitud de router (RS).

El routing IPv6 no está habilitado de manera predeterminada. Para habilitar un router como router IPv6, se debe usar el comando de configuración global **ipv6 unicast-routing**.

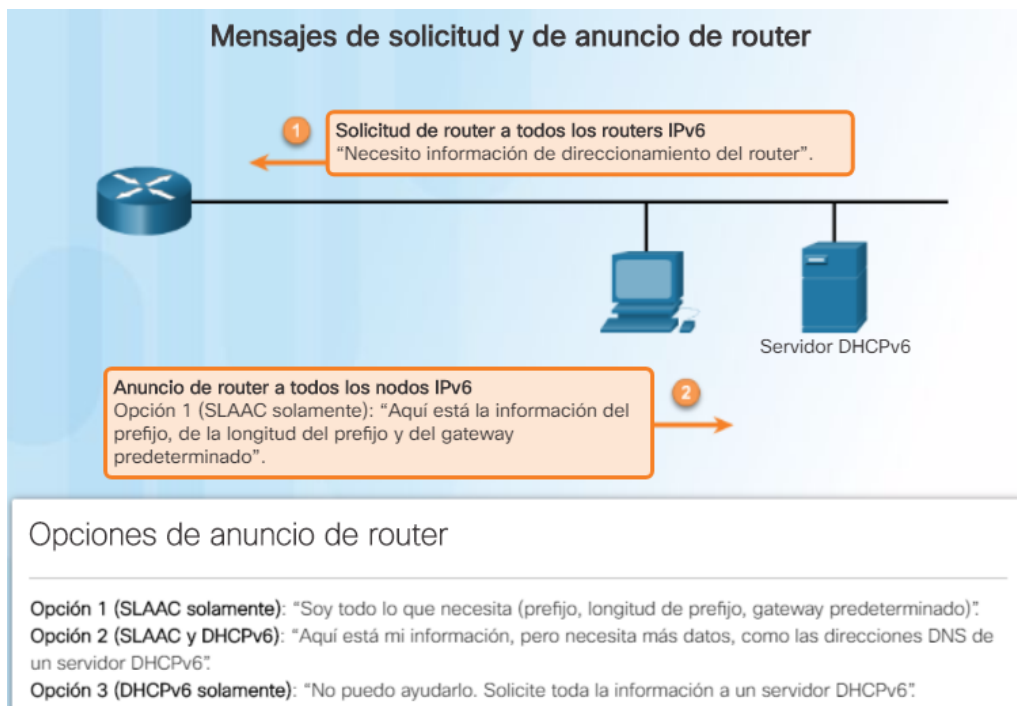
**Nota:** se pueden configurar direcciones IPv6 en un router sin que sea un router IPv6.

El mensaje RA de ICMPv6 es una sugerencia a un dispositivo sobre cómo obtener una dirección IPv6 de unidifusión global. La decisión final la tiene el sistema operativo del dispositivo. El mensaje RA de ICMPv6 incluye lo siguiente:

- **Prefijo de red y longitud de prefijo:** indica al dispositivo a qué red pertenece.
- **Dirección de gateway predeterminado:** es una dirección IPv6 link-local, la dirección IPv6 de origen del mensaje RA.
- **Direcciones DNS y nombre de dominio:** direcciones de los servidores DNS y un nombre de dominio.

Como se muestra en la figura 1, existen tres opciones para los mensajes RA:

- Opción 1: SLAAC
- Opción 2: SLAAC con un servidor DHCPv6 sin información de estado
- Opción 3: DHCPv6 con información de estado (no SLAAC)



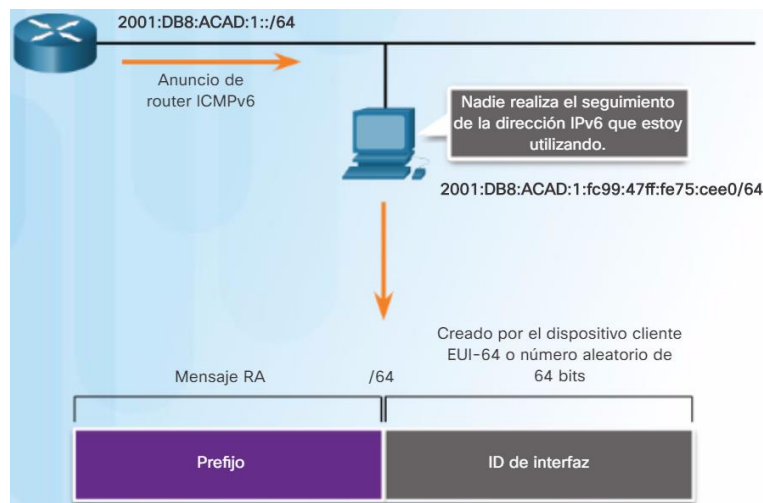
### Opción 1 de RA: SLAAC

De manera predeterminada, el mensaje RA sugiere que el dispositivo receptor use la información de dicho mensaje para crear su propia dirección IPv6 de unidifusión global y para toda la demás información. No se requieren los servicios de un servidor DHCPv6.

SLAAC es independiente del estado, o sea que no existe un servidor central (por ejemplo, un servidor DHCPv6 con información de estado) que asigne direcciones de unidifusión globales y mantenga una lista de los dispositivos y sus direcciones. Las dos partes de la dirección se crean del siguiente modo:

- **Prefijo:** se recibe en el mensaje RA.
- **ID de interfaz:** usa el proceso EUI-64 o genera un número aleatorio de 64 bits.

De manera predeterminada, el mensaje RA es la opción 1, solo SLAAC. La interfaz del router puede configurarse para enviar un anuncio de router mediante SLAAC y un DHCPv6 sin información de estado, o solo DHCPv6 con información de estado.



### Opción 2 de RA: SLAAC y DHCPv6 sin información de estado

Con esta opción, el mensaje RA sugiere que el dispositivo use lo siguiente:

- SLAAC para crear su propia dirección IPv6 de unidifusión global.
- La dirección link-local del router, la dirección IPv6 de origen del RA para la dirección de gateway predeterminado
- Un servidor DHCPv6 sin información de estado que obtendrá otra información como la dirección del servidor DNS y el nombre de dominio

Un servidor DHCPv6 sin información de estado distribuye las direcciones del servidor DNS y los nombres de dominio. No asigna direcciones de unidifusión globales.

