

Planificación y Administración de Redes

T.5 La capa de red

Índice

1. Características de la capa de red (8.1)
2. Paquetes IPv4 e IPv6 (8.2, 8.3)
3. Reenvío de host (8.4)
4. Introducción al enrutamiento (8.5)
5. Resolución de dirección (9.1, 9.2)
6. Direcciones IPv4 (11.1, 11.2, 11.3)
7. Subnetting (11.4, 11.5, 11.6, 11.7)
8. VLSM (11.8)
9. ICMPv4 (13)
10. IPv6 (12)
11. ICMPv6 (13.1.5)

1 Características de la capa de red

Características de la capa de red

La capa de red, o Capa OSI 3, proporciona servicios para permitir que los dispositivos finales intercambien datos a través de redes.



Características de la capa de red

IPv4 e IPv6 son los principales protocolos de comunicación de la capa de red.

Otros protocolos de capa de red incluyen **protocolos de enrutamiento** como Open Shortest Path First (**OSPF**) y **protocolos de mensajería** como Internet Control Message Protocol (**ICMP**).

Características de la capa de red

Para lograr comunicaciones end-to-end a través de los límites de la red, los protocolos de capa de red realizan cuatro operaciones básicas:

Direccionamiento de dispositivos finales : los dispositivos finales deben configurarse con una dirección IP única para la identificación en la red.

Encapsulación: La capa de red encapsula la unidad de datos de protocolo (PDU) de la capa de transporte en un paquete. El proceso de encapsulamiento agrega información de encabezado IP, como la dirección IP de los hosts de origen (emisores) y de destino (receptores). El proceso de encapsulación lo realiza el origen del paquete IP.

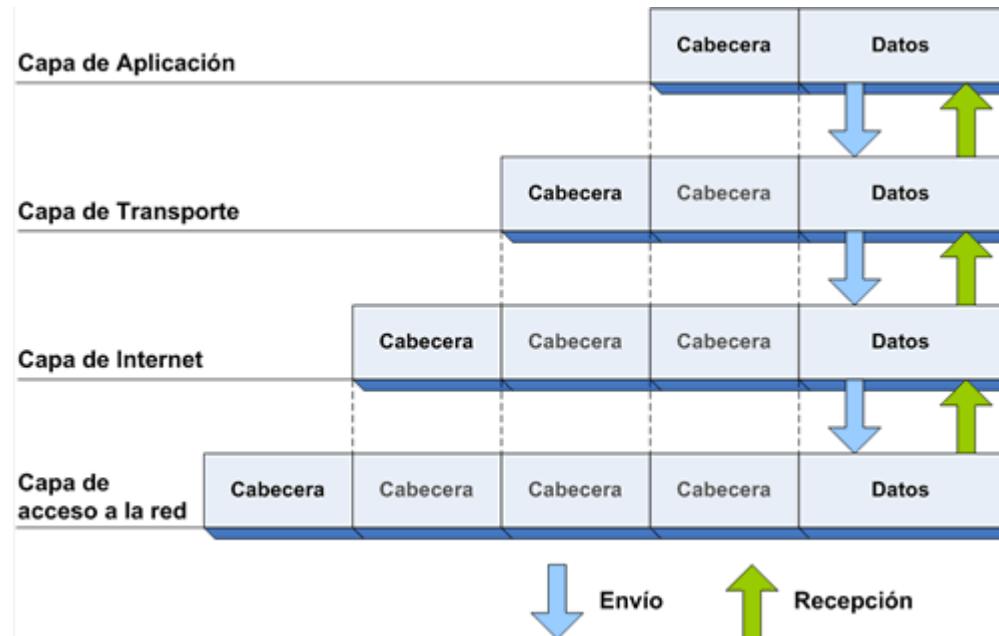
Características de la capa de red

Enrutamiento: La capa de red proporciona servicios para dirigir los paquetes a un host de destino en otra red. Para transferir un paquete a otras redes, debe procesarlo un router. La función del router es seleccionar la mejor ruta y dirigir los paquetes al host de destino en un proceso que se denomina "enrutamiento". Un paquete puede cruzar muchos routers antes de llegar al host de destino. Se denomina "salto" a cada router que cruza un paquete antes de alcanzar el host de destino.

Desencapsulación: Cuando el paquete llega a la capa de red del host de destino, el host verifica el encabezado IP del paquete. Si la dirección IP de destino dentro del encabezado coincide con su propia dirección IP, se elimina el encabezado IP del paquete. Una vez que la capa de red desencapsula el paquete, la PDU de capa 4 que se obtiene se transfiere al servicio apropiado en la capa de transporte. El proceso de desencapsulación lo realiza el host de destino del paquete IP.

Características de la capa de red

El encabezado IP es examinado por dispositivos de Capa 3 (es decir, routers y switches de Capa 3) a medida que viaja a través de una red a su destino. La información de direccionamiento IP permanece igual desde el momento en que el paquete sale del host de origen hasta que llega al host de destino, excepto cuando se traduce por el dispositivo que realiza NAT para IPv4.



Características de la capa de red

IP se diseñó como un protocolo con sobrecarga baja. Provee solo las funciones necesarias para enviar un paquete de un origen a un destino. El protocolo **no fue diseñado para rastrear ni administrar el flujo de paquetes** (si es necesario, TCP en la capa 4).

Características de IP:

- **Sin conexión:** - no hay conexión con el destino establecido antes de enviar paquetes de datos.
- **Best-effort:** - poco confiable porque no se garantiza la entrega de paquetes.
- **Independiente de los medios:** - la operación es independiente del medio (es decir, cobre, fibra óptica o inalámbrico) que transporta los datos.

2 Paquetes IPv4 e IPv6

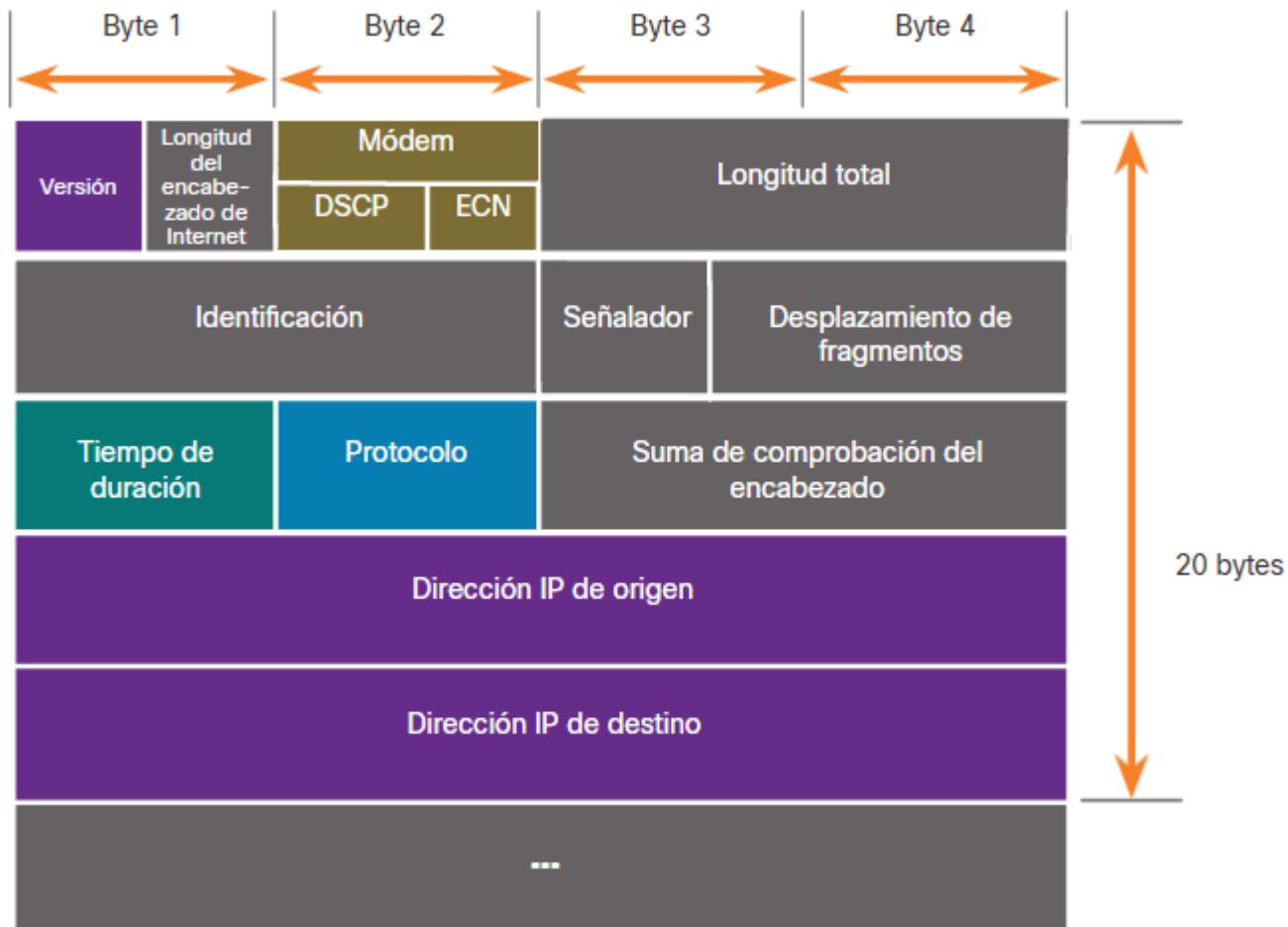
Paquetes IPv4 e IPv6

IPv4 es uno de los protocolos de comunicación de la capa de red principal. El encabezado del paquete IPv4 se utiliza para garantizar que este paquete se entrega en su siguiente parada en el camino a su dispositivo final de destino.

El encabezado de paquetes IPv4 consta de campos que contienen información importante sobre el paquete. Estos campos tienen números binarios que examinan el proceso de capa 3.

Paquetes IPv4 e IPv6

Cabecera IPv4



Paquetes IPv4 e IPv6

- **Versión** - Contiene un valor binario de 4 bits establecido en 0100 que identifica esto como un paquete IPv4.
- **Servicios diferenciados o DiffServ (DS)** - Este campo, formalmente conocido como Tipo de servicio (ToS), es un campo de 8 bits que se utiliza para determinar la prioridad de cada paquete.
- **Suma de comprobación de encabezado** - Se utiliza para detectar daños en el encabezado IPv4.

Paquetes IPv4 e IPv6

- **Tiempo de duración (Time to Live,TTL)** - TTL contiene un valor binario de 8 bits que se utiliza para limitar la vida útil de un paquete. El dispositivo de origen del paquete IPv4 establece el valor TTL inicial. Se reduce en uno cada vez que el paquete es procesado por un router. Si el campo TTL llega a cero, el router descarta el paquete y envía a la dirección IP de origen un mensaje de tiempo superado del protocolo de mensajes de control de Internet (ICMP). Debido a que el router disminuye el TTL de cada paquete, el router también debe volver a calcular la suma de comprobación del encabezado.

Paquetes IPv4 e IPv6

- **Protocolo** - Este campo se utiliza para identificar el protocolo del siguiente nivel.
- **Dirección IPv4 de origen** - Contiene un valor binario de 32 bits que representa la dirección IPv4 de origen del paquete. La dirección IPv4 de origen es siempre una dirección unicast.
- **Dirección IPv4 de destino** - Contiene un valor binario de 32 bits que representa la dirección IPv4 de destino del paquete. La dirección IPv4 de destino es una dirección unicast, multicast o de difusión.

Paquetes IPv4 e IPv6

Problemas de IPv4:

- **Agotamiento de la dirección IPv4:** IPv4 tiene un número limitado de direcciones públicas únicas disponibles.
- **Falta de conectividad de extremo a extremo:** La traducción de direcciones de red (NAT) es una tecnología comúnmente implementada dentro de las redes IPv4. NAT proporciona una manera para que varios dispositivos comparten una única dirección IPv4 pública. Sin embargo, dado que la dirección IPv4 pública se comparte, se oculta la dirección IPv4 de un host de la red interna. Esto puede ser un problema para las tecnologías que necesitan conectividad completa.
- **Mayor complejidad de la red :** mientras que NAT ha ampliado la vida útil de IPv4, solo se trataba de un mecanismo de transición a IPv6. NAT en sus diversas implementaciones crea una complejidad adicional en la red, creando latencia y haciendo más difícil la solución de problemas.

Paquetes IPv4 e IPv6

IPv6 supera las limitaciones de IPv4 y **representa una mejora importante con características que se adaptan mejor a las demandas de red actuales y previsibles.**

Las mejoras que ofrece IPv6 incluyen las siguientes:

- **Tamaño de dirección ampliado:** - las direcciones IPv6 se basan en el direccionamiento jerárquico de 128 bits en lugar de IPv4 con 32 bits.
- **Mejor manejo de paquetes** - el encabezado IPv6 se ha simplificado con menos campos.
- **Elimina la necesidad de NAT:** - con una cantidad tan grande de direcciones IPv6 públicas, no se necesita NAT entre una dirección IPv4 privada y una IPv4 pública. Esto evita algunos de los problemas inducidos por NAT que experimentan las aplicaciones que requieren conectividad de extremo a extremo.

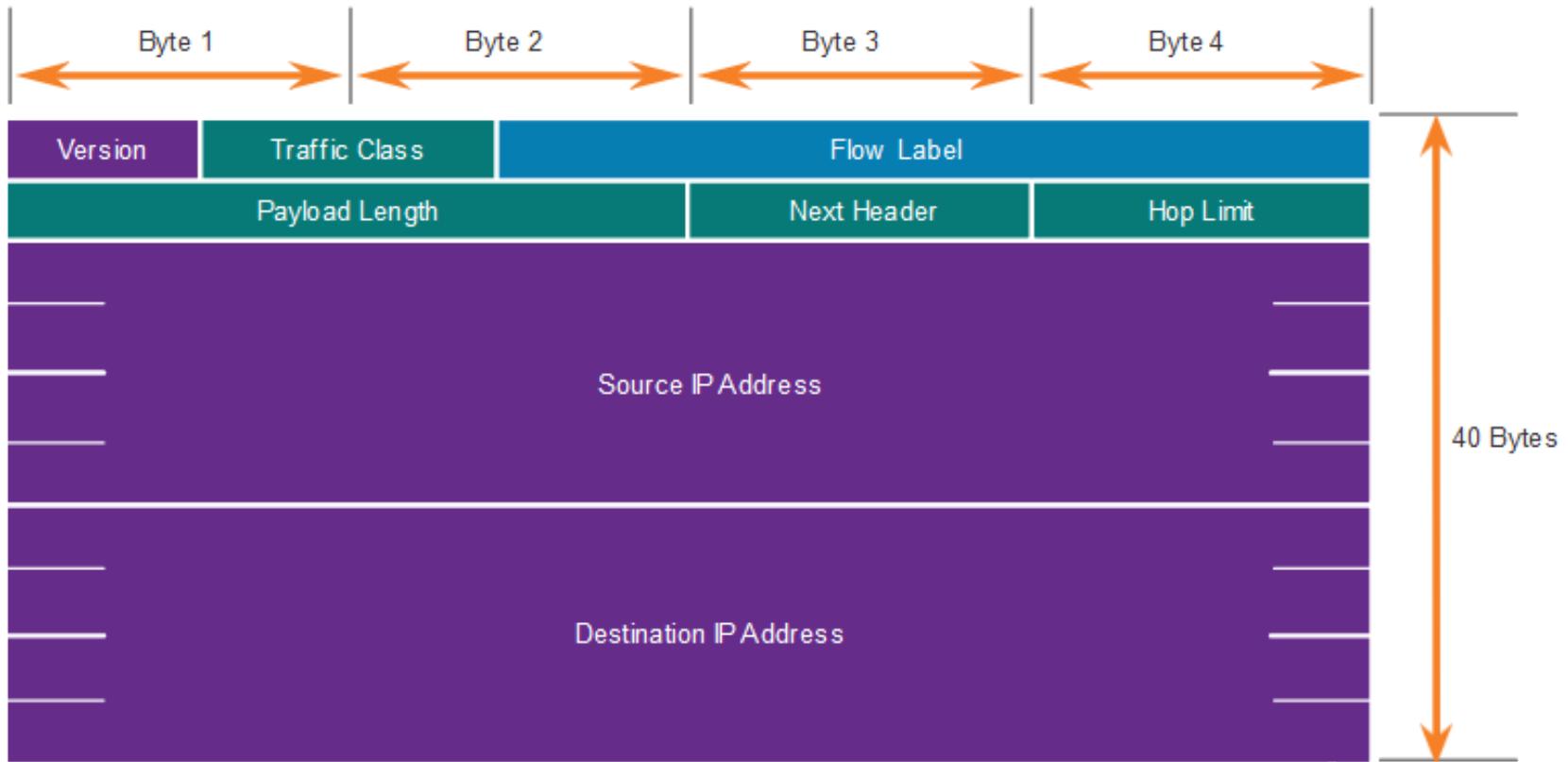
Paquetes IPv4 e IPv6

Direcciones **IPv4** vs **IPv6**:

Nombre del número	Notación científica	Cantidad de ceros	Number Name	Scientific Notation
Mil	10^3	1000	1 Thousand	10^3
1 millón	10^6	1 000000	1 Million	10^6
1000 millones	10^9	1000000000	1 Billion	10^9
1 billón	10^{12}	1000000000000	1 Trillion	10^{12}
1000 billones	10^{15}	1000000000000000	1 Quadrillion	10^{15}
1 trillón	10^{18}	10000000000000000	1 Quintillion	10^{18}
1000 trillones	10^{21}	100000000000000000	1 Sextillion	10^{21}
1 cuatrillón	10^{24}	1000000000000000000	1 Septillion	10^{24}
1000 cuatrillones	10^{27}	10000000000000000000	1 Octillion	10^{27}
1 quintillón	10^{30}	100000000000000000000	1 Nonillion	10^{30}
1000 quintillones	10^{33}	1000000000000000000000	1 Decillion	10^{33}
1 sextillón	10^{36}	10000000000000000000000	1 Undecillion	10^{36}

Paquetes IPv4 e IPv6

Cabecera IPv6



Paquetes IPv4 e IPv6

- **Versión** - Este campo contiene un valor binario de 4 bits establecido en 0110 que identifica esto como un paquete IP versión 6.
- **Clase de tráfico** - Este campo de 8 bits es equivalente al campo de Servicios diferenciados (DS) IPv4.
- **Etiqueta de flujo** - Este campo de 20 bits sugiere que todos los paquetes con la misma etiqueta de flujo reciben el mismo tipo de manejo por routers.
- **Longitud de carga útil** - Este campo de 16 bits indica la longitud de la porción de datos o carga útil del paquete IPv6. Esto no incluye la longitud del encabezado IPv6, que es un encabezado fijo de 40 bytes.

Paquetes IPv4 e IPv6

- **Encabezado siguiente** - Este campo de 8 bits es equivalente al campo de Protocolo IPv4. Es un valor que indica el tipo de contenido de datos que lleva el paquete, lo que permite que la capa de red transmita la información al protocolo de capa superior apropiado.
- **Límite de salto** - este campo de 8 bits reemplaza al campo TTL de IPv4. Cada router que reenvía el paquete reduce este valor en 1. Cuando el contador llega a 0, el paquete se descarta y se reenvía un mensaje ICMPv6 Tiempo excedido al host emisor. Esto indica que el paquete no llegó a su destino porque se excedió el límite de saltos. A diferencia de IPv4, IPv6 no incluye una suma de comprobación de encabezado IPv6, ya que esta función se realiza tanto en las capas inferior como superior. Esto significa que la suma de comprobación no necesita ser recalculada por cada router cuando disminuye el campo Límite de saltos, lo que también mejora el rendimiento de la red.

Paquetes IPv4 e IPv6

- **Dirección IPv6 de origen** - Este campo de 128 bits identifica la dirección IPv6 del host emisor.
- **Dirección IPv6 de destino** - Este campo de 128 bits identifica la dirección IPv6 del host receptor.

3 Reenvío de host

Reenvío de host

Con IPv4 e IPv6, los paquetes siempre se crean en el host de origen. El host de origen debe poder dirigir el paquete al host de destino. Para ello, los dispositivos finales de host crean su propia tabla de enrutamiento.

Otra función de la capa de red es dirigir los paquetes entre hosts.

Un host puede enviar un paquete a lo siguiente:

- **Sí mismo**- ping a sí mismo **IPv4 (127.0.0.1) o IPv6 (::1), dirección de loopback.** Verifica la pila del protocolo TCP/IP en el host.
- **Host local** - este es un host de destino que se encuentra en la misma red local que el host emisor. Los hosts de origen y destino comparten la misma dirección de red.
- **Host remoto** - este es un host de destino en una red remota. Los hosts de origen y destino no comparten la misma dirección de red.

Reenvío de host

El dispositivo final de origen determina si un paquete está destinado a un host local o a un host remoto. El dispositivo final de origen determina si la dirección IP de destino está en la misma red en la que está el propio dispositivo de origen. El método de determinación varía según la versión IP:

- **En IPv4 :** el dispositivo de origen utiliza su propia máscara de subred junto con su propia dirección IPv4 y la dirección IPv4 de destino para realizar esta determinación.
- **En IPv6 :** el router local anuncia la dirección de red local (prefijo) a todos los dispositivos de la red.

Reenvío de host

La puerta de enlace predeterminada es el dispositivo de red (es decir, el router o el switch de capa 3) **que puede enrutar el tráfico a otras redes.** En una red, una puerta de enlace predeterminada suele ser un router con estas características:

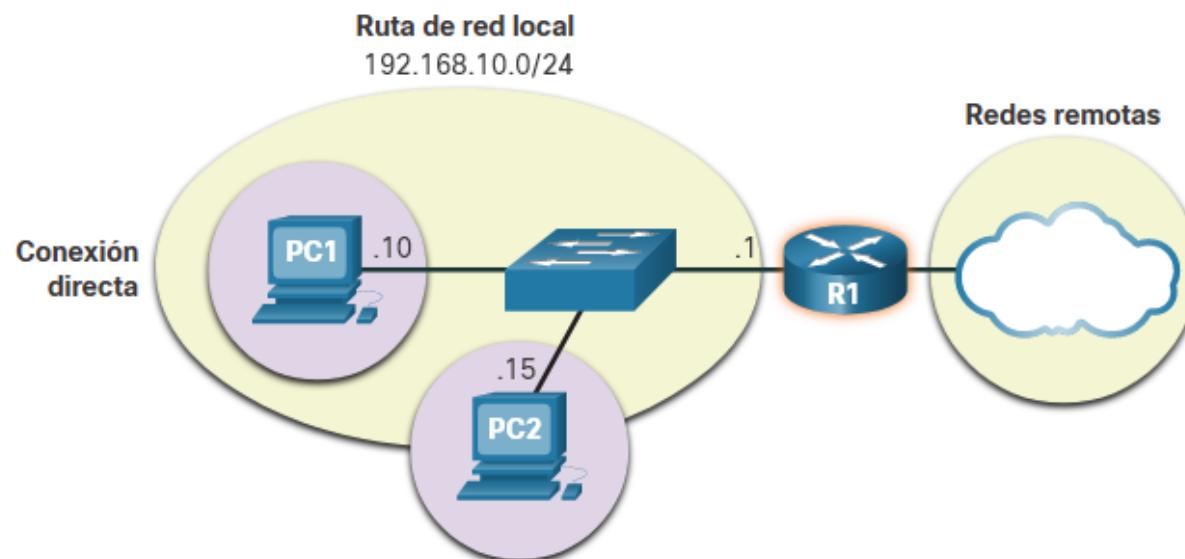
- Tiene una dirección IP local en el mismo rango de direcciones que otros hosts en la red local.
- Puede aceptar datos en la red local y reenviar datos fuera de la red local.
- Enruta el tráfico a otras redes.

Se requiere una puerta de enlace predeterminada para enviar tráfico fuera de la red local. El tráfico no se puede reenviar fuera de la red local si no hay una puerta de enlace predeterminada, la dirección de la puerta de enlace predeterminada no está configurada o la puerta de enlace predeterminada está desactivada.

Reenvío de host

Una tabla de enrutamiento de host generalmente incluirá una puerta de enlace predeterminada.

La configuración de un gateway predeterminado genera una ruta predeterminada en la tabla de enrutamiento de la PC. Una ruta predeterminada es la ruta o camino que la PC utiliza cuando intenta conectarse a la red remota.

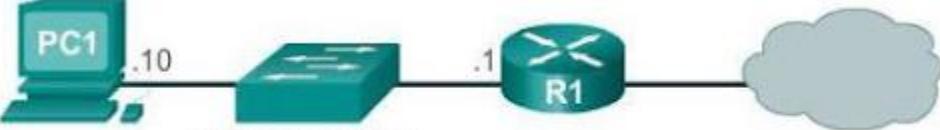


Campos de una trama

En un host de Windows, el comando **route print** o **netstat -r** se puede usar para mostrar la tabla de enrutamiento del host.

<https://www.ingenieriasystems.com/2017/03/Entradas-de-enrutamiento-de-host-IPv4-y-Tabla-de-enrutamiento-de-muestra-CCNA1-V5-CISCO-C6.html>

```
C:\Users\PC1> netstat -r  
<Resultado omitido>  
  
IPv4 Route Table  
=====  
Active Routes:  
Network Destination      Netmask        Gateway       Interface     Metric  
0.0.0.0          0.0.0.0    192.168.10.1  192.168.10.10    25  
127.0.0.0        255.0.0.0   On-link        127.0.0.1    306  
127.0.0.1        255.255.255.255  On-link        127.0.0.1    306  
127.255.255.255 255.255.255.255  On-link        127.0.0.1    306  
192.168.10.0      255.255.255.0  On-link        192.168.10.10   281  
192.168.10.10     255.255.255.255  On-link        192.168.10.10   281  
192.168.10.255     255.255.255.255  On-link        192.168.10.10   281  
224.0.0.0          240.0.0.0   On-link        127.0.0.1    306  
224.0.0.0          240.0.0.0   On-link        192.168.10.10   281  
255.255.255.255    255.255.255.255  On-link        127.0.0.1    306  
255.255.255.255    255.255.255.255  On-link        192.168.10.10   281  
=====  
<Resultado omitido>
```



The diagram illustrates a simple network topology. A computer labeled "PC1" is connected to a switch. The switch is connected to a router labeled "R1". Router R1 is connected to a cloud icon, representing the external network or Internet.

Reenvío de host

- **Destino de red:** enumera las redes que se pueden alcanzar.
- **Máscara de red:** incluye una máscara de subred que le indica al host cómo determinar las porciones de red y de host de la dirección IP.
- **Puerta de acceso:** indica la dirección que utiliza la PC local para llegar a un destino en una red remota. Si un destino es directamente accesible, se muestra como “En enlace” en esta columna.
- **Interfaz:** indica la dirección de la interfaz física utilizada para enviar el paquete al gateway que se emplea para llegar al destino de red.
- **Métrica:** indica el costo de cada ruta y se utiliza para determinar la mejor ruta a un destino.

4 Introducción al enrutamiento

Introducción al enrutamiento

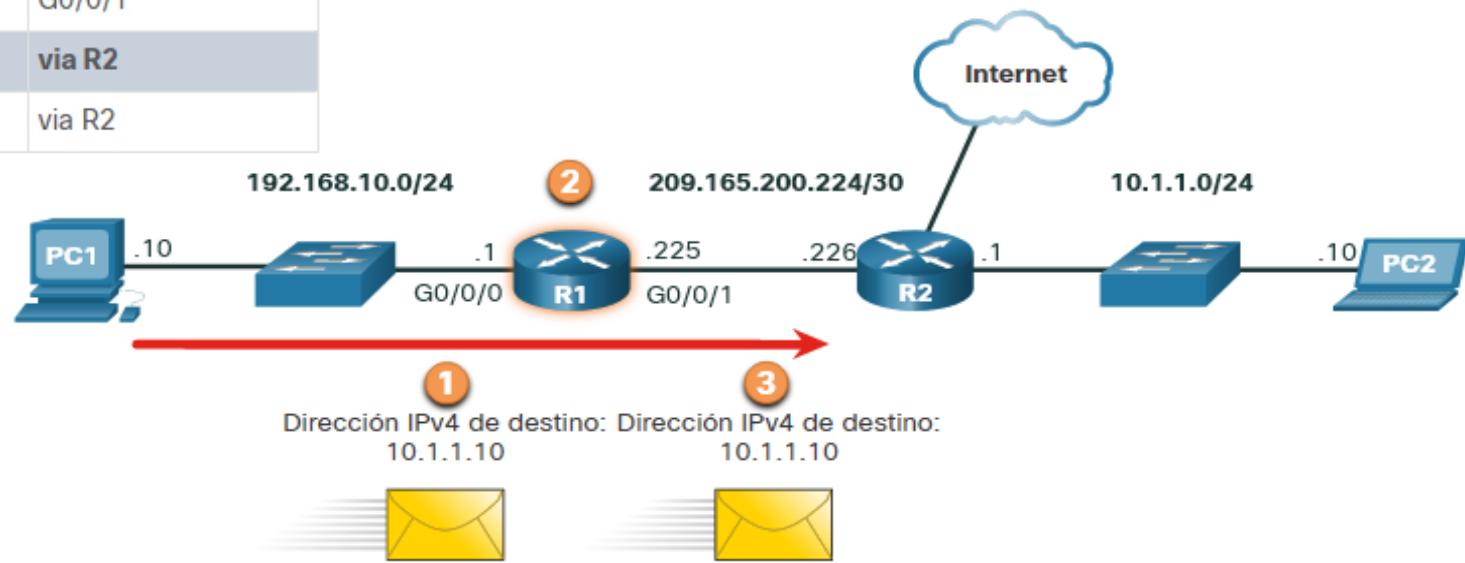
Cuando un host envía un paquete a otro host, consulta su tabla de enrutamiento para determinar dónde enviar el paquete. Si el host de destino está en una red remota, el paquete se reenvía a la puerta de enlace predeterminada, que generalmente es el router local.

El router examina la dirección IP de destino del paquete y busca en su tabla de enrutamiento para determinar dónde reenviar el paquete. La tabla de enrutamiento contiene una lista de todas las direcciones de red conocidas (prefijos) y a dónde reenviar el paquete. Estas entradas se conocen como entradas de ruta o rutas. El router reenviará el paquete utilizando la mejor entrada de ruta que coincide (más larga).

Introducción al enrutamiento

R1 Routing Table

Route	Next Hop or Exit Interface
192.168.10.0 /24	G0/0/0
209.165.200.224/30	G0/0/1
10.1.1.0/24	via R2
Default Route 0.0.0.0/0	via R2



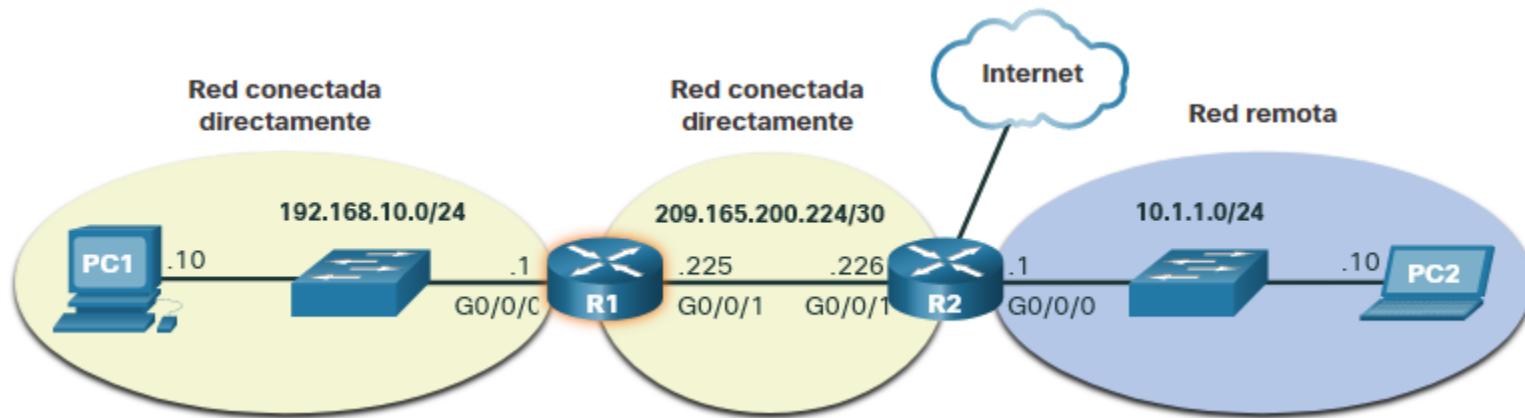
1. El paquete llega a la interfaz Gigabit Ethernet 0/0/0 del router R1. R1 desencapsula el encabezado Ethernet de Capa 2 y el remolque.
2. El router R1 examina la dirección IPv4 de destino del paquete y busca la mejor coincidencia en su tabla de enrutamiento IPv4. La entrada de ruta indica que este paquete se reenviará al router R2.
3. El router R1 encapsula el paquete en un nuevo encabezado Ethernet y remolque, y reenvía el paquete al siguiente router de salto R2.

Introducción al enrutamiento

La tabla de enrutamiento almacena tres tipos de entradas de ruta:

- **Redes conectadas directamente** - estas entradas de ruta de red son interfaces de router activas. Los routers agregan una ruta conectada directamente cuando una interfaz se configura con una dirección IP y se activa. Cada interfaz de router está conectada a un segmento de red diferente. En la figura, serían 192.168.10.0/24 y 209.165.200.224/30.
- **Redes remotas** - estas entradas de ruta de red están conectadas a otros routers. Los routers aprenden acerca de las redes remotas ya sea mediante la configuración explícita de un administrador o mediante el intercambio de información de ruta mediante un protocolo de enrutamiento dinámico. En la figura, la red remota en la tabla de enrutamiento IPv4 R1 sería 10.1.1.0/24.
- **Ruta predeterminada** - al igual que un host, la mayoría de los routers también incluyen una entrada de ruta predeterminada, una puerta de enlace de último recurso. La ruta predeterminada se utiliza cuando no hay una mejor coincidencia (más larga) en la tabla de enrutamiento IP. En la figura, la tabla de enrutamiento IPv4 R1 probablemente incluiría una ruta predeterminada para reenviar todos los paquetes al router R2.

Introducción al enrutamiento



Un router puede descubrir redes remotas de dos maneras:

- **Manualmente** - las redes remotas se ingresan manualmente en la tabla de rutas mediante rutas estáticas.
- **Dinámicamente** - las rutas remotas se aprenden automáticamente mediante un protocolo de enrutamiento dinámico.

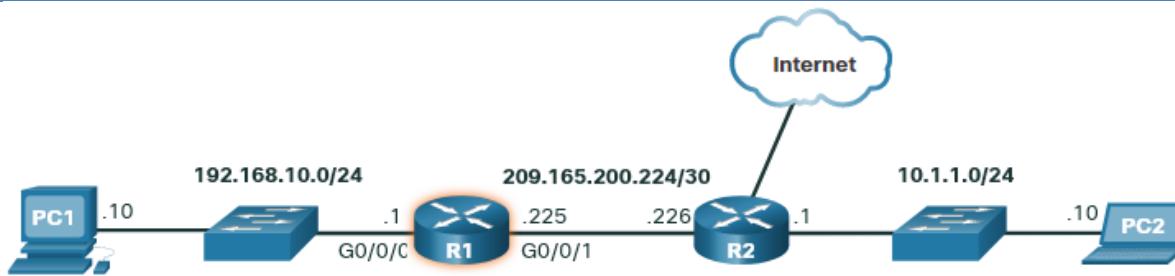
Introducción al enrutamiento

El comando **show ip route** de EXEC mode privilegiado se utiliza para ver la tabla de enrutamiento IPv4 en un router Cisco IOS.

