

Redes



Manual

Vol. 2 (Capa 3 Modelo OSI)



ALHUBO

Alejandro Huerta Bolaños

Primera Edición

2023

Índice

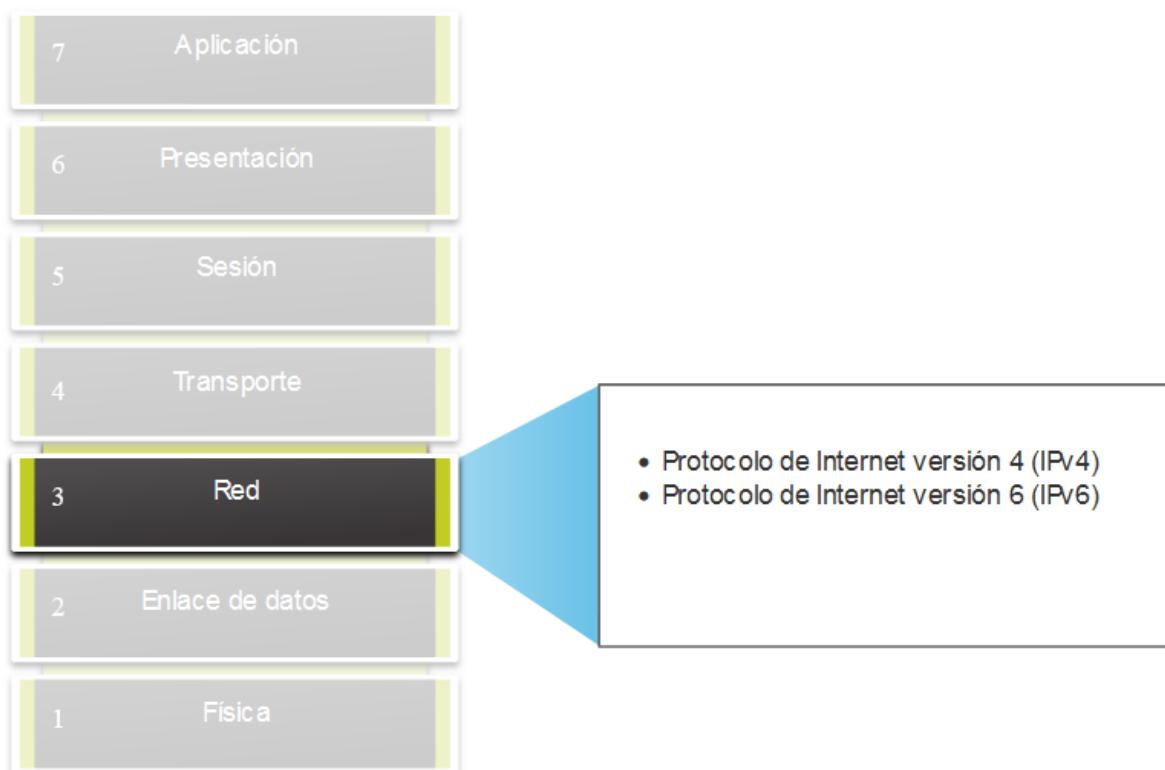
Índice	1
La capa de red	2
Encapsulación IP	5
Características de IP	6
Sin conexión	7
Mejor esfuerzo	7
Independiente de los medios	7
Paquete IPv4	9
Encabezado de paquetes IPv4	9
Campos de encabezado de paquete IPv4	9
Paquete IPv6	11
Limitaciones de IPv4	11
Las mejoras que ofrece IPv6 incluyen las siguientes:	12
Campos de encabezado de paquete IPv4 en el encabezado de paquete IPv6	12
Encabezado de paquetes IPv4	13
Encabezado de paquetes IPv6	14
La decisión de reenvío de host	15
MAC e IP	16
Destino en la misma red	16
Destino en una red remota	17
Descripción general de ARP	18
Funciones del ARP	20
Solicitud de ARP	21
Respuesta de ARP	22
Rol ARP en Comunicaciones Remotas	23
Eliminación de entradas de una tabla ARP	23
Problemas de ARP - Difusión ARP y suplantación ARP	24
Detección de vecinos IPv6	26
Mensajes de descubrimiento de vecinos IPv6	33
Descubrimiento de vecinos IPv6: resolución de direcciones	34
Mensajes ICMPv4 e ICMPv6	35
Accesibilidad al host	35
Destino o servicio inaccesible	36
Tiempo excedido	37
Mensajes ICMPv6	37
Mensaje RA	38
Mensaje RS	38
Mensaje NS	39
Mensaje NA	40
Ping: Prueba de Conectividad	40
Hacer ping al loopback	41

Hacer ping al gateway predeterminado	42
Hacer ping a un Host Remoto	43
Traceroute: Prueba el Camino	45

Nota [Este volumen solo abarca el funcionamiento de la capa 3 del modelo OSI.]

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. Como se muestra en la figura, IP versión 4 (**IPv4**) e IP versión 6 (**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**).