### Opción 3 de RA: DHCPv6 con información de estado

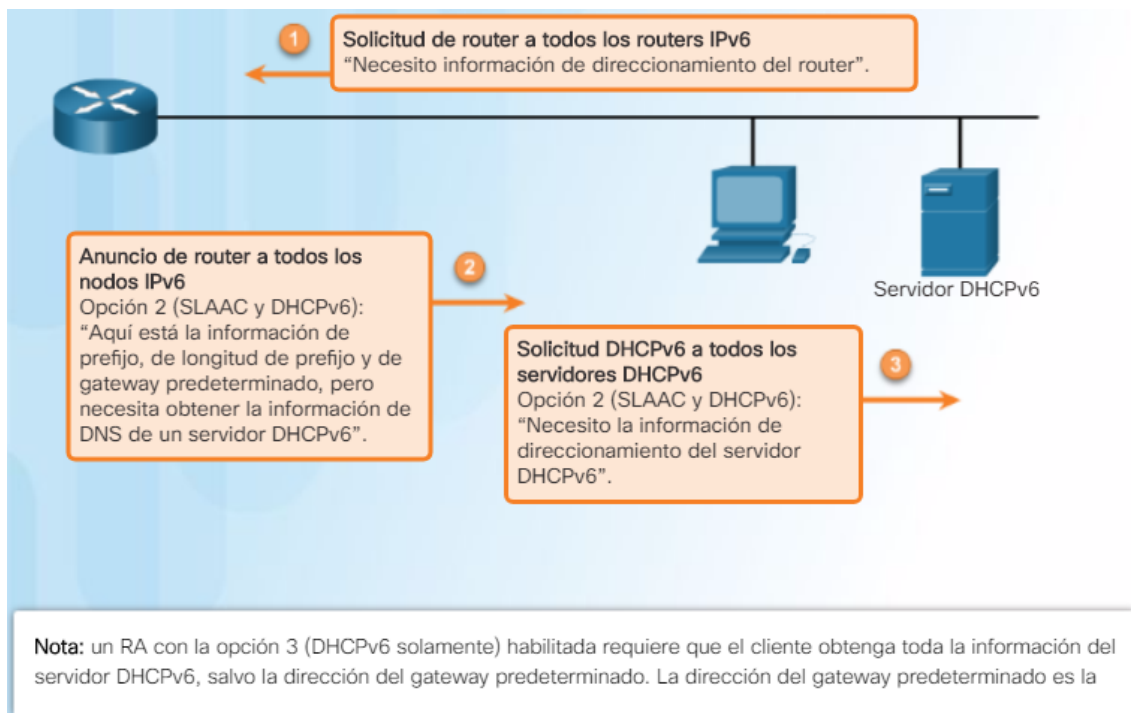
DHCPv6 con información de estado es similar a DHCP para IPv4. Un dispositivo puede recibir automáticamente la información de direccionamiento, que incluye una dirección de unidifusión global, la longitud de prefijo y las direcciones de los servidores DNS que usan los servicios de un servidor DHCPv6 con información de estado.

Con esta opción, el mensaje RA sugiere que el dispositivo use lo siguiente:

- La dirección link-local del router, la dirección IPv6 de origen del RA para la dirección de gateway predeterminado
- Un servidor DHCPv6 con información de estado para obtener una dirección de unidifusión global, una dirección del servidor DNS, un nombre de dominio y toda la información restante.

Un servidor DHCPv6 con información de estado asigna y mantiene una lista de qué dispositivo recibe cuál dirección IPv6. DHCP para IPv4 tiene información de estado.

**Nota:** la dirección de gateway predeterminado solo puede obtenerse de manera dinámica del mensaje RA. El servidor DHCPv6 con información de estado o sin ella no brinda la dirección de gateway predeterminado.



#### 7.2.4.5 Proceso EUI-64 y generación aleatoria

Cuando el mensaje RA es SLAAC o SLAAC con DHCPv6 sin información de estado, el cliente debe generar su propia ID de interfaz. El cliente conoce la porción de prefijo de la dirección del mensaje RA, pero debe crear su propia ID de interfaz. La ID de interfaz puede crearse mediante el proceso EUI-64 o mediante un número de 64 bits de generación aleatoria.

##### Proceso EUI-64

El IEEE definió el identificador único extendido (EUI) o proceso EUI-64 modificado. Este proceso utiliza la dirección MAC de Ethernet de 48 bits de un cliente e introduce otros 16 bits en medio de la dirección MAC de 48 bits para crear una ID de interfaz de 64 bits.

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 (6 dígitos hexadecimales) asignado por el IEEE.
- **Identificador de dispositivo:** el identificador de dispositivo es un valor único de 24 bits (6 dígitos hexadecimales) dentro de un OUI común.

Las ID de interfaz EUI-64 se representan en sistema binario y constan de tres partes:

- OUI de 24 bits de la dirección MAC del cliente, pero el séptimo bit (bit universal/local, U/L) se invierte. Esto quiere decir que si el séptimo bit es un 0, se transforma en un 1, y viceversa.
- Valor de 16 bits FFFE introducido (en formato hexadecimal)
- Identificador de dispositivo de 24 bits de la dirección MAC del cliente

En la figura 1, se ilustra el proceso EUI-64, con la siguiente dirección MAC de GigabitEthernet de R1: FC99:4775:CEE0.