Al principio de cada entrada de tabla de enrutamiento hay un código que se utiliza para identificar el tipo de ruta o cómo se aprendió la ruta. Entre las fuentes de ruta comunes (códigos) se incluyen las siguientes:

- L** - Dirección IP de interfaz local conectada directamente
- C** - Red conectada directamente
- S** - La ruta estática fue configurada manualmente por un admin.
- O** - OSPF
- D** – EIGRP
- R** - RIP

Introducción al enrutamiento



```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S*   0.0.0.0/0 [1/0] via 209.165.200.226, GigabitEthernet0/0/1
      10.0.0.0/24 is subnetted, 1 subnets
O     10.1.1.0 [110/2] via 209.165.200.226, 00:02:45, GigabitEthernet0/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L     192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C     209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L     209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```

Introducción al enrutamiento

Entradas conectadas directamente:

Origen de la ruta	Red de destino	Interfaz de salida
C	172.16.1.0/24 is directly connected, GigabitEthernet0/0	
L	172.16.1.1/32 is directly connected, GigabitEthernet0/0	

Convenciones



- Identifica de qué manera el router detectó la red.



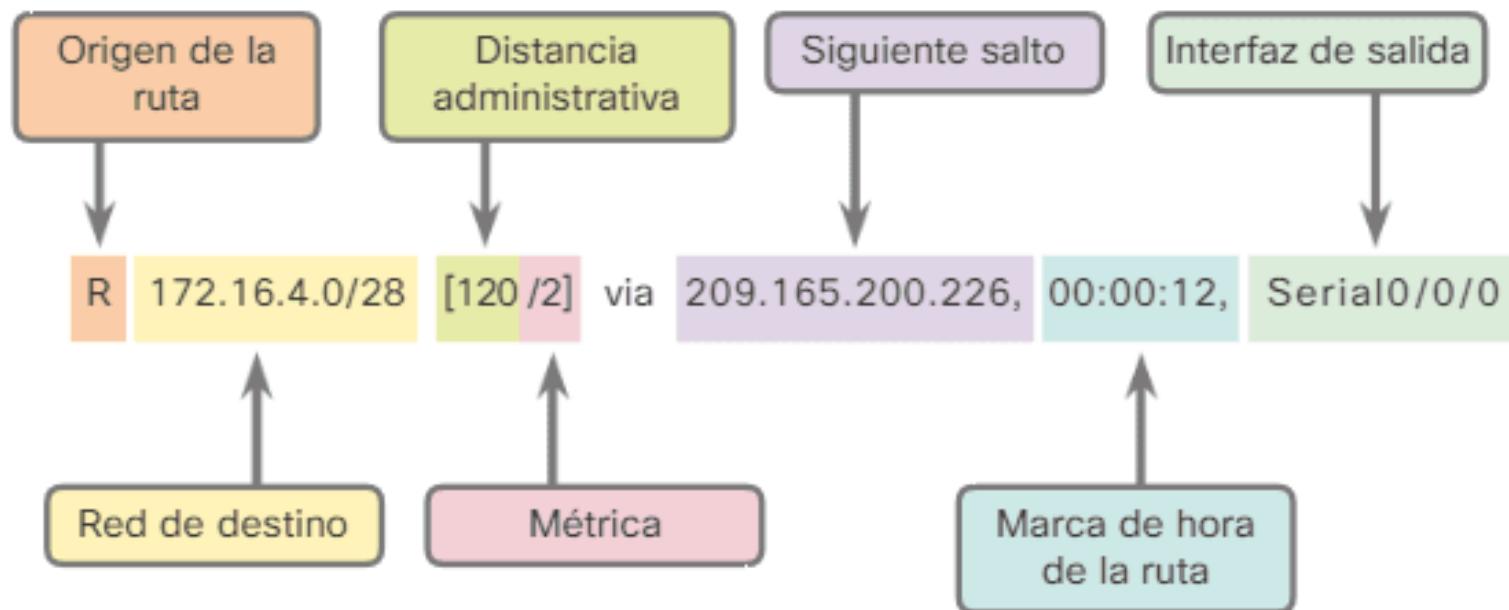
- Identifica la red de destino y cómo está conectada.



Identifica la interfaz en el router conectado a la red de destino.

Introducción al enrutamiento

Entradas de redes remotas:



5 Resolución de dirección

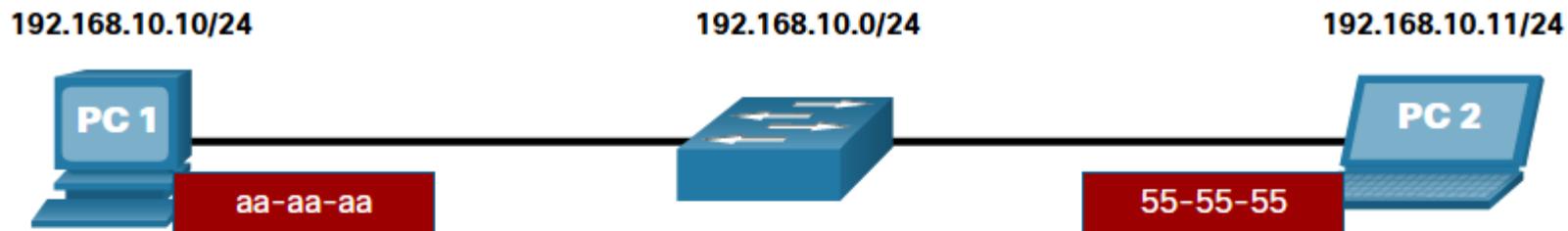
Resolución de dirección

A veces, un host debe enviar un mensaje, pero solo conoce la dirección IP del dispositivo de destino. El host necesita saber la dirección MAC de ese dispositivo, pero ¿cómo se puede descubrir? Ahí es donde la resolución de direcciones se vuelve crítica. Hay dos direcciones primarias asignadas a un dispositivo en una LAN Ethernet:

- **Dirección física (la dirección MAC)** – Se utiliza para comunicaciones NIC a NIC en la misma red Ethernet.
- **Dirección lógica (la dirección IP)** – Se utiliza para enviar el paquete desde el dispositivo de origen al dispositivo de destino. La dirección IP de destino puede estar en la misma red IP que la de origen o en una red remota.

Resolución de dirección

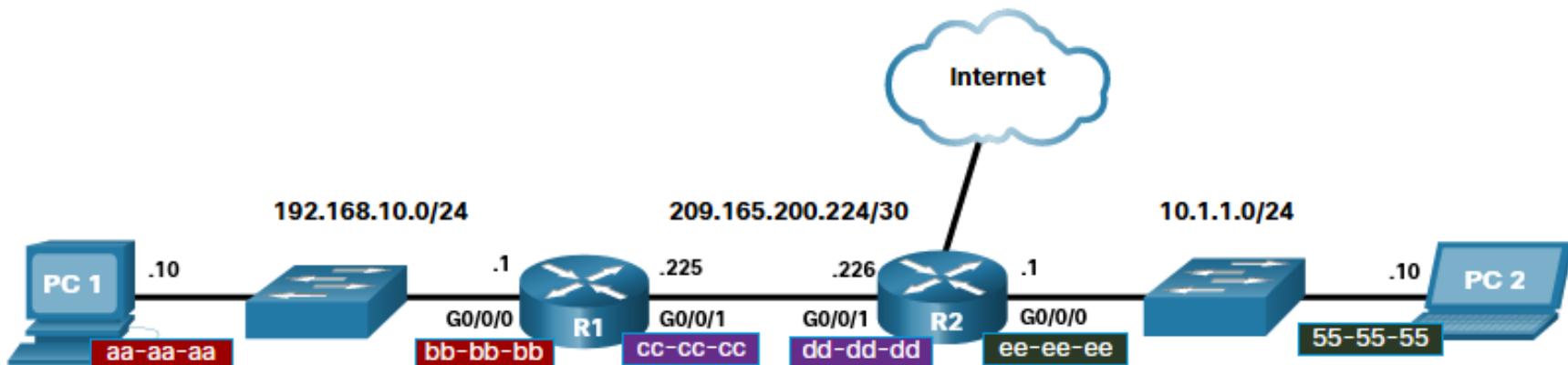
Las direcciones físicas de capa 2 (es decir, las direcciones MAC de Ethernet) se utilizan para entregar la trama de enlace de datos con el paquete IP encapsulado de una NIC a otra NIC que está en la misma red. Si la dirección IP de destino está en la misma red, la dirección MAC de destino es la del dispositivo de destino.



MAC de destino	MAC de origen	IPv4 de origen	IPv4 de destino
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

Resolución de dirección

Cuando la dirección IP de destino (IPv4 o IPv6) está en una red remota, la dirección MAC de destino será la dirección de gateway predeterminada del host (es decir, la interfaz del router).



MAC de destino	MAC de origen	IPv4 de origen	IPv4 de destino
bb-bb-bb	aa-aa-aa	192.168.10.10	10.1.1.10

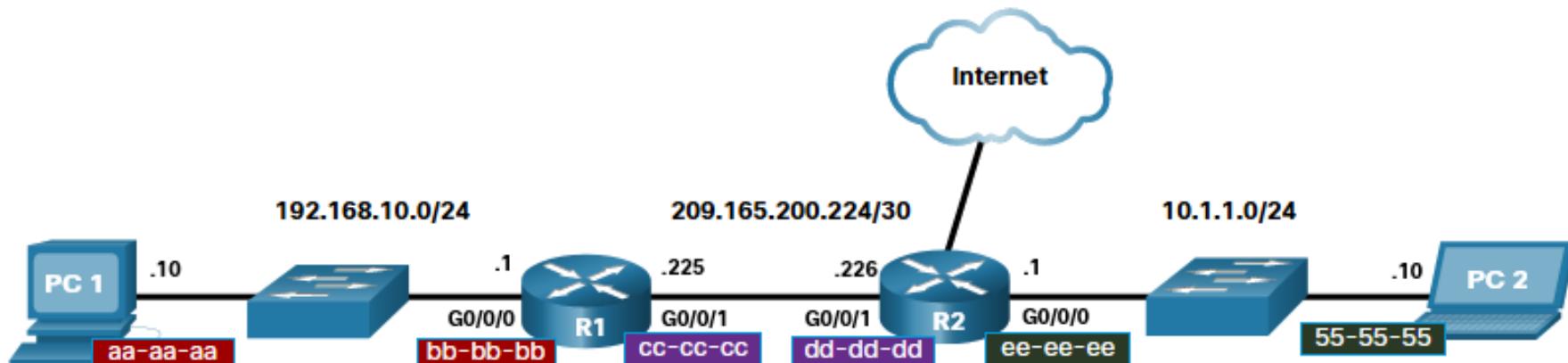
Resolución de dirección

En este ejemplo, PC1 desea enviar un paquete a PC2. PC2 se encuentra en una red remota. Dado que la dirección IPv4 de destino no está en la misma red local que PC1, la dirección MAC de destino es la del gateway predeterminado local en el router.

Los routers examinan la dirección IPv4 de destino para determinar la mejor ruta para reenviar el paquete IPv4. Cuando el router recibe una trama de Ethernet, desencapsula la información de capa 2. Por medio de la dirección IP de destino, determina el dispositivo del siguiente salto y desencapsula el paquete IP en una nueva trama de enlace de datos para la interfaz de salida.

Resolución de dirección

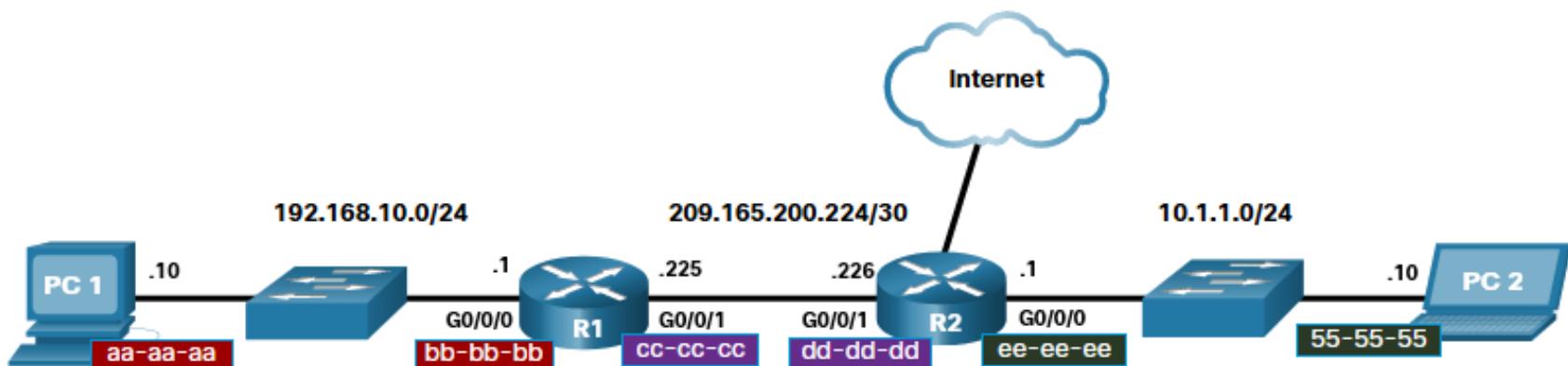
La nueva dirección MAC de destino sería la de la interfaz R2 G0/0/1 y la nueva dirección MAC de origen sería la de la interfaz R1 G0/0/1.



MAC de destino	MAC de origen	IPv4 de origen	IPv4 de destino
dd-dd-dd	cc-cc-cc	192.168.10.10	10.1.1.10

Resolución de dirección

A lo largo de cada enlace de una ruta, un paquete IP se encapsula en una trama. La trama es específica de la tecnología de enlace de datos asociada a ese vínculo, como Ethernet. Si el dispositivo del siguiente salto es el destino final, la dirección MAC de destino será la del NIC de Ethernet del dispositivo.



MAC de destino	MAC de origen	IPv4 de origen	IPv4 de destino
55-55-55	ee-ee-ee	192.168.10.10	10.1.1.10

Resolución de dirección

Cada dispositivo IP de una red Ethernet tiene una dirección MAC Ethernet única. Cuando un dispositivo envía una trama de capa 2 de Ethernet, contiene estas dos direcciones:

- Dirección MAC de destino
- Dirección MAC de origen

Un dispositivo utiliza el Protocolo de resolución de direcciones (ARP) para determinar la dirección MAC de destino de un dispositivo local cuando conoce su dirección IPv4.

ARP proporciona dos funciones básicas:

- Resolución de direcciones IPv4 a direcciones MAC
- Mantener una tabla de asignaciones de direcciones IPv4 a MAC.

ARP Request

Los mensajes de ARP se encapsulan directamente dentro de una trama de Ethernet. No se utiliza un encabezado de IPv4. La solicitud de ARP se encapsula en una trama de Ethernet con la siguiente información de encabezado:

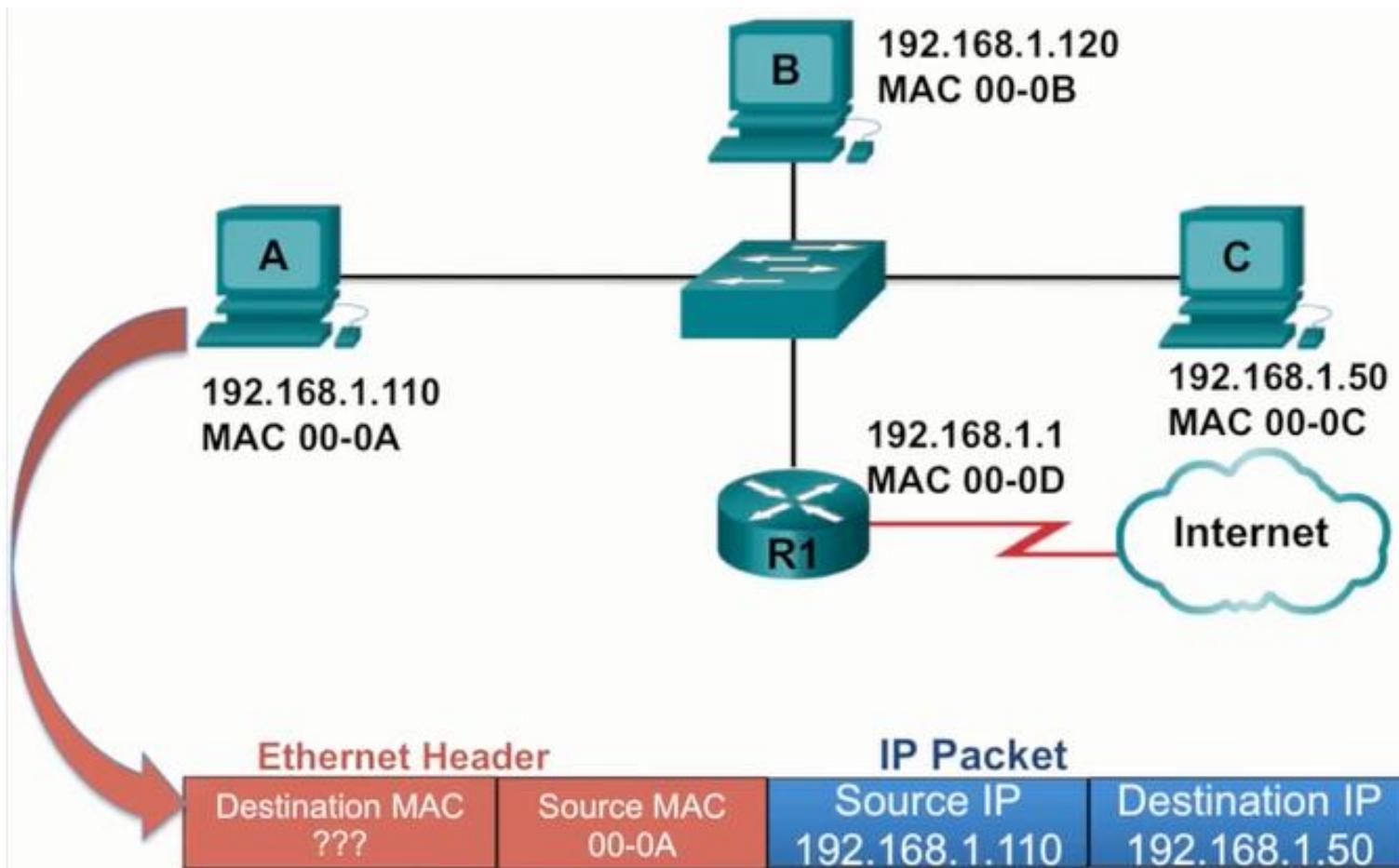
- **Dirección MAC de destino** – esta es una dirección broadcast que requiere que todas las NIC Ethernet de la LAN acepten y procesen la solicitud de ARP.
- **Dirección MAC de origen** – Esta es la dirección MAC del remitente de la solicitud ARP.
- **Tipo** - Los mensajes ARP tienen un campo de tipo de 0x806. Esto informa a la NIC receptora que la porción de datos de la trama se debe enviar al proceso ARP.

ARP Request

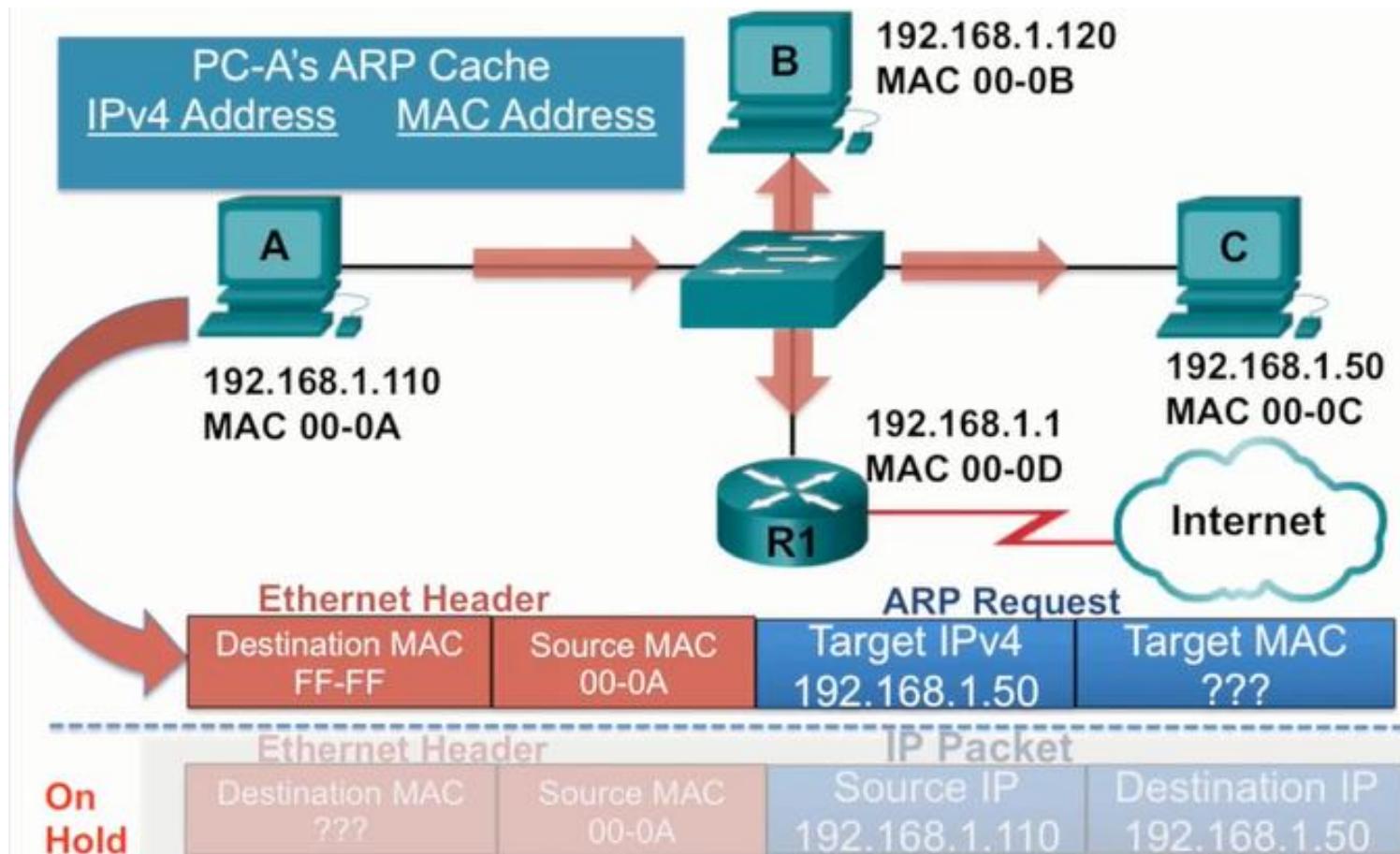
Como las solicitudes de ARP son de broadcast, el switch las envía por todos los puertos, excepto el de recepción. Todas las NIC Ethernet de la LAN procesan transmisiones y deben entregar la solicitud ARP a su sistema operativo para su procesamiento. Cada dispositivo debe procesar la solicitud de ARP para ver si la dirección IPv4 objetivo coincide con la suya. Un router no reenvía broadcasts por otras interfaces.

Solo un dispositivo de la LAN tiene la dirección IPv4 que coincide con la dirección IPv4 objetivo de la solicitud de ARP. Todos los demás dispositivos no envían una respuesta.

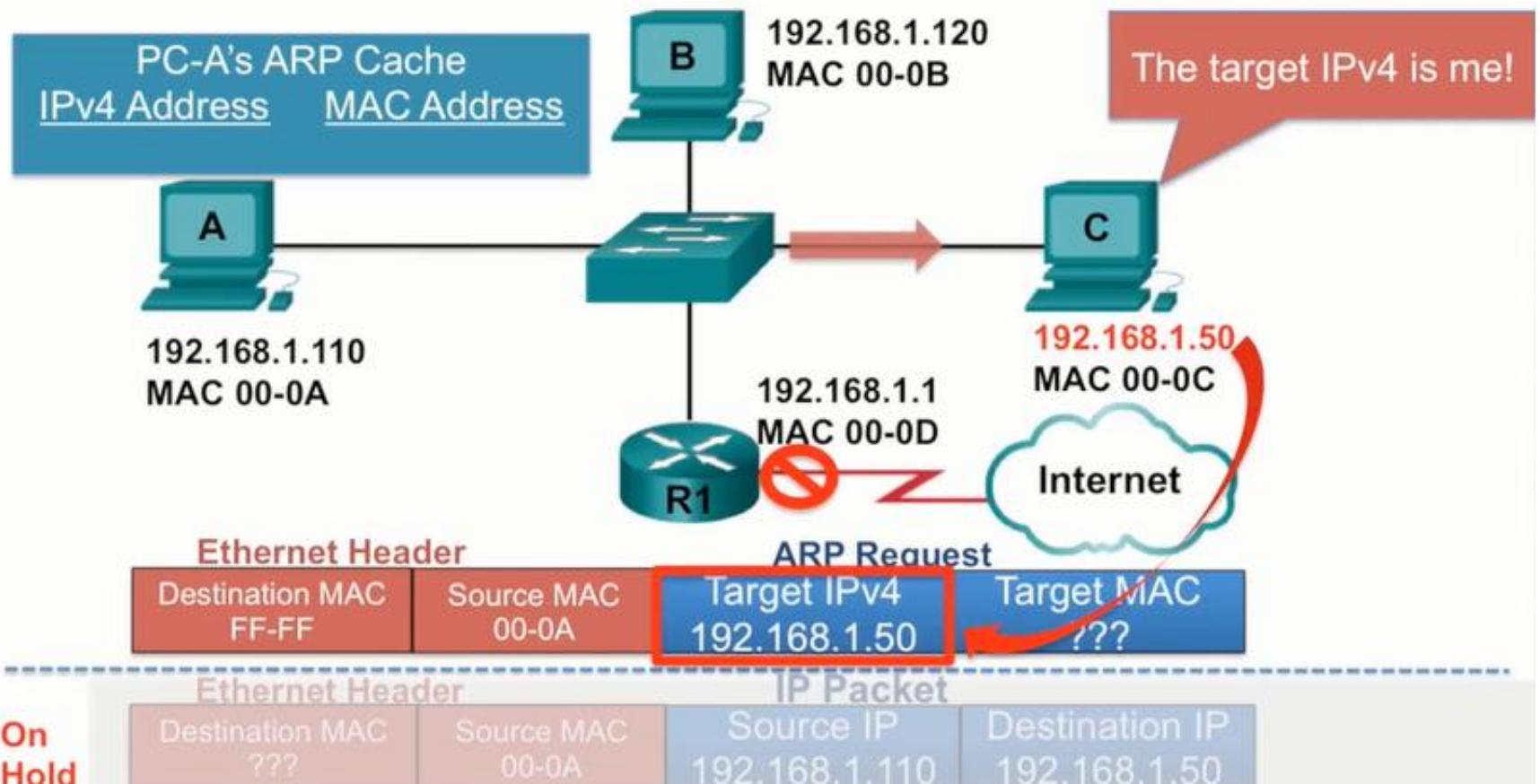
ARP Request



ARP Request



ARP Request



ARP Reply

Solo el dispositivo con la dirección IPv4 de destino asociada con la solicitud ARP responderá con una respuesta ARP. La respuesta de ARP se encapsula en una trama de Ethernet con la siguiente información de encabezado:

Dirección MAC de destino – Es la dirección MAC del remitente de la solicitud de ARP.

Dirección MAC de origen – Esta es la dirección MAC del remitente de la respuesta ARP.

Tipo - Los mensajes ARP tienen un campo de tipo de 0x806. Esto informa a la NIC receptora que la porción de datos de la trama se debe enviar al proceso ARP.

ARP Reply

Solamente el dispositivo que envió inicialmente la solicitud de ARP recibe la respuesta de ARP de unicast. Una vez que recibe la respuesta de ARP, el dispositivo agrega la dirección IPv4 y la dirección MAC correspondiente a su tabla ARP. A partir de ese momento, los paquetes destinados para esa dirección IPv4 se pueden encapsular en las tramas con su dirección MAC correspondiente.

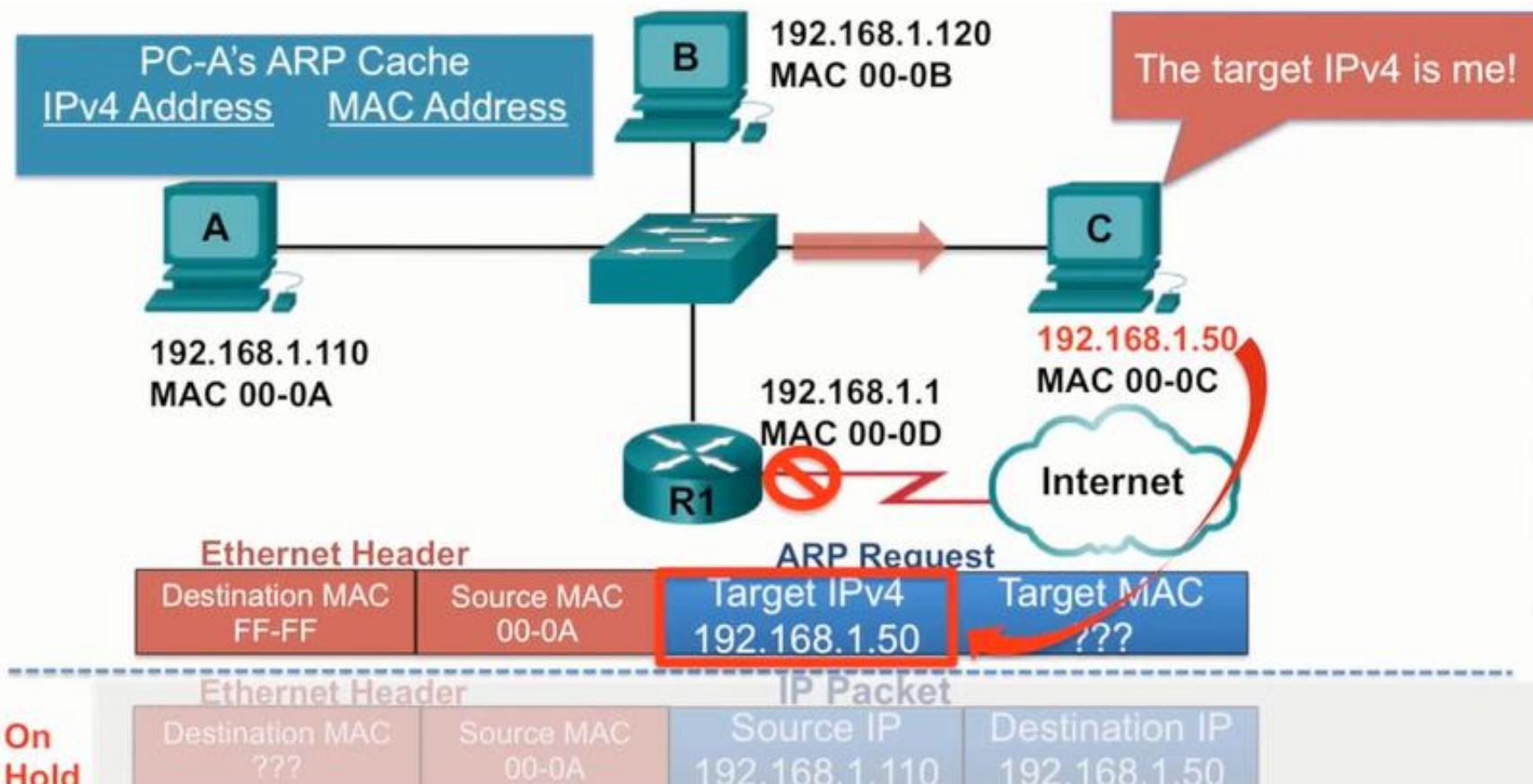
Si ningún dispositivo responde a la solicitud de ARP, el paquete se descarta porque no se puede crear una trama.

Las entradas de la tabla ARP tienen marcas de tiempo. Si un dispositivo no recibe una trama de un dispositivo en particular antes de que caduque la marca de tiempo, la entrada para este dispositivo se elimina de la tabla ARP.

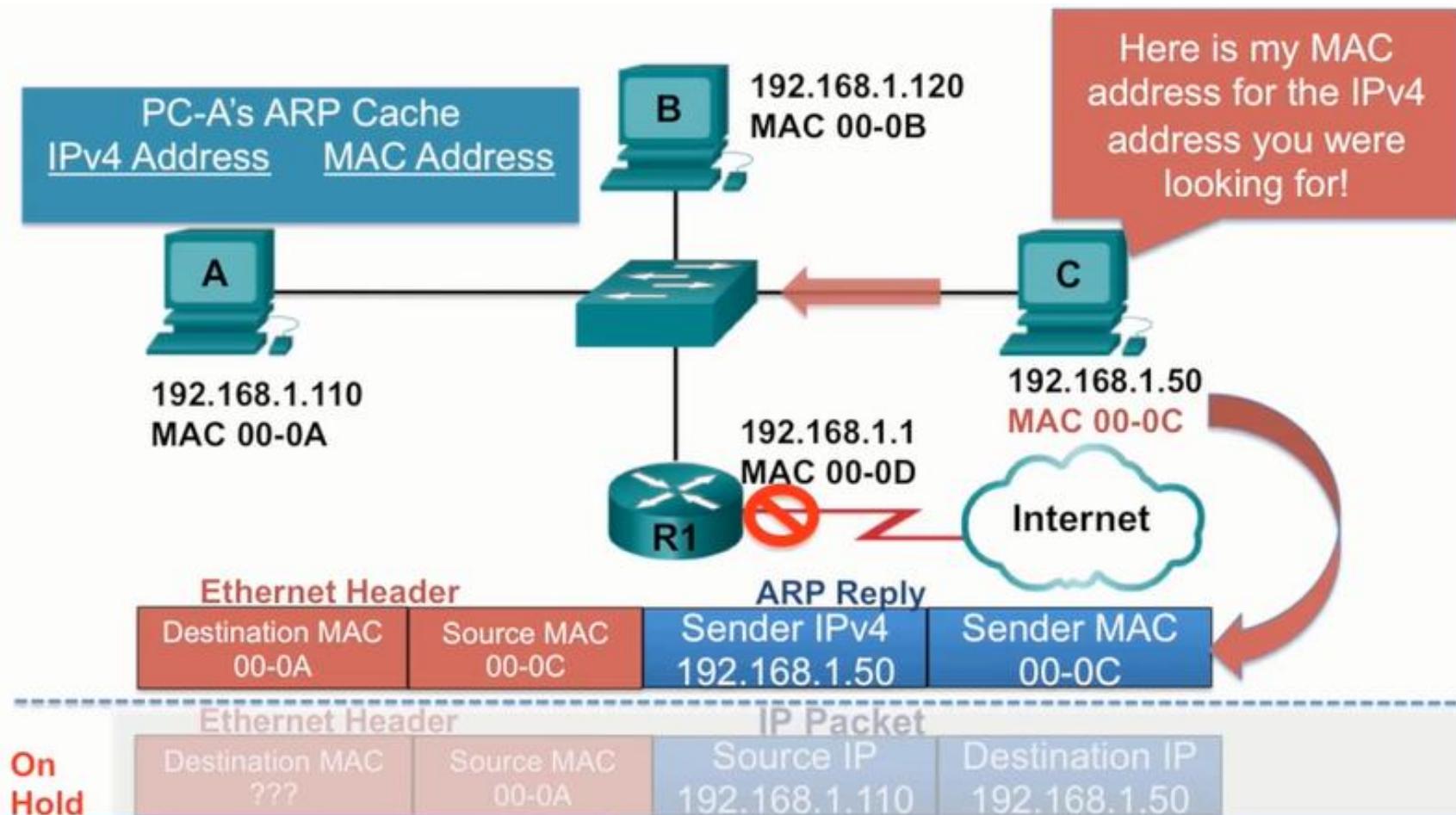
Además, se pueden introducir entradas estáticas de asignaciones en una tabla ARP, pero esto no sucede con frecuencia. Las entradas estáticas de la tabla ARP no caducan con el tiempo y se deben eliminar de forma manual.

ARP Reply

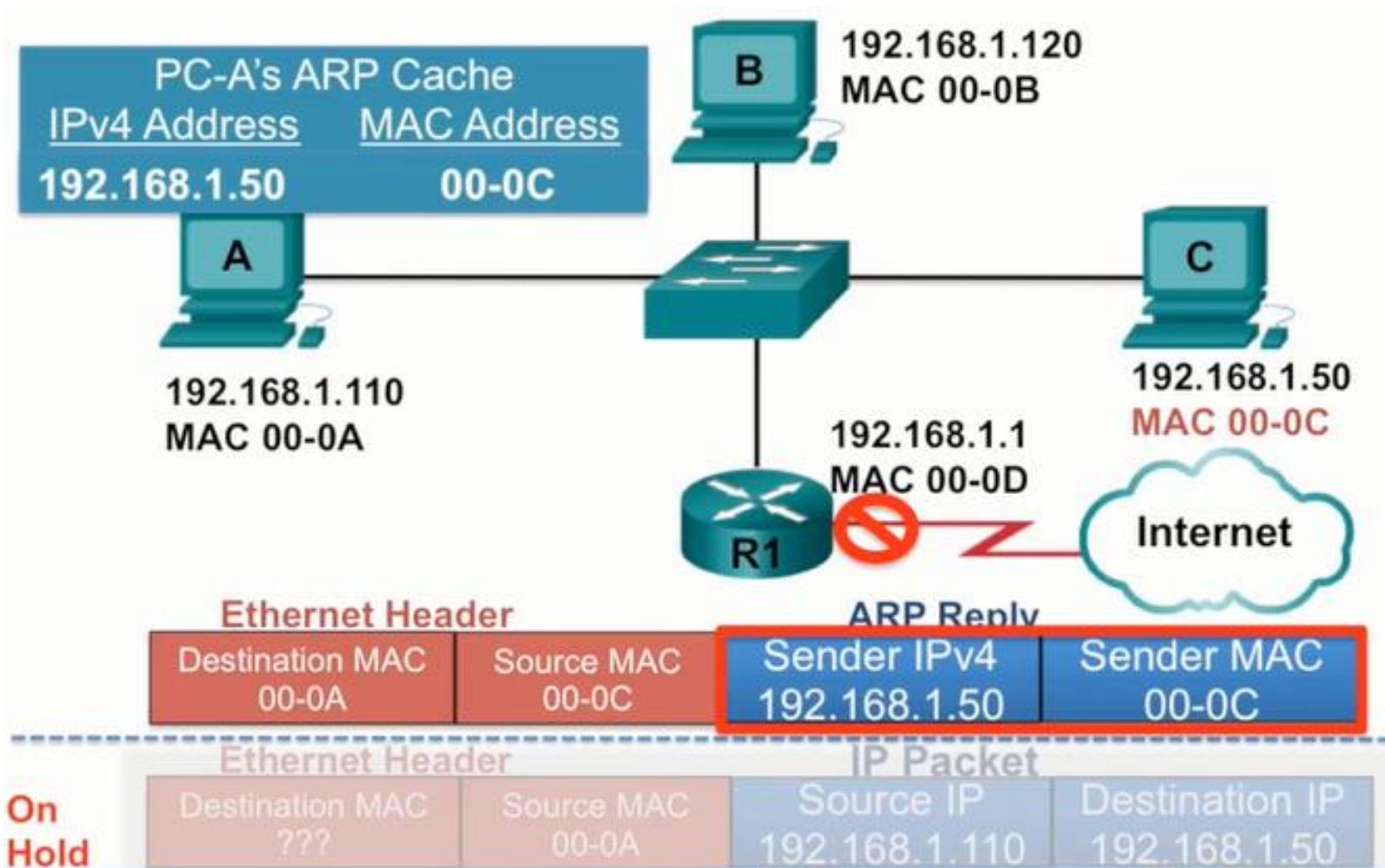
En capítulos anteriores ...



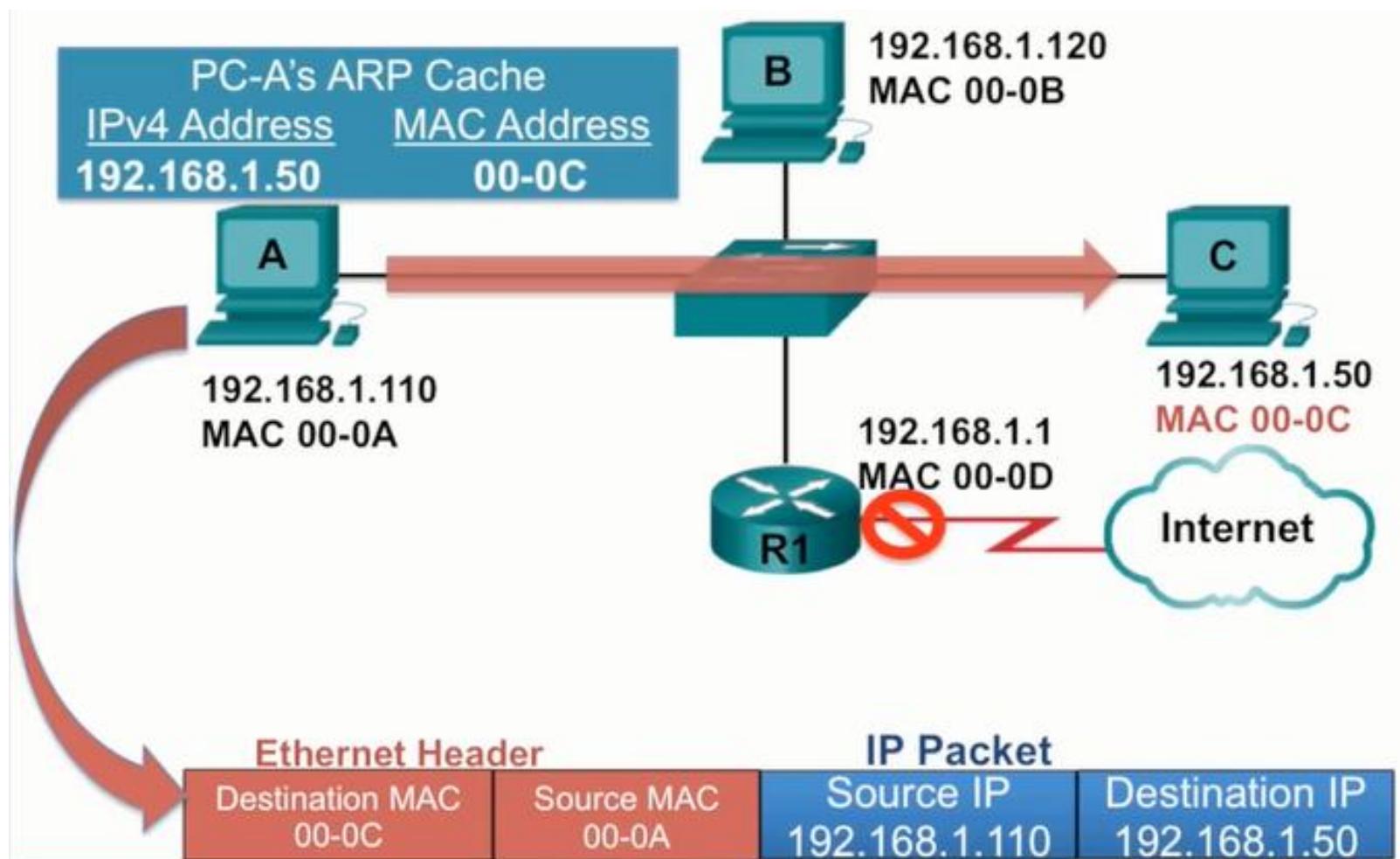
ARP Reply



ARP Reply



ARP Reply



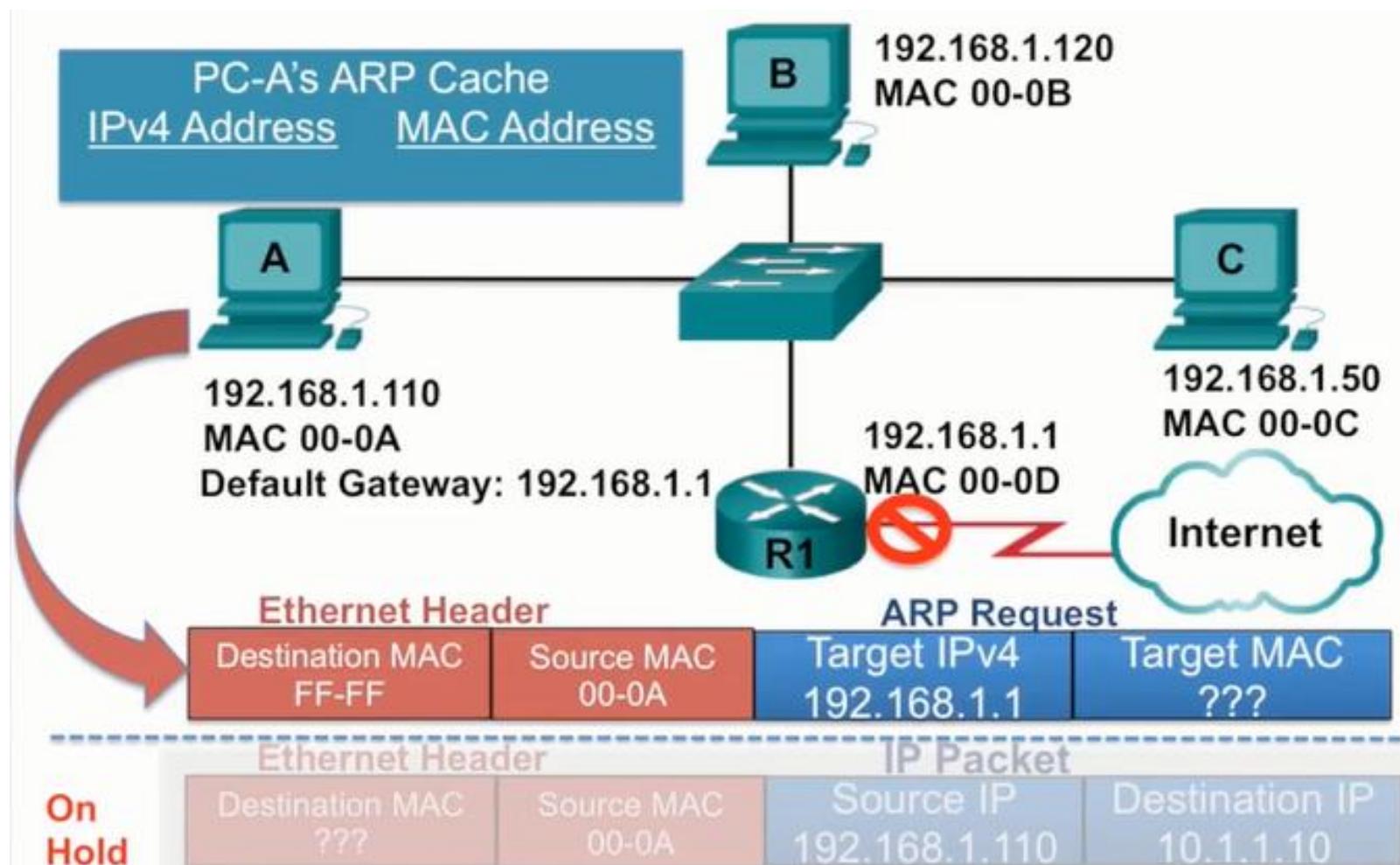
ARP en comunicaciones remotas

Cuando la dirección IPv4 de destino no está en la misma red que la dirección IPv4 de origen, el dispositivo de origen debe enviar la trama al gateway predeterminado. Esta es la interfaz del router local.

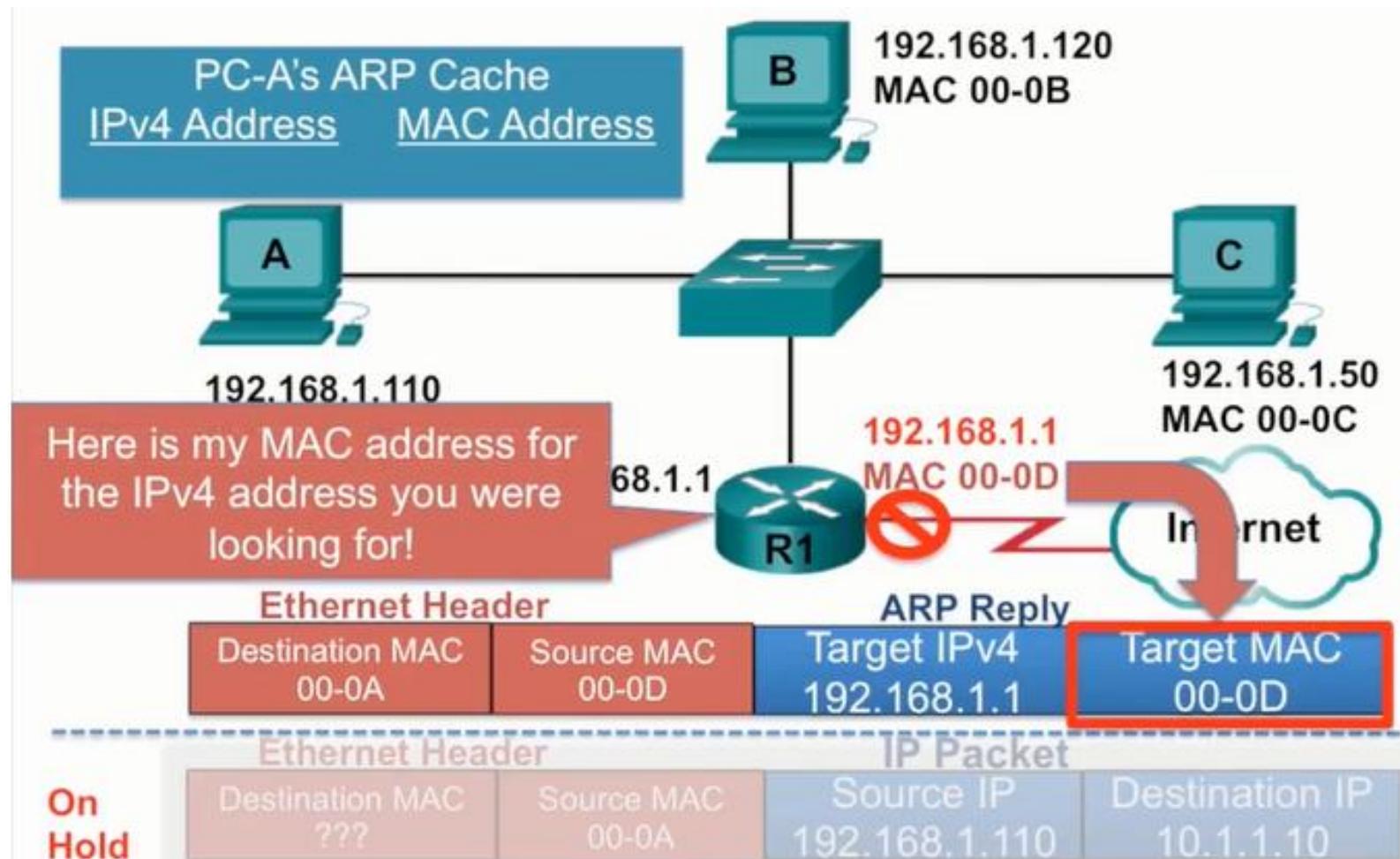
Cuando un dispositivo de origen tiene un paquete con una dirección IPv4 de otra red, lo encapsula en una trama con la dirección MAC de destino del router.

La dirección IPv4 de la dirección del gateway predeterminado se almacena en la configuración IPv4 de los hosts. Cuando un host crea un paquete para un destino, compara la dirección IPv4 de destino con la propia para determinar si ambas están ubicadas en la misma red de capa 3. Si el host de destino no está en la misma red, el origen busca en la tabla ARP una entrada que contenga la dirección IPv4 del gateway predeterminado. Si no existe una entrada, utiliza el proceso ARP para determinar la dirección MAC del gateway predeterminado.

ARP en comunicaciones remotas



ARP en comunicaciones remotas



ARP en comunicaciones remotas

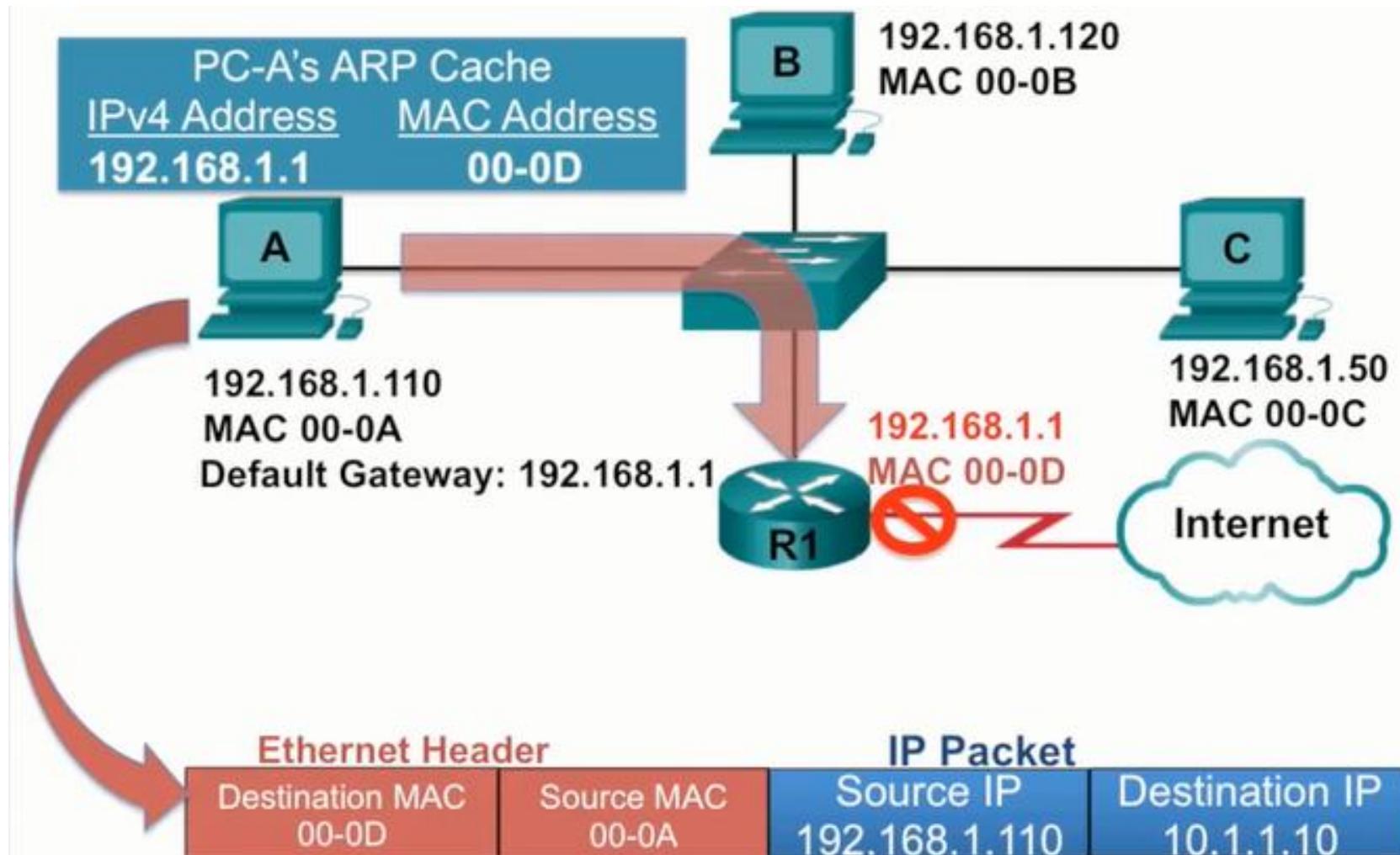


Tabla ARP

Para cada dispositivo, un temporizador de memoria caché ARP elimina las entradas de ARP que no se hayan utilizado durante un período especificado. Los tiempos varían según el sistema operativo del dispositivo. Por ejemplo, los sistemas operativos Windows más recientes almacenan entradas de tabla ARP entre 15 y 45 segundos.

Los comandos también se pueden usar para **eliminar manualmente algunas o todas las entradas de la tabla ARP**.

Después de eliminar una entrada, el proceso de envío de una solicitud de ARP y de recepción de una respuesta de ARP debe ocurrir nuevamente para que se introduzca la asignación en la tabla ARP.

Tabla ARP

En un router Cisco, el **show ip arp** comando se utiliza para mostrar la tabla ARP

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr  Type    Interface
Internet  192.168.10.1      -          a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
Internet  209.165.200.225    -          a0e0.af0d.e141  ARPA   GigabitEthernet0/0/1
Internet  209.165.200.226    1          a03d.6fe1.9d91  ARPA   GigabitEthernet0/0/1
R1#
```