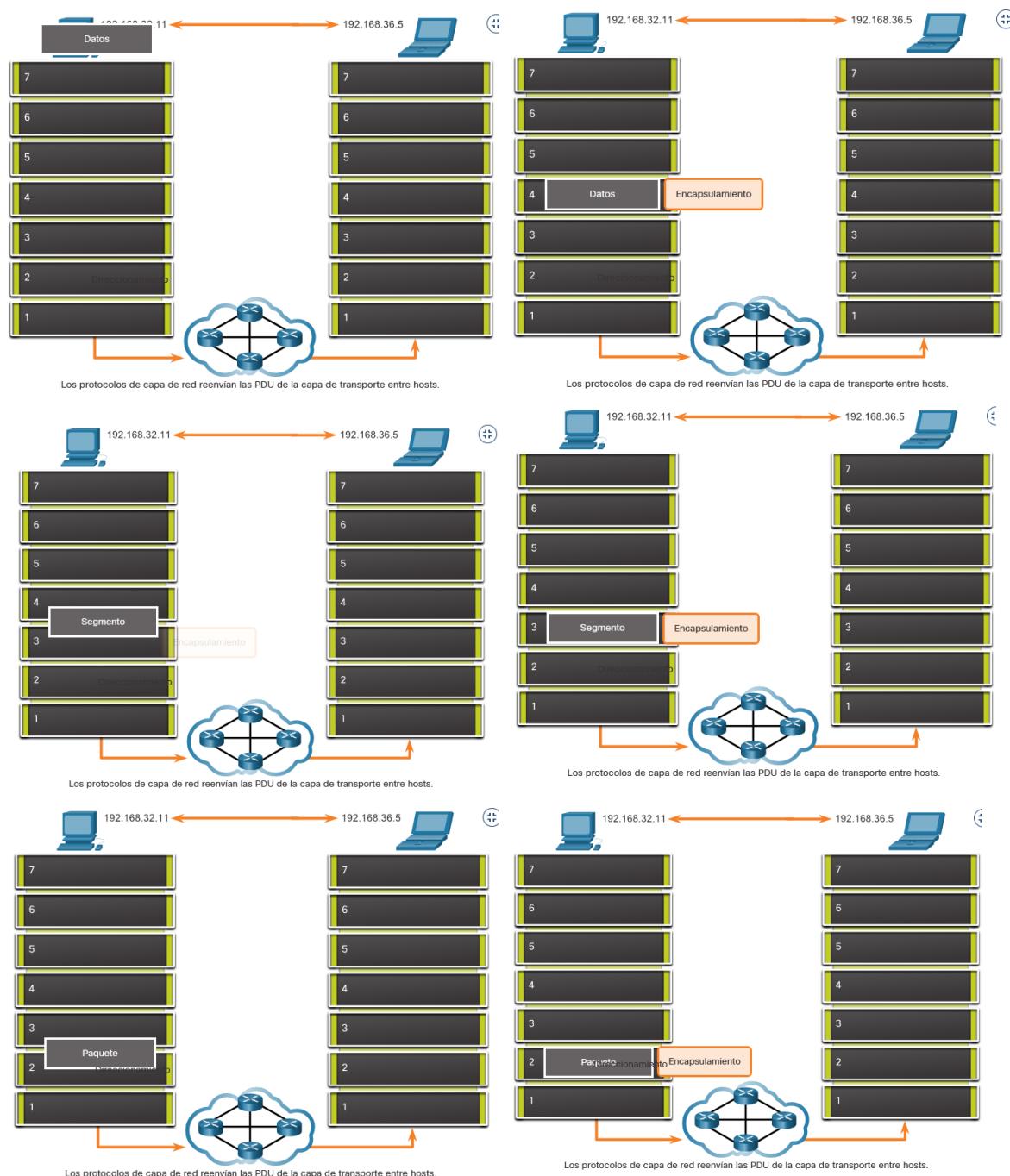


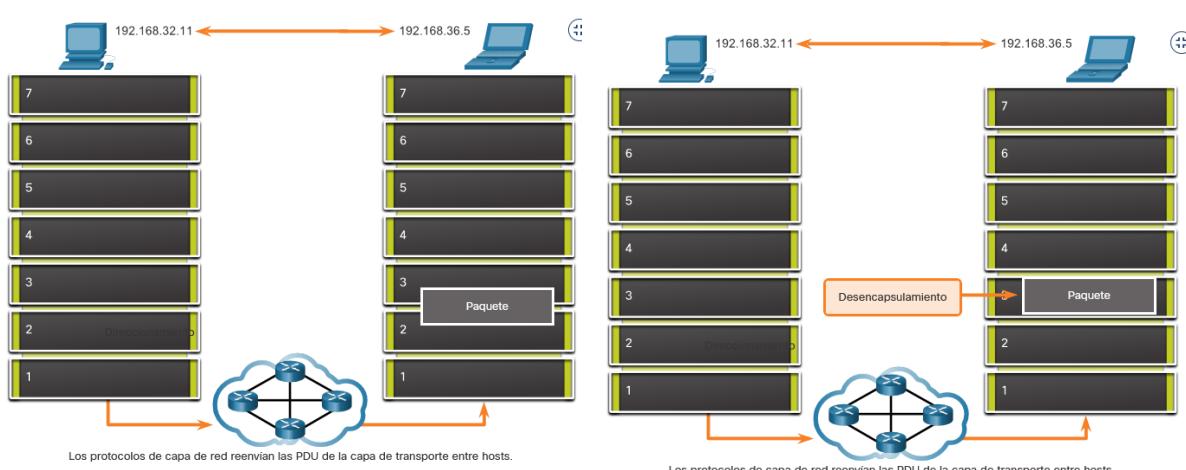
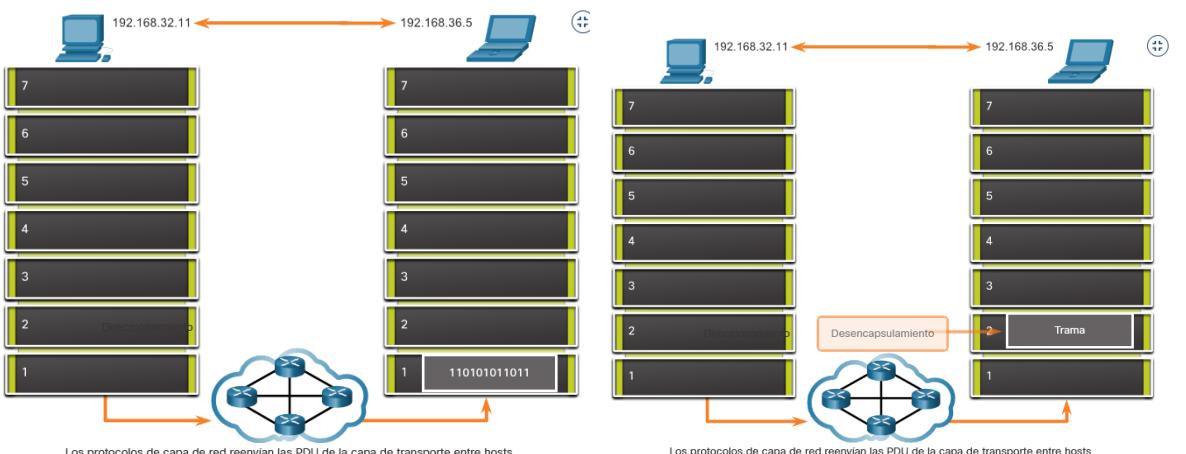
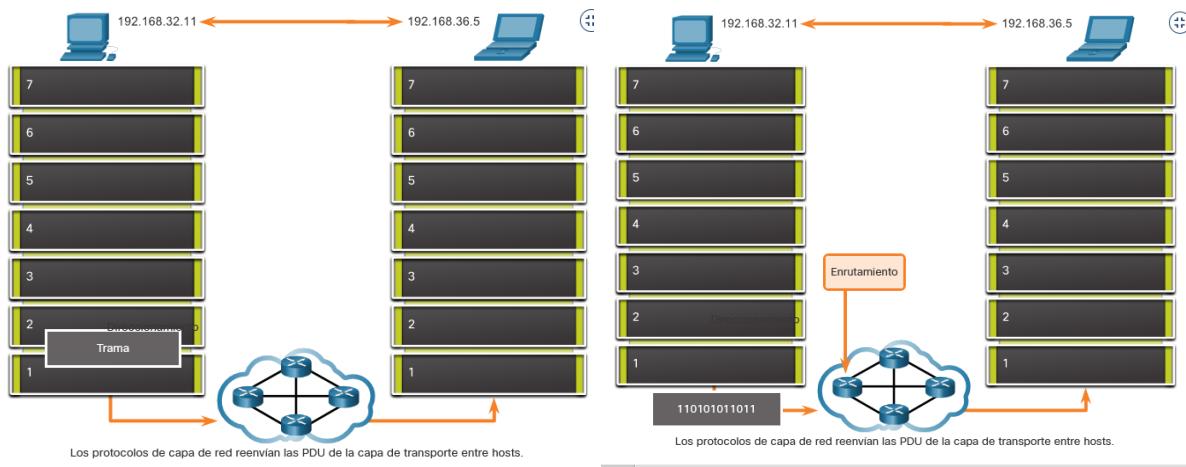
Para lograr comunicaciones end-to-end a través de los límites de la red, los protocolos de capa de red realizan cuatro operaciones básicas:

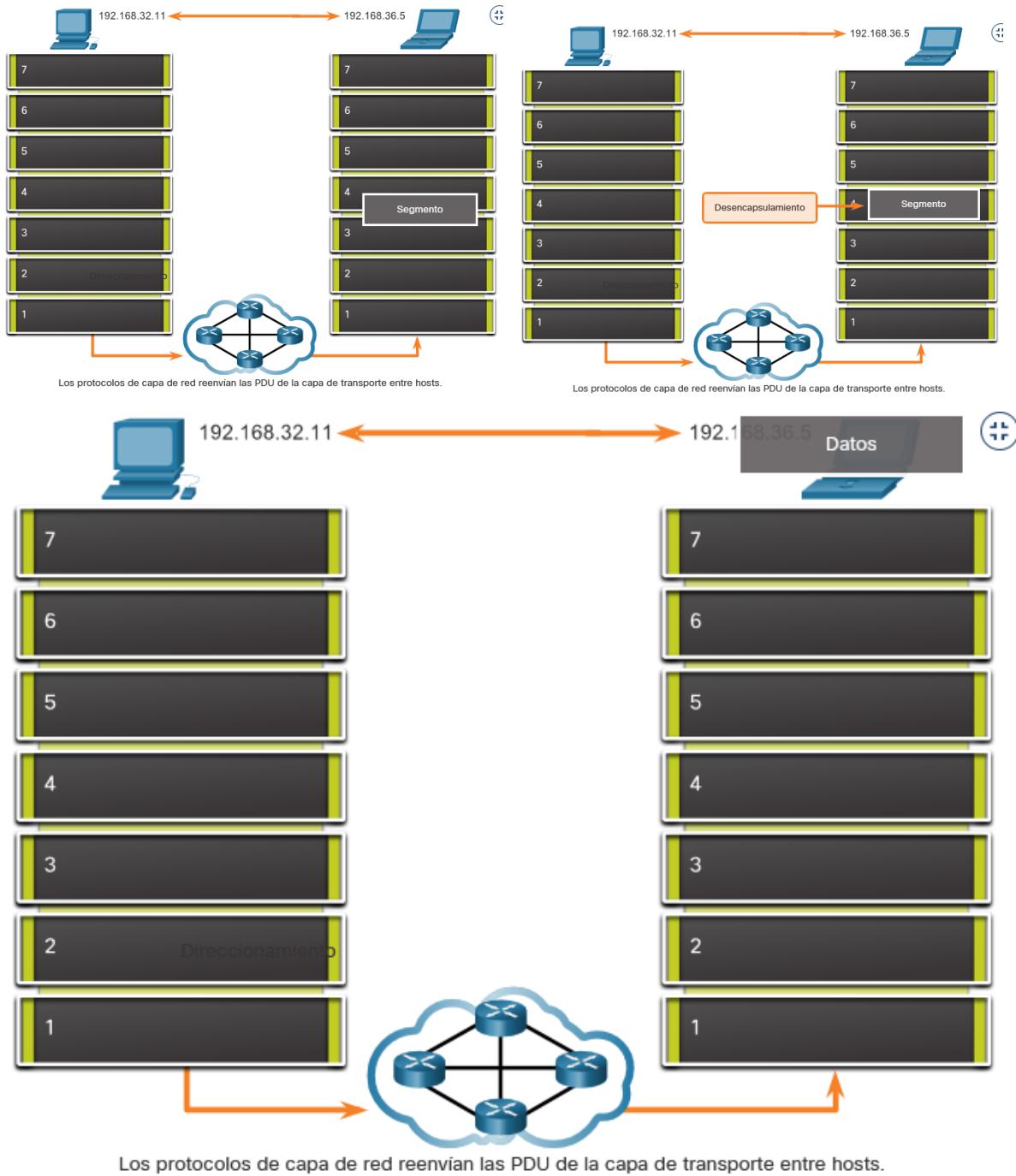
- **Direccionamiento de dispositivos finales**: los dispositivos finales deben configurarse con una dirección IP única para la identificación en la red.
- **Encapsulación**: La capa de red encapsula la unidad de datos de protocolo (PDU) de la capa de transporte en un paquete. El proceso de encapsulamiento 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.
- **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.



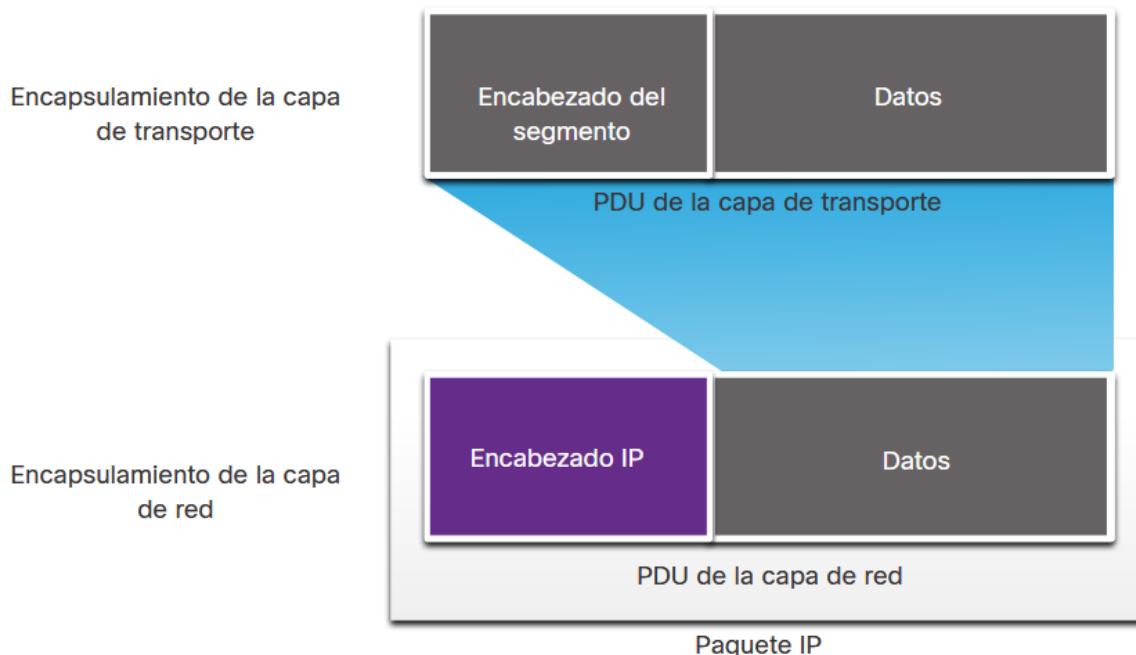




Encapsulación IP

IP encapsula el segmento de la capa de transporte u otros datos agregando un encabezado IP. El encabezado IP se usa para entregar el paquete al host de destino.