**Paso 1:** Dividir la dirección MAC entre el OUI y el identificador de dispositivo.

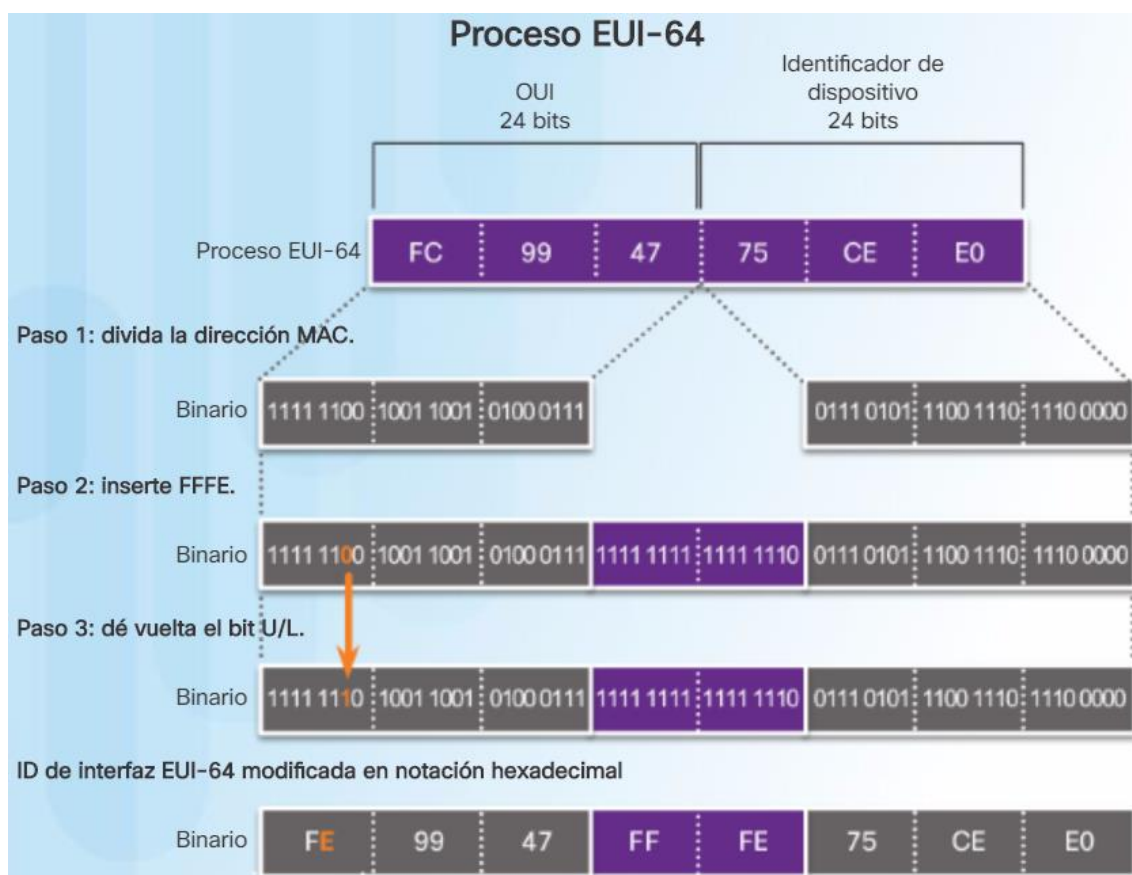
**Paso 2:** Insertar el valor hexadecimal FFFE, que en sistema binario es 1111 1111 1111 1110.

**Paso 3:** Convertir los primeros 2 valores hexadecimales del OUI a sistema binario y cambie el bit U/L (bit 7). En este ejemplo, el 0 en el bit 7 se cambia a 1.

El resultado es una ID de interfaz FE99:47FF:FE75:CEE0 generada mediante EUI-64.

**Nota:** en RFC 5342, se analiza el uso del bit U/L y las razones para invertir su valor.





En la figura 2, se muestra la dirección IPv6 de unidifusión global de la PCA creada de manera dinámica mediante SLAAC y el proceso EUI-64. Una manera sencilla de identificar que una dirección muy probablemente se creó mediante EUI-64 es el valor FFFE ubicado en medio de la ID de interfaz, como se muestra en la figura 2.

```

PCA> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection: Mensaje RA Generado mediante EUI-64
Connection-specific DNS Suffix :
IPv6 Address. . . . . : 2001:db8:acad:1:fc99:47ff:Ffe75:cee0
Link-local IPv6 Address . . . . : fe80::fc99:47FF:FE75:CEE0
Default Gateway . . . . . : fe80::1
    
```

La ventaja de EUI-64 es que se puede utilizar la dirección MAC de Ethernet para determinar la ID de interfaz. También permite que los administradores de redes rastreen fácilmente una dirección IPv6 a un terminal mediante la dirección MAC única. Sin embargo, esto generó inquietudes a muchos usuarios con respecto a la privacidad. Les preocupa que los paquetes puedan ser rastreados a la PC física real. Debido a estas inquietudes, se puede utilizar en cambio una ID de interfaz generada aleatoriamente.

**ID de interfaz generadas aleatoriamente**

Según el sistema operativo, un dispositivo puede utilizar una ID de interfaz generada aleatoriamente en lugar de utilizar la dirección MAC y el proceso EUI-64. Por ejemplo, a partir de Windows Vista, Windows utiliza una ID de interfaz generada aleatoriamente en lugar de una ID de interfaz creada mediante EUI-64. Windows XP y los sistemas operativos Windows anteriores utilizaban EUI-64.

Después de establecer la ID de interfaz, ya sea mediante el proceso EUI-64 o mediante la generación aleatoria, se la puede combinar con un prefijo IPv6 en el mensaje RA para crear una dirección de unidifusión global, como se muestra en la figura 3.

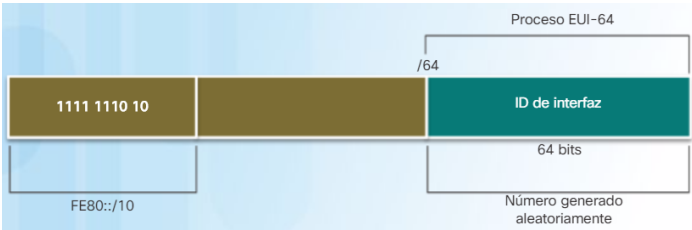
**Nota:** para garantizar la exclusividad de cualquier dirección IPv6 de unidifusión, el cliente puede usar un proceso denominado "detección de direcciones duplicadas" (DAD). Es similar a una solicitud de ARP para su propia dirección. Si no se obtiene una respuesta, la dirección es única.

```
PCB> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix  : 
    IPv6 Address. . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
    Link-local IPv6 Address . . . . : fe80::50a5:8a35:a5bb:66e1
    Default Gateway . . . . . : fe80::1
```