Tabla ARP

En un PC con Windows 10, el **arp -a** comando se usa para mostrar la tabla ARP.

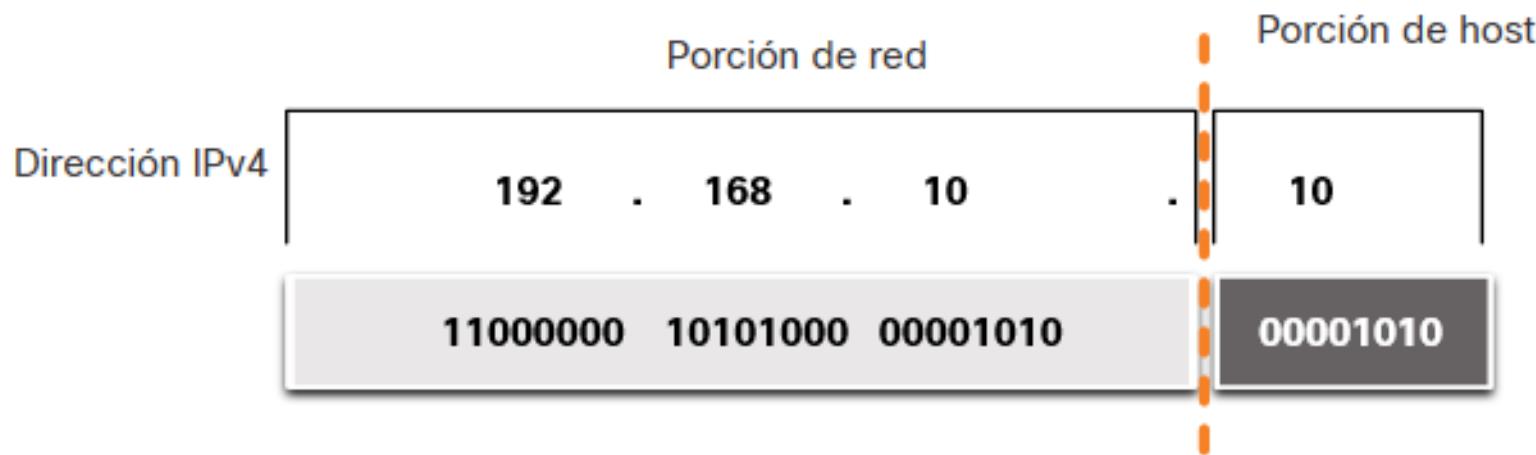
```
C:\Users\PC> arp -a
Interface: 192.168.1.124 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c8-d7-19-cc-a0-86    dynamic
  192.168.1.101         08-3e-0c-f5-f7-77    dynamic
  192.168.1.110         08-3e-0c-f5-f7-56    dynamic
  192.168.1.112         ac-b3-13-4a-bd-d0    dynamic
  192.168.1.117         08-3e-0c-f5-f7-5c    dynamic
  192.168.1.126         24-77-03-45-5d-c4    dynamic
  192.168.1.146         94-57-a5-0c-5b-02    dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff    static
  224.0.0.22            01-00-5e-00-00-16    static
  224.0.0.251           01-00-5e-00-00-fb    static
  239.255.255.250       01-00-5e-7f-ff-fa    static
  255.255.255.255       ff-ff-ff-ff-ff-ff    static
C:\Users\PC>
```

6 Direcciones IPv4

Direcciones IPv4

Una dirección IPv4 es una dirección de 32 bits que se compone de 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.

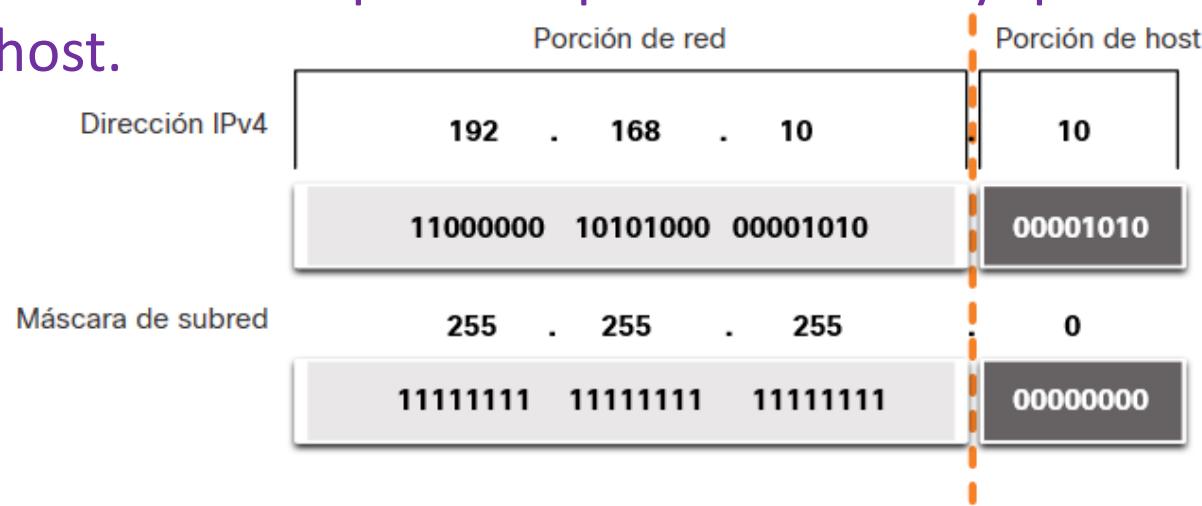


Direcciones IPv4

Asignar una dirección IPv4 a un host requiere lo siguiente:

- **Dirección IPv4** - Esta es la dirección IPv4 única del host.
- **Máscara de subred** - se usa para identificar la parte de red/host de la dirección IPv4.

La **máscara de subred** en realidad no contiene la porción de red o host de una dirección IPv4, solo **le dice a la computadora dónde buscar la parte de la dirección IPv4 que es la porción de red y qué parte es la porción de host.**



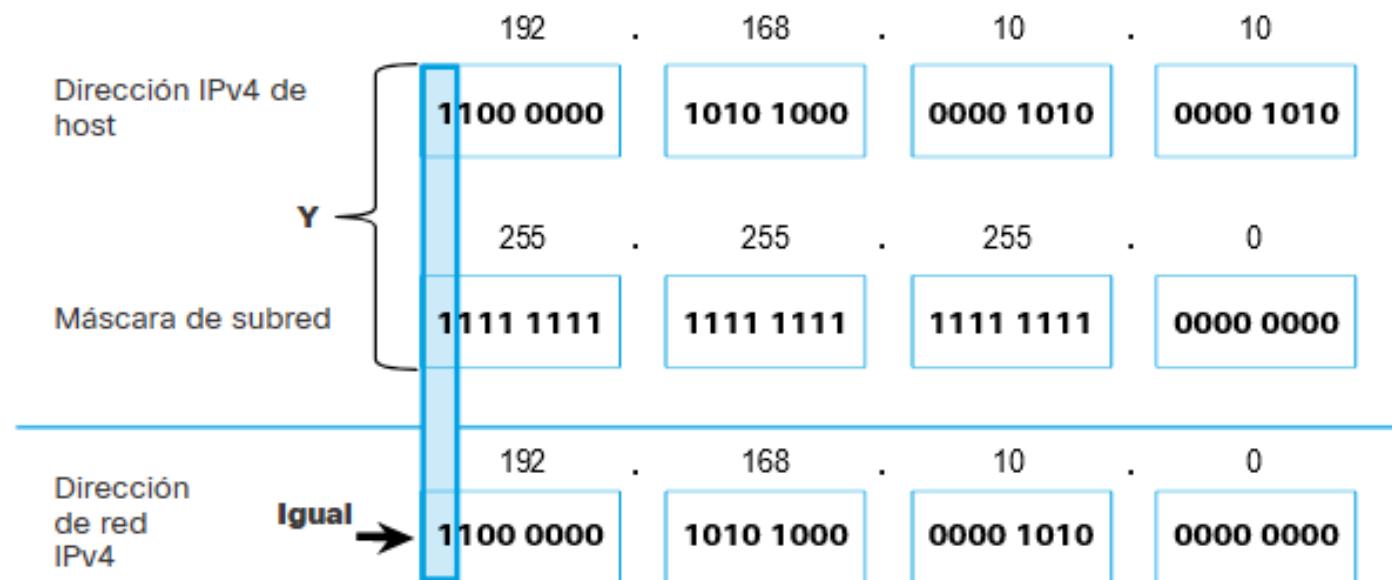
Direcciones IPv4

Longitud de prefijo:

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

Direcciones IPv4

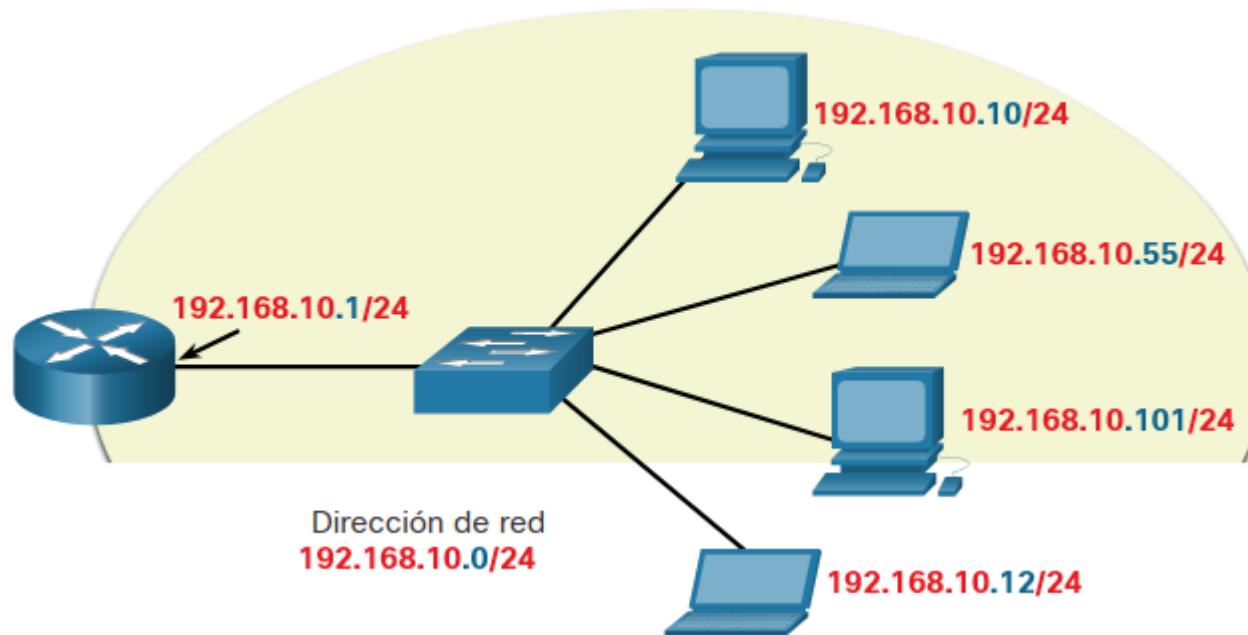
Determinación de la red: proceso ANDing



Direcciones IPv4

Dentro de cada red hay tres tipos de direcciones IP:

- Dirección de red
- Direcciones de host
- Dirección de broadcast



Direcciones IPv4

Dirección de red

Una dirección de red es una dirección que representa una red específica. Un dispositivo pertenece a esta red si cumple tres criterios:

- Tiene la misma máscara de subred que la dirección de red.
- Tiene los mismos bits de red que la dirección de red, como indica la máscara de subred.
- Se encuentra en el mismo dominio de difusión que otros hosts con la misma dirección de red.

Un host determina su dirección de red realizando una operación AND entre su dirección IPv4 y su máscara de subred.

La dirección de red tiene todos los 0 bits en la parte del host, según lo determinado por la máscara de subred. En este ejemplo, la dirección de red es 192.168.10.0/24. NO se puede asignar una dirección de red a un dispositivo.

Direcciones IPv4

	Porción de red			Porción de host	Bits de host
Máscara de subred 255.255.255.0 ó /24	255 11111111	255 11111111	255 11111111	0 00000000	
La <u>dirección de red</u> es 192.168.10.0 ó /24	192 11000000	168 10100000	10 00001010	0 00000000	Todos los 0
Primera dirección 192.168.10.1 ó /24	192 11000000	168 10100000	10 00001010	1 00000001	Todos los 0s y un 1
Última dirección 192.168.10.254 or /24	192 11000000	168 10100000	10 00001010	254 11111110	Todos los 1s y un 0
Dirección de difusión 192.168.10.255 ó /24	192 11000000	168 10100000	10 00001010	255 11111111	Todos los 1s

Direcciones IPv4

Direcciones de host

Las direcciones de host son direcciones que se pueden asignar a un dispositivo.

La parte de host de la dirección son los bits indicados por 0 bits en la máscara de subred. Las direcciones de host pueden tener cualquier combinación de bits en la parte del host excepto los 0 bits (esto sería una dirección de red) o los 1 bits (esto sería una dirección de difusión).

Todos los dispositivos dentro de la misma red deben tener la misma máscara de subred y los mismos bits de red. SOLO los bits del host serán diferentes y deben ser únicos.

Primera dirección de host : este primer host dentro de una red tiene todos los 0 bits con el último bit (más a la derecha) como 1 bit.

Última dirección de host : este último host dentro de una red tiene los 1 bits con el último bit (más a la derecha) como 0 bit.

Cualquier dirección entre 192.168.10.1/24 y 192.168.10.254/24 se puede asignar a un dispositivo de la red.

Direcciones IPv4

	Porción de red			Porción de host	Bits de host
Máscara de subred 255.255.255.0 ó /24	255 11111111	255 11111111	255 11111111	0 00000000	
La <u>dirección de red</u> es 192.168.10.0 ó /24	192 11000000	168 10100000	10 00001010	0 00000000	Todos los 0
Primera dirección 192.168.10.1 ó /24	192 11000000	168 10100000	10 00001010	1 00000001	Todos los 0s y un 1
Última dirección 192.168.10.254 or /24	192 11000000	168 10100000	10 00001010	254 11111110	Todos los 1s y un 0
Dirección de difusión 192.168.10.255 ó /24	192 11000000	168 10100000	10 00001010	255 11111111	Todos los 1s

Direcciones IPv4

Dirección de difusión o *broadcast*

Una dirección de difusión es una dirección que se utiliza cuando se requiere llegar a todos los dispositivos de la red IPv4.

La dirección de difusión de red tiene los 1 bits en la parte del host, según lo determinado por la máscara de subred. En este ejemplo, la dirección de red es 192.168.10.255/24.

NO se puede asignar una dirección de difusión a un dispositivo.

Direcciones IPv4

	Porción de red			Porción de host	Bits de host
Máscara de subred 255.255.255.0 ó /24	255 11111111	255 11111111	255 11111111	0 00000000	
La <u>dirección de red</u> es 192.168.10.0 ó /24	192 11000000	168 10100000	10 00001010	0 00000000	Todos los 0
Primera dirección 192.168.10.1 ó /24	192 11000000	168 10100000	10 00001010	1 00000001	Todos los 0s y un 1
Última dirección 192.168.10.254 or /24	192 11000000	168 10100000	10 00001010	254 11111110	Todos los 1s y un 0
Dirección de difusión 192.168.10.255 ó /24	192 11000000	168 10100000	10 00001010	255 11111111	Todos los 1s

Unicast

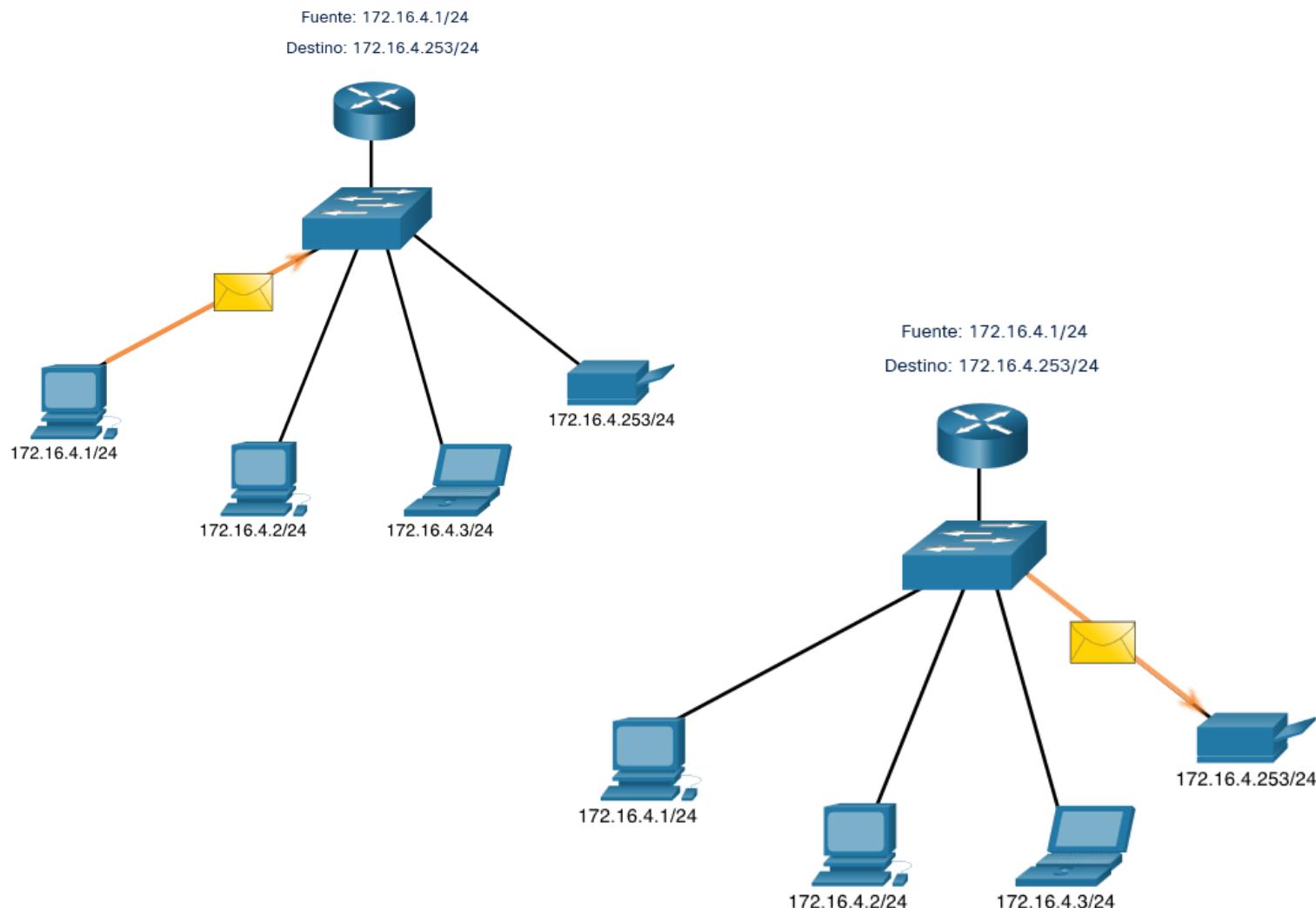
Existen diferentes formas de enviar un paquete desde un dispositivo de origen, y estas diferentes transmisiones afectan a las direcciones IPv4 de destino.

La transmisión unidifusión se refiere a un dispositivo que envía un mensaje a otro dispositivo en comunicaciones uno a uno.

Un paquete de unidifusión tiene una dirección IP de destino que es una dirección de unidifusión que va a un único destinatario.

Una dirección IP de origen sólo puede ser una dirección de unidifusión, ya que el paquete sólo puede originarse de un único origen. Esto es independientemente de si la dirección IP de destino es una unidifusión, difusión o multidifusión.

Unicast



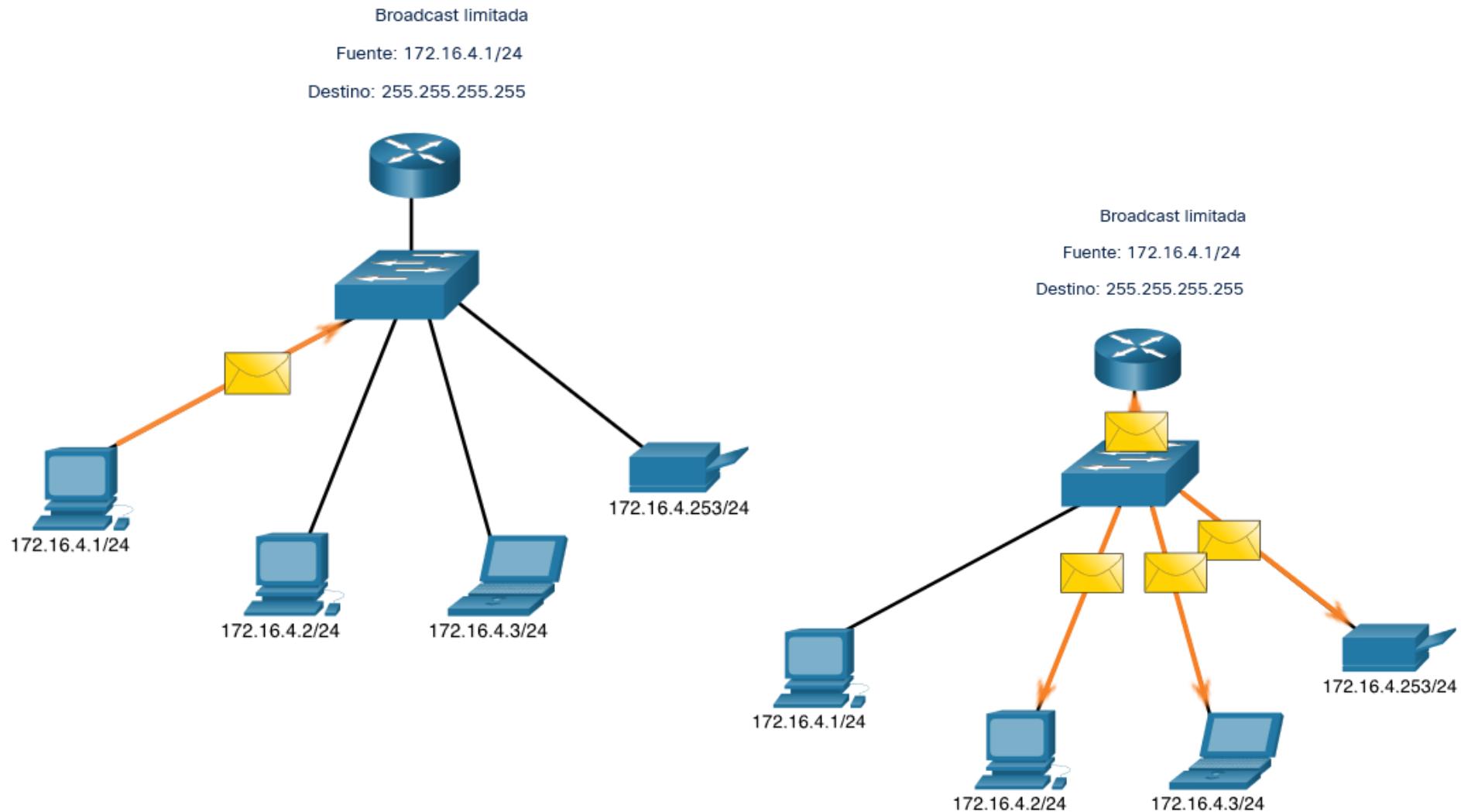
Broadcast

Transmisión de difusión o *broadcast* hace referencia a un dispositivo que envía un mensaje a todos los dispositivos de una red en comunicaciones unipersonales.

Los paquetes de difusión tienen una dirección IPv4 de destino que contiene solo números uno (1) en la porción de host.

Todos los dispositivos del mismo dominio deben procesar un paquete de difusión. Un dominio de difusión identifica todos los hosts del mismo segmento de red. Un *broadcast* 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.

Broadcast



Broadcast

Los paquetes de difusión usan recursos en la red y hacen que cada host receptor en la red procese el paquete. Por lo tanto, **se debe limitar el tráfico de difusión para que no afecte negativamente el rendimiento de la red o de los dispositivos.** Debido a que los routers separan los dominios de difusión, la subdivisión de redes puede mejorar el rendimiento de la red al eliminar el exceso de tráfico de difusión.

Difusiones dirigidas por IP

Además de la dirección de difusión 255.255.255.255, hay una dirección IPv4 de difusión para cada red, llamada difusión dirigida. Esta dirección utiliza la dirección más alta de la red, que es la dirección donde todos los bits de host son 1s. Por ejemplo, la dirección de difusión dirigida para 192.168.1.0/24 es 192.168.1.255. Esta dirección permite la comunicación con todos los hosts de esa red. Para enviar datos a todos los hosts de una red, un host puede enviar un solo paquete dirigido a la dirección de difusión de la red.

Multidifusión

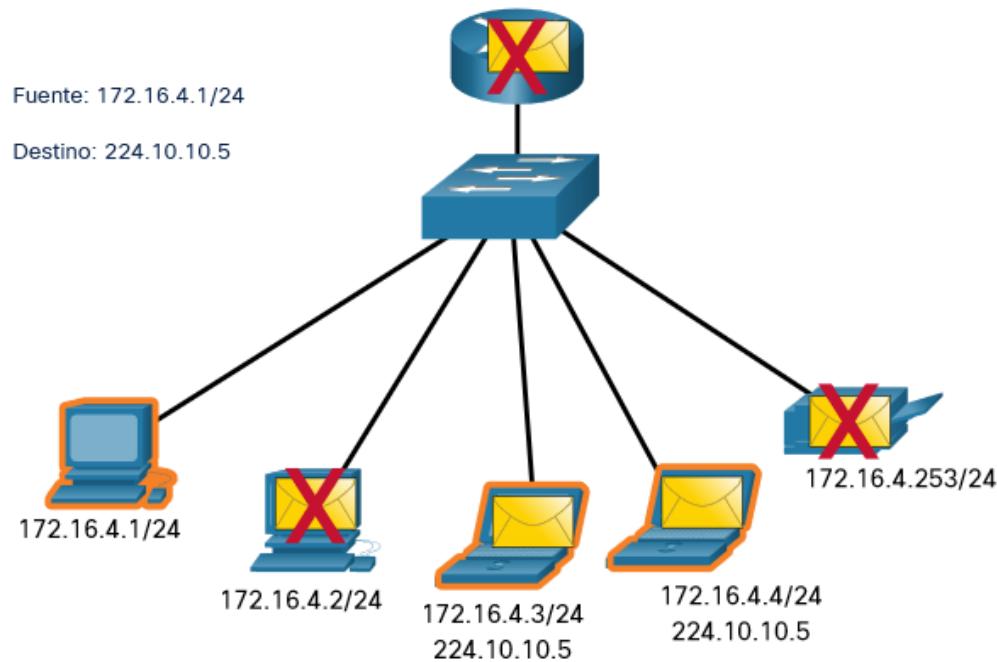
La transmisión de multidifusión reduce el tráfico al permitir que un host envíe un único paquete a un grupo seleccionado de hosts que estén suscritos a un grupo de multidifusión.

Un paquete de multidifusión es un paquete con una dirección IP de destino que es una dirección de multidifusión. IPv4 reservó las direcciones de 224.0.0.0 a 239.255.255.255 como rango de multidifusión.

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

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.



Tipos de direcciones IPv4

Algunas direcciones IPv4 no se pueden usar para salir a Internet, y otras se asignan específicamente para enrutar a Internet.

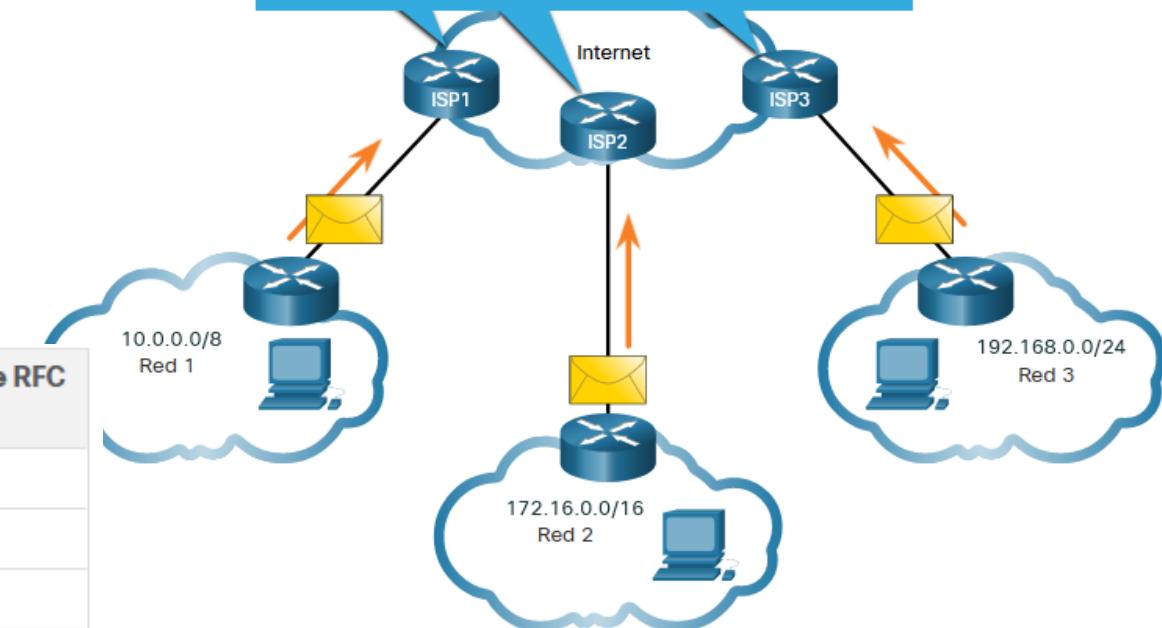
Algunos se utilizan para verificar una conexión y otros se autoasignan.