La figura ilustra cómo la PDU de la capa de transporte es encapsulada por la PDU de la capa de red para crear un paquete IP.



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. Es importante tener en cuenta que 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 la traducción de direcciones de red (NAT) para IPv4.

Características de IP

IP se diseñó como un protocolo con sobrecarga baja. Provee solo las funciones necesarias para enviar un paquete de un origen a un destino a través de un sistema interconectado de redes. El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. Estas funciones, si es necesario, están a cargo de otros protocolos en otras capas, principalmente TCP en la capa 4.

Estas son las características básicas de la propiedad intelectual:

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

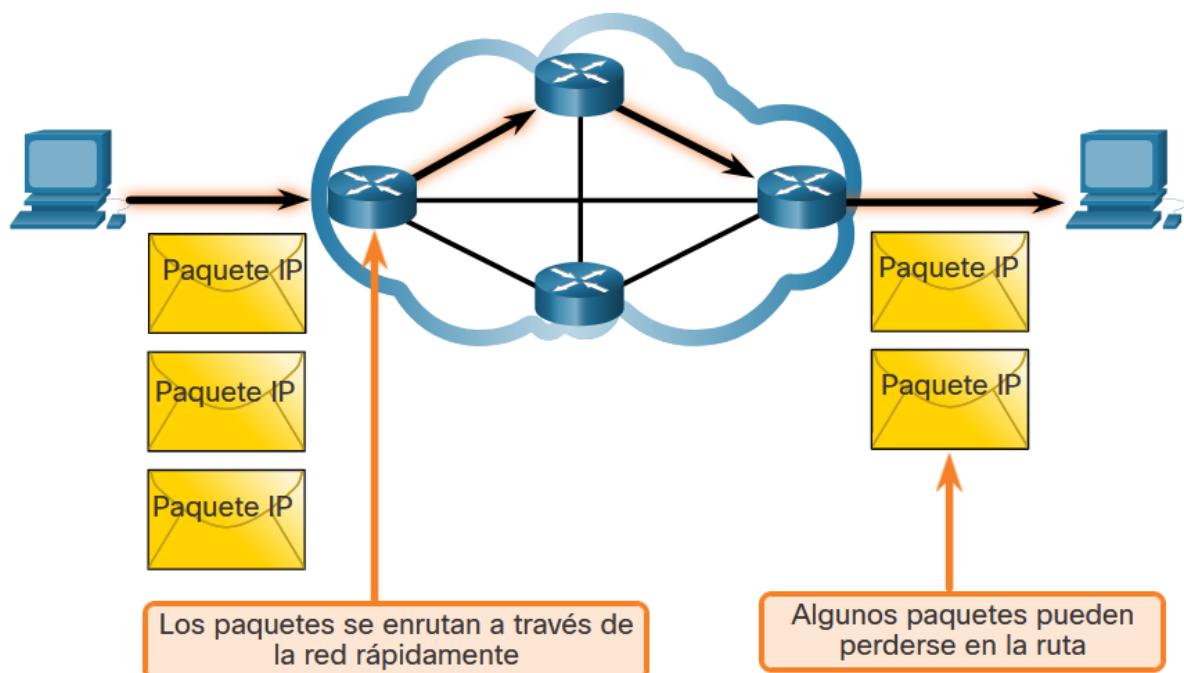
Sin conexión

IP no tiene conexión, lo que significa que IP no crea una conexión de extremo a extremo dedicada antes de enviar los datos. IP no requiere un intercambio inicial de información de control para establecer una conexión de extremo a extremo antes de que se reenvíen los paquetes.

Mejor esfuerzo

La IP tampoco necesita campos adicionales en el encabezado para mantener una conexión establecida. Este proceso reduce en gran medida la sobrecarga del protocolo IP. Sin embargo, sin una conexión completa preestablecida, los remitentes no saben si los dispositivos de destino están presentes y en funcionamiento cuando envían paquetes, ni tampoco si el destinatario recibe el paquete o si puede acceder al paquete y leerlo.

El protocolo IP no garantiza que todos los paquetes que se envían, ni que se reciban. En la ilustración, se muestran las características de entrega de mejor esfuerzo o poco confiable del protocolo IP.



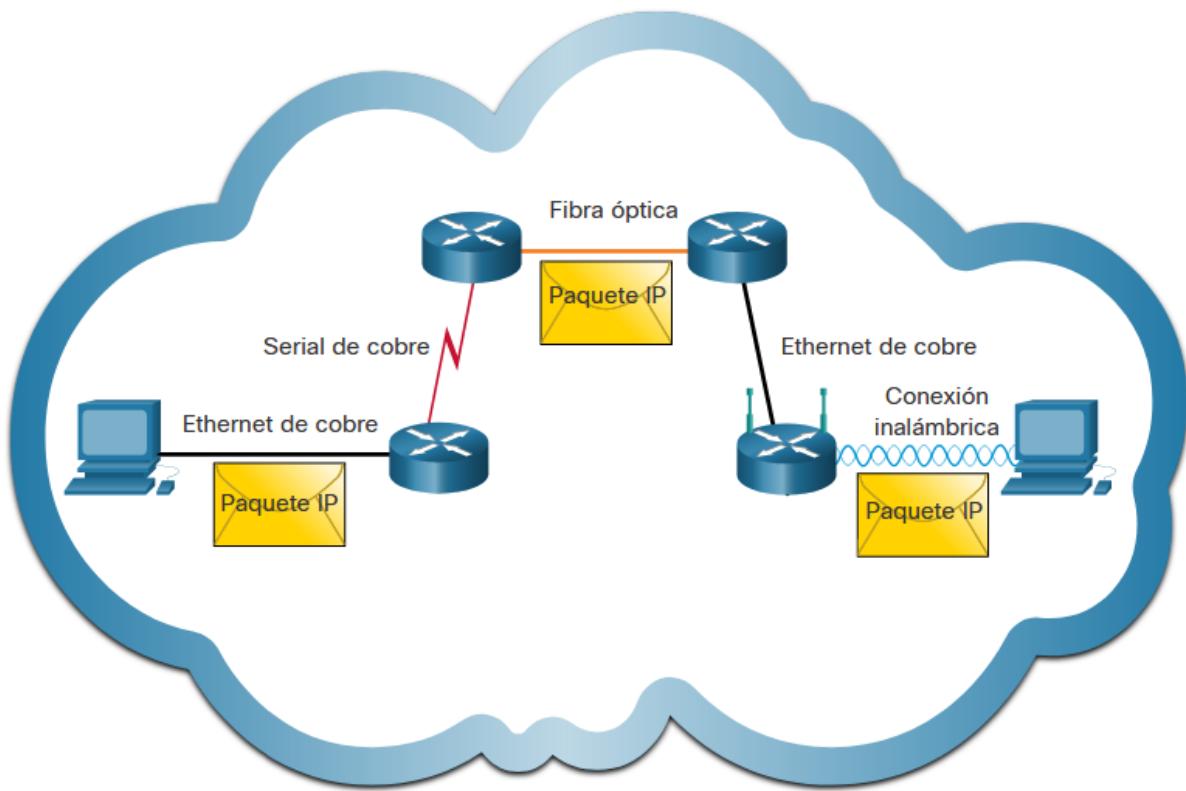
Independiente de los medios

Que sea poco confiable significa que IP no tiene la funcionalidad para administrar o recuperar paquetes no recibidos o dañados. Esto se debe a que, si bien los paquetes IP se envían con información sobre la ubicación de la entrega, no contienen información que pueda procesarse para informar al remitente si la entrega fue exitosa. Es posible que los paquetes lleguen dañados o fuera de secuencia al

destino o que no lleguen en absoluto. IP no tiene la funcionalidad de retransmitir paquetes si se producen errores.

Las aplicaciones que utilizan los datos o los servicios de capas superiores deben solucionar problemas como el envío de paquetes fuera de orden o la pérdida de paquetes. Esta característica permite que IP funcione de manera muy eficaz. En el conjunto de protocolos TCP / IP, la confiabilidad es la función del protocolo TCP en la capa de transporte.

IP funciona independientemente de los medios que transportan los datos en las capas más bajas de la pila de protocolos. Como se muestra en la ilustración, los paquetes IP pueden ser señales electrónicas que se transmiten por cables de cobre, señales ópticas que se transmiten por fibra óptica o señales de radio inalámbricas.



La capa de enlace de datos OSI es responsable de tomar un paquete IP y prepararlo para la transmisión a través del medio de comunicación. Esto significa que la entrega de paquetes IP no se limita a ningún medio en particular.

Sin embargo, la capa de red tiene en cuenta una de las características más importantes del medio, que es el tamaño máximo de PDU que cada medio puede transportar. Esta característica se conoce como "unidad de transmisión máxima" (MTU). Parte del control de la comunicación entre la capa de enlace de datos y la capa de red consiste en establecer el tamaño máximo del paquete. La capa de enlace de datos pasa el valor de MTU a la capa de red. La capa de red luego determina qué tamaño pueden tener los paquetes.