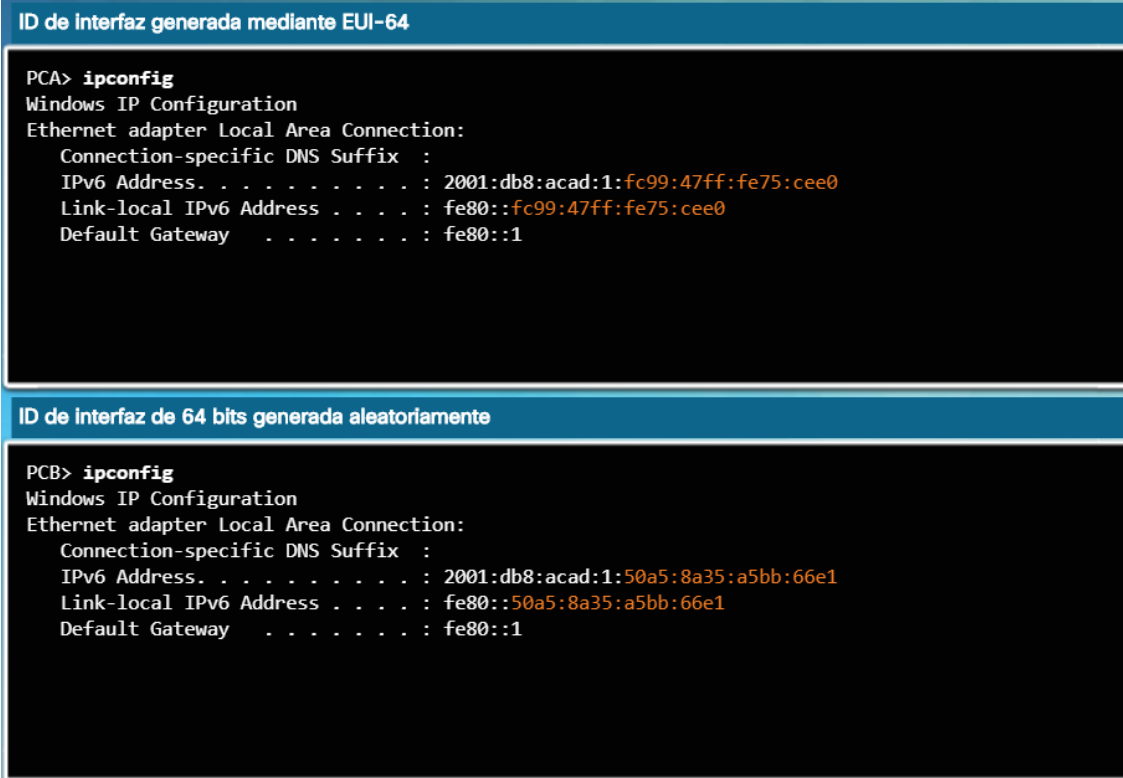
**7.2.4.6 Direcciones link-local dinámicas**

Todos los dispositivos IPv6 deben tener direcciones IPv6 link-local. Las direcciones link-local se pueden establecer dinámicamente o se pueden configurar de forma manual como direcciones link-local estáticas.

En la figura 1, se muestra que la dirección link-local fue creada de manera dinámica con el prefijo FE80::/10 y la ID de interfaz mediante el proceso EUI-64 o un número de 64 bits de generación aleatoria.



En general, los sistemas operativos usan el mismo método, tanto para una dirección de unidifusión global creada por SLAAC como para una dirección link-local asignada de manera dinámica, como se muestra en la figura 2.



The figure consists of two screenshots of a Windows command prompt window showing the output of the `ipconfig` command. The first screenshot is titled "ID de interfaz generada mediante EUI-64" and shows the IPv6 address `2001:db8:acad:1:fc99:47ff:fe75:cee0` and the link-local address `fe80::fc99:47ff:fe75:cee0`. The second screenshot is titled "ID de interfaz de 64 bits generada aleatoriamente" and shows the IPv6 address `2001:db8:acad:1:50a5:8a35:a5bb:66e1` and the link-local address `fe80::50a5:8a35:a5bb:66e1`.

```
PCA> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix  :
    IPv6 Address. . . . . : 2001:db8:acad:1:fc99:47ff:fe75:cee0
    Link-local IPv6 Address . . . . : fe80::fc99:47ff:fe75:cee0
    Default Gateway . . . . . : fe80::1

PCB> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix  :
    IPv6 Address. . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
    Link-local IPv6 Address . . . . : fe80::50a5:8a35:a5bb:66e1
    Default Gateway . . . . . : fe80::1
```

Los routers Cisco crean automáticamente una dirección IPv6 link-local cada vez que se asigna una dirección de unidifusión global a la interfaz. De manera predeterminada, los routers con Cisco IOS utilizan EUI-64 para generar la ID de interfaz para todas las direcciones link-local en las interfaces IPv6. Para las interfaces seriales, el router utiliza la dirección MAC de una interfaz Ethernet. Recuerde que una dirección link-local debe ser única solo en ese enlace o red.

Sin embargo, una desventaja de utilizar direcciones de enlace local asignadas dinámicamente es su ID de interfaz larga, que dificulta identificar y recordar las direcciones asignadas. En la figura 3, se muestra la dirección MAC en la interfaz GigabitEthernet 0/0 del router R1. Esta dirección se usa para crear de manera dinámica las direcciones link-local en la misma interfaz.

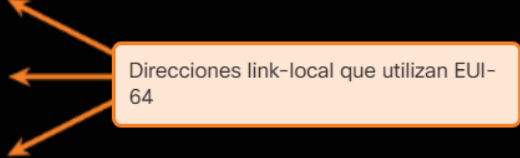
Para que sea más fácil reconocer y recordar estas direcciones en los routers, es habitual configurar las direcciones IPv6 link-local de manera estática en ellos.

```

R1# show interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e0
(bia fc99.4775.c3e0)
<se omitió el resultado>

R1# show ipv6 interface brief
GigabitEthernet0/0    [up/up]
  FE80::FE99:47FF:FE75:C3E0
  2001:DB8:ACAD:1::1
GigabitEthernet0/1    [up/up]
  FE80::FE99:47FF:FE75:C3E1
  2001:DB8:ACAD:2::1
Serial0/0/0           [up/up]
  FE80::FE99:47FF:FE75:C3E0
  2001:DB8:ACAD:3::1
Serial0/0/1           [administratively down/down]
  unassigned
R1#

```



Direcciones link-local que utilizan EUI-64

#### 7.2.4.7 Direcciones link-local estáticas

Configurar la dirección link-local manualmente permite crear una dirección reconocible y más fácil de recordar. Por lo general, solo es necesario crear direcciones de enlace local reconocibles en los routers. Esto es útil, ya que utilizan direcciones de enlace local del router como direcciones de gateway predeterminado y en los mensajes routing de anuncios.