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

Tipos de direcciones IPv4

La mayoría de las redes internas, desde grandes empresas hasta redes domésticas, utilizan direcciones IPv4 privadas para dirigirse a todos los dispositivos internos (intranet), incluidos los hosts y routers. Sin embargo, **las direcciones privadas no son enruteables globalmente.**

Este paquete tiene una dirección IPv4 de origen que es una dirección privada. Lo traduciré a una dirección IPv4 pública usando NAT



Dirección de red y prefijo	Rango de direcciones privadas de RFC 1918
10.0.0.0/8	10.0.0.0 a 10.255.255.255
172.16.0.0/12	172.16.0.0 a 172.31.255.255
192.168.0.0/16	192.168.0.0 a 192.168.255.255

Tipos de direcciones IPv4

Direcciones de Loopback

Direcciones de Loopback (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. Por ejemplo, se puede usar en un host para probar si la configuración TCP/IP funciona.

Direcciones link-local

Direcciones link-local o direcciones IP privadas automáticas (APIPA) 169.254.0.0/16 o 169.254.0.1 a 169.254.255.254 Los utiliza un cliente DHCP de Windows para autoconfigurarse en caso de que no haya servidores DHCP disponibles.

7 Subnetting

Segmentar la red

En el diseño de una red se debe tener especial cuidado con los llamados Dominios de Colisión y Dominio de difusión (Broadcast)

Dominio de colisión: Grupo de dispositivos conectados al mismo medio físico, de tal manera que si dos dispositivos acceden al medio al mismo tiempo, el resultado será una colisión entre las dos señales. Como resultado de estas colisiones se produce un consumo inadecuado de recursos y de ancho de banda. Cuanto menor sea la cantidad de dispositivos afectados a un dominio de colisión mejor desempeño de la red.

Segmentar la red

Dominio de difusión. Grupo de dispositivos de la red que envían y reciben mensajes de difusión entre ellos. Una cantidad inapropiada de estos mensajes de difusión (broadcast) provocara un bajo rendimiento en la red, una cantidad exagerada (tormenta de broadcast) dará como resultado el mal funcionamiento de la red hasta tal punto de poder dejarla completamente congestionada.

Segmentar la red

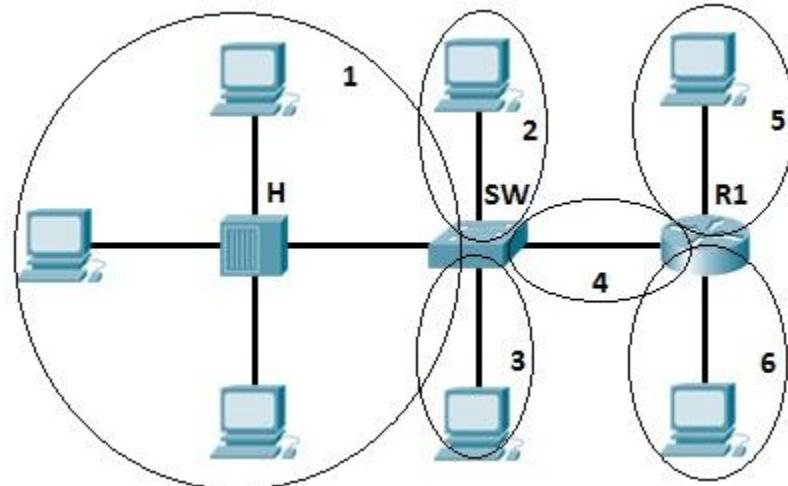
Los **hubs** o concentradores tienen un único dominio de colisión, eso quiere decir que si dos equipos provocan una colisión en un segmento asociado a un puerto del hubs, todos los demás dispositivos aun estando en diferentes puertos se verán afectados. De igual manera se verían afectados si una estación envía un **Broadcast**, debido a que un hub también tiene un solo dominio de difusión.

Los **switches** propagan las difusiones por todas las interfaces, salvo por aquella en la cual se recibieron.

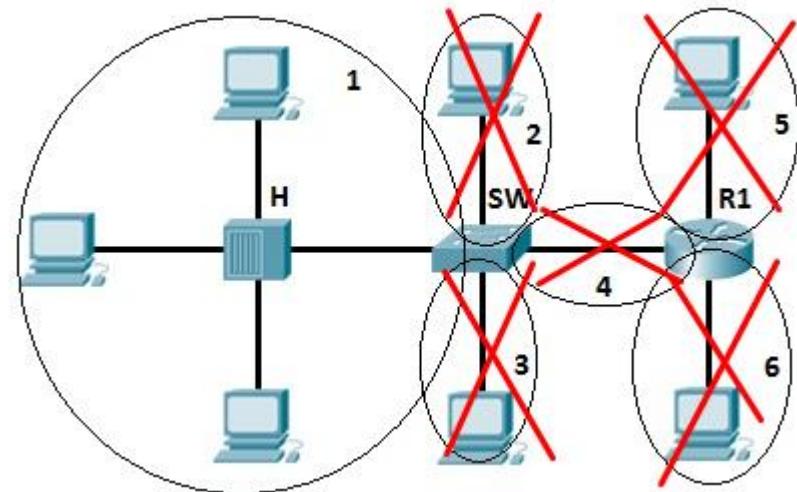
Los **routers** no propagan difusiones. Cuando un router recibe una difusión, no la reenvía por otras interfaces.

Segmentar la red

Dominio colisión si SW y R1 operan half duplex:

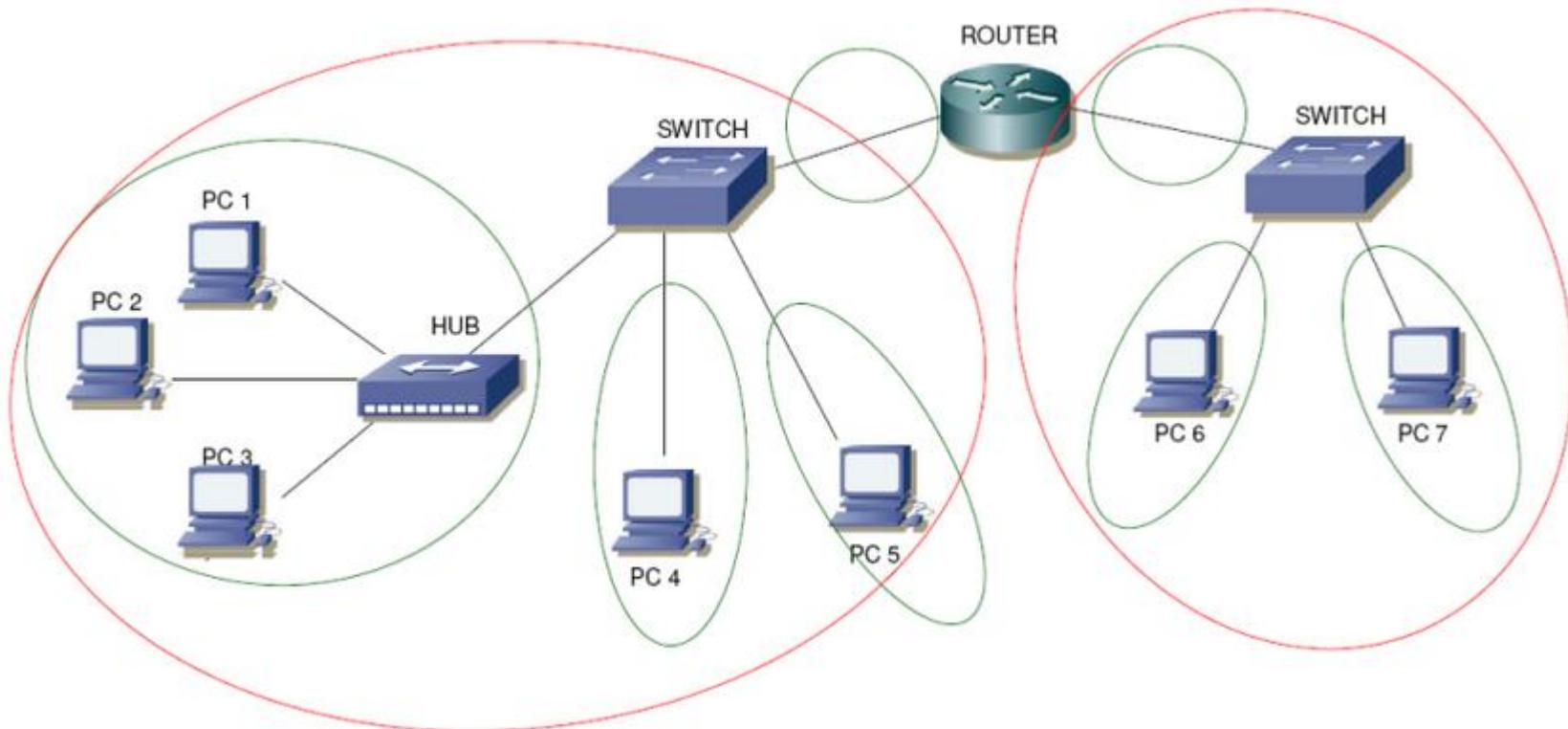


Si el enlace es full-duplex no hay colisión



Segmentar la red

Dominios de **colisión** y **difusión**



Segmentar la red

Un dominio de difusión grande es una red que conecta muchos hosts. Un problema con un dominio de difusión grande es que estos hosts **pueden generar difusiones excesivas y afectar la red de manera negativa.**

Esto da como resultado operaciones de red lentas debido a la cantidad significativa de tráfico que puede causar, y operaciones de dispositivo lentas porque un dispositivo debe aceptar y procesar cada paquete de difusión.

Segmentar la red

La solución es reducir el tamaño de la red para crear dominios de difusión más pequeños mediante un proceso que se denomina división en subredes. Estos espacios de red más pequeños se denominan subredes.

La división en subredes disminuye el tráfico de red general y mejora su rendimiento. A su vez, le permite a un administrador implementar políticas de seguridad, por ejemplo, qué subredes están habilitadas para comunicarse entre sí y cuáles no lo están. Otra razón es que reduce el número de dispositivos afectados por el tráfico de difusión anormal debido a configuraciones incorrectas, problemas de hardware o software o intenciones malintencionadas.

División de subredes de una red IPv4

Las subredes IPv4 se crean utilizando uno o más de los bits de host como bits de red. Esto se realiza por medio de la ampliación de la máscara de subred para que tome prestados algunos de los bits de la porción de host de la dirección a fin de crear bits de red adicionales.

Cuantos más bits de host se tomen prestados, mayor será la cantidad de subredes que puedan definirse. Cuantos más bits se prestan para aumentar el número de subredes reduce el número de hosts por subred.

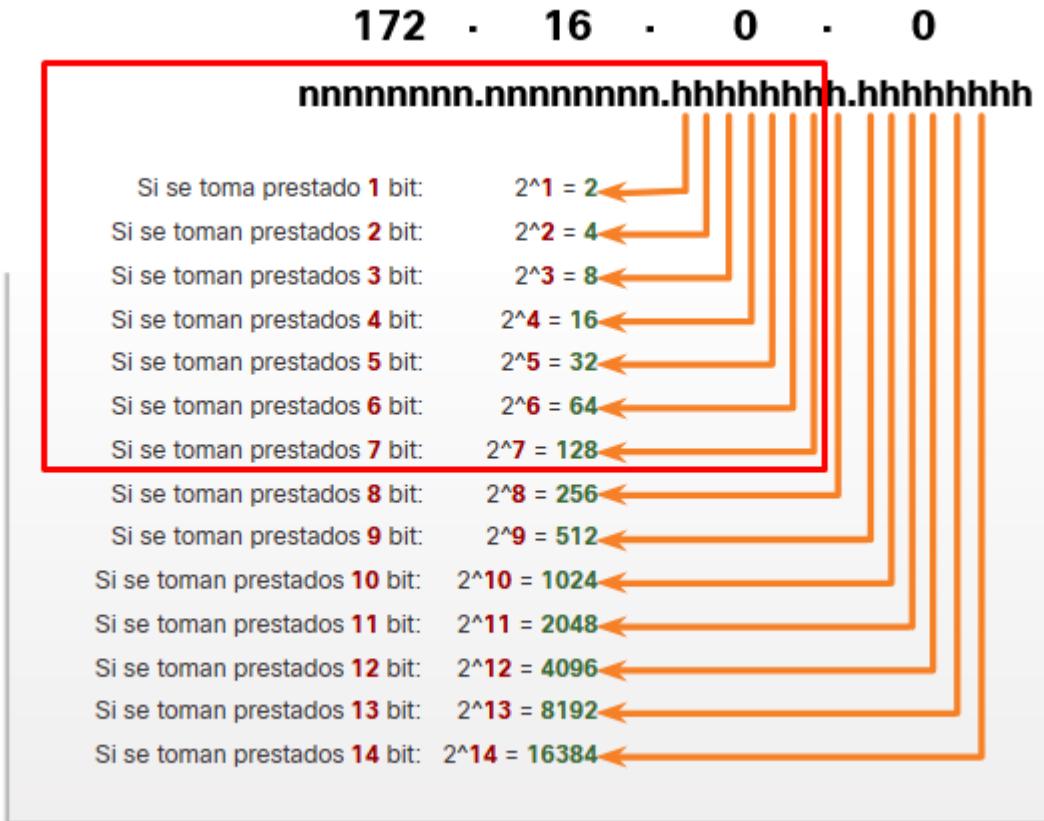
División de subredes de una red IPv4

Subnetting de una red /24

Longitud de prefijo	Máscara de subred	Máscara de subred en binario (n = network, h = host)	# de subredes	# de hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhh 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnnh 11111111.11111111.11111111.11111100	64	2

División de subredes de una red IPv4

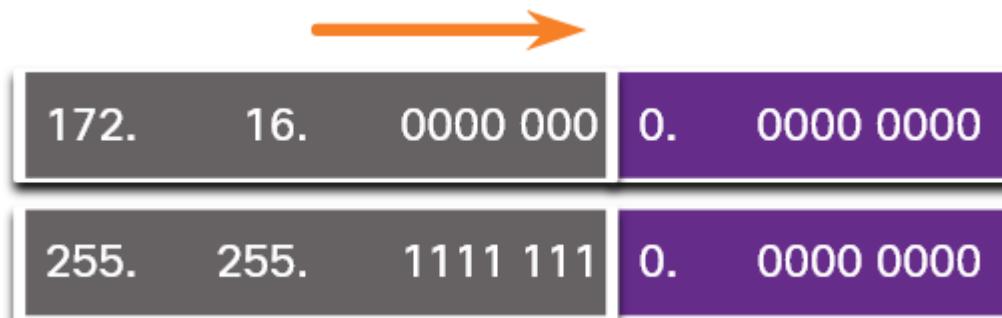
Crear 100 subredes en 172.16.0.0/16



División de subredes de una red IPv4

La máscara de subred se extiende 7 bits en el tercer octeto:

172.16.0.0/23

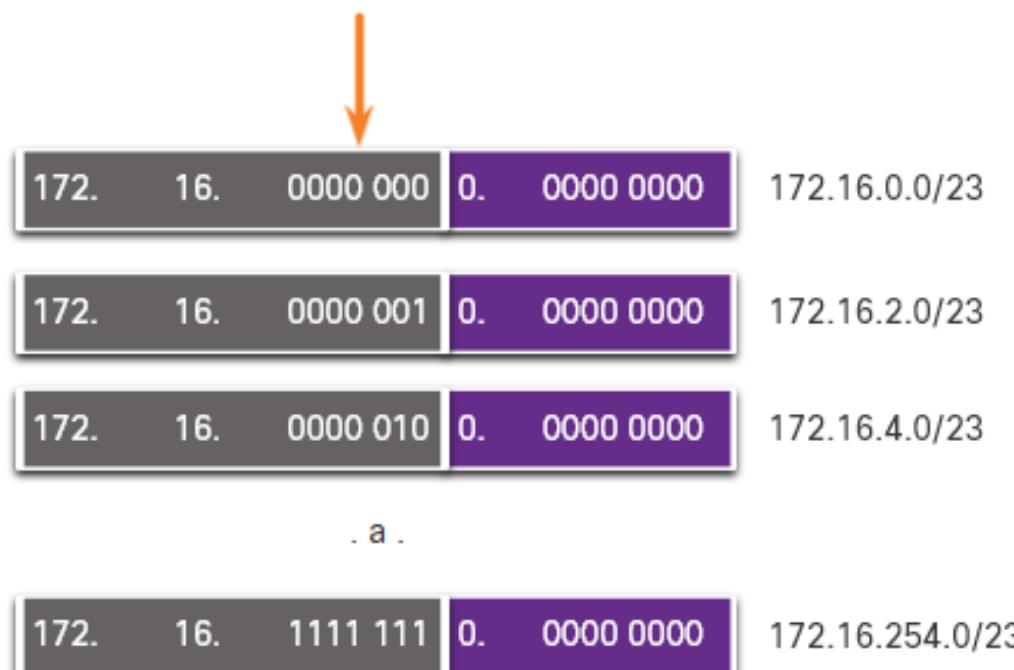


División de subredes de una red IPv4

Las subredes de 172.16.0.0/23:



Si se toman prestados 7 bits, se crean 128 subredes.



División de subredes de una red IPv4

Intervalo de direcciones para la subred 172.16.0.0/23:

Dirección de red

172.	16.	00 00 00 0	0.	0000 0000	= 172.16.0.0/23
------	-----	------------	----	-----------	-----------------

Primera dirección de host

172.	16.	00 00 00 0	0.	0000 0001	= 172.16.0.1/23
------	-----	------------	----	-----------	-----------------

Última dirección de host

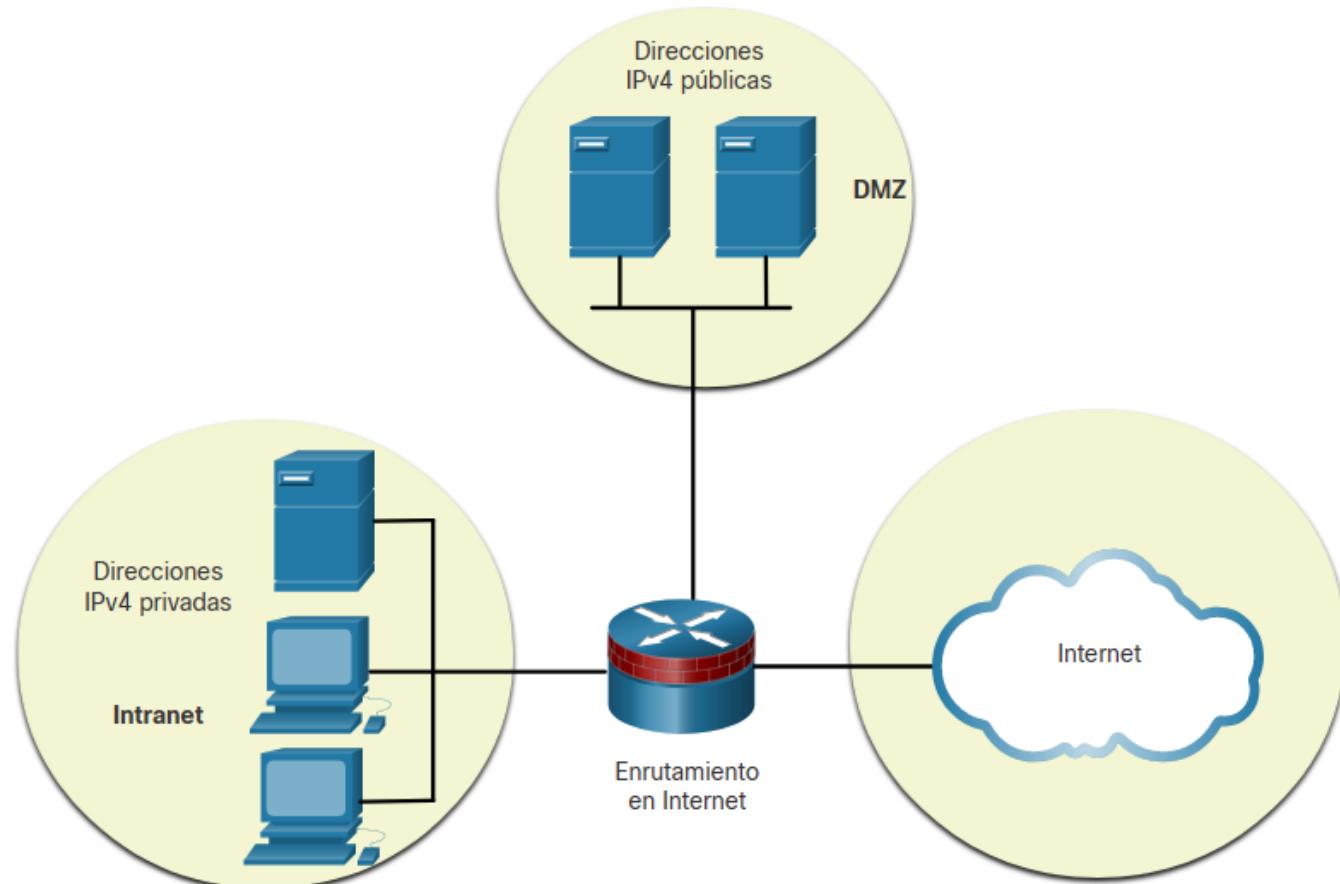
172.	16.	00 00 00 0	1.	1111 1110	= 172.16.1.254/23
------	-----	------------	----	-----------	-------------------

Dirección de difusión

172.	16.	00 00 00 0	1.	1111 1111	= 172.16.1.255/23
------	-----	------------	----	-----------	-------------------

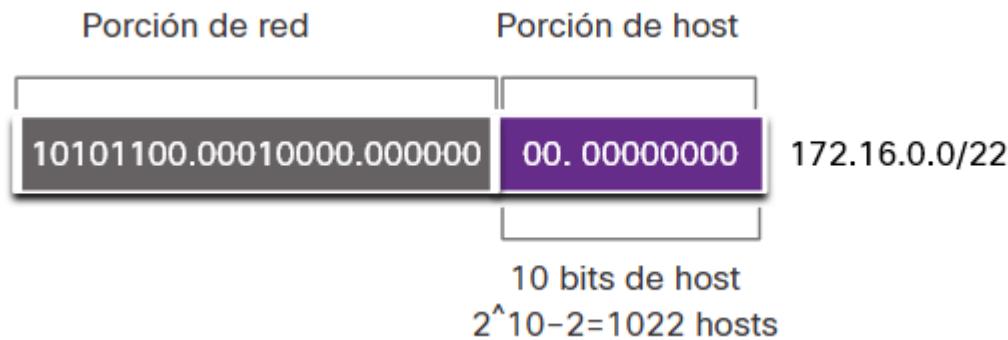
División de subredes de una red IPv4

Problemas de eficiencia con subnetting con direcciones públicas en DMZ -> **Direcciones host = $2^n - 2$**



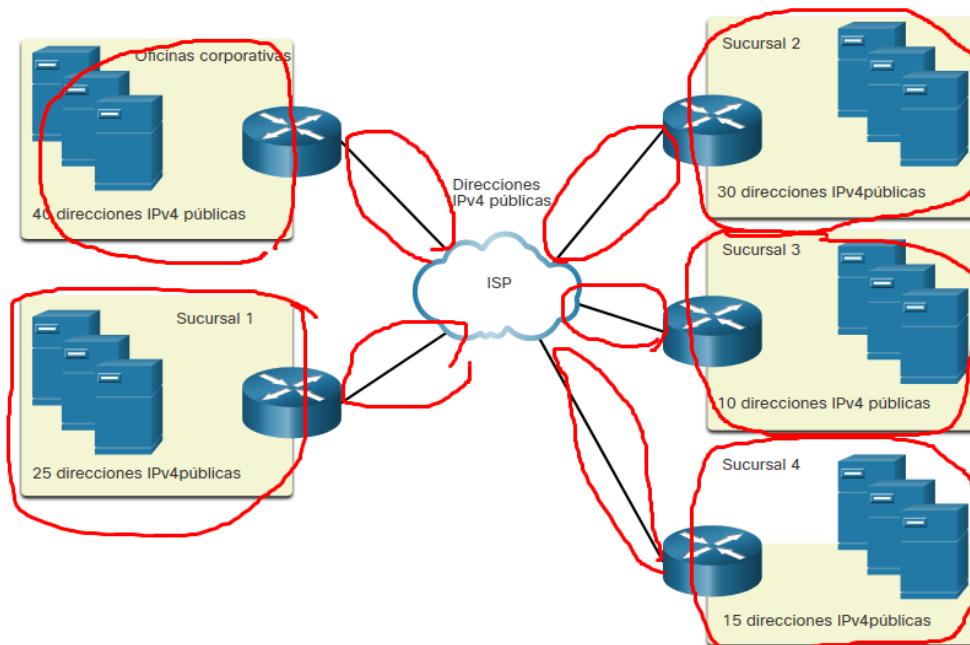
División de subredes de una red IPv4

Ejemplo: Suponer red “pública” 172.16.0.0/22



División de subredes de una red IPv4

La dirección de red 172.16.0.0/22 tiene 10 bits de host, como se muestra en la figura. Debido a que la subred más grande requiere 40 hosts, se debe tomar prestado un mínimo de 6 bits de host para proporcionar el direccionamiento de los 40 hosts. Esto se determina utilizando esta fórmula: $2^6 - 2 = 62$ hosts.



División de subredes de una red IPv4

Esquema de subredes

	Porción de red	Porción de host		Decimal punteada
	10101100.00010000.000000	00.00	000000	172.16.0.0/22
0	10101100.00010000.000000	00.00	000000	172.16.0.0/26
1	10101100.00010000.000000	00.01	000000	172.16.0.64/26
2	10101100.00010000.000000	00.10	000000	172.16.0.128/26
3	10101100.00010000.000000	00.11	000000	172.16.0.192/26
4	10101100.00010000.000000	01.00	000000	172.16.1.0/26
5	10101100.00010000.000000	01.01	000000	172.16.1.64/26
6	10101100.00010000.000000	01.10	000000	172.16.1.128/26

Las redes 7 a 13 no se muestran.

14	10101100.00010000.000000	11.10	000000	172.16.3.128/26
15	10101100.00010000.000000	11.11	000000	172.16.3.192/26

Se toman prestados 4 bits de la porción de host para crear subredes.

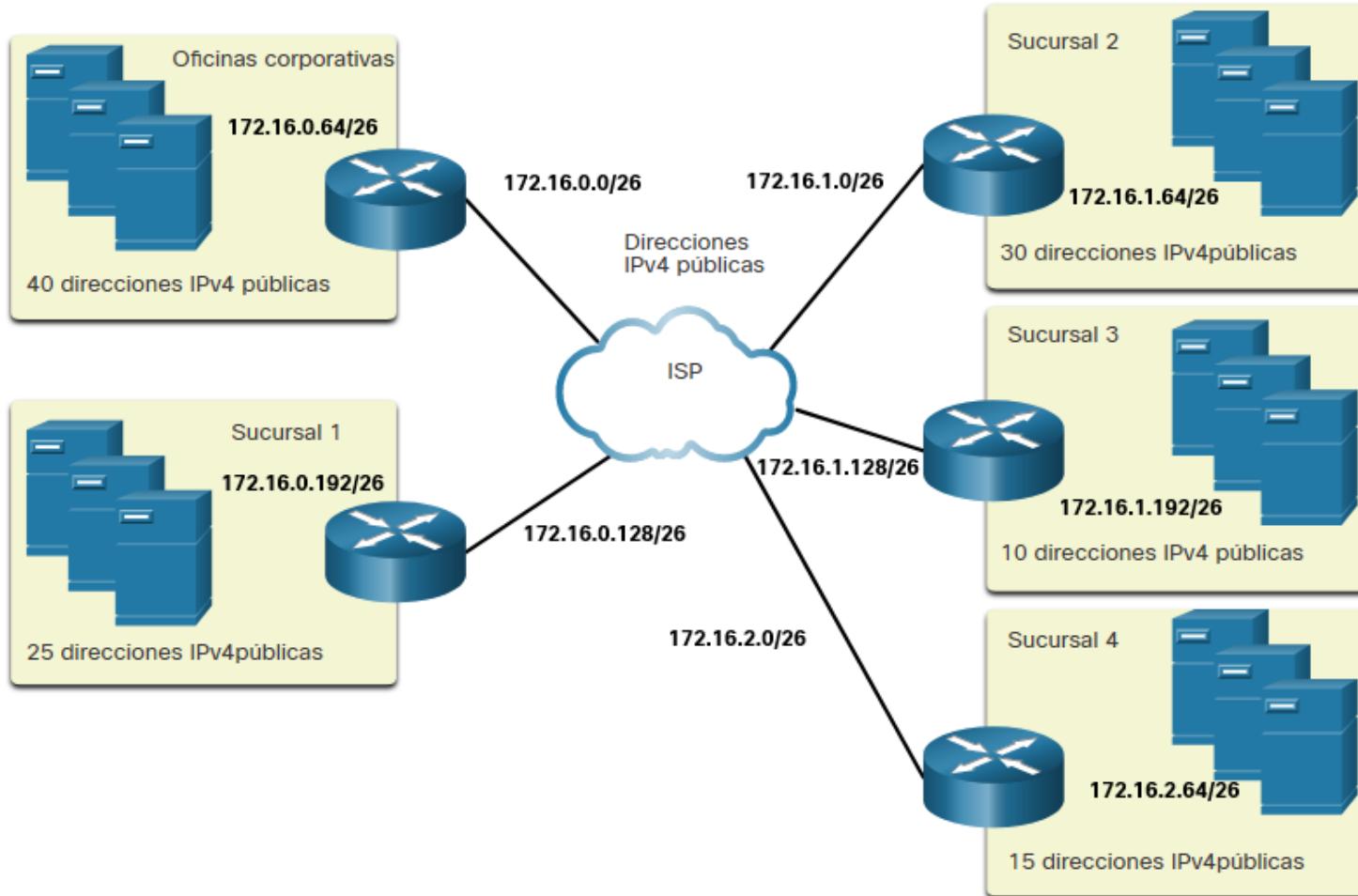
División de subredes de una red IPv4

La fórmula para determinar subredes da un resultado de 16 subredes: $2^4 = 16$. Debido a que la interconexión de redes de ejemplo requiere 10 subredes, esto cumplirá con el requisito y permitirá un crecimiento adicional.

Por lo tanto, los primeros 4 bits de host se pueden usar para asignar subredes. Esto significa que se prestarán dos bits del 3er octeto y dos bits del 4to octeto. Cuando se piden prestados 4 bits, la nueva longitud de prefijo es /26, con la máscara de subred 255.255.255.192.

División de subredes de una red IPv4

Se crean 16 subredes con 62 direcciones de host cada una



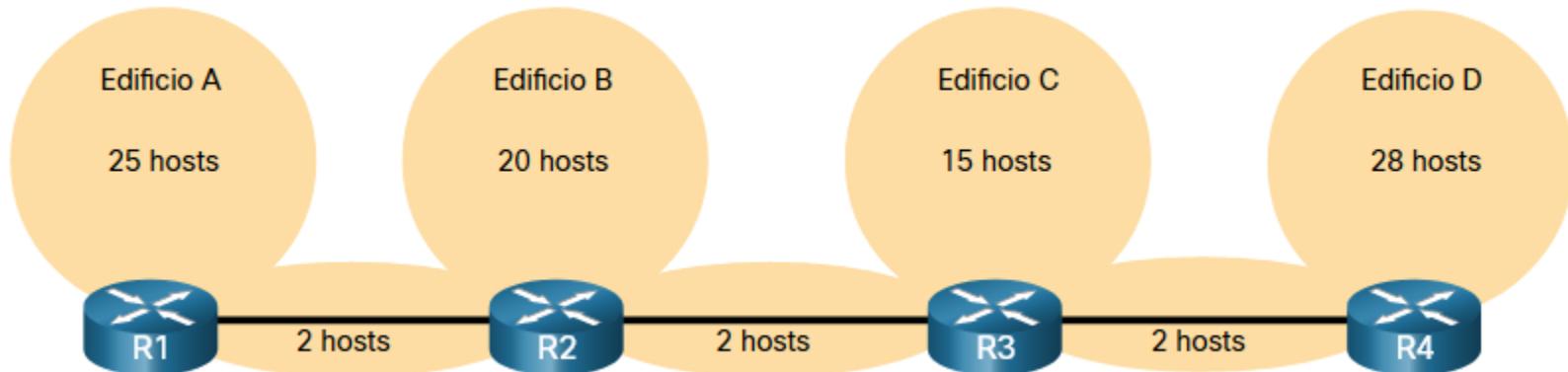
8 VLSM

VLSM

Debido al agotamiento del espacio de direcciones IPv4 público, sacar el máximo partido a las direcciones de host disponibles es una preocupación primordial cuando se subredes de redes IPv4.

Mediante la división en subredes tradicional, se asigna la misma cantidad de direcciones a cada subred. Si todas las subredes tienen los mismos requisitos para la cantidad de hosts, o si la conservación del espacio de direcciones IPv4 no es un problema, estos bloques de direcciones de tamaño fijo serían eficientes. Normalmente, con direcciones IPv4 públicas, ese no es el caso.

VLSM



Utilizando la división en subredes tradicional con la dirección dada de 192.168.20.0/24, se pueden tomar prestados tres bits de la parte del host en el último octeto para cumplir con el requisito de subred de siete subredes. Tomar prestados 3 bits crea 8 subredes y deja 5 bits de host con 30 hosts utilizables por subred. Mediante este esquema, se crean las subredes necesarias y se cumplen los requisitos de host de la LAN más grande.

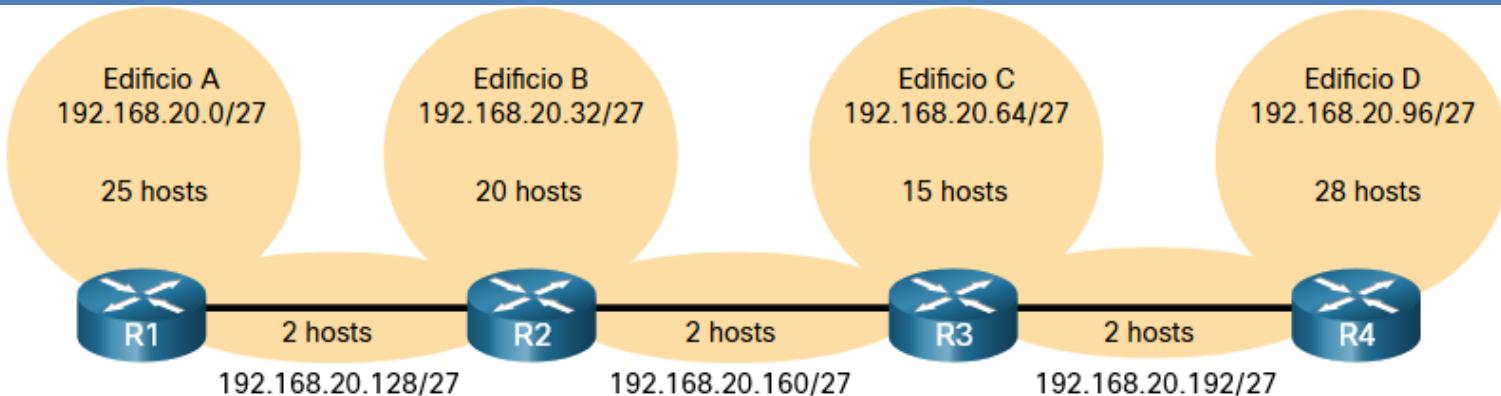
VLSM

	Porción de red	Porción de host			
	11000000.10101000.00010100	.000	00000	192.168.20.0/24	
0	11000000.10101000.00010100	.000	00000	192.168.20.0/27	Redes LAN del edificio A, B, C y D
1	11000000.10101000.00010100	.001	00000	192.168.20.32/27	
2	11000000.10101000.00010100	.010	00000	192.168.20.64/27	
3	11000000.10101000.00010100	.011	00000	192.168.20.96/27	
4	11000000.10101000.00010100	.100	00000	192.168.20.128/27	
5	11000000.10101000.00010100	.101	00000	192.168.20.160/27	
6	11000000.10101000.00010100	.110	00000	192.168.20.192/27	
7	11000000.10101000.00010100	.111	00000	192.168.20.224/27	Sin utilizar/disponible

Porción de subred
 $2^3 = 8$ subredes

Porción de host
 $2^5 - 2 = 30$ direcciones IP de host por subred

VLSM



Si bien la división en subredes tradicional satisface las necesidades de la LAN más grande y divide el espacio de direcciones en una cantidad adecuada de subredes, da como resultado un desperdicio significativo de direcciones sin utilizar. Por ejemplo, solo se necesitan dos direcciones en cada subred para los tres enlaces WAN. Dado que cada subred tiene 30 direcciones utilizables, hay 28 direcciones sin utilizar en cada una de estas subredes. Como se muestra en la figura, esto da como resultado 84 direcciones no utilizadas (28×3).

VLSM

	Porción de red	Porción de host	Decimal punteada
4	11000000.10101000.00010100	.100 00000	192.168.20.128/27
5	11000000.10101000.00010100	.101 00000	192.168.20.160/27
6	11000000.10101000.00010100	.110 00000	192.168.20.192/27

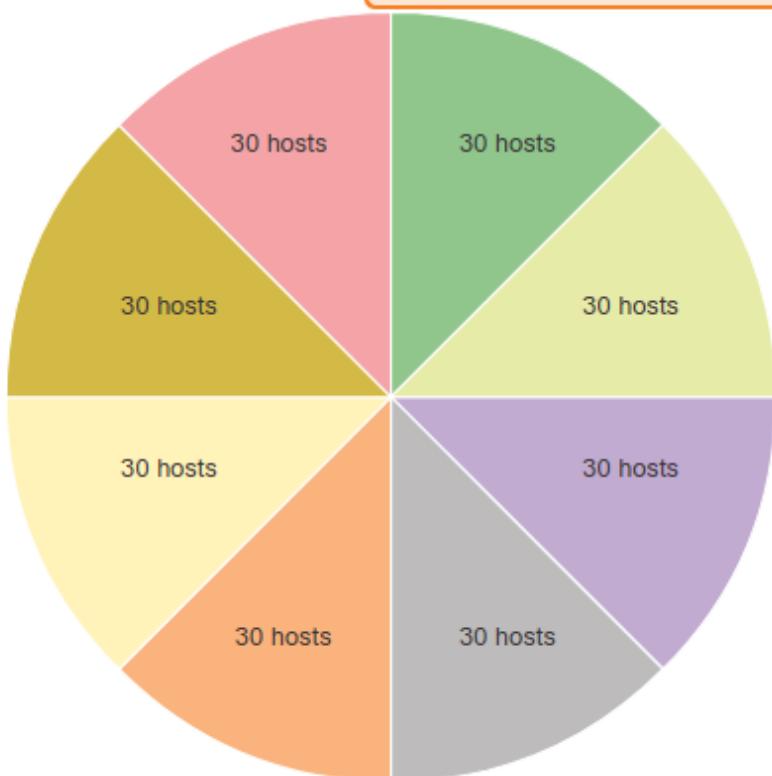
Porción de host
 $2^5 - 2 = 30$ direcciones IP de host por subred
 $30 - 2 = 28$
Cada subred WAN desperdicia 28 direcciones
 $28 \times 3 = 84$
84 direcciones no se utilizan

VLSM

Mediante la división en subredes tradicional se crean subredes de igual tamaño. Cada subred en un esquema tradicional utiliza la misma máscara de subred. Como se muestra en la figura, VLSM permite dividir un espacio de red en partes desiguales. Con VLSM, la máscara de subred varía según la cantidad de bits que se toman prestados para una subred específica, de lo cual deriva la parte “variable” de la VLSM.