En algunos casos, un dispositivo intermedio, generalmente un router, debe dividir un paquete IPv4 cuando lo reenvía de un medio a otro con una MTU más pequeña. Este proceso se denomina “fragmentación de paquetes” o “fragmentación”. La fragmentación provoca latencia. El router no puede fragmentar los paquetes IPv6.

Paquete IPv4

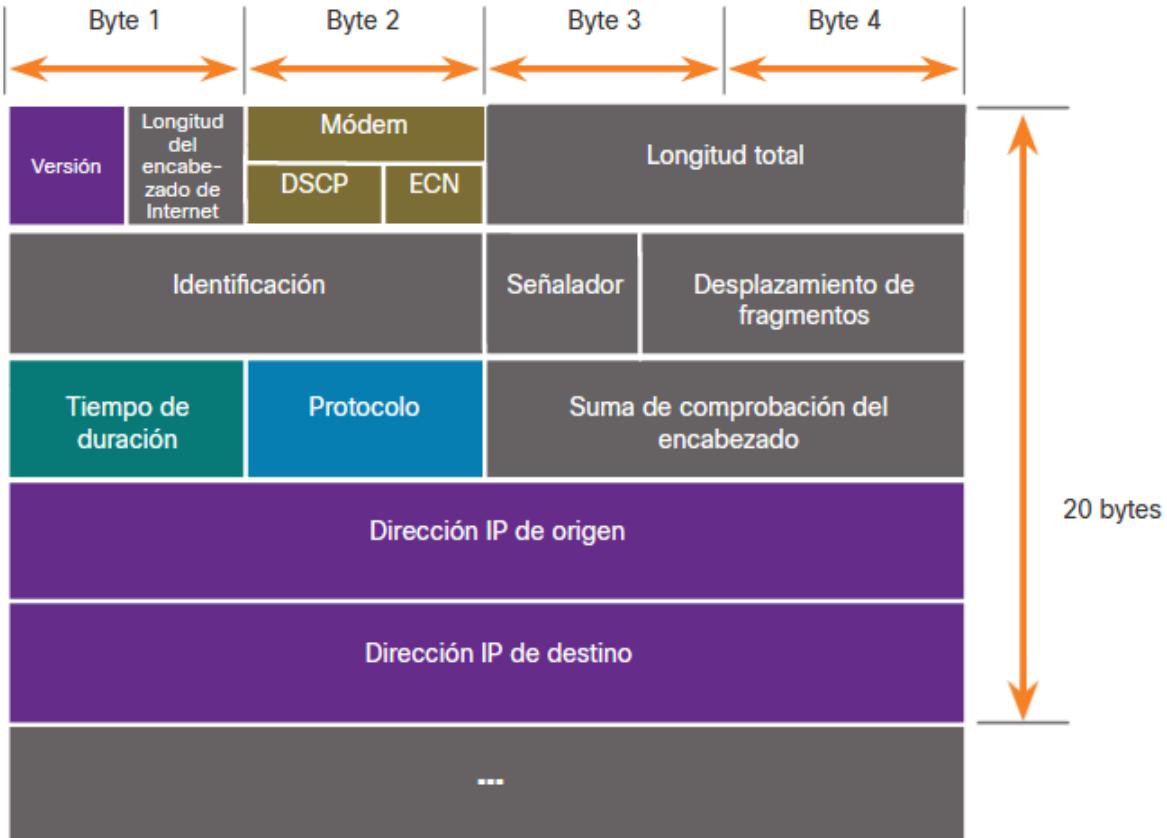
Encabezado de paquetes IPv4

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.

Campos de encabezado de paquete IPv4

Los valores binarios de cada campo identifican diversos parámetros de configuración del paquete IP. Los diagramas de encabezado del protocolo, que se leen de izquierda a derecha y de arriba hacia abajo, proporcionan una representación visual de consulta al analizar los campos de protocolo. El diagrama de encabezado del protocolo IP en la ilustración identifica los campos de un paquete IPv4.



Los campos significativos en el encabezado IPv4 incluyen lo siguiente:

- **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. Los seis bits más significativos del campo DiffServ son los bits de punto de código de servicios diferenciados (DSCP) y los dos últimos bits son los bits de notificación de congestión explícita (ECN).
- **Suma de comprobación de encabezado** - Se utiliza para detectar daños en el encabezado IPv4.
- **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.

- **Protocolo** - Este campo se utiliza para identificar el protocolo del siguiente nivel. Este valor binario de 8 bits indica el tipo de carga de datos que lleva el paquete, lo que permite que la capa de red transmita los datos al protocolo de la capa superior apropiado. ICMP (1), TCP (6) y UDP (17) son algunos valores comunes.
- **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.

Los dos campos a los que se hace más referencia son los de dirección IP de origen y de destino. En estos campos, se identifica de dónde viene el paquete y a dónde va. Por lo general, estas direcciones no cambian mientras se viaja desde el origen hasta el destino.

Para identificar y validar el paquete, se usan los campos de longitud del encabezado de Internet (IHL), longitud total y el encabezado checksum.

Para reordenar un paquete fragmentado, se usan otros campos. Específicamente, el paquete IPv4 utiliza los campos de identificación, señaladores y desplazamiento de fragmentos para llevar un control de los fragmentos. Un router puede tener que fragmentar un paquete IPv4 cuando lo reenvía de un medio a otro con una MTU más pequeña.

Paquete IPv6

Limitaciones de IPv4

IPv4 todavía está en uso hoy en día. A lo largo de los años, se han elaborado protocolos y procesos adicionales para hacer frente a los nuevos desafíos. Sin embargo, incluso con los cambios, IPv4 aún tiene tres grandes problemas:

- **Agotamiento de la dirección IPv4:** IPv4 tiene un número limitado de direcciones públicas únicas disponibles. Si bien hay aproximadamente 4000 millones de direcciones IPv4, el incremento en la cantidad de dispositivos nuevos con IP habilitado, las conexiones constantes y el crecimiento potencial de regiones menos desarrolladas aumentaron la necesidad de direcciones.
- **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

compartan 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.

Las mejoras que ofrece IPv6 incluyen las siguientes:

- **Manejo de paquetes mejorado**: - las direcciones IPv6 se basan en el direccionamiento jerárquico de 128 bits en lugar de IPv4 con 32 bits.
- **Mejor manejo de paquetes** - Manejo de paquetes mejorado: el encabezado IPv6 se ha simplificado con menos campos.
- **Elimina la necesidad de NAT**: - 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.

El espacio de las direcciones IPv4 de 32 bits ofrece aproximadamente 4.294.967.296 direcciones únicas. El espacio de direcciones IPv6 proporciona 340,282,366,920,938,463,463,374,607,431,768,211,456, o 340 undecillones de direcciones. Esto es aproximadamente equivalente a cada grano de arena en la Tierra.

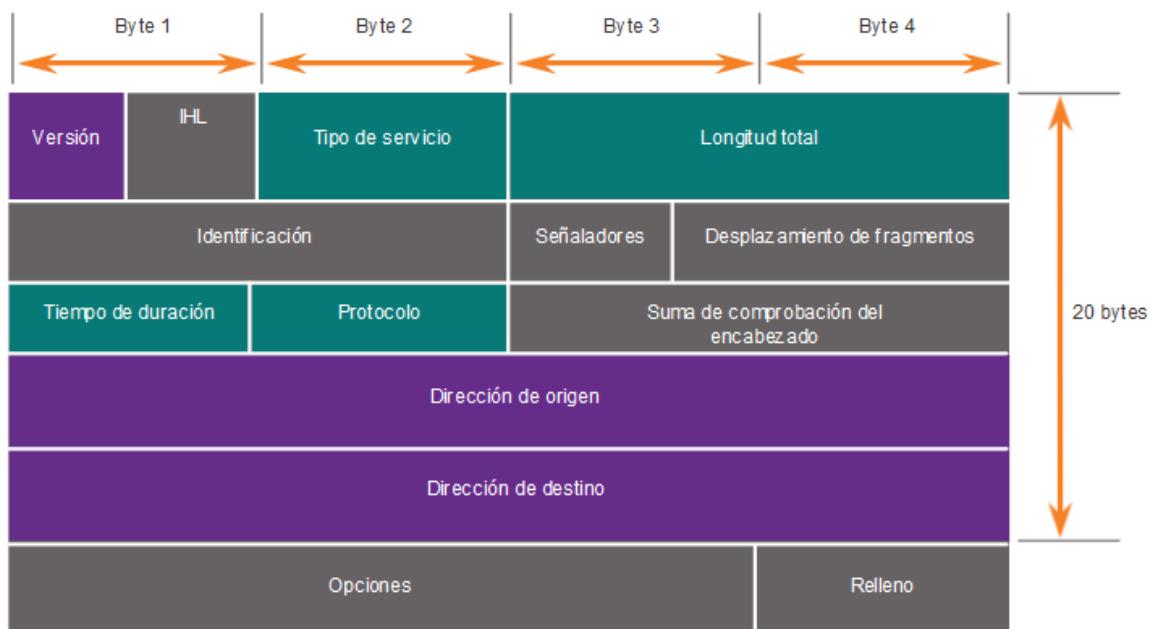
Campos de encabezado de paquete IPv4 en el encabezado de paquete IPv6

Uno de las mejoras de diseño más importantes de IPv6 con respecto a IPv4 es el encabezado simplificado de IPv6.

Por ejemplo, el encabezado IPv4 consiste en un encabezado de longitud variable de 20 octetos (hasta 60 bytes si se usa el campo Opciones) y 12 campos de encabezado básicos, sin incluir el campo Opciones y el campo Relleno.

Para IPv6, algunos campos se han mantenido igual, algunos campos han cambiado de nombre y posición, y algunos campos de IPv4 ya no son necesarios, como se destaca en la figura.