Las direcciones link-local pueden configurarse manualmente mediante el mismo comando de interfaz utilizado para crear las direcciones IPv6 de unidifusión globales, pero con un parámetro **link-local** adicional. Cuando una dirección comienza con este hexeteto dentro del rango de FE80 a FEBF, el parámetro de link-local debe seguir a la dirección.

En la ilustración, se muestra la configuración de una dirección link-local con el comando de interfaz **ipv6 address**. La dirección link-local FE80::1 se utiliza para que sea posible reconocer fácilmente que pertenece al router R1. Se configura la misma dirección IPv6 link-local en todas las interfaces del R1. Se puede configurar FE80::1 en cada enlace, debido a que solamente tiene que ser única en ese enlace.

De manera similar al R1, el router R2 se configura con FE80::2 como la dirección IPv6 link-local en todas las interfaces.

```

Router(config-if)#

ipv6 address link-local-address link-local

R1(config)# interface gigabitethernet 0/0
R1(config-if)# ipv6 address fe80::1 ?
    link-local Use link-local address

R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/1
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)#

```

#### 7.2.4.8 Verificación de la configuración de la dirección IPv6

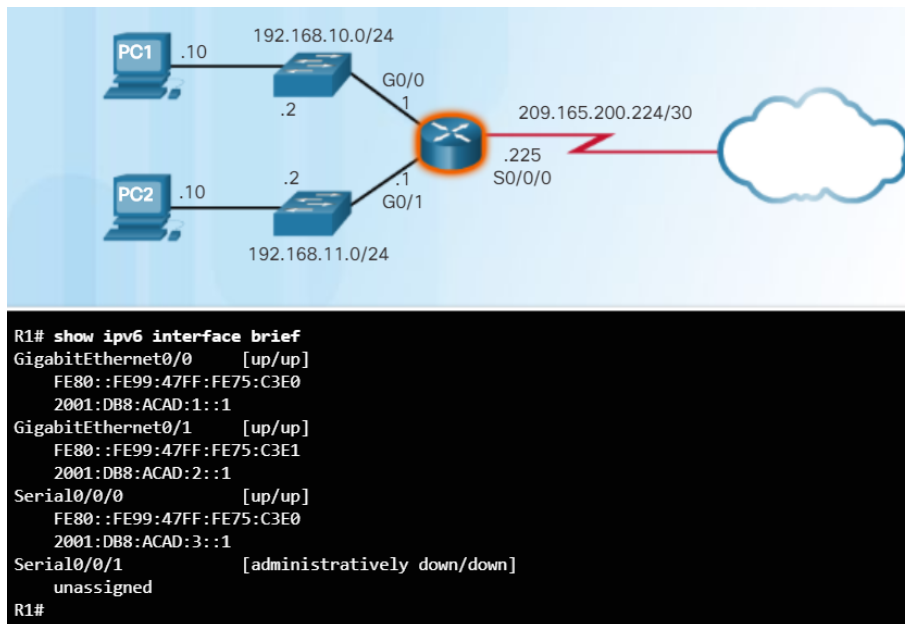
Como se muestra en la figura 1, el comando para verificar la configuración de la interfaz IPv6 es similar al comando que se utiliza para IPv4.

El comando **show interface** muestra la dirección MAC de las interfaces Ethernet. EUI-64 utiliza esta dirección MAC para generar la ID de interfaz para la dirección link-local. Además, el comando **show ipv6 interface brief** muestra el resultado abreviado para cada una de las interfaces. El resultado **[up/up]** en la misma línea que la interfaz indica el estado de interfaz de la capa 1 y la capa 2. Esto es lo mismo que las columnas **Status** Estado y **Protocol** (Protocolo) en el comando IPv4 equivalente.

Observe que cada interfaz tiene dos direcciones IPv6. La segunda dirección para cada interfaz es la dirección de unidifusión global que se configuró. La primera dirección, la que comienza con FE80, es la dirección de unidifusión link-local para la interfaz. Recuerde que la dirección link-local se agrega automáticamente a la interfaz cuando se asigna una dirección de unidifusión global.

Además, observe que la dirección link-local Serial 0/0/0 de R1 es igual a la interfaz GigabitEthernet 0/0. Las interfaces seriales no tienen direcciones MAC de Ethernet, por lo que Cisco IOS usa la dirección MAC de la primera interfaz Ethernet disponible. Esto es posible porque las interfaces link-local solo deben ser únicas en ese enlace.

La dirección link-local de la interfaz de router suele ser la dirección de gateway predeterminado para los dispositivos en ese enlace o red.



Como se muestra en la figura 2, se puede usar el comando **show ipv6 route** para verificar que las redes IPv6 y las direcciones de interfaz IPv6 específicas se hayan instalado en la tabla de routing IPv6. El comando **show ipv6 route** muestra solamente las redes IPv6, no las redes IPv4.

Dentro de la tabla de rutas, una **C** junto a la ruta indica que es una red conectada directamente. Cuando la interfaz de router se configura con una dirección de unidifusión global y su estado es “up/up”, se agrega el prefijo y la longitud de prefijo IPv6 a la tabla de routing IPv6 como una ruta conectada.

**Note:** La **L** indica una ruta local, la dirección IPv6 específica asignada a la interfaz. Esta no es una dirección de enlace local. Las direcciones de enlace local no están incluidas en la tabla de routing del router, ya que no son direcciones enrutables.