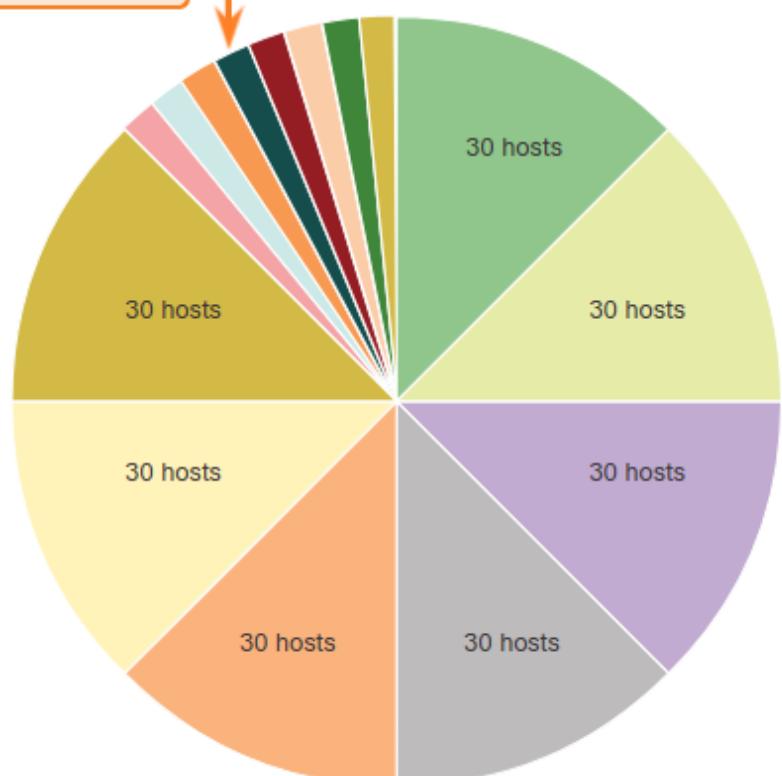
VLSM

La división en subredes crea subredes de igual tamaño



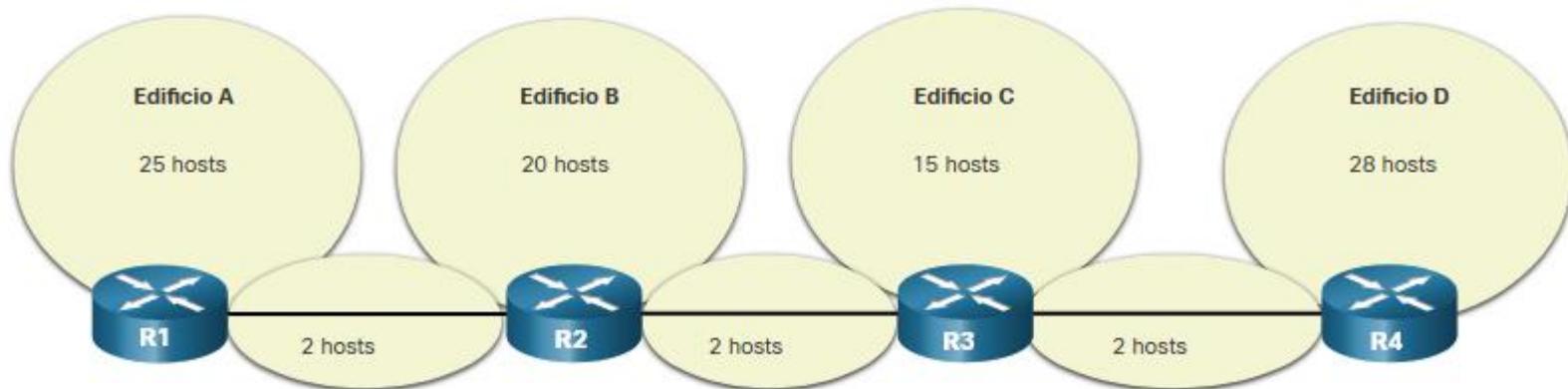
Una subred se dividió aún más usando una máscara de subred / 30 para crear 8 subredes más pequeñas de 2 hosts cada una.

Subredes de distintos tamaños



VLSM

VLSM simplemente subdivide una subred. La misma topología utilizada anteriormente se muestra en la figura. Nuevamente, usaremos la red 192.168.20.0/24 y la subred para siete subredes, una para cada una de las cuatro LAN, y una para cada una de las tres conexiones entre los routeres.



VLSM

La figura muestra cómo la red 192.168.20.0/24 se divide en ocho subredes de igual tamaño con 30 direcciones de host utilizables por subred. Se usan cuatro subredes para las LAN y tres subredes para las conexiones entre los routers.

VLSM

VLSM hace subnetting de la subred 7 para ahorrar direcciones en las redes de enlace entre routers (WAN)

	Porción de red	Porción de host	Decimal punteada	
7	11000000.10101000.00010100	.111	00000	192.168.20.224/27
				¿3 bits más prestados de la subred?
7:0	11000000.10101000.00010100	.111000	00	192.168.20.224/30
7:1	11000000.10101000.00010100	.111001	00	192.168.20.228/30
7:2	11000000.10101000.00010100	.111010	00	192.168.20.232/30
7:3	11000000.10101000.00010100	.111011	00	192.168.20.236/30
7:4	11000000.10101000.00010100	.111100	00	192.168.20.240/30
7:5	11000000.10101000.00010100	.111101	00	192.168.20.244/30
7:6	11000000.10101000.00010100	.111110	00	192.168.20.248/30
7:7	11000000.10101000.00010100	.111111	00	192.168.20.252/30
				Subdivisión de subredes
				Redes WAN
				Sin utilizar/disponible

VLSM

Cuando se conoce el número de direcciones de host necesarias, se puede usar la fórmula $2^n - 2$ (donde n es igual al número de bits de host restantes). Para proporcionar dos direcciones utilizables, se deben dejar dos bits de host en la parte del host.

Debido a que hay cinco bits de host en el espacio de direcciones subred 192.168.20.224/27, se pueden pedir prestados tres bits más, dejando dos bits en la porción de host. Los cálculos que se realizan llegado este punto son exactamente los mismos que se utilizan para la división en subredes tradicional: Se toman prestados los bits, y se determinan los rangos de subred. La figura muestra cómo las cuatro subredes /27 se han asignado a las LAN y tres de las subredes /30 se han asignado a los enlaces entre routers.

9 ICMP

ICMP

Aunque IP es sólo un protocolo de mayor esfuerzo, **el conjunto TCP/IP proporciona mensajes de error y mensajes informativos cuando se comunica con otro dispositivo IP**. Estos mensajes se envían mediante los servicios de ICMP. El objetivo de estos mensajes 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.

Los mensajes ICMP comunes a ICMPv4 e ICMPv6 incluyen:

- Accesibilidad al host
- Destino o servicio inaccessible
- Tiempo superado

ICMP

Accesibilidad al host

Se puede utilizar un mensaje de eco ICMP para **probar la accesibilidad de un host en una red IP**. 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.

Este uso de los mensajes ICMP Echo es la base de la utilidad de **ping**.

ICMP

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

ICMP

Tiempo excedido

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.

Ping

Para probar la conectividad a otro host en una red, se envía una solicitud de eco a la dirección del host utilizando el comando **ping**. Si el host en la dirección especificada recibe la solicitud de eco, responde con una respuesta de eco. A medida que se recibe cada respuesta de eco, **ping** proporciona comentarios sobre el tiempo entre el momento en que se envió la solicitud y el momento en que se recibió la respuesta. Esto puede ser una medida del rendimiento de la red.

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.

Esto puede indicar que hay un problema, pero también **podría indicar que las funciones de seguridad que bloquean los mensajes de ping se han habilitado en la red**. Es común que el primer ping se agote si es necesario realizar la resolución de direcciones (ARP o ND) antes de enviar la solicitud de eco ICMP.

Ping

Después de enviar todas las solicitudes, la utilidad ping proporciona un resumen que incluye la tasa de éxito y el tiempo promedio de ida y vuelta al destino.

Los tipos de pruebas de conectividad que se realizan con ping son los siguientes:

- Hacer ping al **loopback** local
- Hacer ping a la **puerta de enlace predeterminada**
- Hacer ping al **host remoto**

Ping

Hacer ping al loopback

Ping se puede usar para probar la configuración interna de IPv4 o IPv6 en el host local. Para realizar esta prueba, ping a dirección de bucle de retorno local de 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 es una indicación de que las direcciones, máscaras o puertas de enlace estén configuradas correctamente. 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.

Ping

Hacer ping al gateway predeterminado

También puede usar para ping probar la capacidad de un host para comunicarse en la red local. Esto generalmente se hace haciendo ping a la dirección IP de la puerta de enlace predeterminada del host. Un éxito ping en la puerta de enlace predeterminada indica que el host y la interfaz del enrutador que sirve como puerta de enlace predeterminada están operativos en la red local.

Para esta prueba, la dirección de puerta de enlace predeterminada se usa con mayor frecuencia porque el enrutador normalmente siempre está operativo. Si la dirección de la puerta de enlace predeterminada no responde, ping se puede enviar a la dirección IP de otro host en la red local que se sabe que está operativa.

Ping

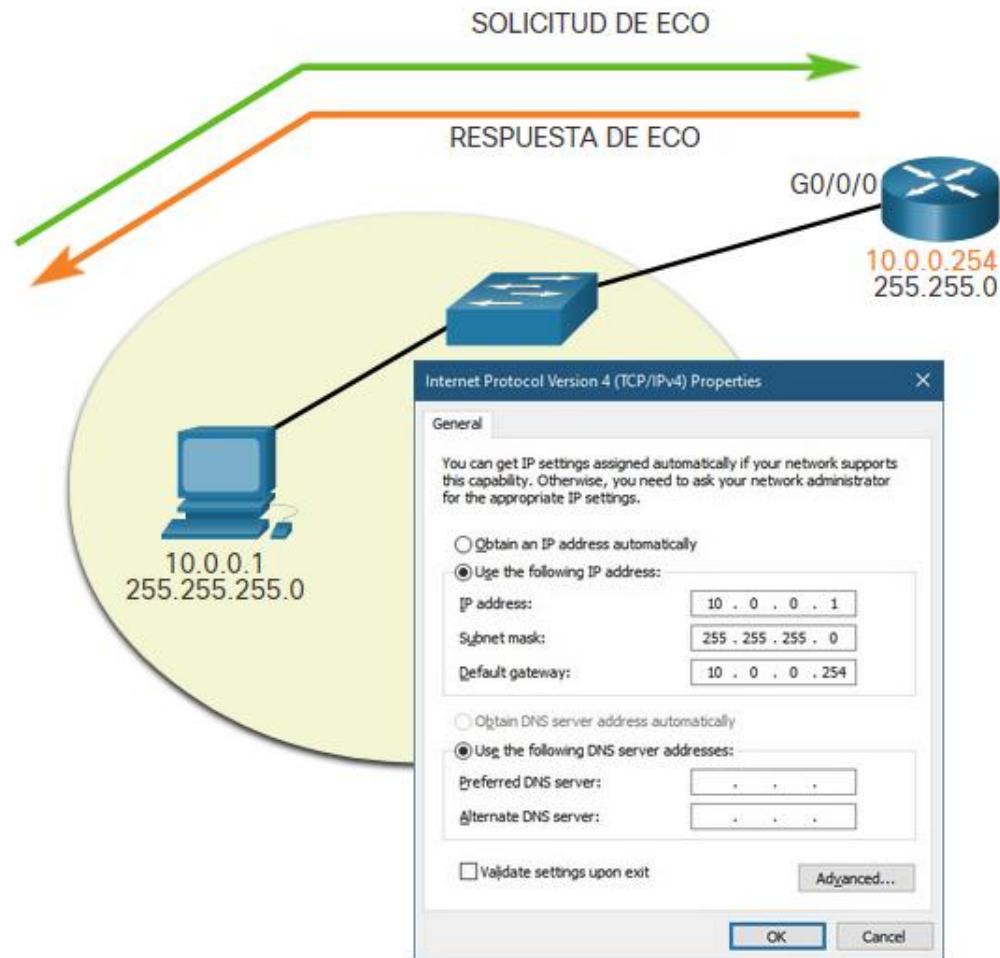
Hacer ping al gateway predeterminado

Si la puerta de enlace predeterminada u otro host responde, entonces el host local puede comunicarse con éxito a través de la red local. Si la puerta de enlace predeterminada no responde pero otro host sí, esto podría indicar un problema con la interfaz del enrutador que funciona como la puerta de enlace predeterminada.

Una posibilidad es que se haya configurado una dirección de puerta de enlace predeterminada 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.

Ping

Hacer ping al gateway predeterminado



Ping

Hacer ping a un Host Remoto

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. El router utiliza su tabla de enrutamiento IP para reenviar los paquetes.

Si este ping se realiza correctamente, se puede verificar el funcionamiento de una amplia porción de la interconexión de redes. Un éxito ping en toda la red confirma la comunicación en la red local, el funcionamiento del enrutador que sirve como puerta de enlace predeterminada y el funcionamiento de todos los demás enrutadores que podrían estar en la ruta entre la red local y la red del host remoto.

Traceroute

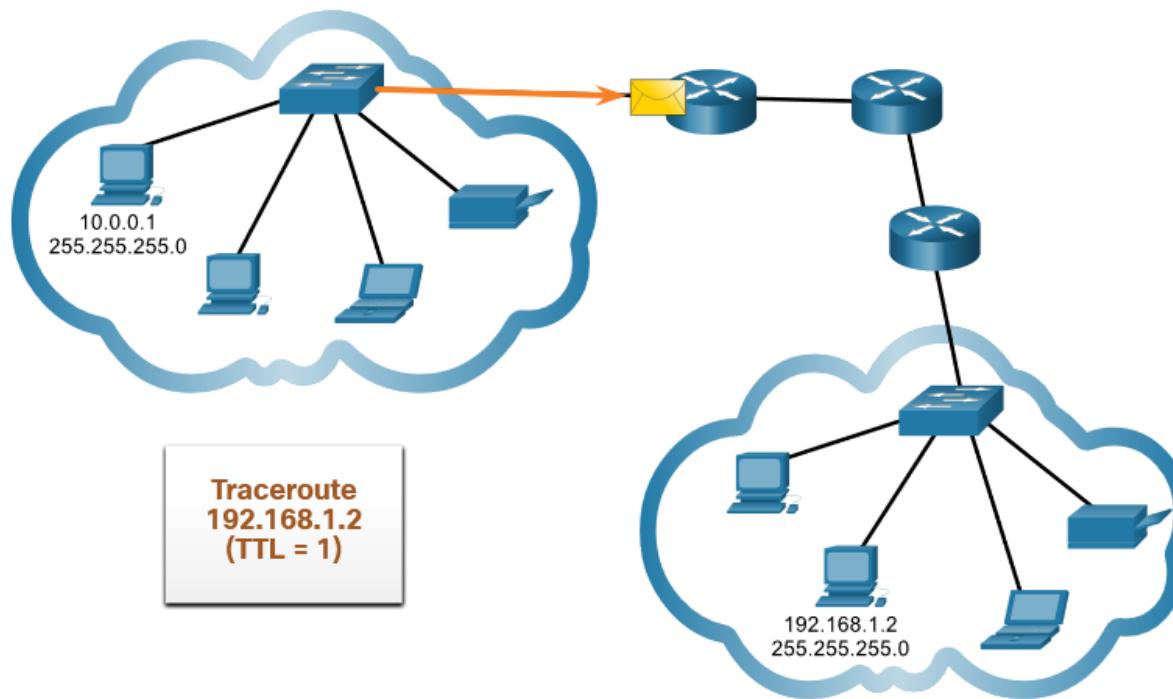
Traceroute: Prueba el Camino

El comando **ping** se usa para probar la conectividad entre dos hosts, pero no proporciona información sobre los detalles de los dispositivos entre los hosts. Traceroute (tracert) es una utilidad que genera una lista de saltos que se alcanzaron con éxito a lo largo de la ruta. Esta lista puede proporcionar información importante sobre la verificación y la solución de problemas. 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.

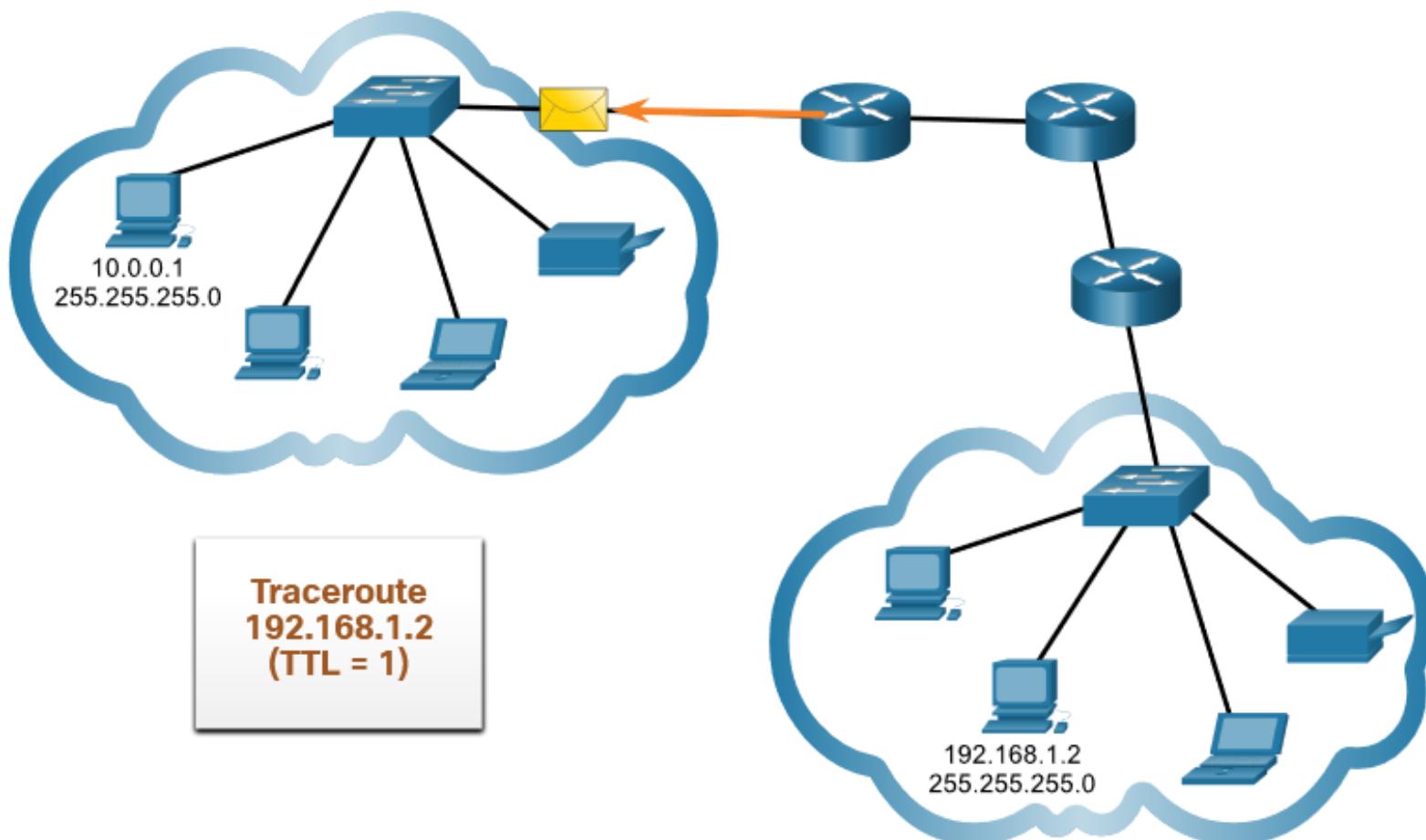
Traceroute

TTL de IPv4 y Límite de Saltos en IPv6

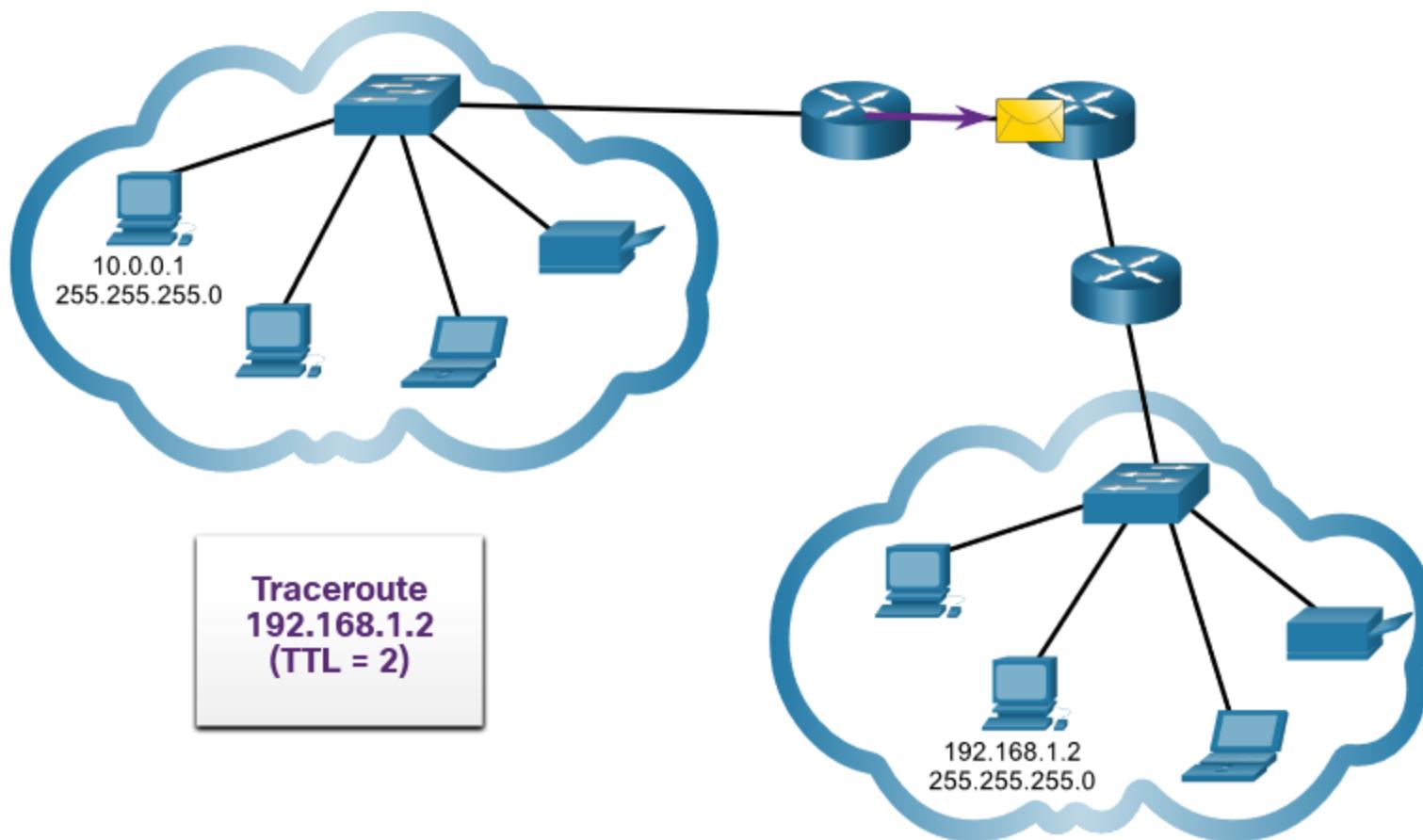
Traceroute utiliza una función del campo TTL en IPv4 y el campo Límite de salto en IPv6 en los encabezados de Capa 3, junto con el mensaje ICMP Time Exceeded.