Encabezado de paquetes IPv4



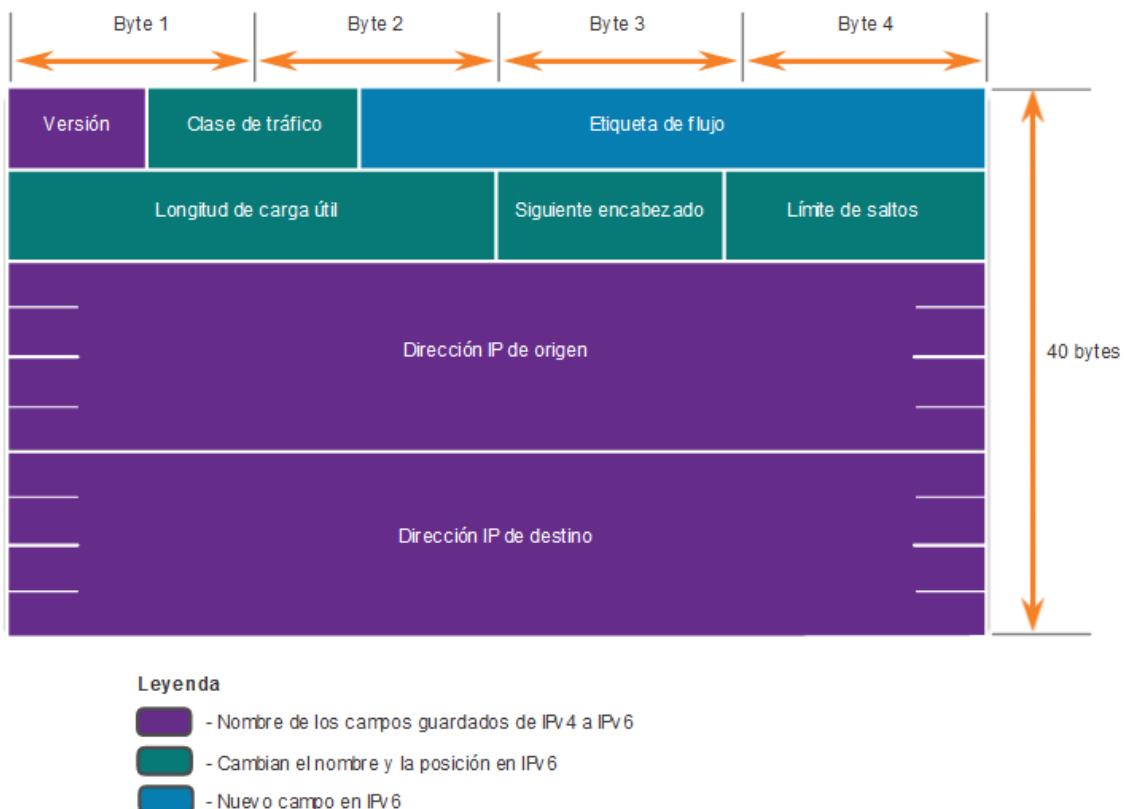
Leyenda

- Nombre de los campos guardados de IPv4 a IPv6
- Cambian el nombre y la posición en IPv6
- Nuevo campo en IPv6

En contraste, el encabezado IPv6 simplificado que se muestra en la siguiente figura consiste en un encabezado de longitud fija de 40 octetos (en gran parte debido a la longitud de las direcciones IPv6 de origen y destino).

El encabezado simplificado IPv6 permite un procesamiento más eficiente de encabezados IPv6.

Encabezado de paquetes IPv6



Los campos en el encabezado del paquete IPv6 incluyen lo siguiente:

- **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.
- **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.

- **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.

Un paquete IPv6 también puede contener encabezados de extensión (EH), que proveen información optativa de la capa de red. Los encabezados de extensión son opcionales y están ubicados entre el encabezado de IPv6 y el contenido. Los EH se usan para fragmentar, dar seguridad, admitir la movilidad y otras acciones.

A diferencia de IPv4, los routers no fragmentan de los paquetes IPv6 enrutados.

La decisión de 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.

Un host puede enviar un paquete a lo siguiente:

- **A si mismo (Itself)** - Un host puede hacer ping a sí mismo enviando un paquete a una especial a la dirección IPv4 127.0.0.1 o a la dirección IPv6 ::1, que se conoce como la interfaz de bucle invertido (loopback). Al hacer ping a la interfaz loopback, pone a prueba la pila del protocolo TCP/IP en el host.
- **Host local (Local host)** - 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 (Remote host)** - este es un host de destino en una red remota. Los hosts de origen y destino no comparten la misma dirección de red.

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.

MAC e IP

Destino en la misma red

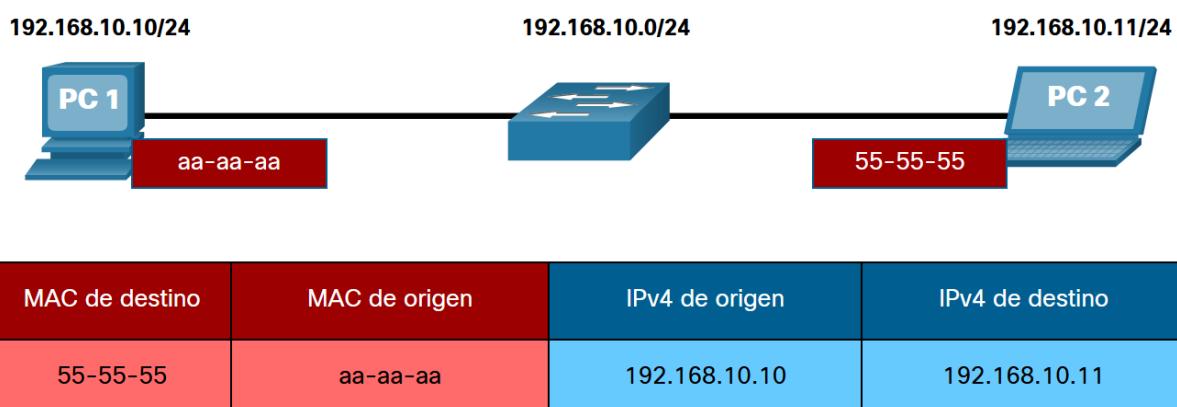
A veces, un host debe enviar un mensaje, pero solo conoce la dirección IP del dispositivo de destino. El host necesita saber la dirección MAC de ese dispositivo, pero ¿cómo se puede descubrir? Ahí es donde la resolución de direcciones se vuelve crítica.

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.

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.

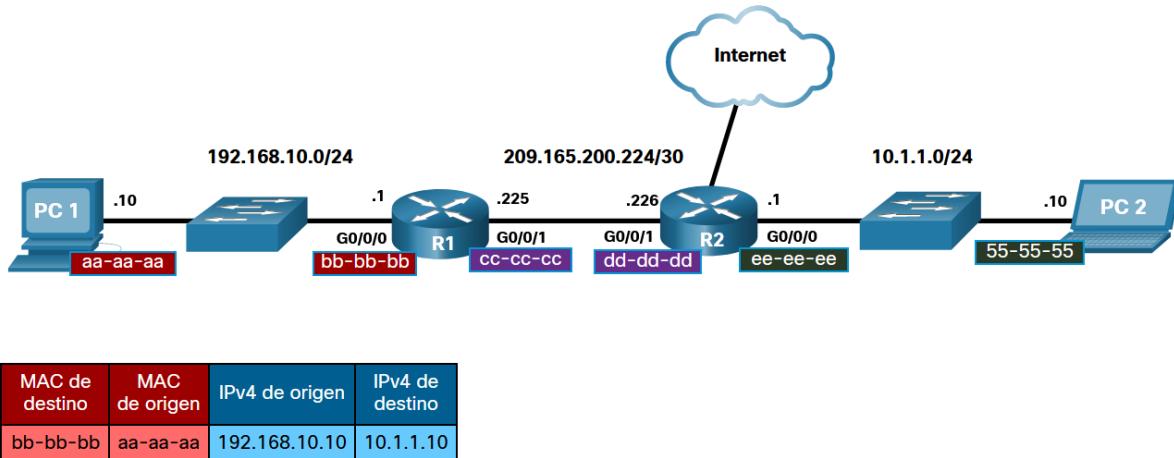
Considere el siguiente ejemplo utilizando representaciones de direcciones MAC simplificadas.



Destino en una red remota

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).

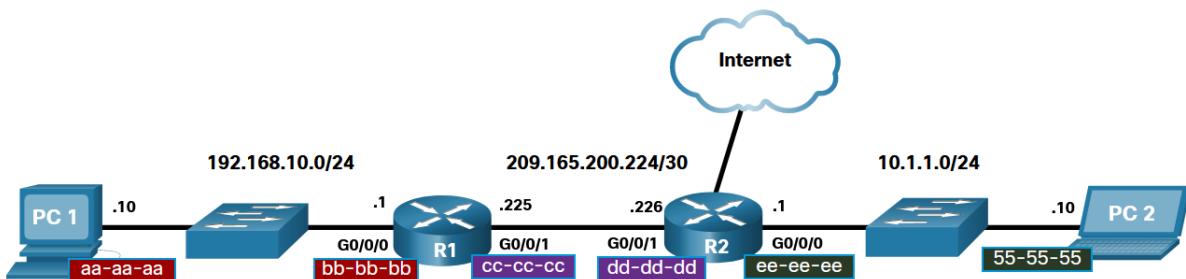
Considere el siguiente ejemplo utilizando una representación de dirección MAC simplificada.



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.