La dirección IPv6 de unidifusión global configurada en la interfaz también se instala en la tabla de routing como una ruta local. La ruta local tiene un prefijo /128. La tabla de routing utiliza las rutas locales para procesar eficazmente paquetes cuya dirección de destino es la dirección de interfaz del router.

```
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static

C  2001:DB8:ACAD:1::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L  2001:DB8:ACAD:1::1/128 [0/0]
    via GigabitEthernet0/0, receive
C  2001:DB8:ACAD:2::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L  2001:DB8:ACAD:2::1/128 [0/0]
    via GigabitEthernet0/1, receive
C  2001:DB8:ACAD:3::/64 [0/0]
    via Serial0/0/0, directly connected
L  2001:DB8:ACAD:3::1/128 [0/0]
    via Serial0/0/0, receive
L  FF00::/8 [0/0]
    via Null0, receive
R1#
```

El comando **ping** de IPv6 es idéntico al comando que se usa en IPv4, excepto que se usa una dirección IPv6. Como se muestra en la figura 3, el comando se utiliza para verificar la conectividad de capa 3 entre el R1 y la PC1. Al hacer ping de un router a una dirección link-local, Cisco IOS solicita al usuario la interfaz de salida. Como la dirección link-local de destino puede ser uno o más de sus enlaces o redes, el router debe saber a qué interfaz enviar el comando ping.

```
R1# ping 2001:db8:acad:1::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5)
R1#
```

### 7.2.5.1 Direcciones IPv6 de multidifusión asignadas

Las direcciones IPv6 de multidifusión son similares a las direcciones IPv4 de multidifusión. Recuerde que las direcciones de multidifusión se utilizan para enviar un único paquete a uno o más destinos (grupo de multidifusión). Las direcciones IPv6 de multidifusión tienen el prefijo FF00::/8.

**Nota:** las direcciones de multidifusión solo pueden ser direcciones de destino y no direcciones de origen.

Existen dos tipos de direcciones IPv6 de multidifusión:

- Dirección de multidifusión asignada
- Dirección de multidifusión de nodo solicitado

#### Dirección de multidifusión asignada

Las direcciones de multidifusión asignadas son direcciones de multidifusión reservadas para grupos predefinidos de dispositivos. Una dirección de multidifusión asignada es una única dirección que se utiliza para llegar a un grupo de dispositivos que ejecutan un protocolo o servicio común. Las direcciones de multidifusión asignadas se utilizan en contexto con protocolos específicos, como DHCPv6.

Dos grupos comunes de direcciones IPv6 de multidifusión asignadas incluyen los siguientes:

- **Grupo de multidifusión FF02::1 para todos los nodos:** este es un grupo de multidifusión al que se unen todos los dispositivos con IPv6 habilitado. Los paquetes que se envían a este grupo son recibidos y procesados por todas las interfaces IPv6 en el enlace o en la red. Esto tiene el mismo efecto que una dirección de difusión en IPv4. En la ilustración, se muestra un ejemplo de comunicación mediante la dirección de multidifusión de todos los nodos. Un router IPv6 envía mensajes de RA de protocolo de mensajes de control de Internet versión 6 (ICMPv6) al grupo de multidifusión de todos los nodos. El mensaje RA proporciona a todos los dispositivos en la red con IPv6 habilitado la información de direccionamiento, como el prefijo, la longitud de prefijo y el gateway predeterminado.
- **Grupo de multidifusión FF02::2 para todos los routers:** este es un grupo de multidifusión al que se unen todos los routers IPv6. Un router comienza a formar parte de este grupo cuando se lo habilita como router IPv6 con el comando de configuración global **ipv6 unicast-routing**. Los paquetes que se envían a este grupo son recibidos y procesados por todos los routers IPv6 en el enlace o en la red.

Los dispositivos con IPv6 habilitado envían mensajes de solicitud de router (RS) de ICMPv6 a la dirección de multidifusión de todos los routers. El mensaje RS solicita un mensaje RA del router IPv6 para contribuir a la configuración de direcciones del dispositivo.



#### 7.2.5.2 Direcciones IPv6 de multidifusión de nodo solicitado

Una dirección de multidifusión de nodo solicitado es similar a una dirección de multidifusión de todos los nodos. La ventaja de una dirección de multidifusión de nodo solicitado es que se asigna a una dirección especial de multidifusión de Ethernet. Esto permite que la NIC Ethernet filtre el marco al examinar la dirección MAC de destino sin enviarla al proceso de IPv6 para ver si el dispositivo es el objetivo previsto del paquete IPv6.





### 7.3.1.1 ICMPv4 e ICMPv6

Son mensajes cuyo objetivo es proporcionar respuestas acerca de temas relacionados con el procesamiento de paquetes IP en determinadas condiciones, no es hacer que IP sea confiable. Los mensajes de ICMP no son obligatorios y, a menudo, no se permiten dentro de una red por razones de seguridad.

El protocolo ICMP está disponible tanto para IPv4 como para IPv6. El protocolo de mensajes para IPv4 es ICMPv4. ICMPv6 proporciona estos mismos servicios para IPv6, pero incluye funcionalidad adicional. En este curso, el término ICMP se utilizará para referirse tanto a ICMPv4 como a ICMPv6.

Existe una gran variedad de tipos de mensajes de ICMP y de razones para enviarlos. Analizaremos algunos de los mensajes más comunes.

Los mensajes ICMP comunes a ICMPv4 y a ICMPv6 incluyen lo siguiente:

- Confirmación de host
- Destino o servicio inaccesible
- Tiempo superado
- Redireccionamiento de ruta

#### Confirmación de host

Se puede utilizar un mensaje de eco ICMP para determinar si un host funciona. El host local envía una solicitud de eco ICMP a un host. Si el host se encuentra disponible, el host de destino responde con una respuesta de eco.

#### Destino o servicio inaccesible

Cuando un host o gateway recibe un paquete que no puede entregar, puede utilizar un mensaje ICMP de destino inalcanzable para notificar al origen que el destino o el servicio son inalcanzables. El mensaje incluye un código que indica el motivo por el cual no se pudo entregar el paquete. Algunos de los códigos de destino inalcanzable para ICMPv4 son los siguientes:

- 0: red inalcanzable
- 1: host inalcanzable
- 2: protocolo inalcanzable
- 3: puerto inalcanzable

**Nota:** ICMPv6 tiene códigos similares, pero levemente diferentes para los mensajes de destino inalcanzable.

#### Tiempo superado

Los routers utilizan los mensajes de tiempo superado de ICMPv4 para indicar que un paquete no puede reenviarse debido a que el campo de tiempo de duración (TTL) del paquete se disminuyó a 0. Si un router recibe un paquete y disminuye el campo TTL en el paquete IPv4 a cero, descarta el paquete y envía un mensaje de tiempo superado al host de origen.