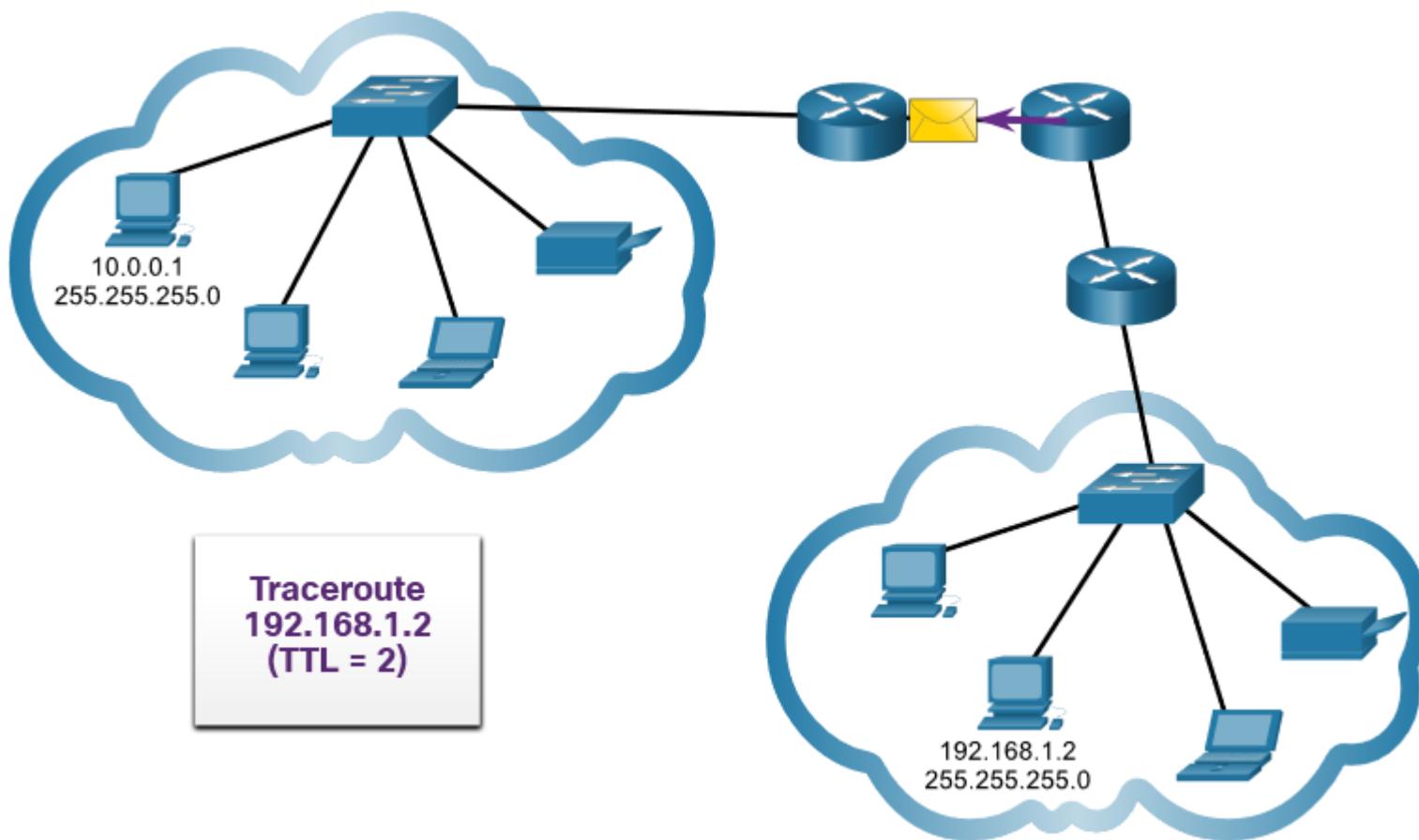
Traceroute



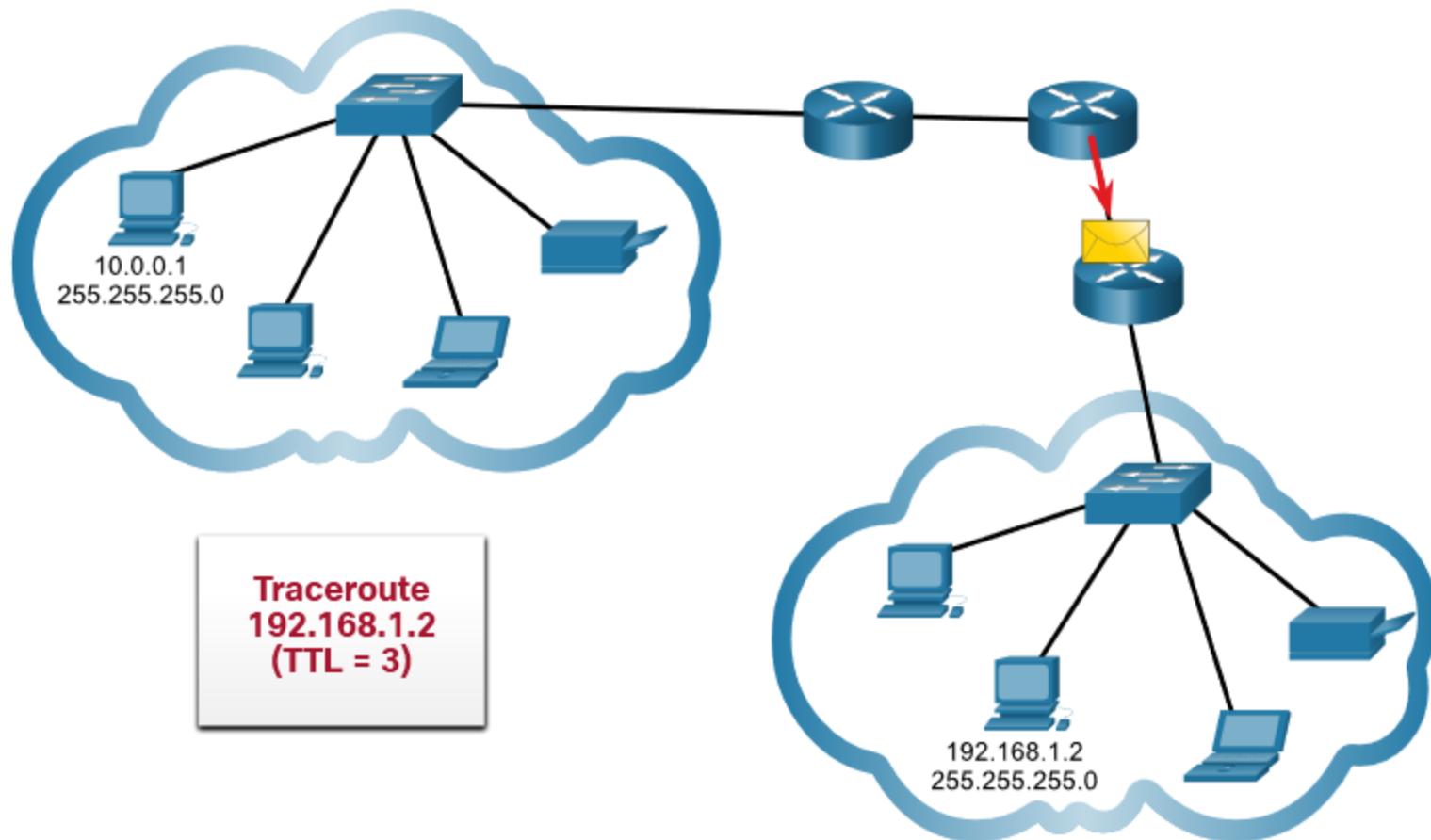
Traceroute



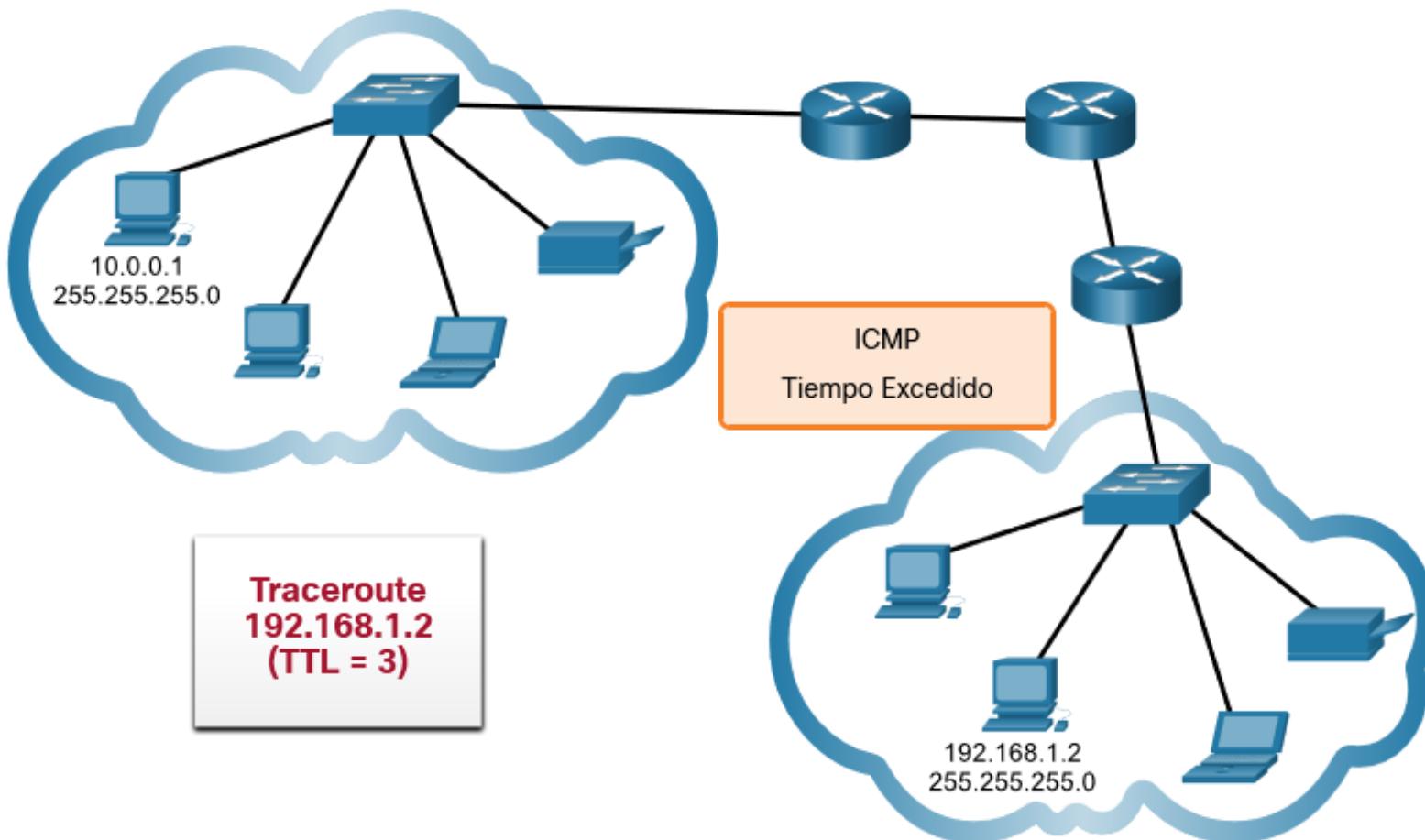
Traceroute



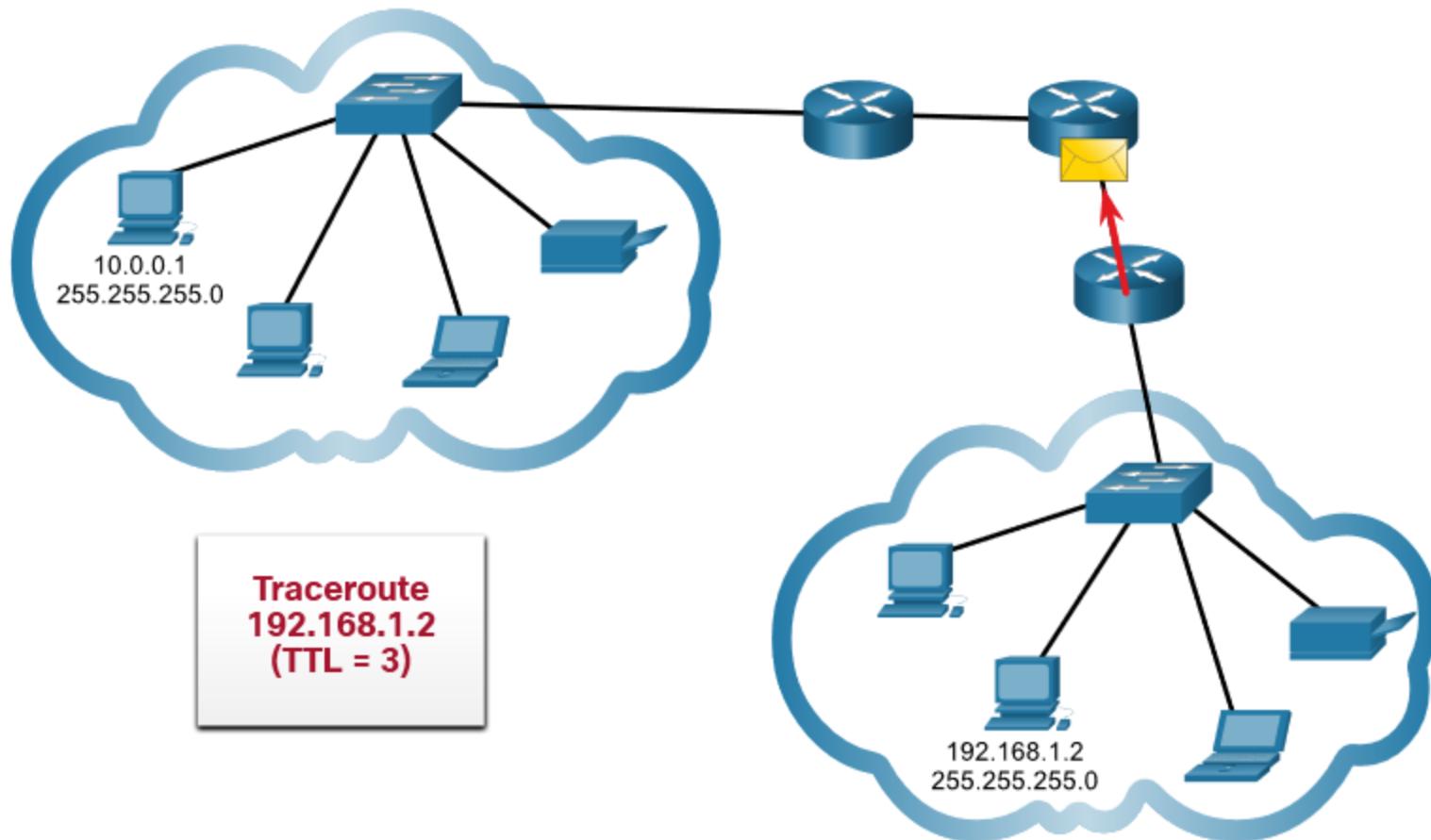
Traceroute



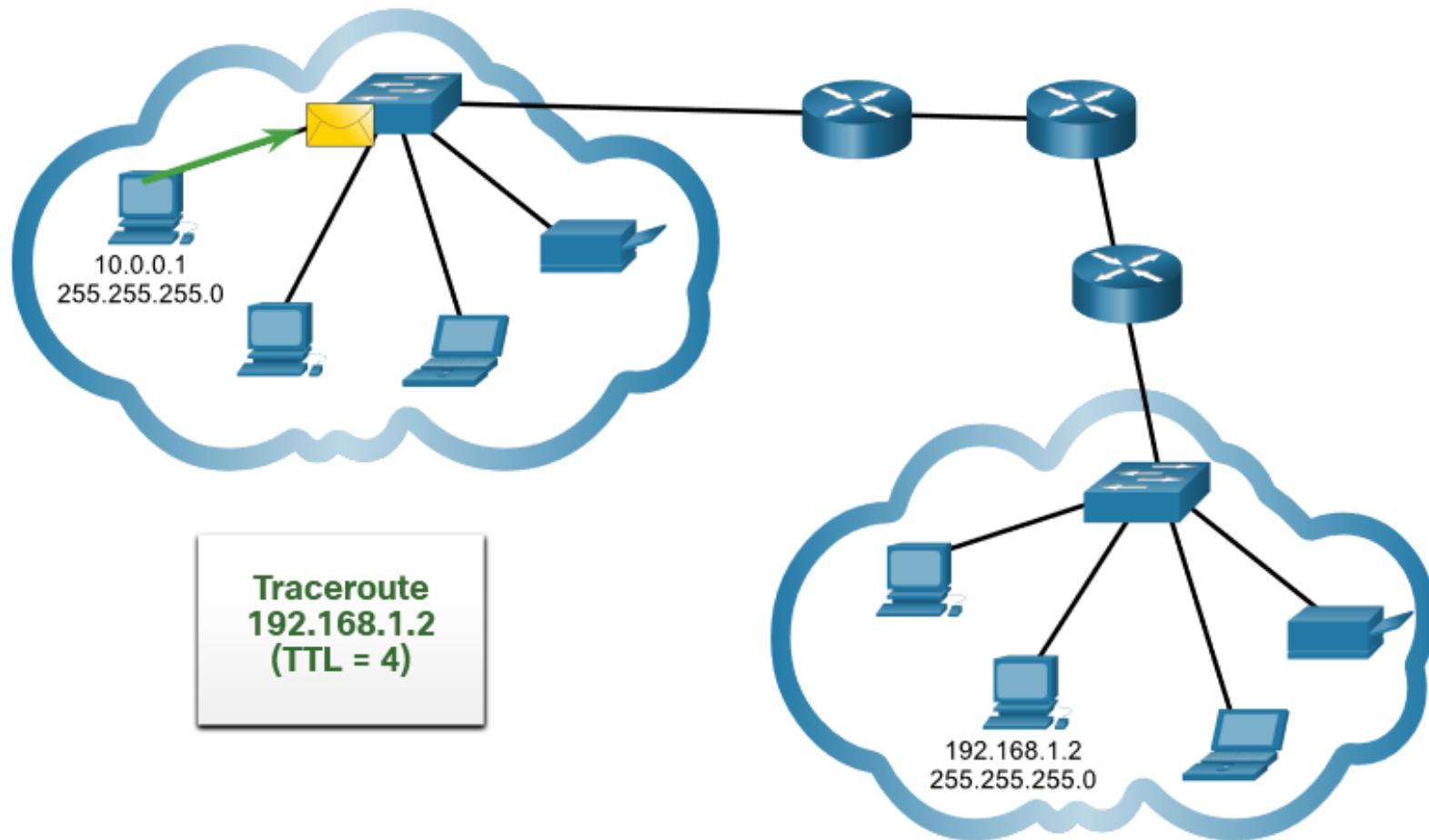
Traceroute



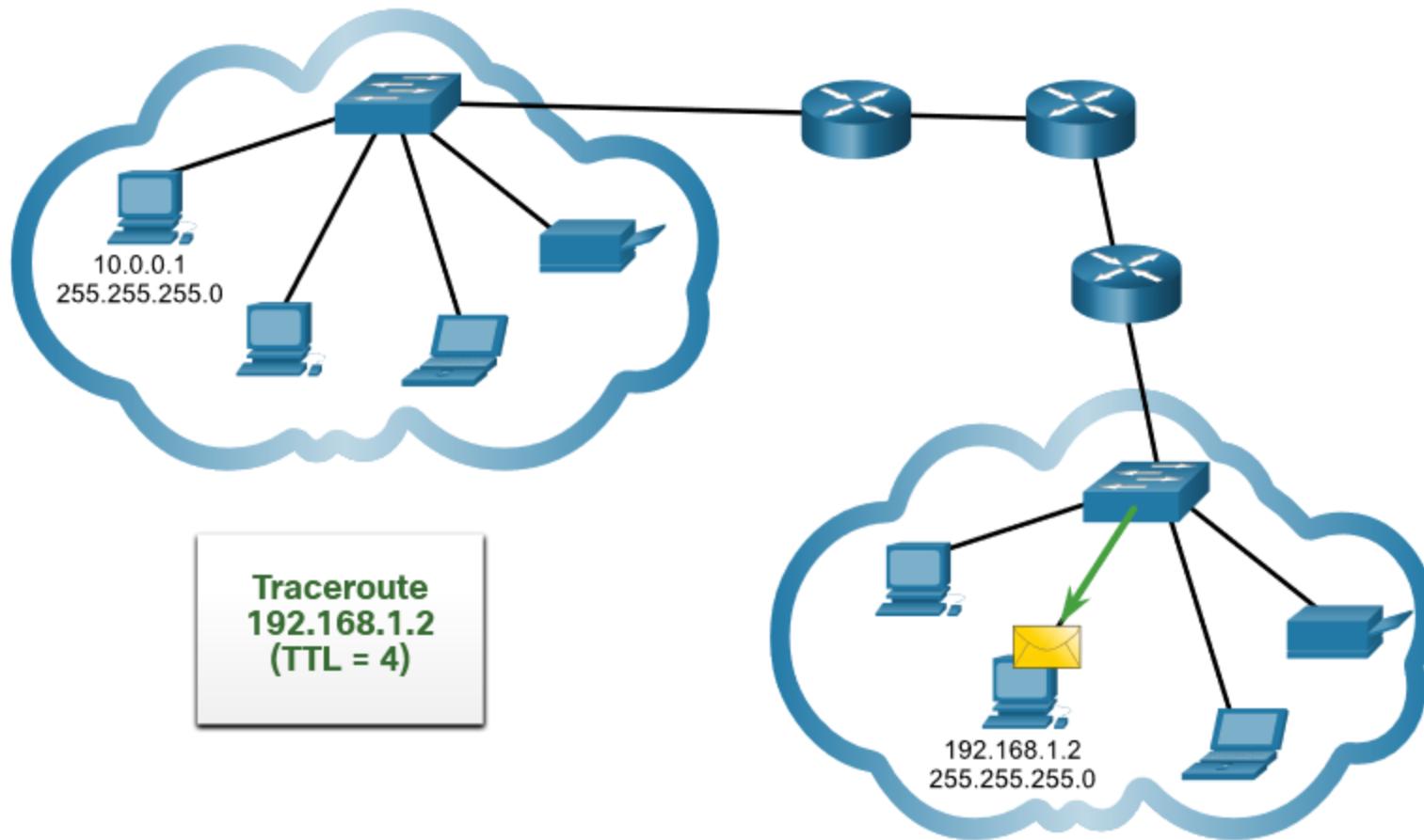
Traceroute



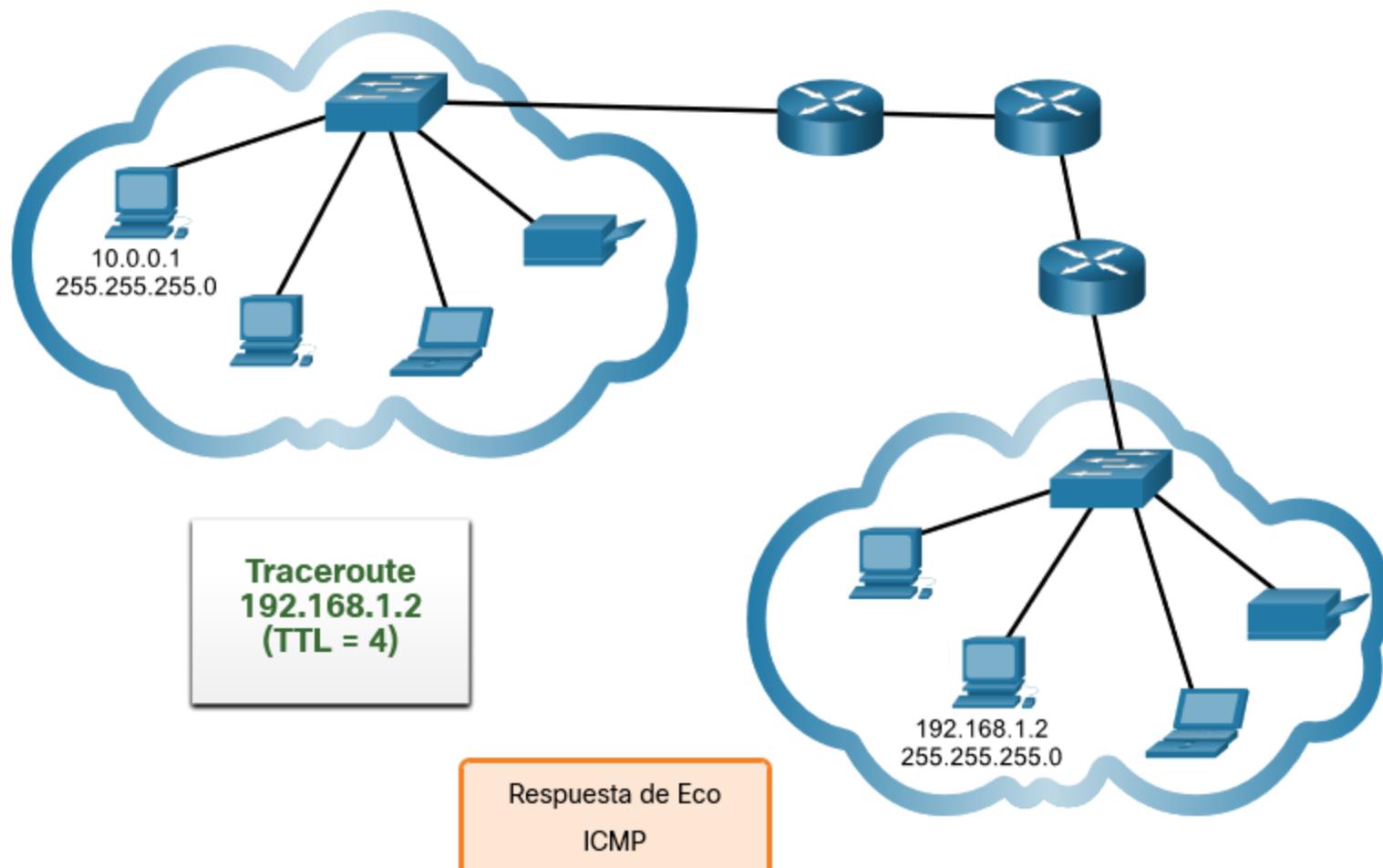
Traceroute



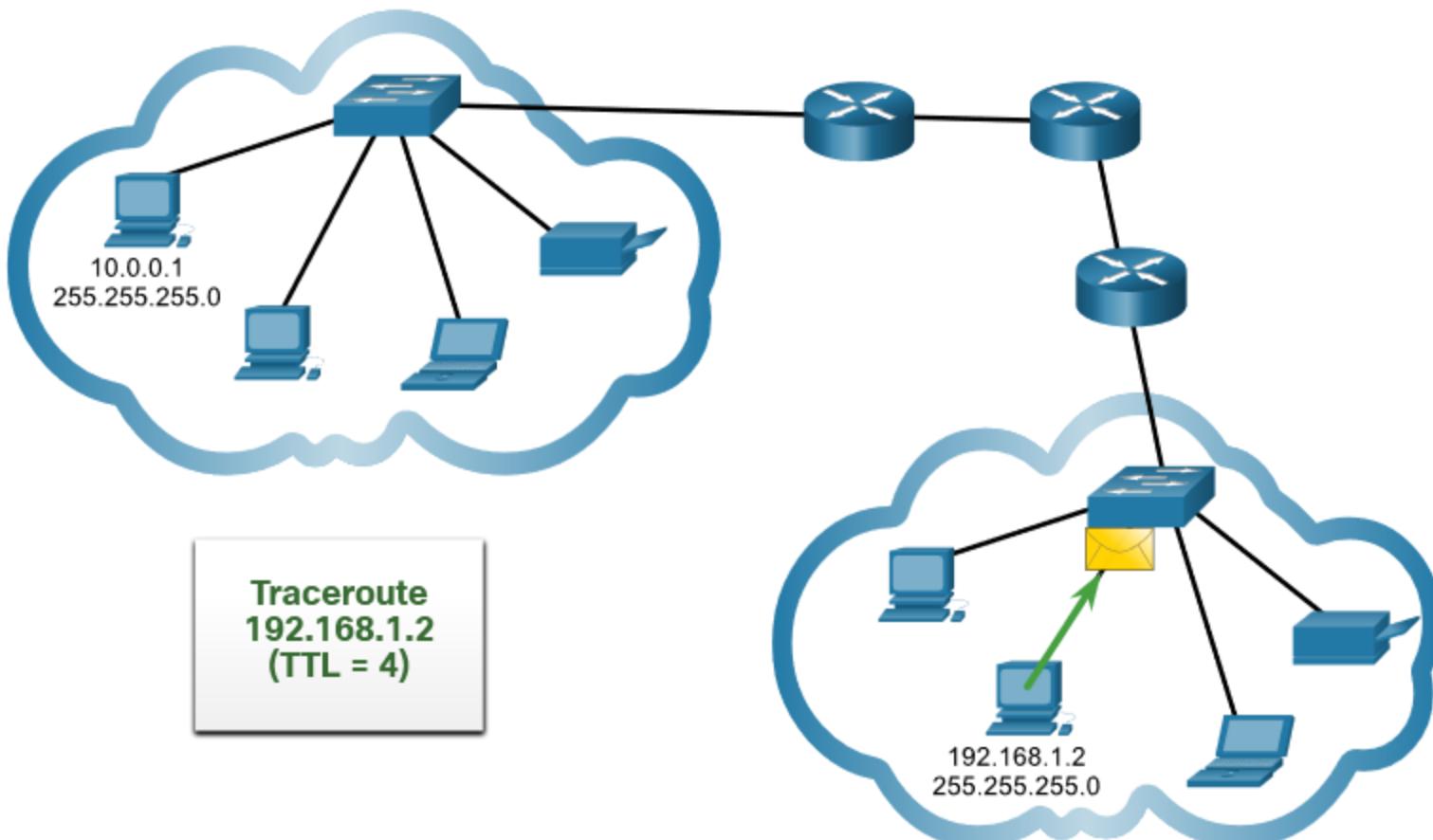
Traceroute



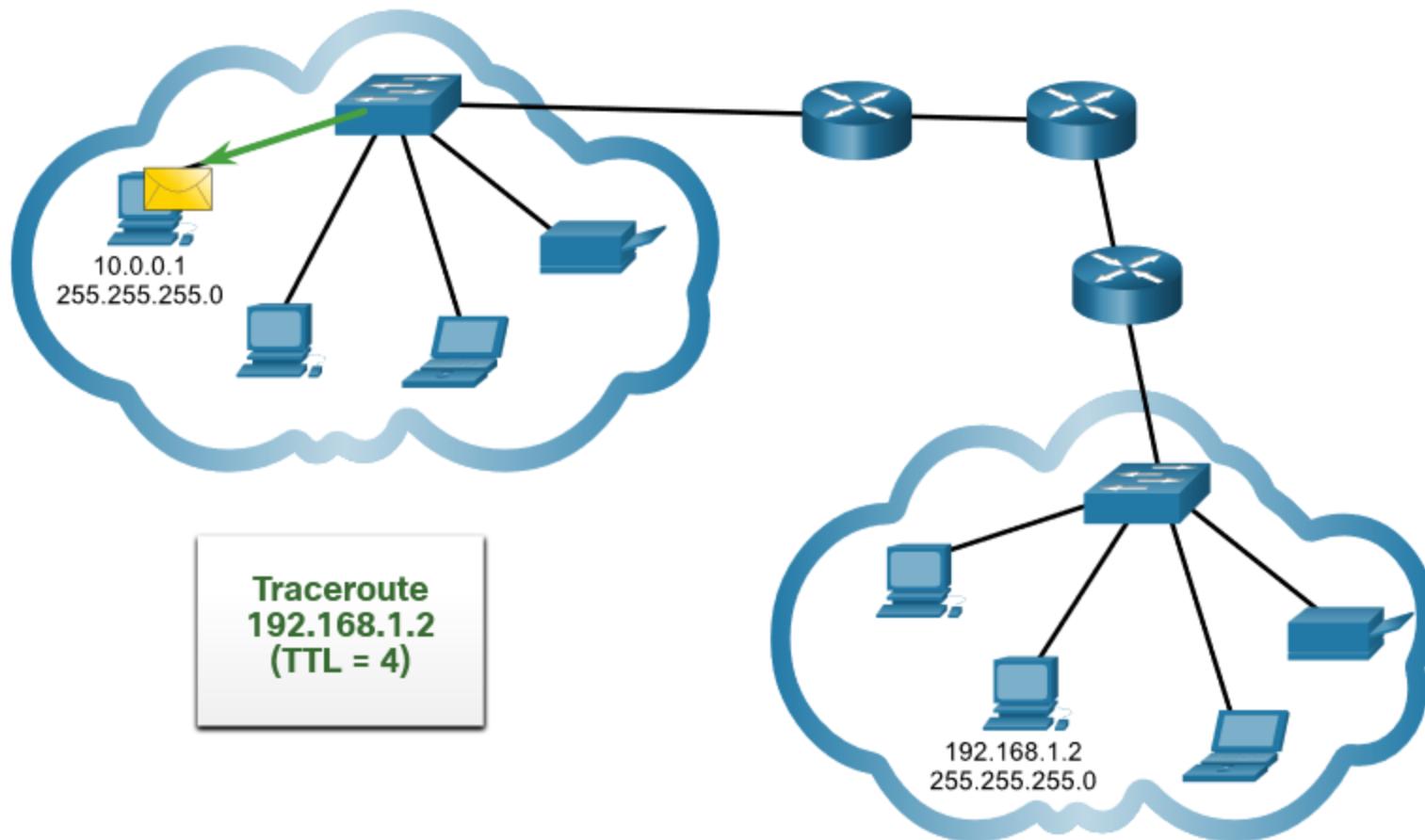
Traceroute



Traceroute



Traceroute



10 | IPv6

Problemas con IPv4

El **agotamiento** del espacio de direcciones **IPv4** fue el factor que motivó la migración a **IPv6**.

IPv4 tiene un máximo teórico de 4300 millones de direcciones. Las direcciones privadas en combinación con la traducción de direcciones de red (NAT) fueron esenciales para demorar la reducción del espacio de direcciones IPv4. Sin embargo, **NAT** es problemático para muchas aplicaciones, crea latencia y tiene limitaciones que impiden severamente las comunicaciones entre pares.

Con una población de Internet cada vez mayor, un espacio limitado de direcciones IPv4, problemas con NAT y el IoT, ha llegado el momento de comenzar la transición a **IPv6**.

Problemas con IPv4

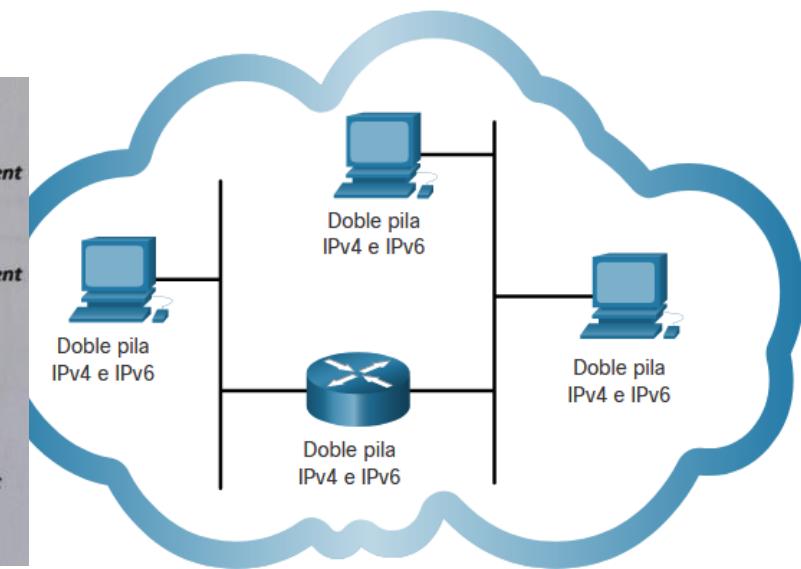
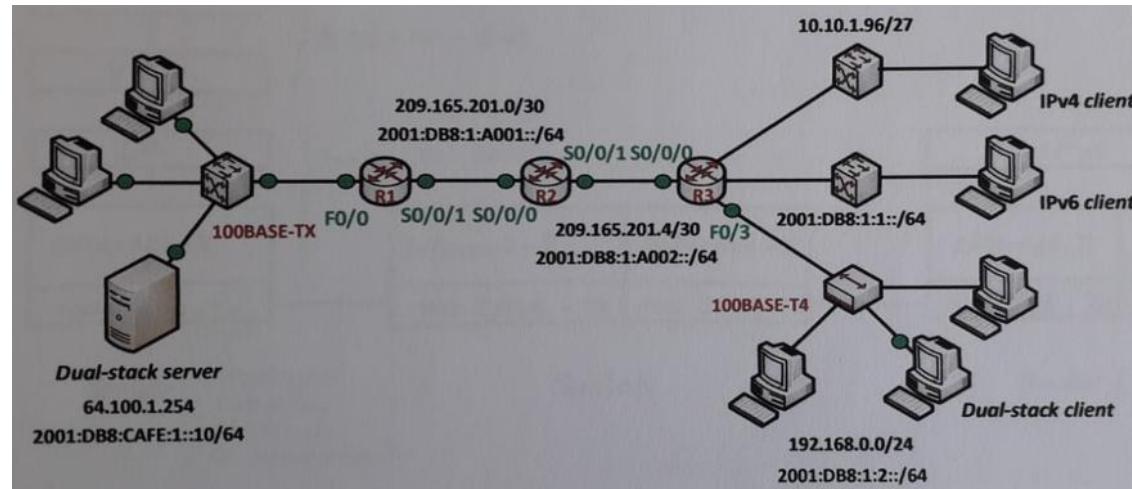
No hay una fecha específica para pasar a IPv6. **Tanto IPv4 como IPv6 coexistirán en un futuro próximo y la transición llevará varios años.** El IETF creó diversos protocolos y herramientas para ayudar a los administradores de redes a migrar las redes a IPv6. Las **técnicas de migración** pueden dividirse en tres categorías:

- Dual-stack
- Tunelización
- Traducción



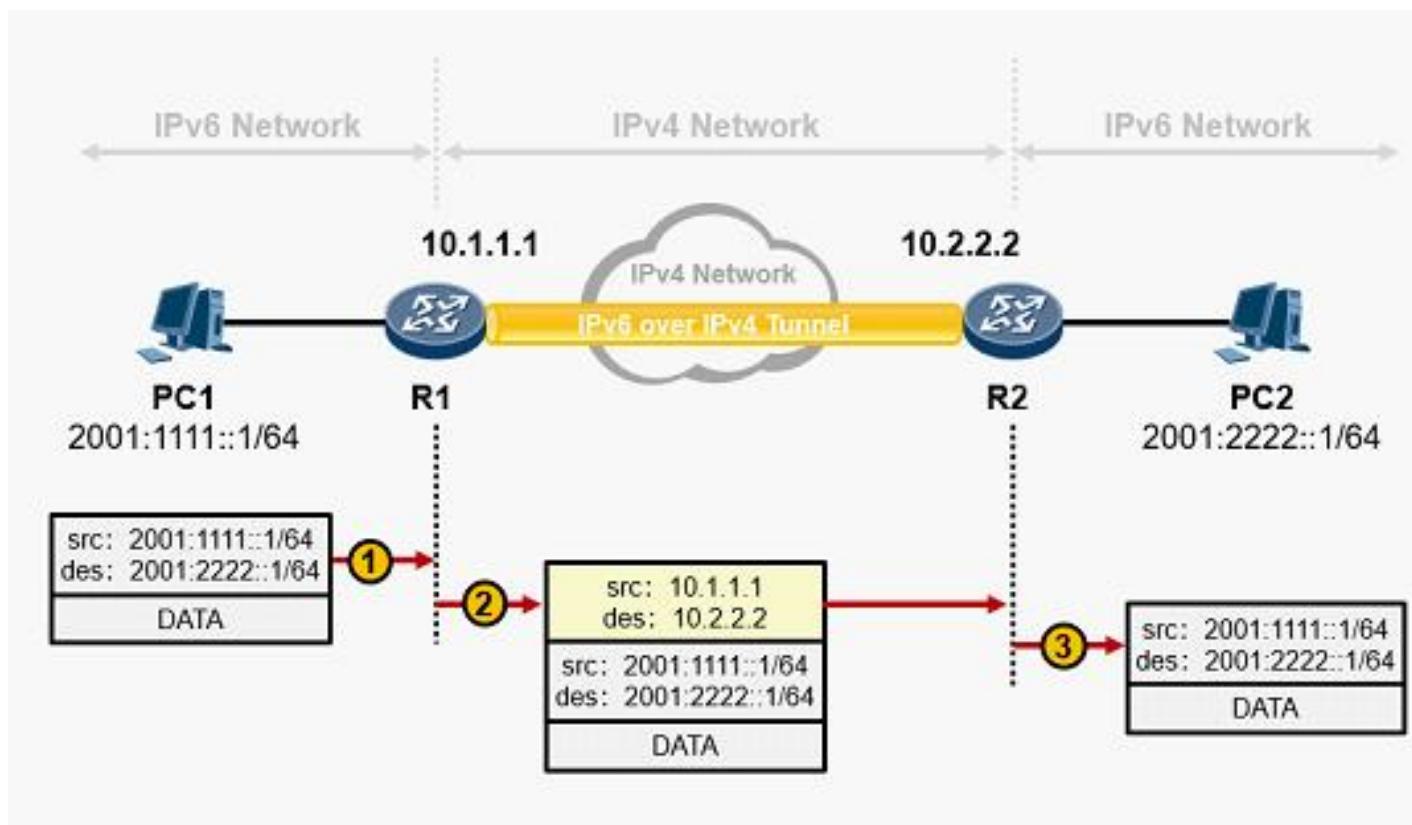
Problemas con IPv4

Dual-stack permite que IPv4 e IPv6 coexisten en el mismo segmento de red. Los dispositivos dual-stack ejecutan pilas de protocolos IPv4 e IPv6 de manera simultánea. Conocido como IPv6 nativo, esto significa que la red del cliente tiene una conexión IPv6 a su ISP y puede acceder al contenido que se encuentra en Internet a través de IPv6.



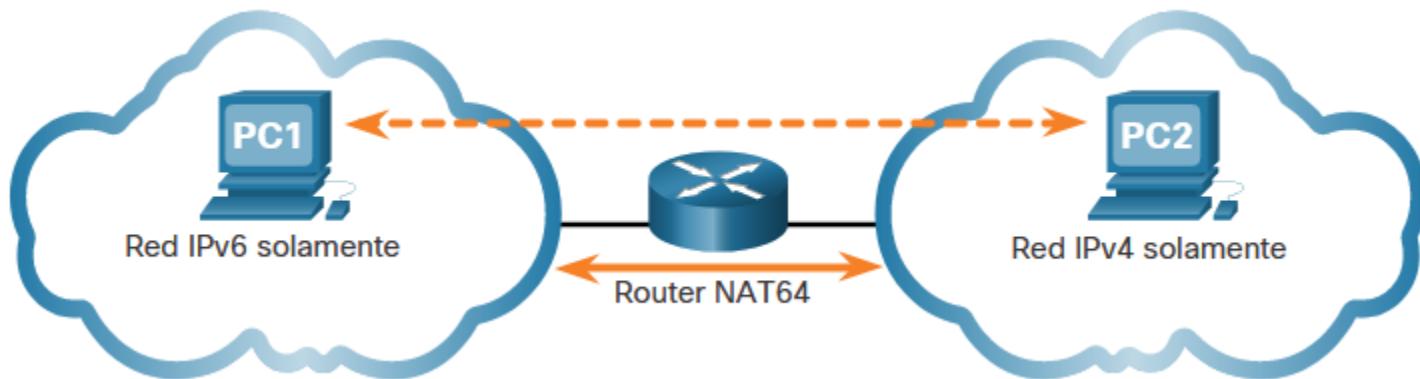
Problemas con IPv4

La tunelización es un método para transportar un paquete IPv6 a través de 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.



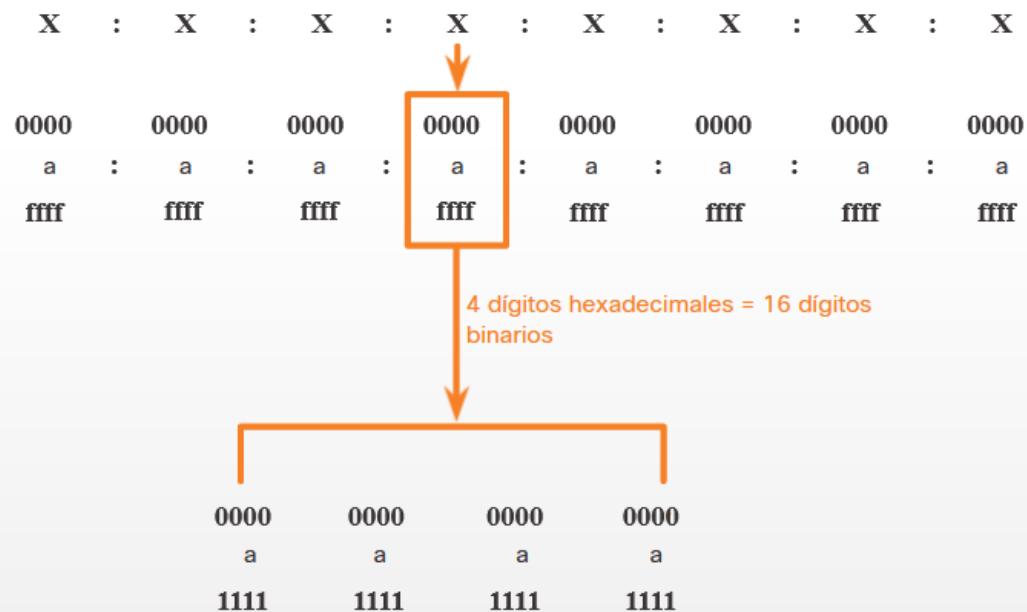
Problemas con IPv4

La traducción de direcciones de redes 64 (NAT64) permite que los dispositivos con IPv6 habilitado se comuniquen con dispositivos con IPv4 habilitado mediante una técnica de traducción similar a la NAT para IPv4. Un paquete IPv6 se traduce a un paquete IPv4 y un paquete IPv4 se traduce a un paquete IPv6.



Formatos de direccionamiento de IPv6

Las **direcciones IPv6** tienen una longitud de **128 bits** y se escriben como una **cadena de valores hexadecimales**. Cada cuatro bits está representado por un solo dígito hexadecimal; para un total de 32 valores hexadecimales. Las direcciones IPv6 no distinguen entre mayúsculas y minúsculas, y pueden escribirse en minúsculas o en mayúsculas.



Formatos de direccionamiento de IPv6

Formato preferido

El formato preferido significa que escribe la dirección IPv6 utilizando los 32 dígitos hexadecimales. No significa necesariamente que sea el método ideal para representar la dirección IPv6.

```
2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
2001 : 0db8 : 0000 : 00a3 : abcd : 0000 : 0000 : 1234
2001 : 0db8 : 000a : 0001 : c012 : 9aff : fe9a : 19ac
2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000 : 0000
fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab : cdef
fe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
fe80 : 0000 : 0000 : 0000 : c012 : 9aff : fe9a : 19ac
fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab : cdef
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000
```

Formatos de direccionamiento de IPv6

Formato preferido

La **primera regla** para ayudar a reducir la notación de las direcciones IPv6 es **omitar los ceros iniciales en cualquier hexteto**. Aquí hay cuatro ejemplos de formas de omitir ceros a la izquierda:

- 01ab se puede representar como 1ab
- 09f0 se puede representar como 9f0
- 0a00 se puede representar como a00
- 00ab se puede representar como ab

Esta regla **solo** es válida para los **ceros iniciales**, y **NO para los ceros finales**; de lo contrario, la dirección sería ambigua. Por ejemplo, el hexteto "abc" podría ser "0abc" o "abc0", pero no representan el mismo valor.

Formatos de direccionamiento de IPv6

Formato preferido

La segunda regla para ayudar a reducir la notación de las direcciones IPv6 es que un doble punto (:) puede reemplazar cualquier cadena única y contigua de uno o más hextetos de 16 bits que consisten en todos los ceros. Por ejemplo, 2001:db8:cafe: 1:0:0:0:1 (0 iniciales omitidos) podría representarse como 2001:db8:cafe:1::1.

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**”.

Aquí hay un ejemplo del uso incorrecto del doble coma: 2001:db8::abcd::1234.

Tipos de direcciones IPv6

Al igual que con IPv4, existen diferentes tipos de direcciones IPv6:

Unidifusión - una dirección de unidifusión IPv6 identifica de forma exclusiva una interfaz en un dispositivo habilitado para IPv6.

Multidifusión - una dirección de multidifusión IPv6 se usa para enviar un único paquete IPv6 a múltiples destinos.

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.

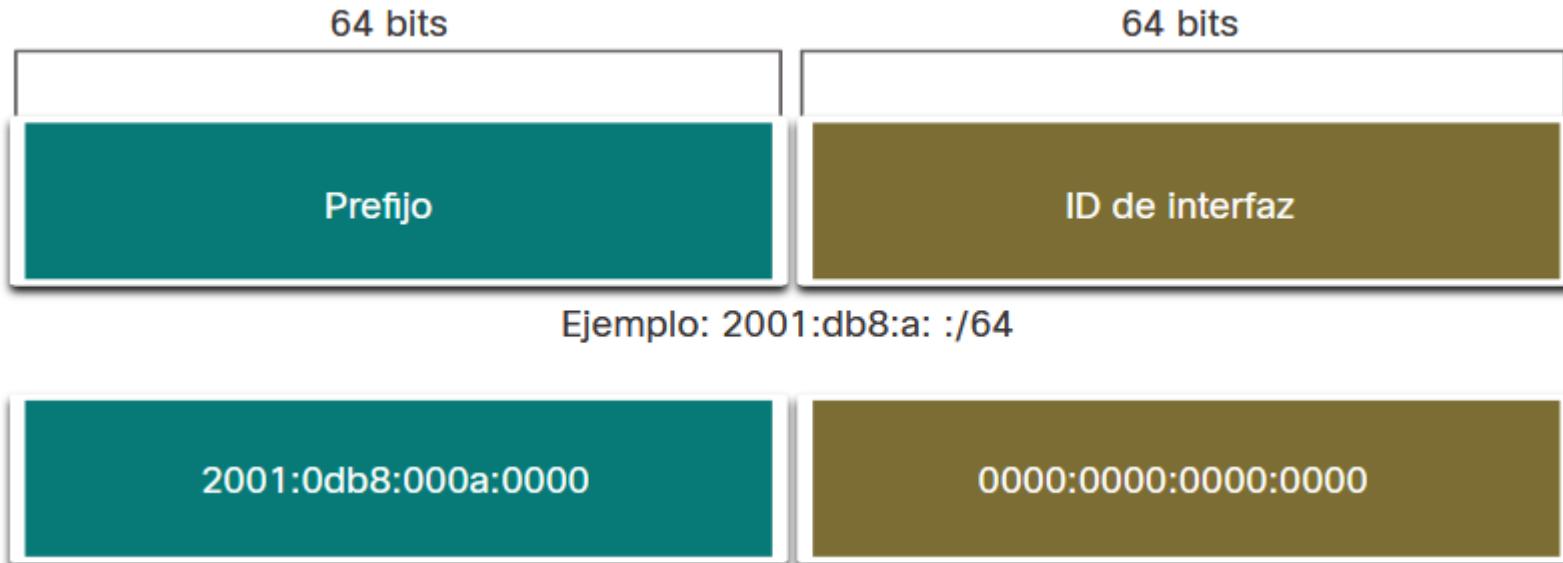
Tipos de direcciones IPv6

El prefijo, o porción de red, de una dirección IPv4 se puede identificar mediante una máscara de subred decimal decimal o longitud de prefijo (notación de barra). Por ejemplo, la dirección IPv4 **192.168.1.10** con la máscara de subred decimal punteada **255.255.255.0** equivale a **192.168.1.10/24**.

En IPv4 el /24 se llama **prefijo**. En IPv6 se llama **longitud de prefijo**. IPv6 no utiliza la notación decimal punteada de máscara de subred. Al igual que IPv4, la longitud del prefijo se representa en **notación de barra inclinada** y se usa para **indicar la porción de red de una dirección IPv6**.

Tipos de direcciones IPv6

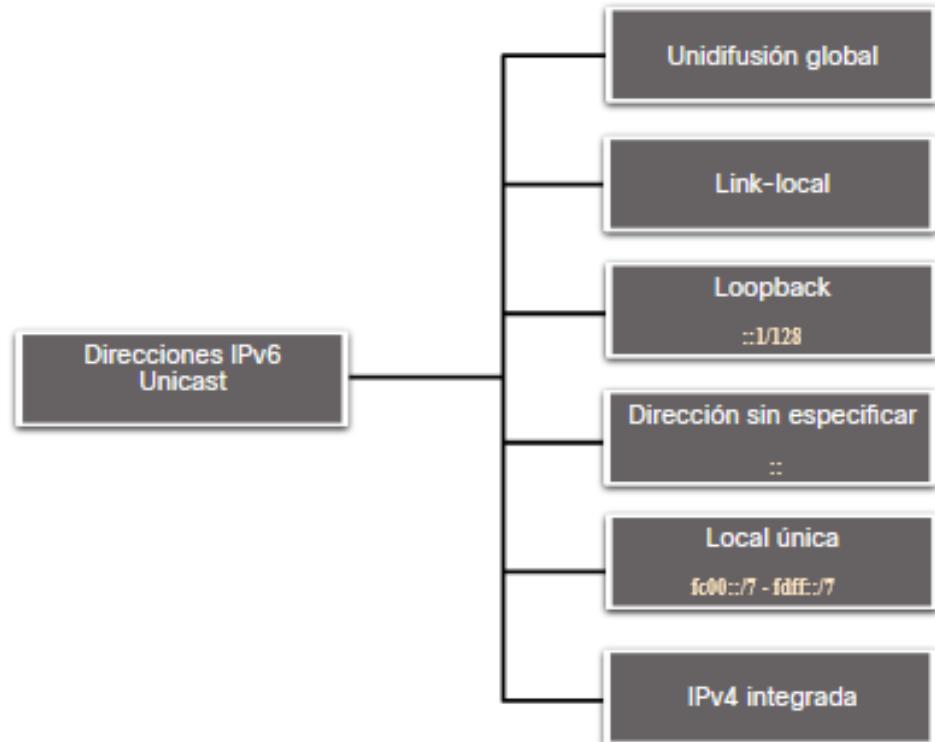
La longitud de prefijo puede ir de 0 a 128. La longitud recomendada del prefijo IPv6 para las LAN y la mayoría de los otros tipos de redes es / 64.



Tipos de direcciones IPv6

Las direcciones IPv6 de unidifusión identifican de forma exclusiva una interfaz en un dispositivo con IPv6 habilitado. La interfaz a la que se le asigna esa dirección recibe un paquete enviado a una dirección de unidifusión. 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.**



Tipos de direcciones IPv6

A diferencia de los dispositivos IPv4 que tienen una sola dirección, **las direcciones IPv6 suelen tener dos direcciones de unidifusión**:

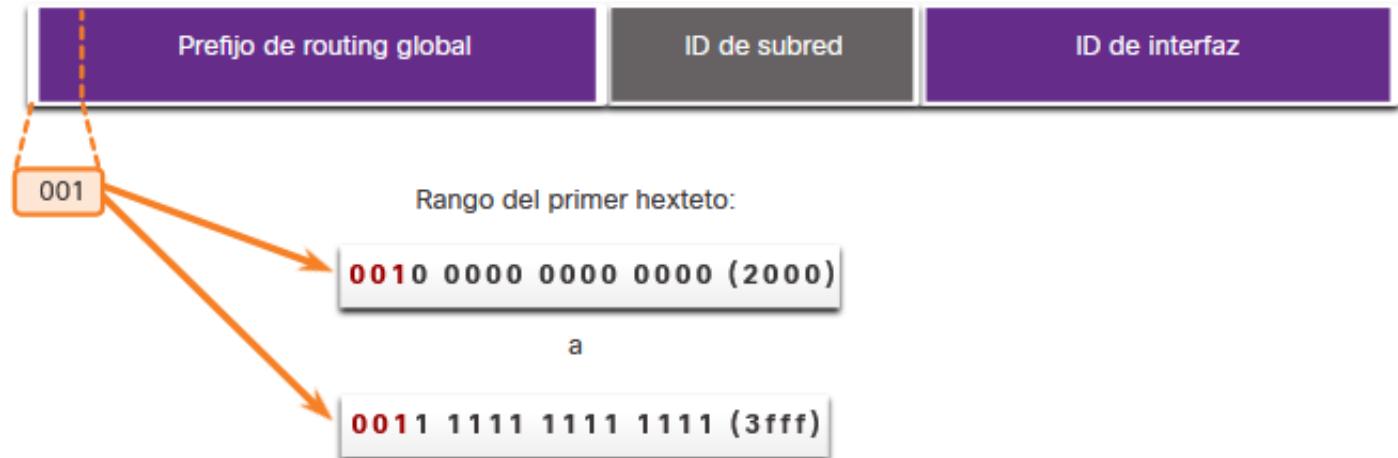
Dirección de unidifusión global (GUA): - es similar a una dirección IPv4 pública. Estas son direcciones enrutables de Internet globalmente exclusivas. Las GUA pueden configurarse estáticamente o asignarse dinámicamente.

Dirección local de enlace (LLA): - se **requiere para cada dispositivo habilitado para IPv6**. Los LLA se utilizan para comunicarse con otros dispositivos en el **mismo enlace local**. Con IPv6, el término “enlace” hace referencia a una subred. **Las LLA 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. En otras palabras, los routers NO reenvían paquetes con una dirección de origen o de destino link-local.

Tipos de direcciones IPv6

IPv6 GUA

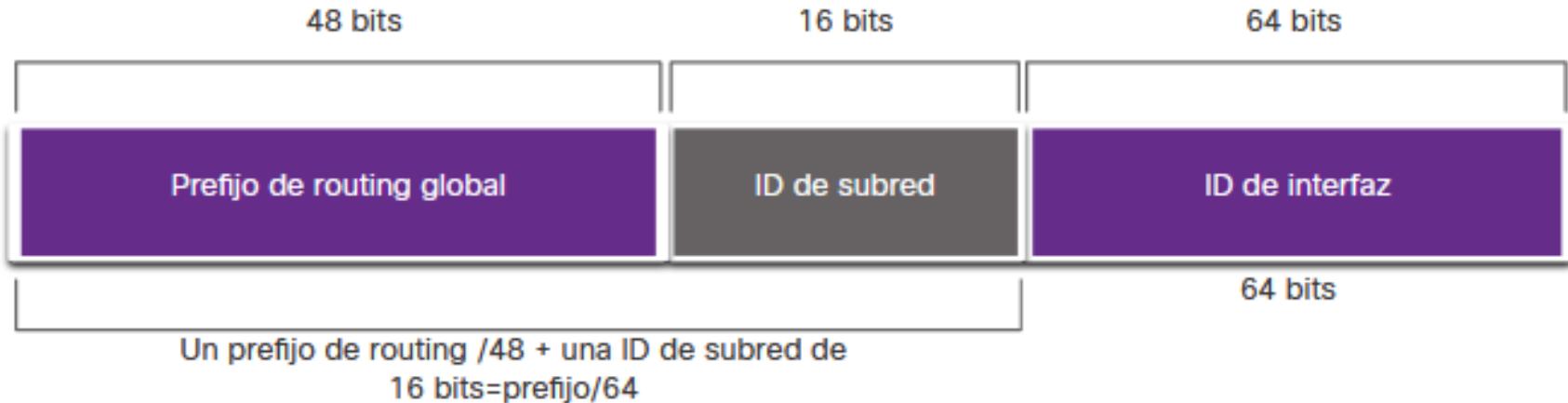
Las direcciones IPv6 unicast globales (GUA) son globalmente únicas y enrutables en Internet IPv6. Estas direcciones son equivalentes a las direcciones IPv4 públicas. La Corporación de Internet para la Asignación de Nombres y Números (ICANN), operador de la IANA, asigna bloques de direcciones IPv6 a los cinco RIR. Actualmente, solo se están asignando GUAs con los primeros tres bits de 001 o 2000 :: / 3.