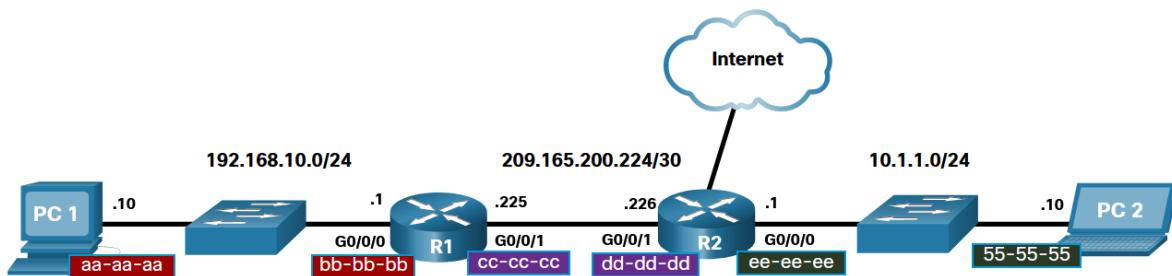
En nuestro ejemplo, R1 ahora encapsularía el paquete con la nueva información de dirección de Capa 2 como se muestra en la figura.



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

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.

A lo largo de cada enlace de una ruta, un paquete IP se encapsula en una trama. El trama es específico 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, como se muestra en la figura.



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

¿Cómo se asocian las direcciones IP de los paquetes IP en un flujo de datos con las direcciones MAC en cada enlace a lo largo de la ruta hacia el destino? Para los paquetes IPv4, esto se realiza a través de un proceso llamado Protocolo de resolución de direcciones (ARP). Para los paquetes IPv6, el proceso es ICMPv6 Neighbor Discovery (ND).

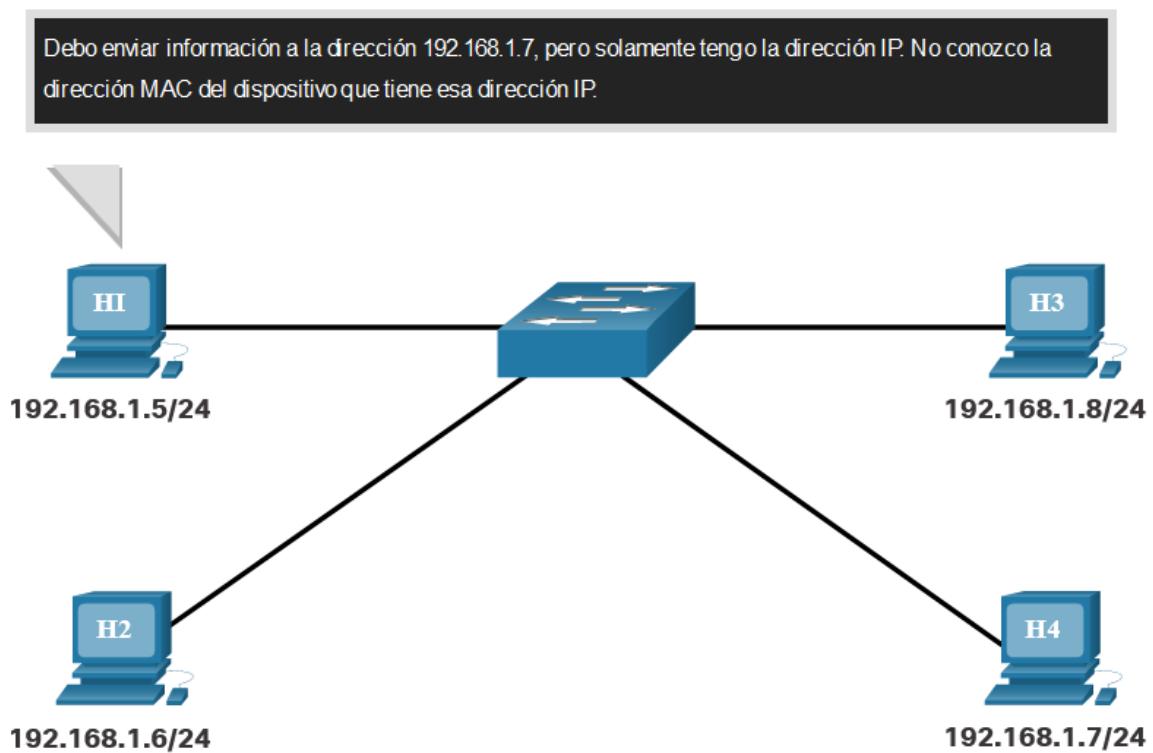
Descripción general de ARP

Si su red utiliza el protocolo de comunicaciones IPv4, el protocolo de resolución de direcciones o ARP(Address Resolution Protocol) es lo que necesita para asignar direcciones IPv4 a direcciones MAC.

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** - La dirección MAC Ethernet del dispositivo de destino en el mismo segmento de red local. Si el host de destino está en otra red, entonces la dirección de destino en el trama sería la del gateway predeterminado (es decir, router).
- **Dirección MAC de origen** - La dirección MAC de la NIC de Ethernet en el host de origen.

La figura ilustra el problema al enviar una trama a otro host en el mismo segmento en una red IPv4.



Para enviar un paquete a otro host en la misma red IPv4 local, un host debe conocer la dirección IPv4 y la dirección MAC del dispositivo de destino. Las direcciones IPv4 de destino del dispositivo se conocen o se resuelven por el nombre del dispositivo. Sin embargo, las direcciones MAC deben ser descubiertas.

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

Funciones del ARP

Cuando se envía un paquete a la capa de enlace de datos para encapsularlo en una trama de Ethernet, el dispositivo consulta una tabla en su memoria para encontrar la dirección MAC que está asignada a la dirección IPv4. Esta tabla se almacena temporalmente en la memoria RAM y se denomina tabla ARP o caché ARP.

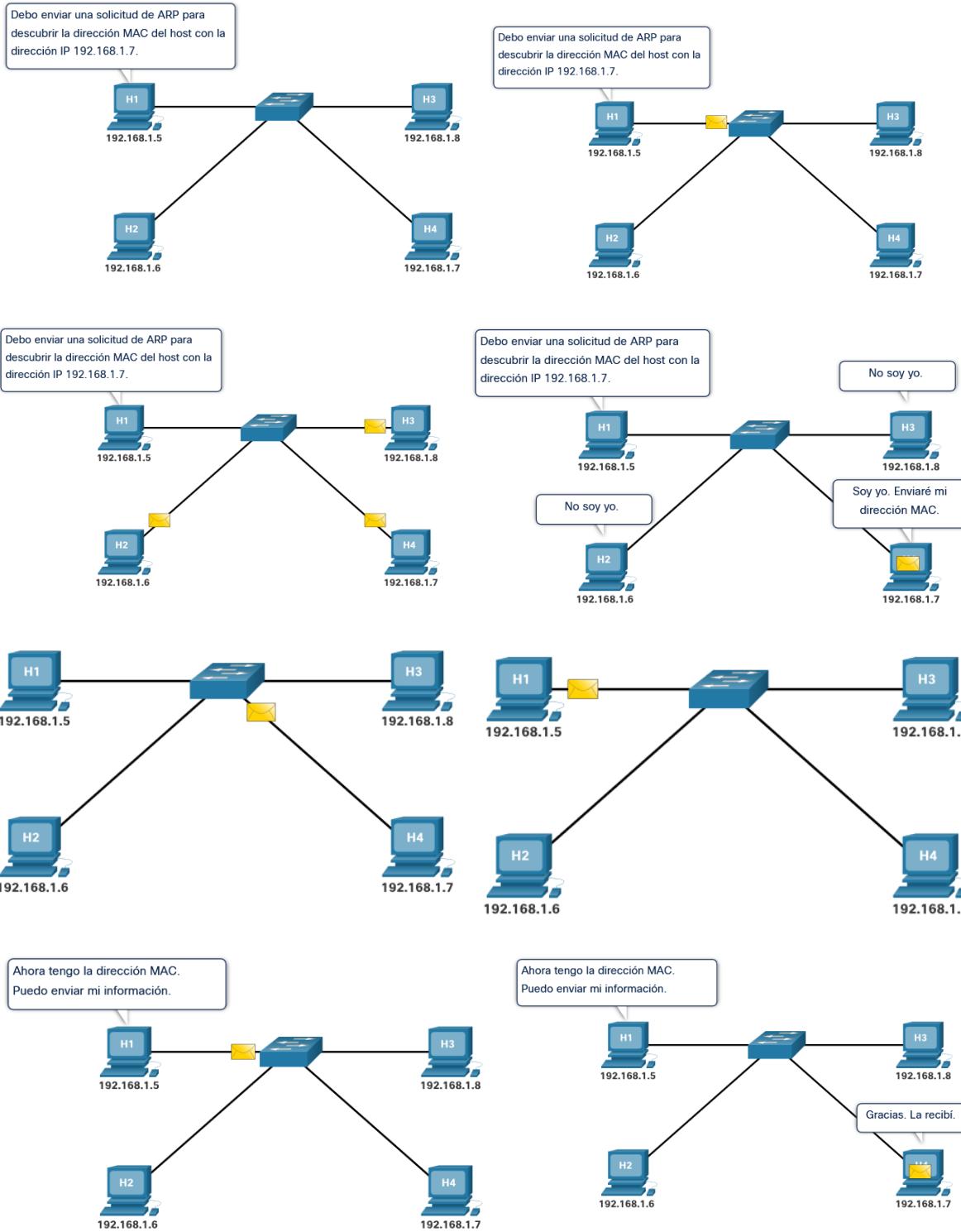
El dispositivo emisor busca en su tabla ARP la dirección IPv4 de destino y la dirección MAC correspondiente.

- Si la dirección IPv4 de destino del paquete está en la misma red que la dirección IPv4 de origen, el dispositivo busca la dirección IPv4 de destino en la tabla ARP.
- Si la dirección IPv4 de destino está en una red diferente que la dirección IPv4 de origen, el dispositivo busca la dirección IPv4 del gateway predeterminado.

En ambos casos, se realiza una búsqueda de la dirección IPv4 y la dirección MAC correspondiente para el dispositivo.

En cada entrada o fila de la tabla ARP, se enlaza una dirección IPv4 con una dirección MAC. Llamamos a la relación entre los dos valores un mapa. Esto solamente significa que es posible buscar una dirección IPv4 en la tabla y encontrar la dirección MAC correspondiente. La tabla ARP almacena temporalmente (en caché) la asignación para los dispositivos de la LAN.