ICMPv6 también envía un mensaje de tiempo superado si el router no puede reenviar un paquete IPv6 debido a que el paquete caducó. IPv6 no tiene un campo TTL, por lo que utiliza el campo de límite de saltos para determinar si el paquete caducó.

### 7.3.1.2 Mensajes de solicitud y de anuncio de router de ICMPv6

Los mensajes informativos y de error que se encuentran en ICMPv6 son muy similares a los mensajes de control y de error que implementa ICMPv4. Sin embargo, ICMPv6 tiene nuevas características y funcionalidad mejorada que no se encuentran en ICMPv4. Los mensajes ICMPv6 están encapsulados en IPv6.

ICMPv6 incluye cuatro protocolos nuevos como parte del protocolo de detección de vecino (ND o NDP).

Mensajería entre un router IPv6 y un dispositivos IPv6:

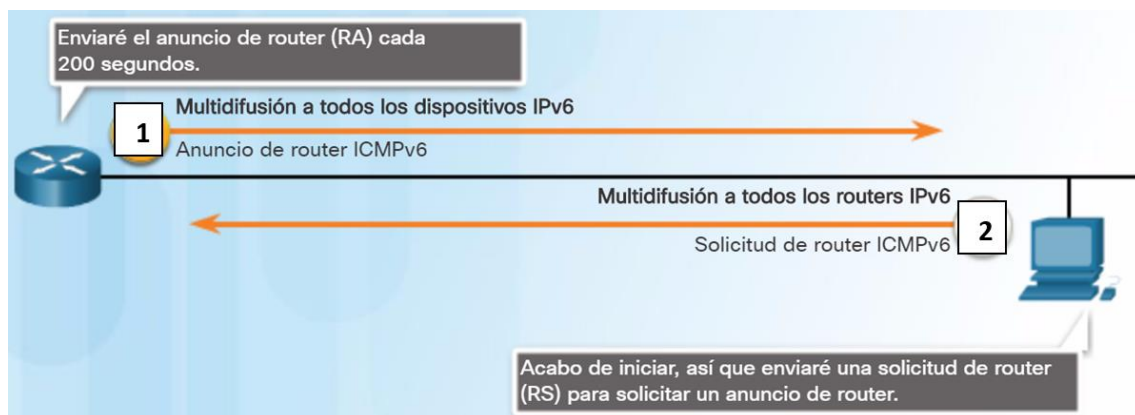
- Mensaje de solicitud de router (RS)
- Mensaje de anuncio de router (RA)

Mensajería entre dispositivos IPv6:

- Mensaje de solicitud de vecino (NS)
- Mensaje de anuncio de vecino (NA)

**Nota:** El ND de ICMPv6 también incluye el mensaje de redireccionamiento, que tiene una función similar al mensaje de redireccionamiento utilizado en ICMPv4.

En la figura 1, se muestra un ejemplo de una PC y un router que intercambian mensajes de anuncio de router y de solicitud. Haga clic en cada mensaje para obtener más información.



1. Los routers envían mensajes de RA para proporcionar información de direccionamiento a los host que utilizan SLAAC. El mensaje de Ra puede incluir información de direccionamiento para el host, como el prefijo, la longitud del prefijo, la dirección DNS y el nombre de dominio. Un router envía un mensaje de RA periódicamente o en respuesta a un mensaje de RS. Un host que utiliza SLAAC establecerá como su gateway predeterminado la dirección link-local del router que envió el RA.

2. Cuando un host está configurado para obtener la información de direccionamiento automáticamente utilizando la configuración automática de dirección independiente del estado (SLAAC), el host envía un mensaje de RS al router que solicita el mensaje de RA.

## Resolución de direcciones

La resolución de direcciones se utiliza cuando un dispositivo en la LAN conoce la dirección IPv6 de un destino, pero no conoce la dirección MAC de Ethernet. Para determinar la dirección MAC del destino, el dispositivo envía un mensaje de NS a la dirección de nodo solicitado. El mensaje incluye la dirección IPv6 conocida (objetivo). El dispositivo que se destinó a la dirección IPv6 responde con un mensaje NA que contiene la dirección MAC de Ethernet. En la figura 2, se muestran dos PC que intercambian mensajes de NS y NA.



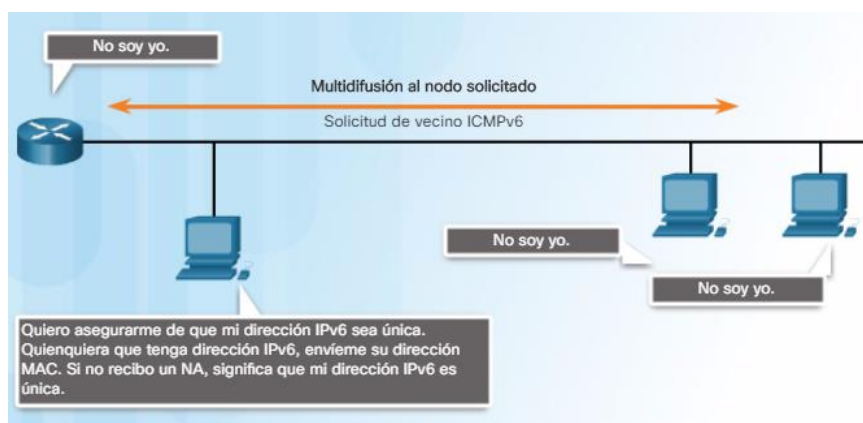
1. Los mensajes de NS se envían cuando un dispositivo conoce la dirección IPv6 de un dispositivo pero no la dirección MAC. Esto equivale a una solicitud de ARP para IPv4.

2. Los mensajes de NA se envían en respuesta a un mensaje de NS y coinciden con la dirección IPv6 de la NS. El mensaje de NA contiene la dirección MAC de Ethernet del dispositivo. Esto equivale a una respuesta de ARP para IPv4.