Tipos de direcciones IPv6

IPv6 GUA

La siguiente figura muestra la **estructura y el rango de una GUA**.



Tipos de direcciones IPv6

Prefijo Global de Enrutamiento

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. Por ejemplo, es común que los ISP asignen un prefijo de enrutamiento global /48 a sus clientes. El prefijo de enrutamiento global suele variar dependiendo de las políticas del ISP.

La dirección IPv6 2001: db8: acad :: / 48 tiene un prefijo de enrutamiento global que indica que los primeros 48 bits (3 hexátes) (2001: db8: acad) es cómo el ISP conoce este prefijo (red).

Tipos de direcciones IPv6

ID de subred

El campo ID de subred es el área entre el Prefijo de enrutamiento global y la ID de interfaz. **A diferencia de IPv4, donde debe tomar prestado bits de la parte del host para crear subredes, IPv6 se diseñó teniendo en cuenta la 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.

La dirección IPv6 de la figura anterior tiene un prefijo de enrutamiento global /48, que es común entre muchas redes empresariales. Esto hace que sea especialmente fácil examinar las diferentes partes de la dirección. Usando una longitud de prefijo / 64 típica, los primeros cuatro hextetos son para la porción de red de la dirección, y **el cuarto hexteto indica la ID de subred.** Los cuatro hextetos restantes son para la ID de interfaz.

Tipos de direcciones IPv6

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. La figura muestra un ejemplo de la estructura de un GUA IPv6. Se recomienda encarecidamente que en la mayoría de los casos se utilicen subredes / 64, lo que crea una ID de interfaz de 64 bits.

Una subred o prefijo /64 (prefijo de enrutamiento global + ID de subred) deja 64 bits para el ID de interfaz. Esto se recomienda para permitir que los dispositivos habilitados para SLAAC creen su propio ID de interfaz de 64 bits. También hace que el desarrollo de un plan de direccionamiento IPv6 sea sencillo y eficaz.

Tipos de direcciones IPv6

IPv6 LLA

Una dirección local de enlace IPv6 (LLA) permite que un dispositivo se comunique con otros dispositivos habilitados para IPv6 en el mismo enlace y solo en ese enlace (subred). Los paquetes con un LLA de origen o destino no se pueden enrutar más allá del enlace desde el que se originó el paquete.

La GUA no es un requisito. Sin embargo, cada interfaz de red habilitada para IPv6 debe tener una LLA.

Tipos de direcciones IPv6

IPv6 LLA

Si un LLA no se configura manualmente en una interfaz, el dispositivo creará automáticamente el suyo sin comunicarse con un servidor DHCP. Los hosts con IPv6 habilitado crean un LLA de IPv6 incluso si el dispositivo no tiene asignada GUA IPv6. Esto permite que los dispositivos con IPv6 habilitado se comuniquen con otros dispositivos con IPv6 habilitado en la misma subred. Esto incluye la comunicación con el gateway predeterminado (router).

Las LLAS IPv6 están en el rango fe80: :/10. /10 indica que los primeros 10 bits son 1111 1110 10xx xxxx. El primer hextet tiene un rango de 1111 1110 1000 0000 (fe80) to 1111 1110 1011 1111 (febf).

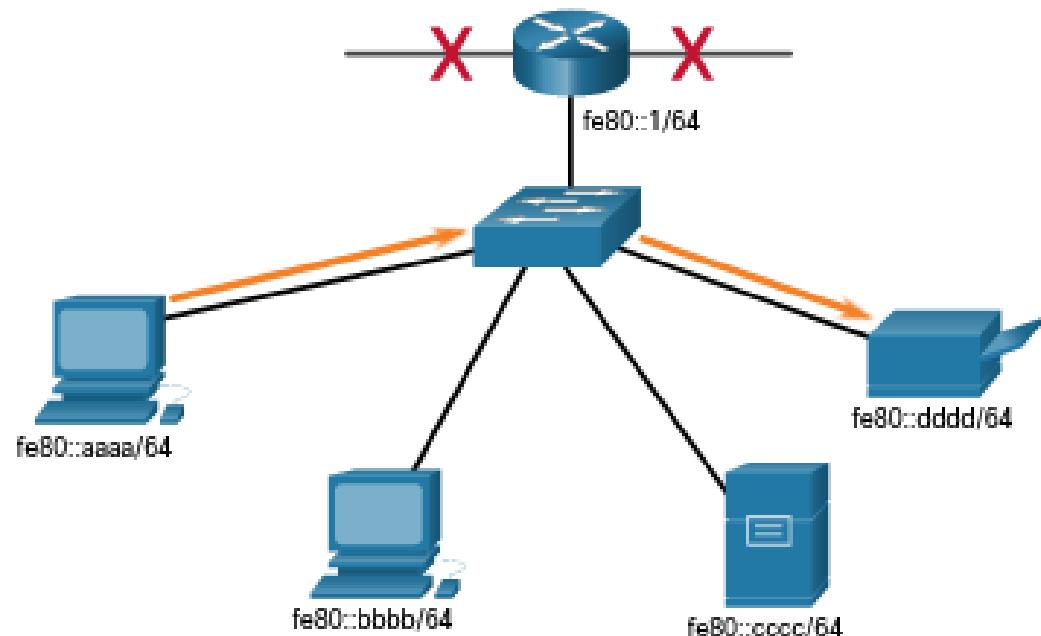
Tipos de direcciones IPv6

IPv6 LLA

Comunicación local entre PC e impresora utilizando LLAs. Las LLAs no son enrutables a Internet.

Paquete IPv6

Dirección IPv6 de origen	Dirección IPv6 de destino
fe80::aaaa	fe80::dddd

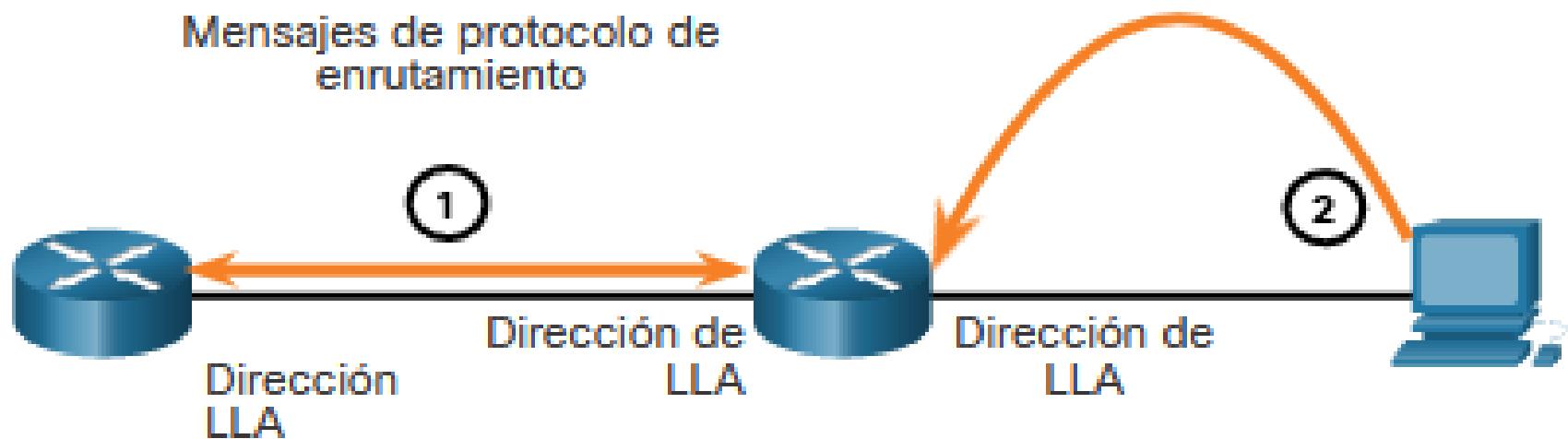


Tipos de direcciones IPv6

IPv6 LLA

Usos de las LLAs en IPv6:

1. Los enrutadores usan el LLA de los enrutadores vecinos para enviar actualizaciones de enrutamiento.
2. Los hosts usan el LLA de un enrutador local como puerta de enlace predeterminada.



Tipos de direcciones IPv6

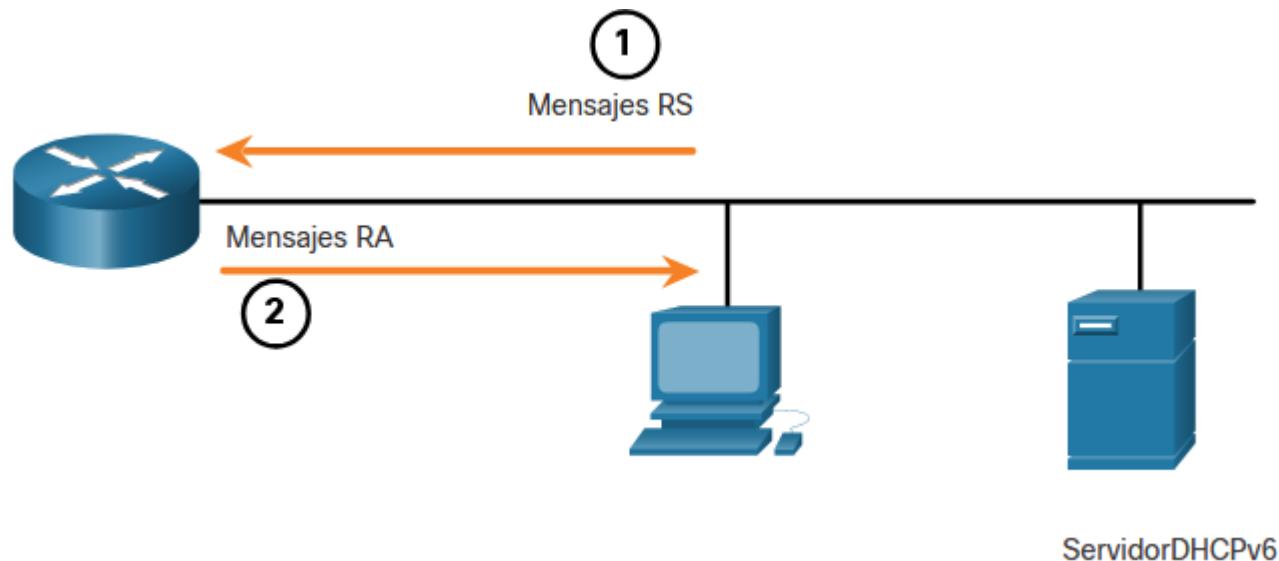
IPv6 LLA

Hay dos maneras en que un dispositivo puede obtener una LLA:

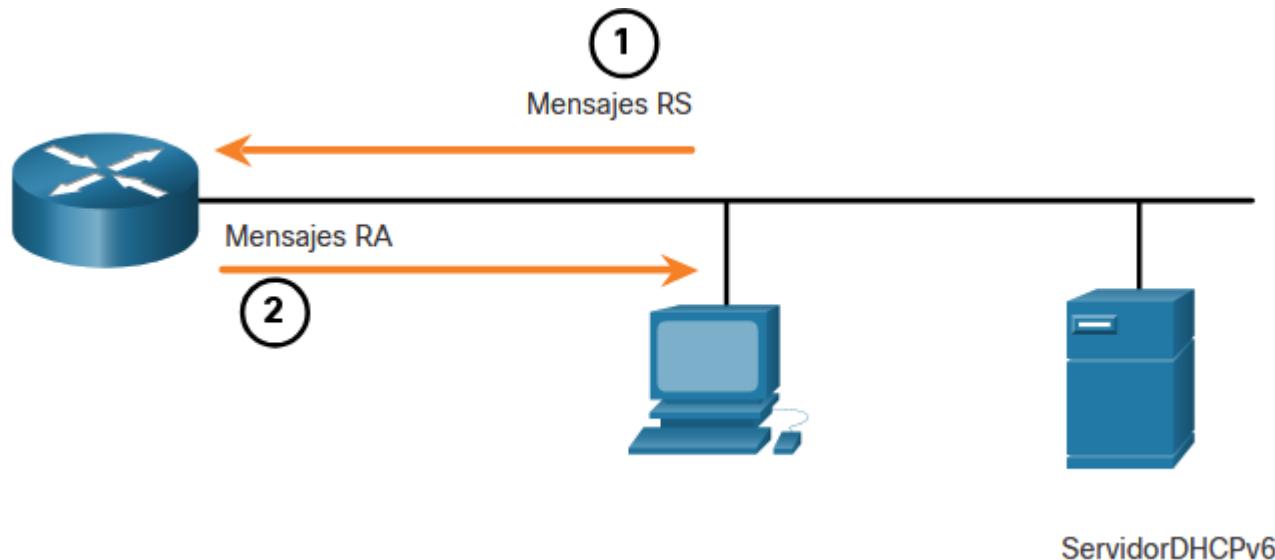
- **Estáticamente** - Esto significa que el dispositivo se ha configurado manualmente.
- **Dinámicamente** - Esto significa que el dispositivo crea su propio ID de interfaz utilizando valores generados aleatoriamente o utilizando el método Identificador único extendido (EUI), que utiliza la dirección MAC del cliente junto con bits adicionales.

Direccionamiento dinámico para GUA IPv6

Para el GUA, un dispositivo obtiene la dirección dinámicamente a través de mensajes del Protocolo de mensajes de control de Internet versión 6 (ICMPv6). Los routers IPv6 envían mensajes RA de ICMPv6 periódicamente, cada **200** segundos, a todos los dispositivos con IPv6 habilitado en la red. También se enviará un mensaje RA en respuesta a un host que envía un mensaje ICMPv6 RS, que es una solicitud de un mensaje RA.



Direccionamiento dinámico para GUA IPv6



1. Los hosts que solicitan información de direccionamiento envían mensajes RS a todos los enrutadores IPv6.
2. Los mensajes RA son enviados a todos los nodos IPv6. Si se utiliza el método 1 (sólo SLAAC), el RA incluye el **prefijo de red**, la **longitud del prefijo** y la **información de la puerta de enlace predeterminada**.

Direccionamiento dinámico para GUA IPv6

El mensaje ICMPv6 **RA** es una **sugerencia** para un dispositivo sobre cómo obtener una **GUA IPv6**. La **decisión** final depende del **sistema operativo del dispositivo**. El mensaje **ICMPv6 RA incluye** lo siguiente:

- **Prefijo de red y longitud del prefijo:** - esto le dice al dispositivo a qué red pertenece.
- **Dirección de puerta de enlace predeterminada:** - es un IPv6 LLA, la dirección IPv6 de origen del mensaje RA.
- **Direcciones DNS y nombre de dominio:** - estas son las direcciones de los servidores DNS y un nombre de dominio.

Direccionamiento dinámico para GUA IPv6

Existen tres métodos para los mensajes de RA:

Method 1: SLAAC - «Tengo todo lo que necesita, incluido el prefijo, la longitud del prefijo y la dirección de la puerta de enlace predeterminada».

Method 2: SLAAC con un servidor DHCPv6 sin estado - "Aquí está mi información, pero necesita obtener otra información, como direcciones DNS, de un servidor DHCPv6 sin estado".

Method 3: DHCPv6 con estado (sin SLAAC) - «Puedo darle su dirección de puerta de enlace predeterminada. Necesita pedir a un servidor DHCPv6 con estado para toda su otra información».

Direccionamiento dinámico para GUA IPv6

SLAAC

SLAAC es un método que permite a un dispositivo **crear su propio GUA sin los servicios de DHCPv6**. Usando SLAAC, los dispositivos confían en los mensajes ICMPv6 RA del enrutador local para obtener la información necesaria.

Por defecto, el mensaje RA sugiere que el dispositivo receptor use la información en el mensaje RA para crear su propia GUA IPv6 y toda la otra información necesaria. No se requieren los servicios de un servidor DHCPv6.

Direccionamiento dinámico para GUA IPv6

SLAAC

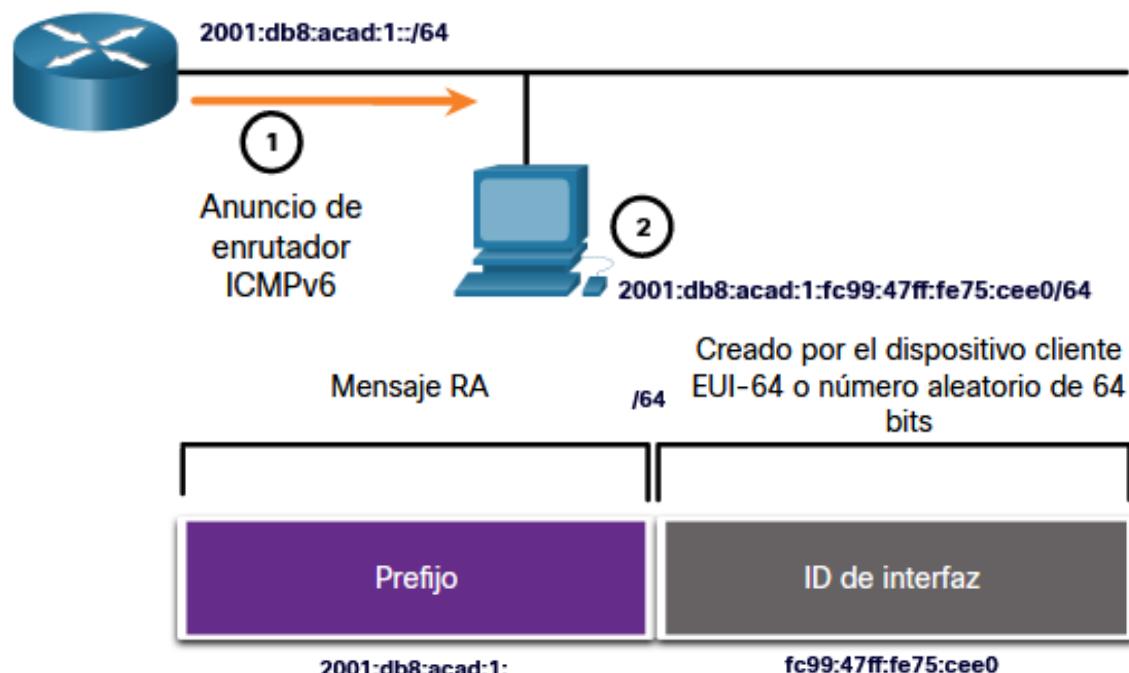
SLAAC no tiene estado, lo que significa que no hay un servidor central (por ejemplo, un servidor DHCPv6 con estado) **que asigne GUA y mantenga una lista de dispositivos y sus direcciones.** Con SLAAC, el dispositivo cliente usa la información en el mensaje RA para crear su propia GUA. Las dos partes de la dirección se crean de la siguiente manera:

- **Prefijo** - se anuncia en el mensaje RA.
- **ID de interfaz** - utiliza el proceso EUI-64 o genera un número aleatorio de 64 bits, según el sistema operativo del dispositivo.

Direccionamiento dinámico para GUA IPv6

SLAAC

1. El enrutador envía un mensaje RA con el prefijo para el enlace local.
2. La PC usa SLAAC para obtener un prefijo del mensaje RA y crea su propia ID de interfaz.



Direccionamiento dinámico para GUA IPv6

SLAAC + DHCPv6 SIN estado

Se puede configurar una interfaz de enrutador para enviar un anuncio de enrutador utilizando **SLAAC y DHCPv6 sin estado**.

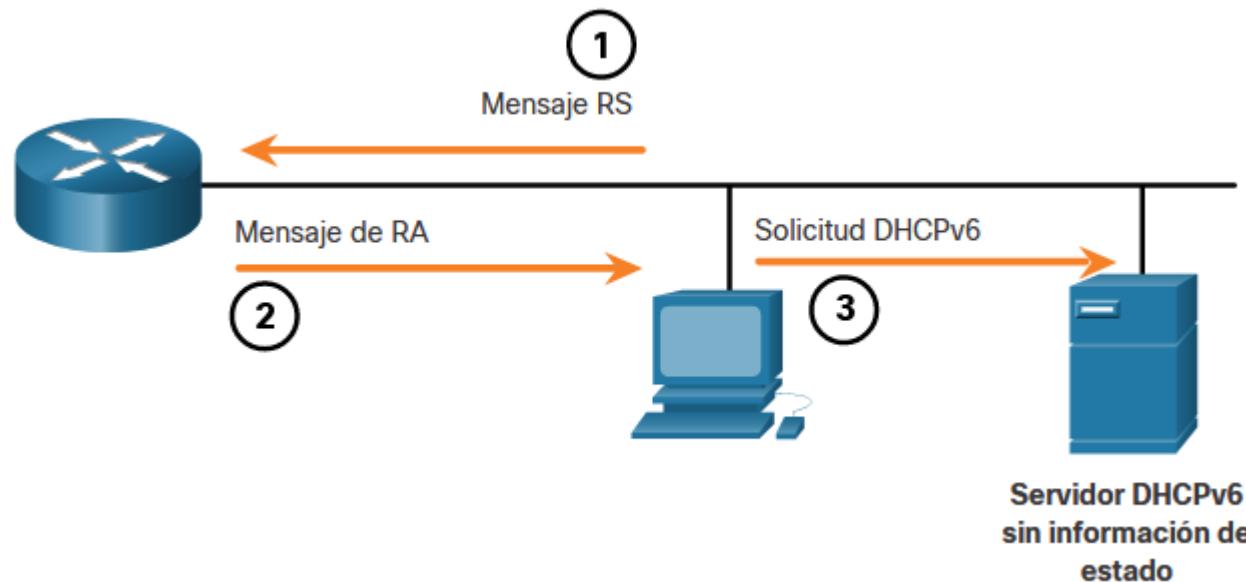
El mensaje RA sugiere que los dispositivos utilicen lo siguiente:

- SLAAC para crear su propio IPv6 GUA
- La dirección link-local del router, la dirección IPv6 de origen del RA para la dirección de gateway predeterminado
- Un servidor DHCPv6 stateless, que obtendrá otra información como la dirección del servidor DNS y el nombre de dominio

Direccionamiento dinámico para GUA IPv6

SLAAC + DHCPv6 SIN estado

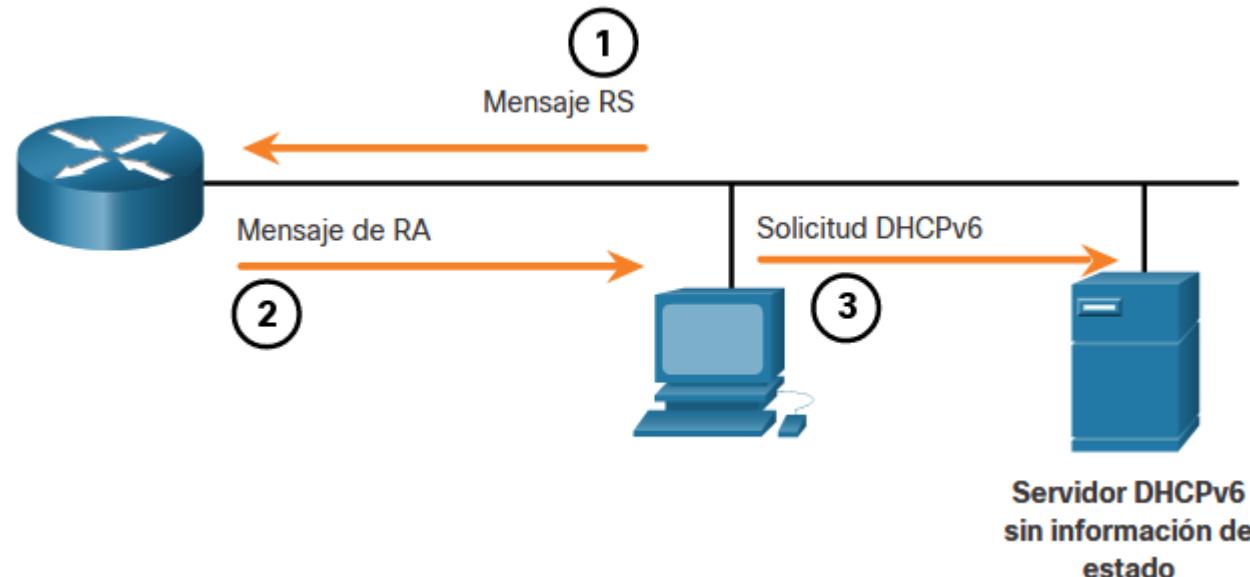
1. El PC envía un RS a todos los enrutadores IPv6, «Necesito información de direccionamiento».



Direccionamiento dinámico para GUA IPv6

SLAAC + DHCPv6 SIN estado

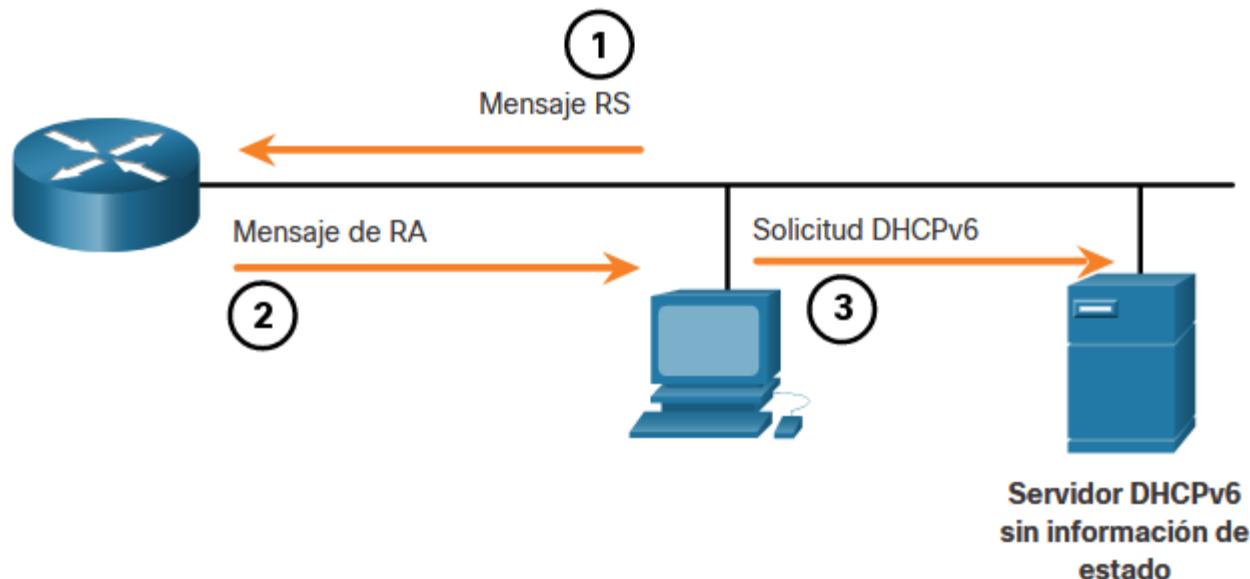
2. El enrutador envía un mensaje RA a todos los nodos IPv6 con el Método 2 (SLAAC y DHCPv6) especificado. “Aquí está la información de su prefijo, longitud de prefijo y puerta de enlace predeterminada. Pero tendrá que obtener información DNS de un servidor DHCPv6».



Direccionamiento dinámico para GUA IPv6

SLAAC + DHCPv6 SIN estado

3. El PC envía un mensaje de solicitud DHCPv6 a todos los servidores DHCPv6. «Utilicé SLAAC para crear mi dirección IPv6 y obtener mi dirección de puerta de enlace predeterminada, pero necesito otra información de un servidor DHCPv6 sin estado.»



Direccionamiento dinámico para GUA IPv6

DHCPv6 CON estado

Una interfaz de router se puede configurar para enviar una RA usando **DHCPv6 con estado** solamente.

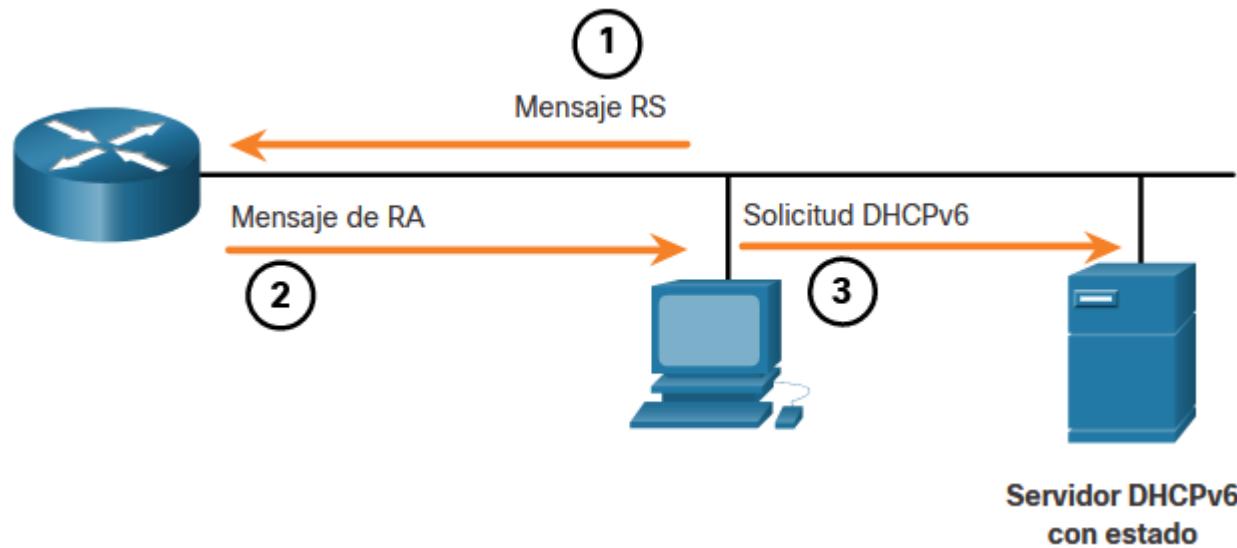
DHCPv6 con información de estado es **similar a DHCP para IPv4**. Un dispositivo puede recibir automáticamente su información de direccionamiento, incluida una GUA, la longitud del prefijo y las direcciones de los servidores DNS de un servidor DHCPv6 con estado.

Direccionamiento dinámico para GUA IPv6

DHCPv6 CON estado

El mensaje RA sugiere que los dispositivos usen lo siguiente:

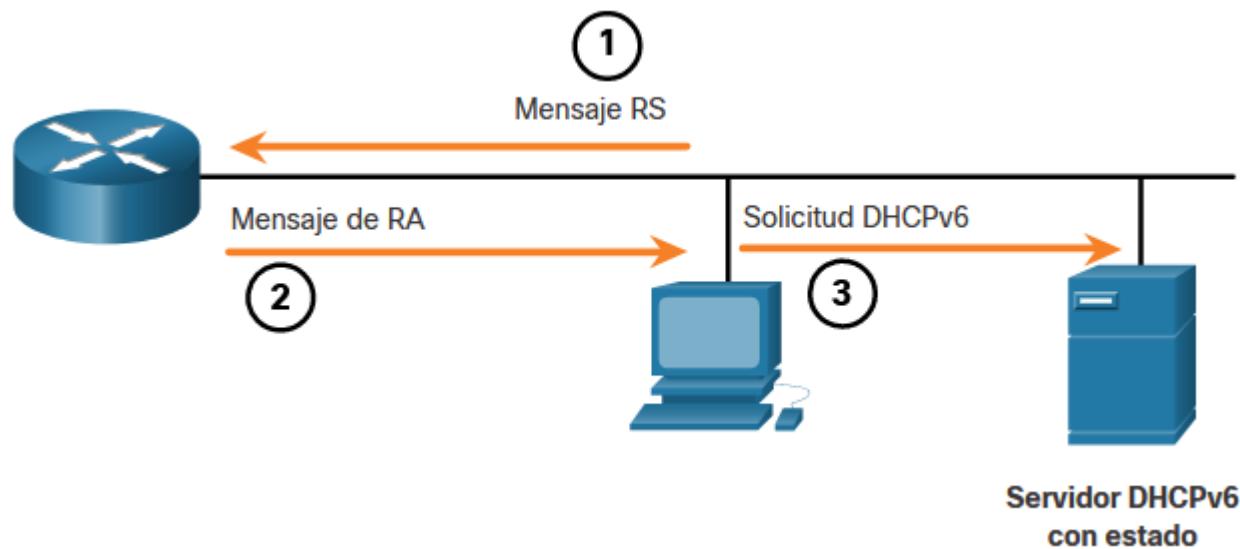
- La dirección LLA del router, que es la dirección IPv6 de origen del RA, para la dirección de gateway predeterminado
- Un servidor DHCPv6 Stateful, para obtener una GUA, otra información como la dirección del servidor DNS y el nombre de dominio.



Direccionamiento dinámico para GUA IPv6

DHCPv6 CON estado

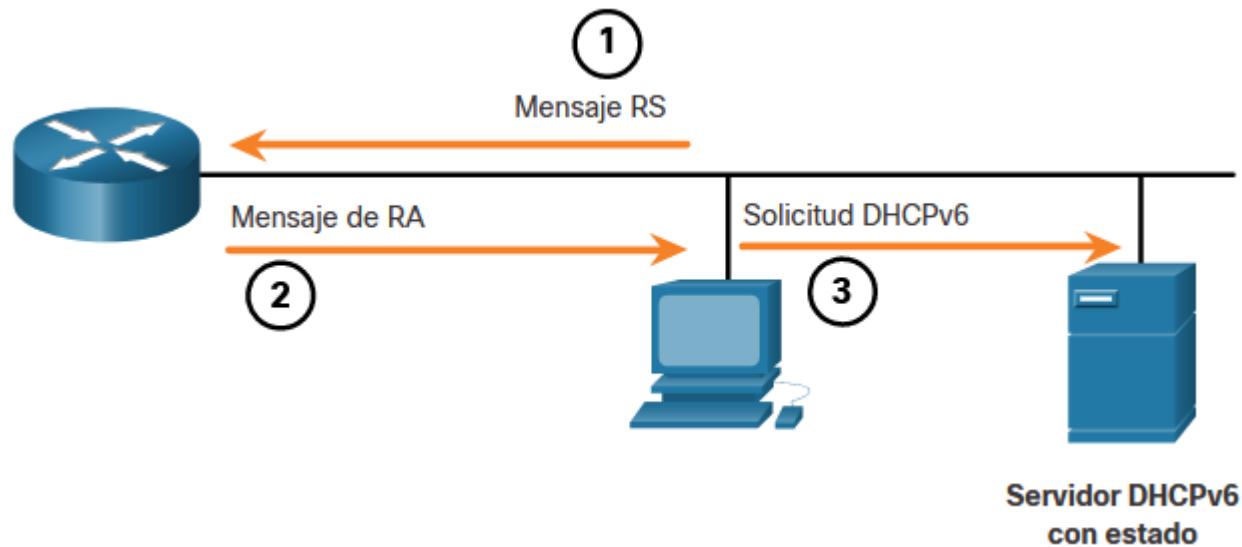
1. La PC envía un RS a todos los enrutadores IPv6, "Necesito información de direccionamiento".



Direccionamiento dinámico para GUA IPv6

DHCPv6 CON estado

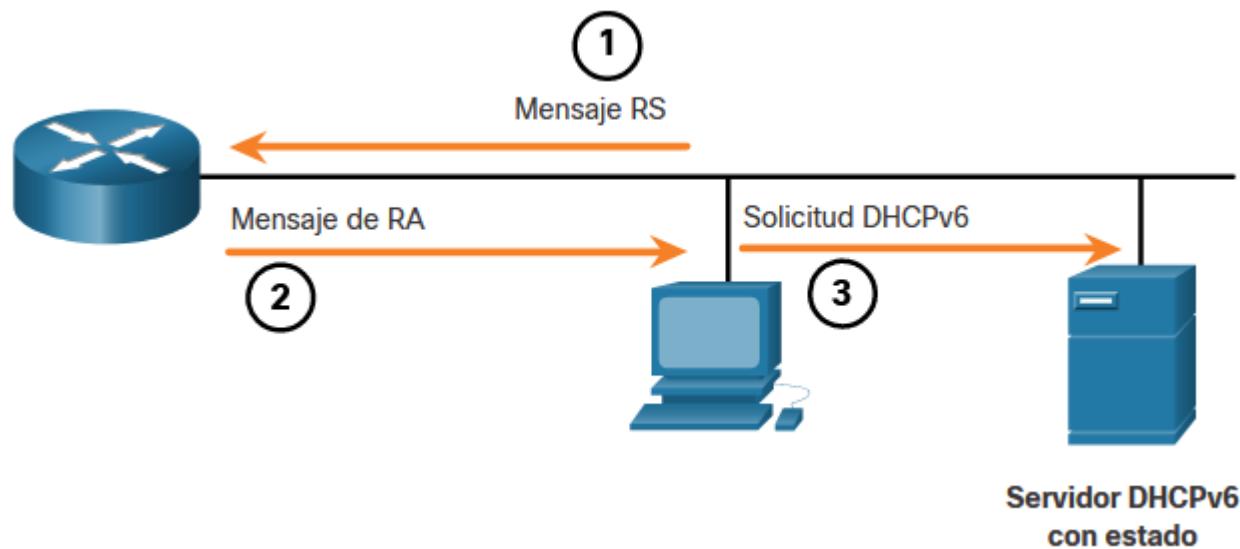
2. El enrutador envía un mensaje RA a todos los nodos IPv6 con el Método 3 (DHCPv6 con estado) especificado: "Soy su puerta de enlace predeterminada, pero debe pedirle a un servidor DHCPv6 con estado su dirección IPv6 y otra información de direccionamiento".



Direccionamiento dinámico para GUA IPv6

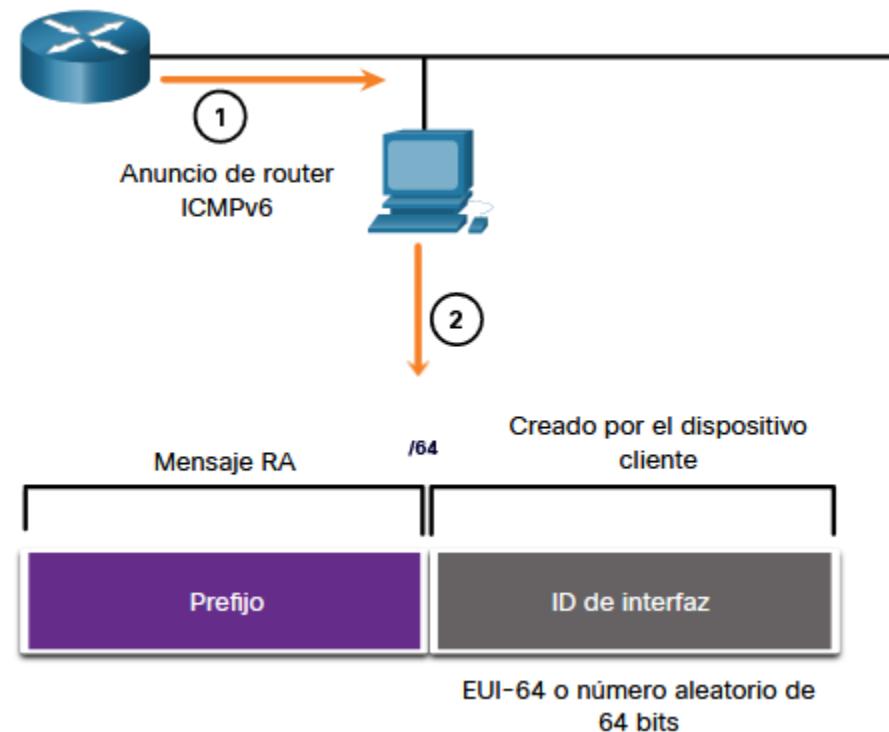
DHCPv6 CON estado

3. La PC envía un mensaje de solicitud de DHCPv6 a todos los servidores DHCPv6, "Recibí mi dirección de puerta de enlace predeterminada del mensaje RA, pero **necesito una dirección IPv6 y toda otra información de direccionamiento de un servidor DHCPv6 con estado**".