Si el dispositivo localiza la dirección IPv4, se utiliza la dirección MAC correspondiente como la dirección MAC de destino de la trama. Si no se encuentra ninguna entrada, el dispositivo envía una solicitud de ARP.



Solicitud de ARP

Se envía una solicitud ARP cuando un dispositivo necesita determinar la dirección MAC que está asociada con una dirección IPv4, y no tiene una entrada para la dirección IPv4 en su tabla ARP.

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.

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.

Respuesta de ARP

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.

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.

Nota [IPv6 utiliza un proceso similar a ARP para IPv4, conocido como ICMPv6 Neighbour Discovery (ND). IPv6 utiliza mensajes de solicitud de vecino y de anuncio de vecino similares a las solicitudes y respuestas de ARP de IPv4.]

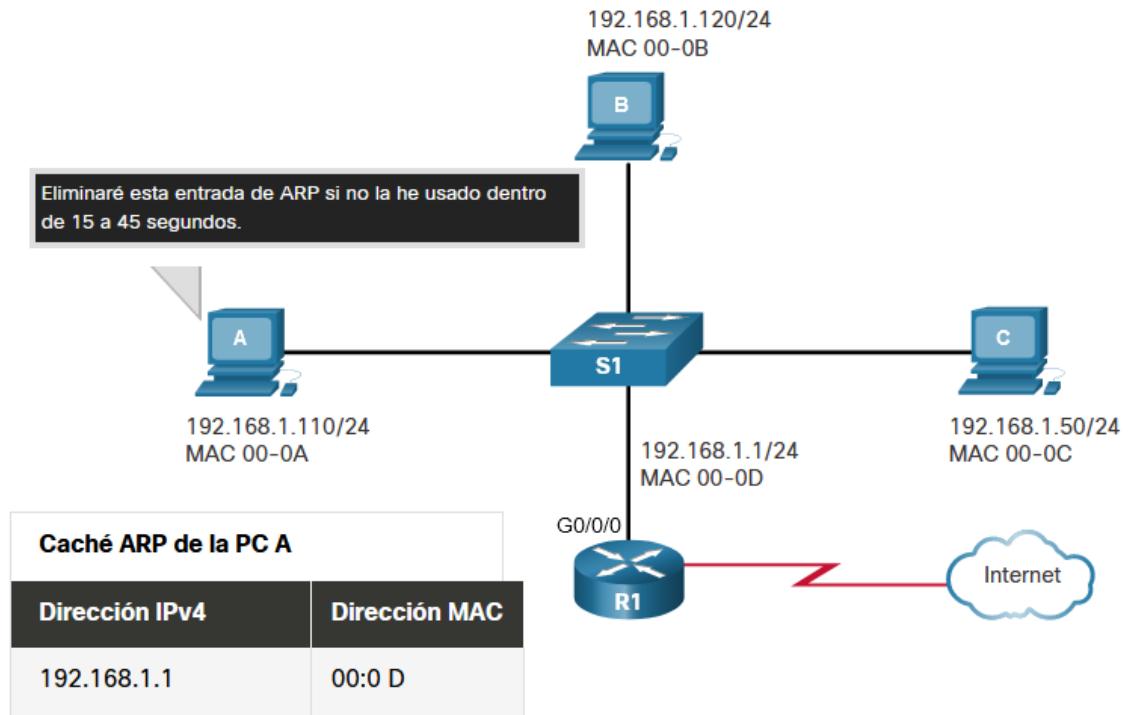
Rol ARP en Comunicaciones Remotas

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.

Eliminación de entradas de una 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, como se ilustra en la figura.



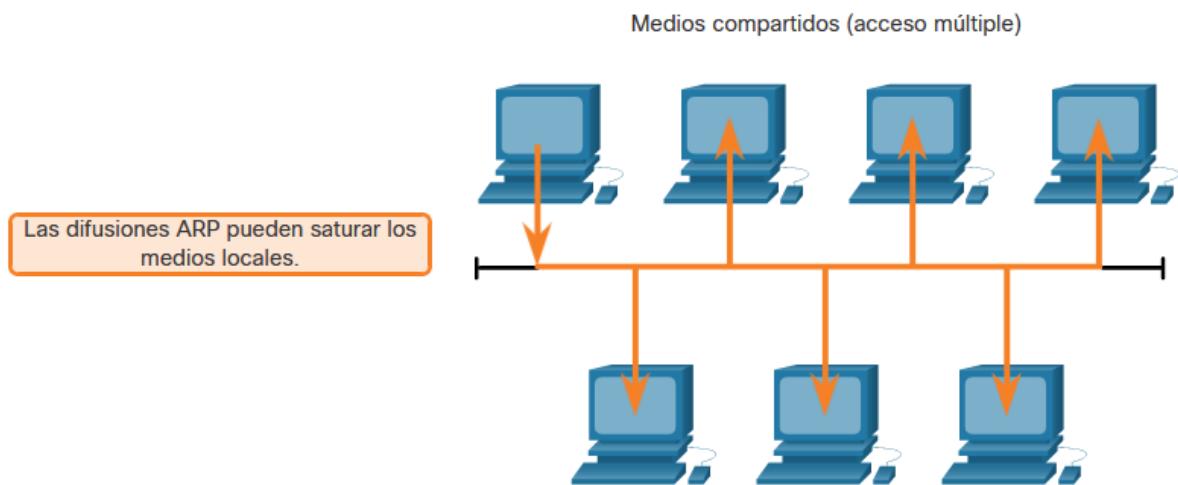
Nota: Las direcciones MAC están acortadas con fines de demostración.

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.

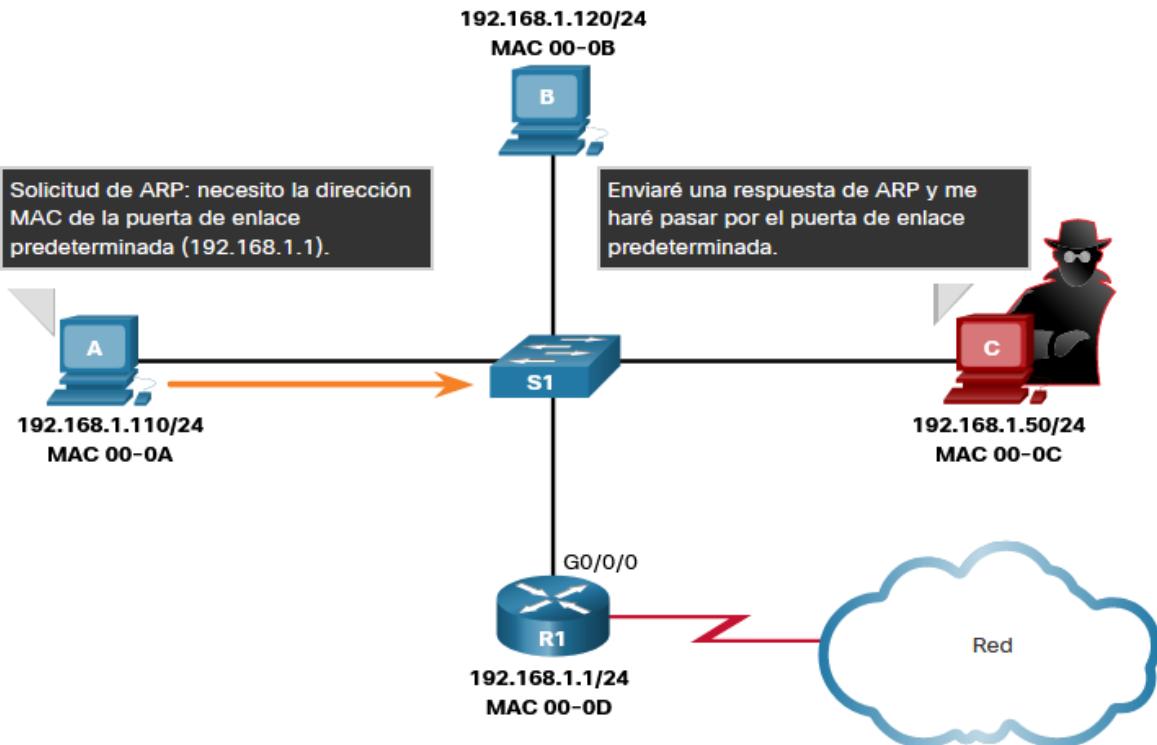
Problemas de ARP - Difusión ARP y suplantación ARP

Todos los dispositivos de la red local reciben y procesan una solicitud de ARP debido a que es una trama de difusión. En una red comercial típica, estas difusiones tendrían, probablemente, un efecto mínimo en el rendimiento de la red. Sin embargo, si se encendiera una gran cantidad de dispositivos que comenzaran a acceder a los servicios de red al mismo tiempo, el rendimiento podría disminuir durante un breve período, como se muestra en la figura. Después que los dispositivos envían las solicitudes de difusión ARP iniciales y obtienen las direcciones MAC necesarias, se minimiza cualquier efecto en la red.