## Detección de direcciones duplicadas

Cuando se asigna una dirección de unidifusión global o link-local a un dispositivo, se recomienda realizar una operación DAD en la dirección para garantizar que sea única. Para verificar la singularidad de una dirección, el dispositivo envía un mensaje de NS con su propia dirección IPv6 como dirección IPv6 de destino, como se muestra en la figura 3. Si otro dispositivo de la red tiene esta dirección, responde con un mensaje NA. Este mensaje NA notifica al dispositivo emisor que la dirección está en uso. Si no se devuelve un mensaje NA correspondiente dentro de determinado período, la dirección de unidifusión es única y su uso es aceptable.

**Nota:** no es necesaria la operación DAD, pero la RFC 4861 recomienda que se realice una DAD en las direcciones de unidifusión.



### 7.3.2.1 Ping: Prueba de la pila local

El comando ping tiene un valor de tiempo de espera para la respuesta. Si no se recibe una respuesta dentro del tiempo de espera, el comando ping proporciona un mensaje que indica que no se recibió una respuesta. Generalmente, esto indica que existe un problema, pero también podría indicar que se habilitaron características de seguridad que bloquean los mensajes ping en la red.

Una vez que se envían todas las solicitudes, la utilidad ping proporciona un resumen que incluye la tasa de éxito y el tiempo promedio del viaje de ida y vuelta al destino.

#### **Ping del bucle invertido local**

Existen casos especiales de prueba y verificación para los cuales se puede usar el comando ping. Un caso es la prueba de la configuración interna de IPv4 o de IPv6 en el host local. Para realizar esta prueba, se debe hacer ping a la dirección de bucle invertido local 127.0.0.1 para IPv4 (::1 para IPv6).

Una respuesta de 127.0.0.1 para IPv4 (o ::1 para IPv6) indica que IP está instalado correctamente en el host. Esta respuesta proviene de la capa de red. Sin embargo, esta respuesta no indica que las direcciones, las máscaras o los gateways estén configurados adecuadamente. Tampoco indica nada acerca del estado de la capa inferior de la pila de red. Simplemente, prueba el protocolo IP en la capa de red de dicho protocolo. Un mensaje de error indica que TCP/IP no funciona en el host.

### 7.3.2.2 Ping: Prueba de la conectividad a la LAN local

También es posible utilizar el comando ping para probar la capacidad de comunicación de un host en la red local. Por lo general, esto se realiza haciendo ping a la dirección IP del gateway del host. Un ping al gateway indica que la interfaz del host y la interfaz del router que cumplen la función de gateway funcionan en la red local.

Para esta prueba, se suele usar la dirección de gateway porque el router generalmente está en funcionamiento. Si la dirección de gateway no responde, se puede enviar un ping a la dirección IP de otro host en la red local que se sepa que funciona.

Si el gateway u otro host responden, los hosts locales pueden comunicarse correctamente en la red local. Si el gateway no responde pero otro host sí lo hace, esto podría indicar un problema con la interfaz de router que sirve como gateway.

Una posibilidad es que se haya configurado la dirección de gateway incorrecta en el host. Otra posibilidad es que la interfaz del router puede estar en funcionamiento, pero se le ha aplicado seguridad, de manera que no procesa o responde solicitudes de ping.

### 7.3.2.3 Ping: Prueba de la conectividad a una red remota

También se puede utilizar el comando ping para probar la capacidad de un host local para comunicarse en una interconexión de redes. El host local puede hacer ping a un host IPv4 operativo de una red remota, como se muestra en la ilustración.

Si este ping se realiza correctamente, se puede verificar el funcionamiento de una amplia porción de la interconexión de redes. Un ping correcto en una interconexión de redes confirma la comunicación en la red local, el funcionamiento del router que sirve como gateway y el funcionamiento de todos los routers que podrían estar en la ruta entre la red local y la red del módulo remoto de E/S.

De manera adicional, se puede verificar la funcionalidad del módulo remoto de E/S. Si el módulo remoto de E/S no podía comunicarse fuera de la red local, no hubiera respondido.

**Nota:** muchos administradores de redes limitan o prohíben la entrada de mensajes ICMP a la red; por lo tanto, la falta de una respuesta ping puede ser por razones de seguridad.

### 7.3.2.4 Traceroute: Prueba de la ruta

Traceroute (tracert) es una utilidad que genera una lista de saltos que se alcanzaron correctamente a lo largo de la ruta. Si los datos llegan al destino, el rastreo indica la interfaz de cada router que aparece en la ruta entre los hosts. Si los datos fallan en algún salto a lo largo del camino, la dirección del último router que respondió al rastreo puede indicar dónde se encuentra el problema o las restricciones de seguridad.

#### Tiempo de ida y vuelta (RTT)

El uso de traceroute proporciona el tiempo de ida y vuelta para cada salto a lo largo de la ruta e indica si un salto no responde. El tiempo de ida y vuelta es el tiempo que le lleva a un paquete llegar al módulo remoto de E/S y el tiempo que la respuesta del host demora en regresar. Se utiliza un asterisco (\*) para indicar un paquete perdido o sin respuesta.

Si en la pantalla se muestran tiempos de respuesta elevados o pérdidas de datos de un salto en particular, esto el router o sus conexiones pueden estar sobrecargados.

#### TTL de IPv4 y límite de saltos de IPv6

Traceroute utiliza una función del campo TTL en IPv4 y del campo límite de saltos de IPv6 en los encabezados de capa 3, junto con el mensaje de tiempo superado de ICMP.

La primera secuencia de mensajes enviados desde traceroute tiene TTL = 1. Esto hace que el TTL agote el tiempo de espera del paquete IPv4 en el primer router. Este router luego responde con un mensaje de ICMPv4. Traceroute ahora tiene la dirección del primer salto.

A continuación, Traceroute incrementa progresivamente el campo TTL (2, 3, 4...) para cada secuencia de mensajes. De esta manera se proporciona al rastreo la dirección de cada salto a medida que los paquetes agotan el límite de tiempo a lo largo del camino. El campo TTL sigue aumentando hasta que se alcanza el destino, o se incrementa a un máximo predefinido.

Después de alcanzar el destino final, el host responde con un mensaje ICMP de puerto inalcanzable o con un mensaje ICMP de respuesta de eco en lugar del mensaje ICMP de tiempo superado.