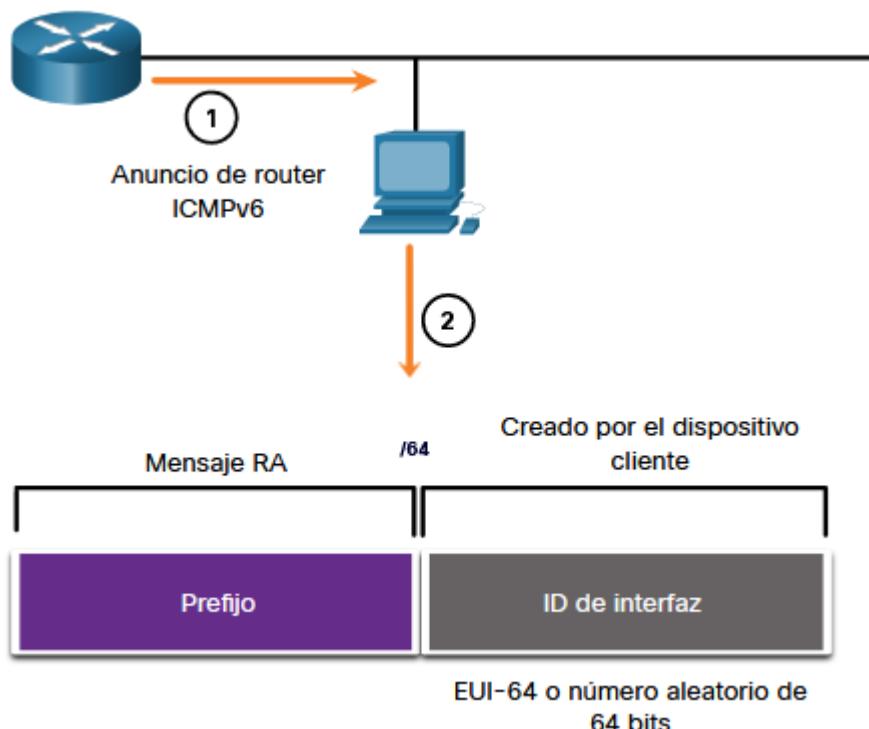
EUI64 vs aleatorio

Cuando el mensaje RA es SLAAC o SLAAC + DHCPv6 **sin estado**, el cliente debe generar su propia ID de interfaz. El cliente conoce la parte del prefijo de la dirección del mensaje RA, pero debe crear su propia ID de interfaz. El ID de la interfaz se puede crear utilizando el proceso **EUI-64** o un número de 64 bits generado aleatoriamente.



EUI64 vs aleatorio

1. El enrutador envía un mensaje RA.
2. El PC utiliza el prefijo del mensaje RA y utiliza EUI-64 o un número aleatorio de 64 bits para generar un ID de interfaz.



Proceso EUI64

El IEEE definió el identificador único extendido (EUI) o proceso **EUI-64** modificado. Este proceso **utiliza la dirección MAC Ethernet de 48 bits de un cliente e inserta otros 16 bits en el 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:

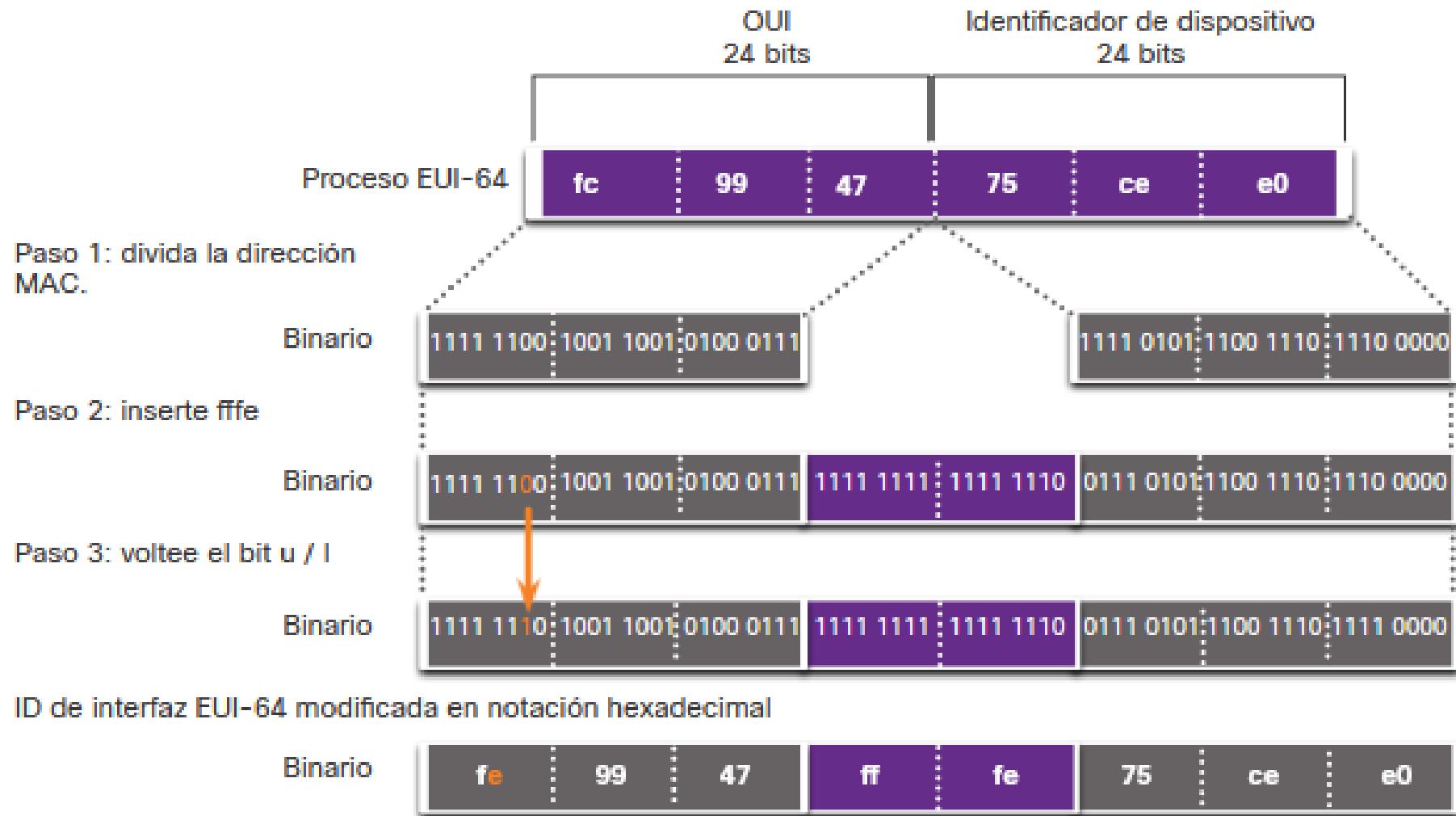
- **Identificador único organizativo (OUI)** - el OUI es un código de proveedor de 24 bits (6 dígitos hexadecimales) asignado por IEEE.
- **Identificador del dispositivo** - el identificador del dispositivo es un valor único de 24 bits (6 dígitos hexadecimales) dentro de una OUI común.

Proceso EUI64

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.
- El valor insertado de 16 bits fffe (en hexadecimal).
- Identificador de dispositivo de 24 bits de la dirección MAC del cliente.

Proceso EUI64



Proceso EUI64

El resultado de ejemplo del **ipconfig** comando muestra el GUA IPv6 que se crea dinámicamente mediante SLAAC y el proceso EUI-64. Una manera fácil de identificar que una dirección probablemente se creó usando EUI-64 es **ffffe** ubicarse en el medio de la ID de la interfaz.

```
C:\> ipconfig
Windows IP Configuration
Conexión de área local del adaptador Ethernet:
  Sufijo de conexión específica DNS. :
  IPv6 Address . . . . . : 2001:db8:acad:1:fc 99:47ff:fe75:cee0
  Link-local IPv6 Address . . . . : fe80::fc 99:47ff:fe75:cee0
  Default Gateway . . . . . : fe80::1
C:\>
```

Generación aleatoria

Dependiendo del sistema operativo, un dispositivo puede usar una ID de interfaz generada aleatoriamente en lugar de usar la dirección MAC y el proceso EUI-64. A partir de Windows Vista, Windows utiliza una ID de interfaz generada aleatoriamente en lugar de una creada con EUI-64. Windows XP y los sistemas operativos Windows anteriores utilizaban EUI-64.

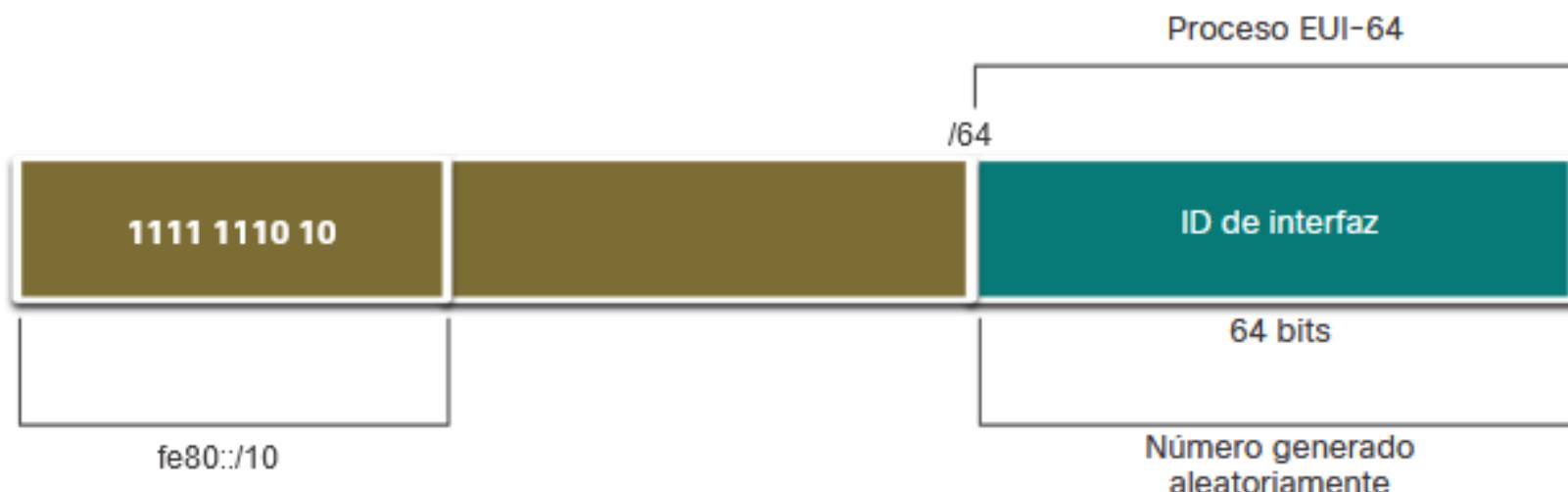
Una vez establecida la ID de la interfaz, ya sea a través del proceso EUI-64 o mediante la generación aleatoria, se puede combinar con un prefijo IPv6 en el mensaje RA para crear una GUA.

```
C:\> 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
C:\>
```

Direccionamiento dinámico para LLA IPv6

Todos los dispositivos IPv6 deben tener una LLA IPv6. Al igual que IPv6 GUA, también puede crearlas dinámicamente.

La LLA se crea dinámicamente usando el **prefijo fe80 :: / 10** y la **ID de interfaz** usando el proceso EUI-64, o un **número de 64 bits generado aleatoriamente**.



Direcciones IPv6 de multidifusión

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 de multidifusión IPv6 tienen el prefijo ff00 :: / 8.

Existen dos tipos de direcciones IPv6 de multidifusión:

- Direcciones de multidifusión conocidas
- Direcciones de multidifusión de nodo solicitadas

Direcciones IPv6 de multidifusión

Direcciones de multidifusión bien conocidas

Se asignan direcciones de multidifusión IPv6 conocidas. Estos son dos grupos de multidifusión asignados por IPv6 comunes:

- **ff02::1 Grupo de multidifusión de todos los nodos** - este es un grupo de multidifusión al que **se unen todos los dispositivos con IPv6**. 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**. Ejemplo de comunicación mediante la dirección de multidifusión de todos los nodos: un enrutador IPv6 envía mensajes RA ICMPv6 al grupo de multidifusión de todos los nodos.

Direcciones IPv6 de multidifusión

Direcciones de multidifusión bien conocidas

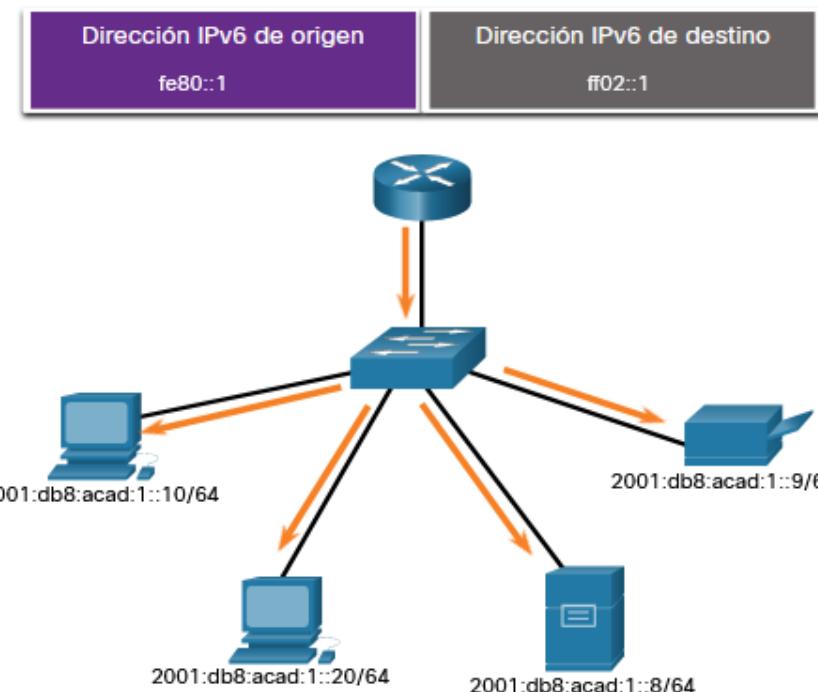
Se asignan direcciones de multidifusión IPv6 conocidas. Estos son dos grupos de multidifusión asignados por IPv6 comunes:

- **ff02:: 2 Grupo multidifusión de todos los enrutadores** - Este es un grupo multicast al que se unen **todos los routers con IPv6 habilitado**. 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.

Direcciones IPv6 de multidifusión

Direcciones de multidifusión bien conocidas

Los dispositivos habilitados para IPv6 envían mensajes ICMPv6 RS a la dirección de multidifusión de todos los enrutadores. El mensaje RS solicita un mensaje RA del router IPv6 para contribuir a la configuración de direcciones del dispositivo.
El enrutador IPv6 responde con un mensaje RA.



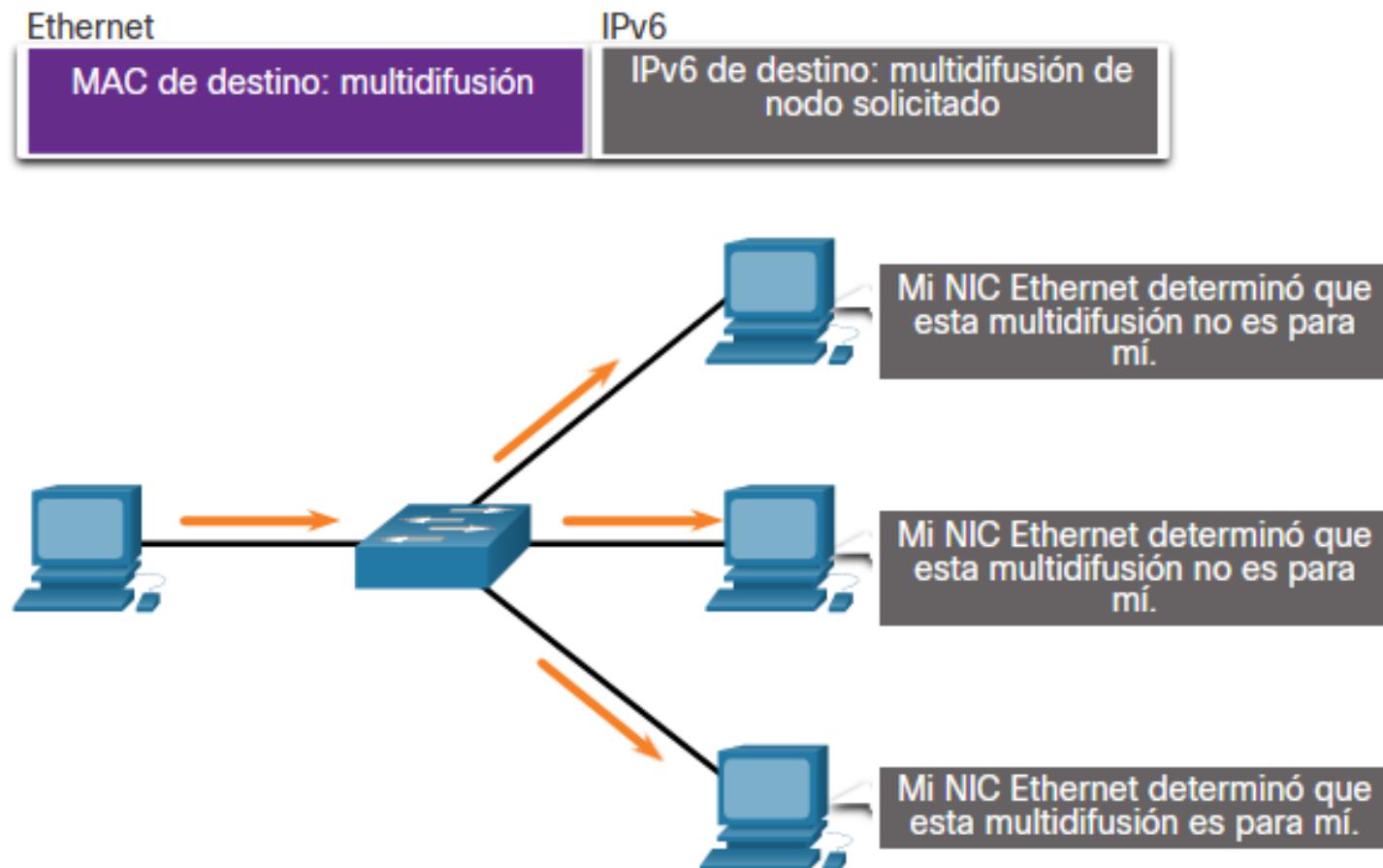
Direcciones IPv6 de multidifusión

Direcciones 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 la trama 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.

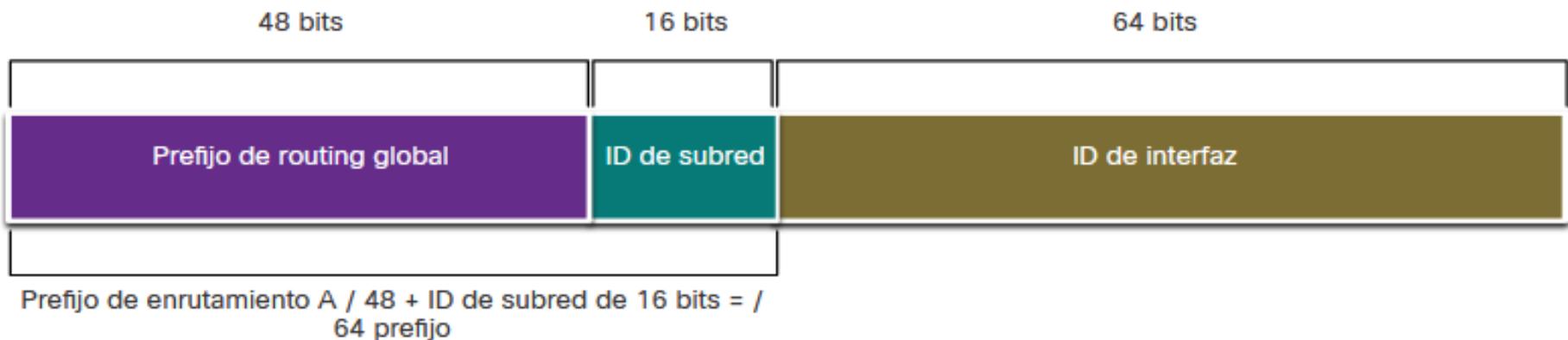
Direcciones IPv6 de multidifusión

Direcciones de multidifusión de nodo solicitado



Subnetting en IPv6

Recordemos que con IPv4, debemos tomar prestados bits de la parte del host para crear subredes. Esto se debe a que la subred fue una idea tardía con IPv4. Sin embargo, IPv6 se diseñó teniendo en cuenta las subredes. Se utiliza un campo ID de subred independiente en IPv6 GUA para crear subredes.



Subnetting en IPv6

La ventaja de una dirección de 128 bits es que puede admitir más que suficientes subredes y hosts por subred, para cada red. **La conservación de direcciones no es un problema.** Por ejemplo, si el prefijo de enrutamiento global es /48, y utilizando un típico 64 bits para el ID de interfaz, esto creará un ID de subred de 16 bits:

- **ID de subred de 16 bits** - crea hasta 65.536 subredes.
- **ID de interfaz de 64 bits** - admite hasta 18 quintillones de direcciones IPv6 de host por subred (es decir, 18,000,000,000,000,000).

Subnetting en IPv6

La división en subredes IPv6 también es más fácil de implementar que la IPv4, ya que no se requiere la conversión al sistema binario. Para determinar la siguiente subred disponible, simplemente se suman los valores en el sistema hexadecimal.

Subnetting en IPv6

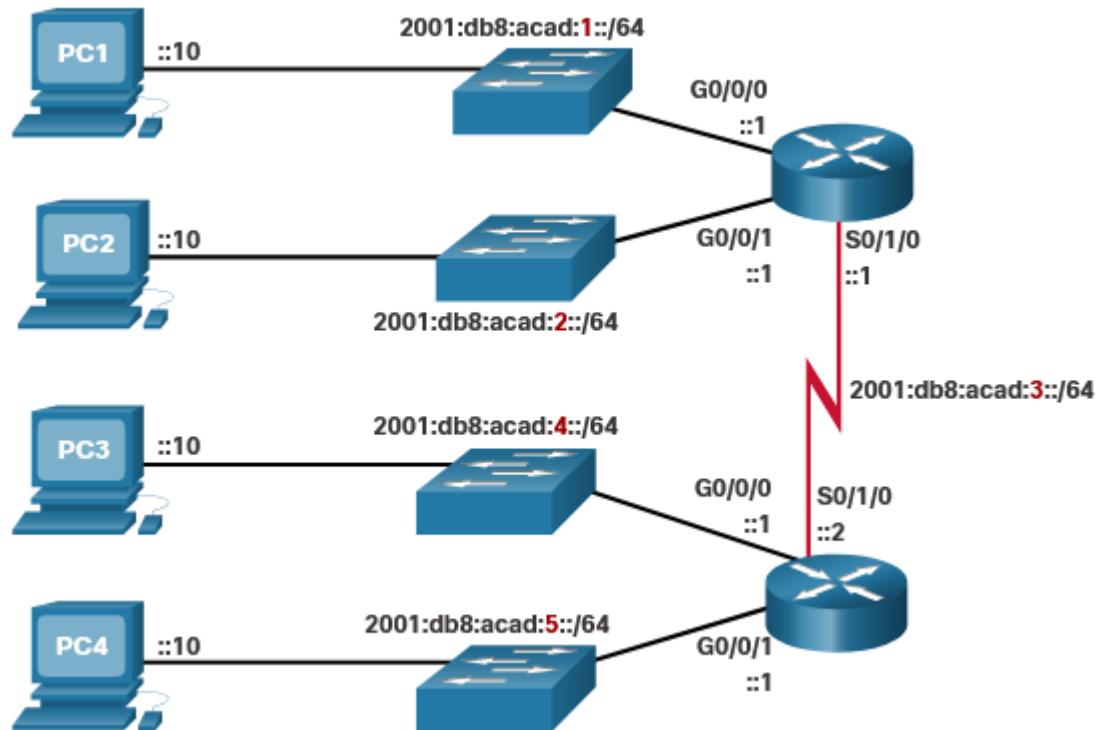
Supongamos que a una organización se le ha asignado el **prefijo** de enrutamiento global **2001: db8: acad :: / 48** con una **ID de subred de 16 bits**. Esto permitiría crear 65.536 / 64 subredes.

Aumentar ID de subred para crear
65,536 subredes

2001:db8:acad:0000::/64
2001:db8:acad:0001::/64
2001:db8:acad:0002::/64
2001:db8:acad:0003::/64
2001:db8:acad:0004::/64
2001:db8:acad:0005::/64
2001:db8:acad:0006::/64
2001:db8:acad:0007::/64
2001:db8:acad:0008::/64
2001:db8:acad:0009::/64
2001:db8:acad:000a::/64
2001:db8:acad:000b::/64
2001:db8:acad:000c::/64
Las subredes 13 a 65,534 no se muestran.
2001:db8:acad:ffff::/64

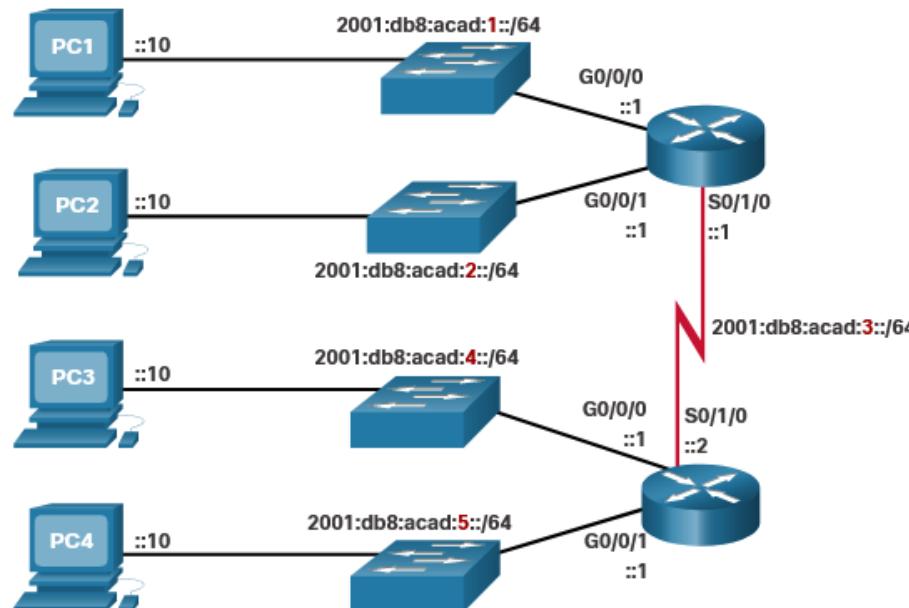
Subnetting en IPv6

Con más de 65.536 subredes para elegir, la tarea del administrador de la red es diseñar un esquema lógico para abordar la red.



Subnetting en IPv6

La topología de ejemplo requiere **cinco subredes**, una para cada LAN, así como para el enlace serie entre R1 y R2. A diferencia del ejemplo de IPv4, **con IPv6 la subred de enlace serie tendrá la misma longitud de prefijo que las LAN**. Aunque esto puede parecer "desperdiciar" direcciones, **la conservación de direcciones no es una preocupación cuando se utiliza IPv6**.



Subnetting en IPv6

Se han asignado las cinco subredes IPv6, con el campo ID de subred 0001 a 0005 utilizado para este ejemplo. Cada subred /64 proporcionará más direcciones de las que jamás se necesitarán.

Bloque de direcciones: 2001:0 db8:acad::/48

Cinco subredes asignadas a partir de
65 536 subredes disponibles



2001:db8:acad:**0000**::/64
2001:db8:acad:**0001**::/64
2001:db8:acad:**0002**::/64
2001:db8:acad:**0003**::/64
2001:db8:acad:**0004**::/64
2001:db8:acad:**0005**::/64
2001:db8:acad:**0006**::/64
2001:db8:acad:**0007**::/64
2001:db8:acad:**0008**::/64

2001:db8:acad:**ffff**::/64

11 ICMPv6

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 mensajes nuevos como parte del protocolo de detección de vecino (ND o NDP).

ICMPv6

Los mensajes entre un enrutador IPv6 y un dispositivo IPv6, incluida la **asignación dinámica de direcciones**, son los siguientes:

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

Los mensajes entre dispositivos IPv6, incluida la **detección de direcciones duplicadas y la resolución de direcciones**, son los siguientes:

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

ICMPv6

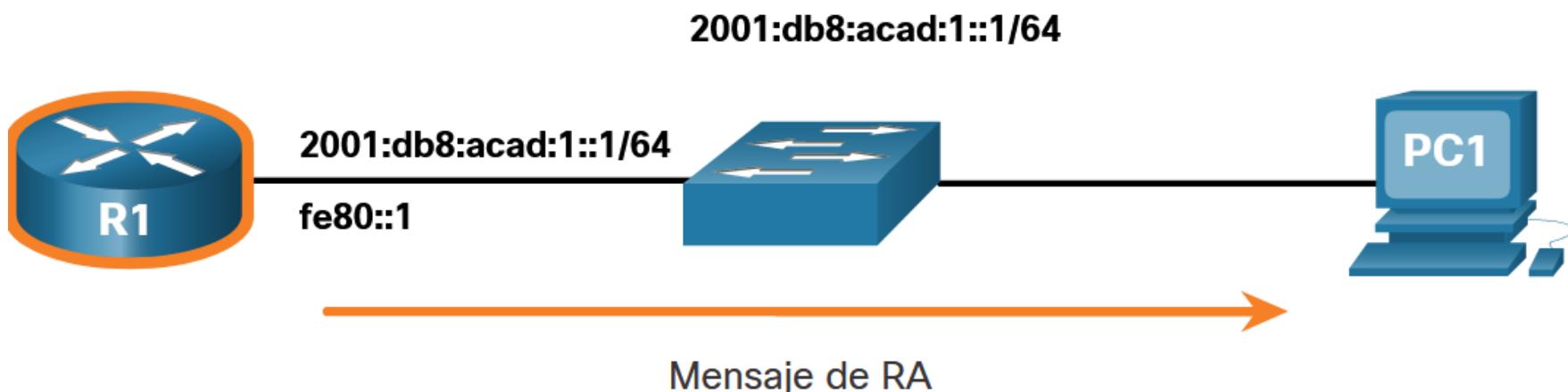
Mensaje de RA

Los enrutadores habilitados para IPv6 envían mensajes de RA cada 200 segundos para **proporcionar información de direccionamiento a los hosts habilitados para IPv6**. El mensaje 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 host que utiliza la Configuración automática de direcciones sin estado (SLAAC) establecerá su puerta de enlace predeterminada en la dirección de enlace local del enrutador que envió el RA.

ICMPv6

Mensaje de RA

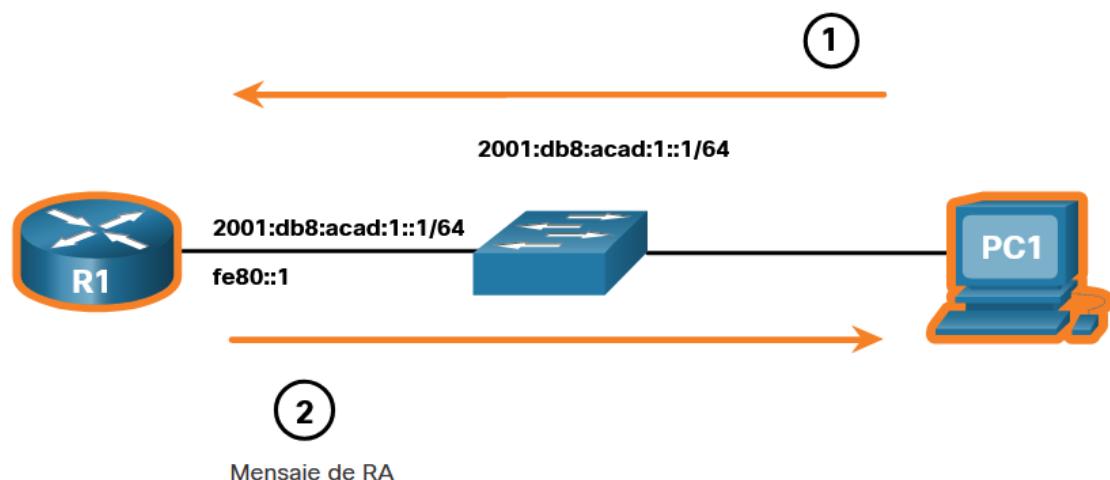
R1 envía un mensaje de RA, «Hola a todos los dispositivos habilitados para IPv6. Soy R1 y puedes usar SLAAC para crear una dirección de unidifusión global IPv6. El prefijo es 2001:db8:acad:1::/64. Por cierto, use mi dirección local de enlace fe80::1 como su puerta de enlace predeterminada.



ICMPv6

Mensaje de RS

Un router habilitado para IPv6 también enviará un mensaje RA en respuesta a un mensaje RS. En la figura, PC1 envía un mensaje RS para determinar cómo recibir dinámicamente su información de dirección IPv6.



ICMPv6

Mensaje de RS

R1 responde a la RS con un mensaje de RA.

1. PC1 envía un mensaje RS, «Hola, acabo de arrancar. ¿Hay un enrutador IPv6 en la red? Necesito saber cómo obtener la información de mi dirección IPv6 de forma dinámica».
2. R1 responde con un mensaje de RA. «Hola a todos los dispositivos habilitados para IPv6. Soy R1 y puedes usar SLAAC para crear una dirección de unidifusión global IPv6. El prefijo es 2001:db8:acad:1: :/64. Por cierto, use mi dirección local de enlace fe80: :1 como su puerta de enlace predeterminada. «

ICMPv6

Mensaje de NS

Cuando a un dispositivo se le asigna una dirección de unidifusión global IPv6 o unidifusión local de enlace, puede realizar una detección de dirección duplicada (DAD) para garantizar que la dirección IPv6 sea **única**. Para verificar la unicidad de una dirección, el dispositivo enviará un mensaje NS con su propia dirección IPv6 como la dirección IPv6 objetivo.

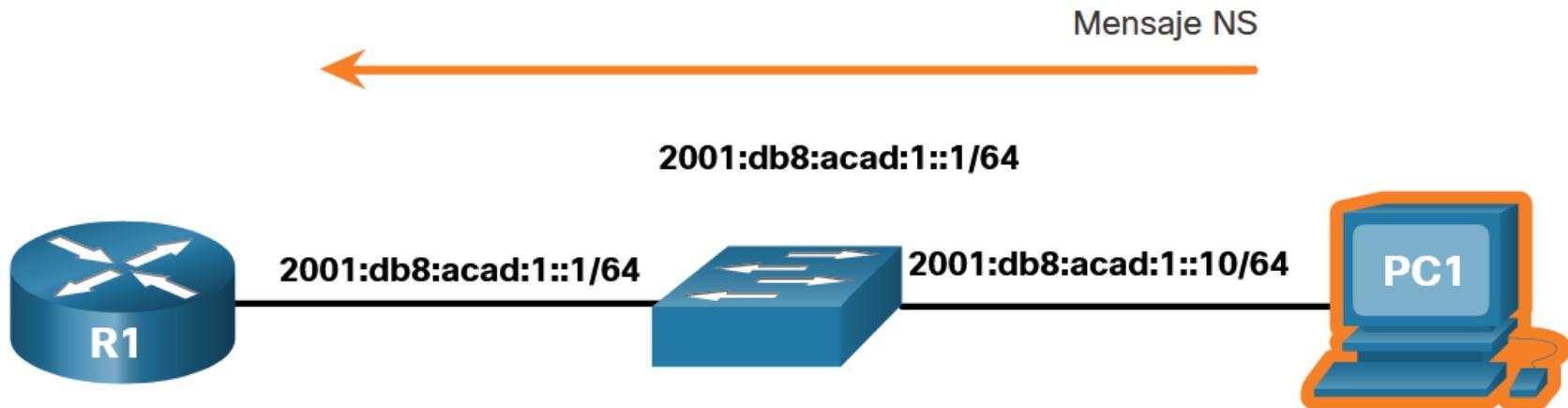
Si otro dispositivo de la red tiene esta dirección, responde con un mensaje NA. Este mensaje NA notifica al dispositivo emisor que la dirección está en uso. Si no se devuelve un mensaje NA correspondiente dentro de un cierto período de tiempo, la dirección de unidifusión es única y aceptable para su uso.

ICMPv6

Mensaje de NS

PC1 envía un mensaje NS para comprobar la singularidad de una dirección, «¿Quién tiene la dirección IPv6 2001:db8:acad:1::10, me enviará su dirección MAC? «

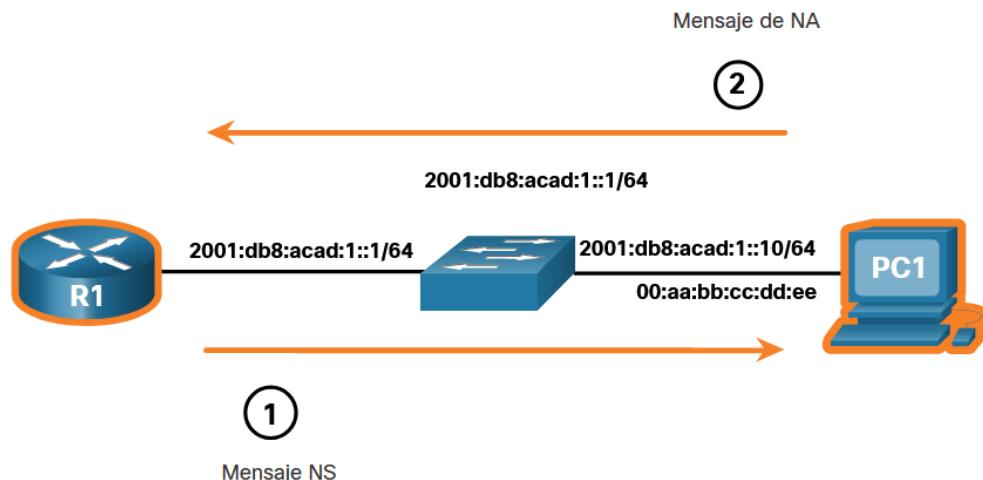
.



ICMPv6

Mensaje de NA

La resolución de direcciones se utiliza cuando un dispositivo en la LAN conoce la dirección IPv6 de unidifusión 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.

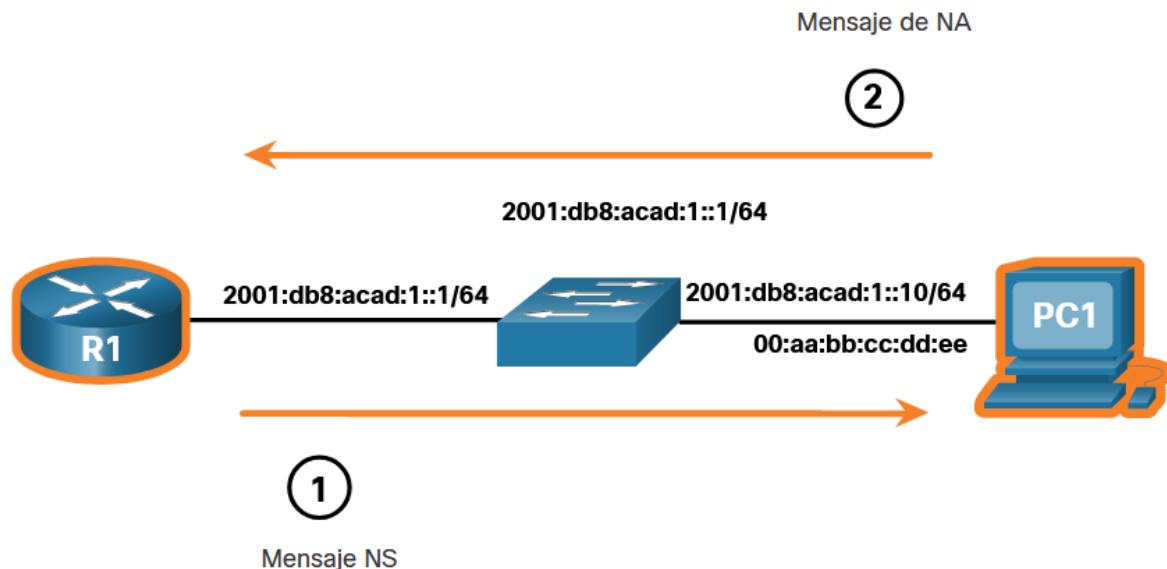


ICMPv6

Mensaje de NA

R1 envía un mensaje NS de resolución de dirección. "¿Quien tenga la dirección IPv6 2001: db8: acad: 1 :: 10, me enviará su dirección MAC?"

PC1 responde con un mensaje NA. «Soy 2001:db8:acad:1: :10 y mi dirección MAC es 00:aa:bb:cc:dd:ee. »



Gracias por la atenshion!