Todos los dispositivos encendidos al mismo tiempo

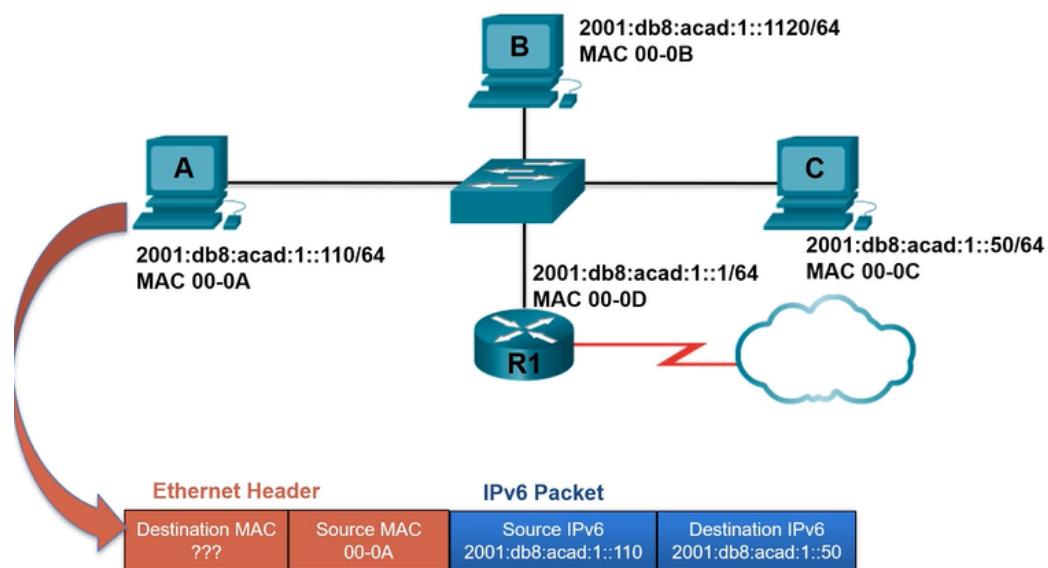


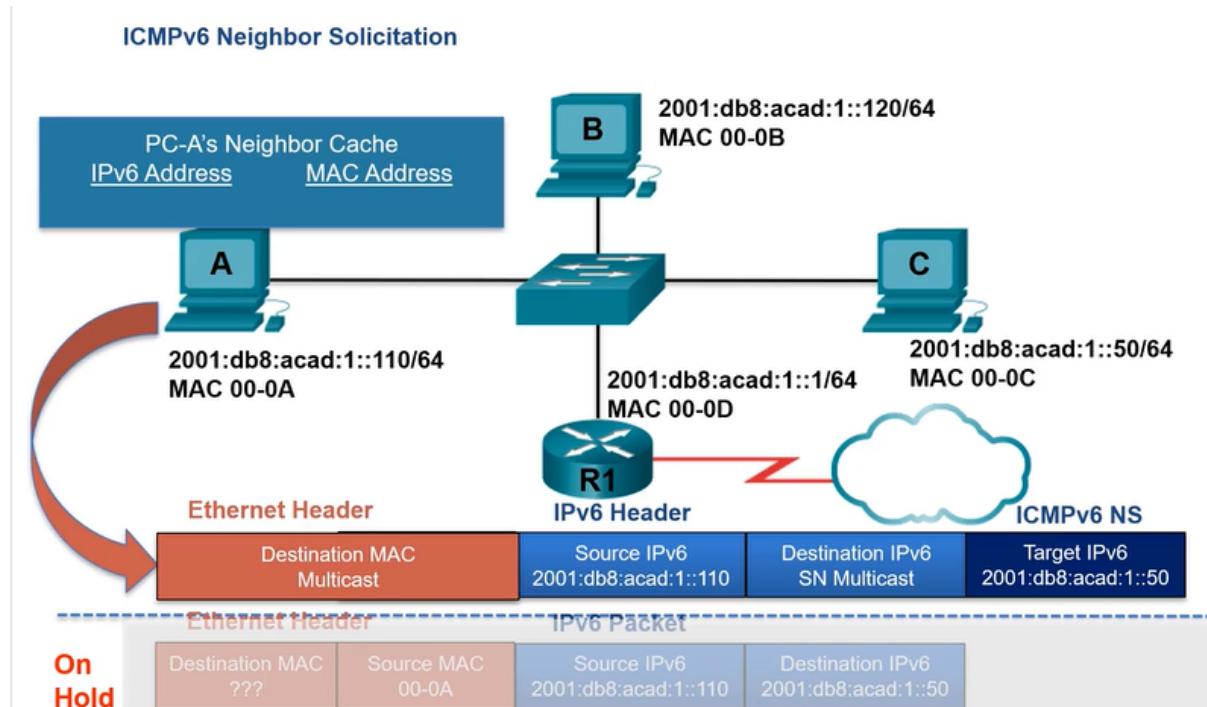
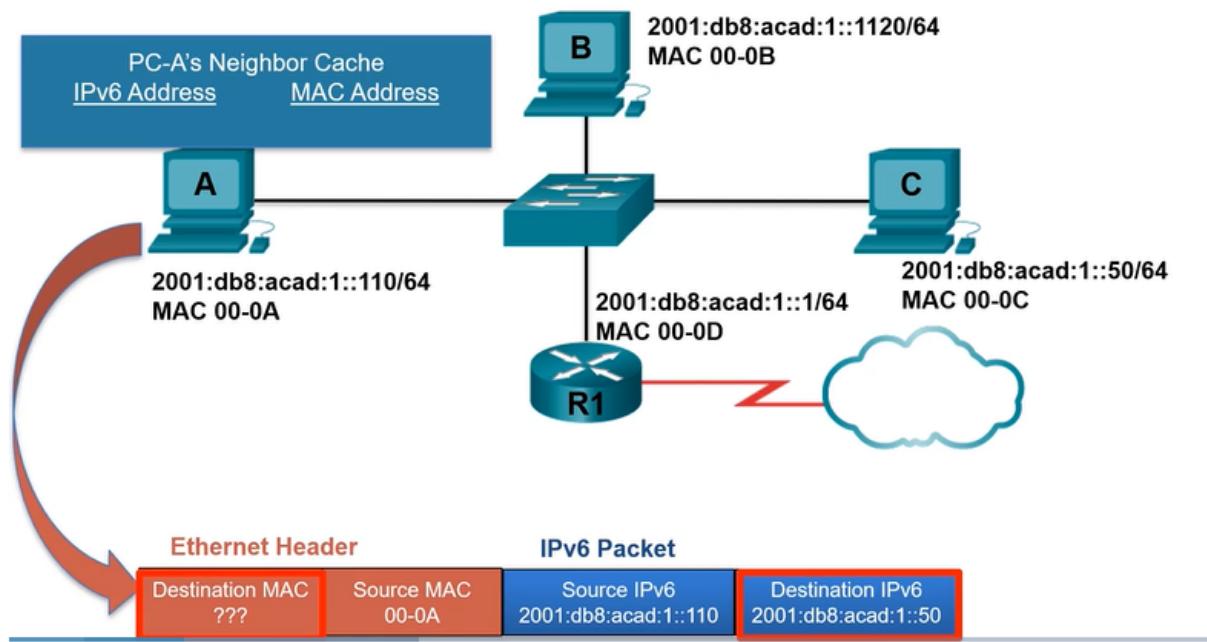
En algunos casos, el uso de ARP puede conducir a un riesgo potencial de seguridad. Un atacante puede usar la suplantación ARP para realizar un ataque de envenenamiento ARP. Esta es una técnica utilizada por un atacante para responder a una solicitud de ARP de una dirección IPv4 que pertenece a otro dispositivo, como la puerta de enlace predeterminada, tal como se muestra en la ilustración. El atacante envía una respuesta de ARP con su propia dirección MAC. El receptor de la respuesta de ARP agrega la dirección MAC incorrecta a la tabla ARP y envía estos paquetes al atacante. Los switches de nivel empresarial incluyen técnicas de mitigación conocidas como “inspección dinámica de ARP (DAI)”. DAI está más allá del alcance de este curso.



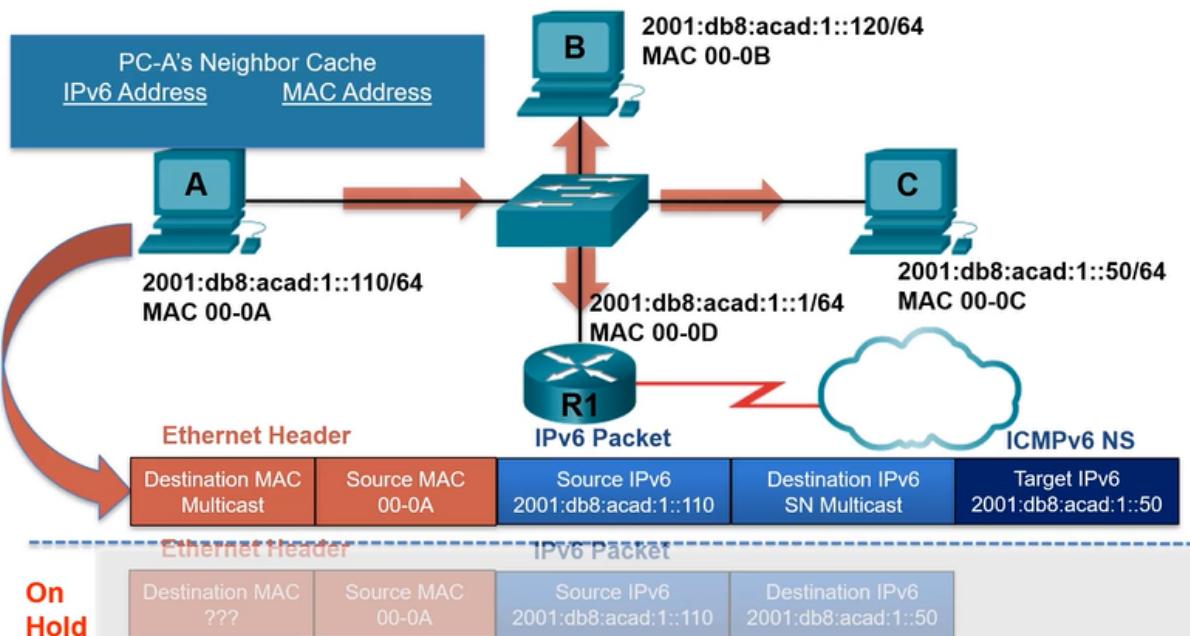
Detección de vecinos IPv6

Si su red utiliza el protocolo de comunicaciones IPv6, el protocolo de detección de vecinos o ND es lo que necesita para hacer coincidir las direcciones IPv6 con las direcciones MAC. En este tema se explica cómo funciona ND.

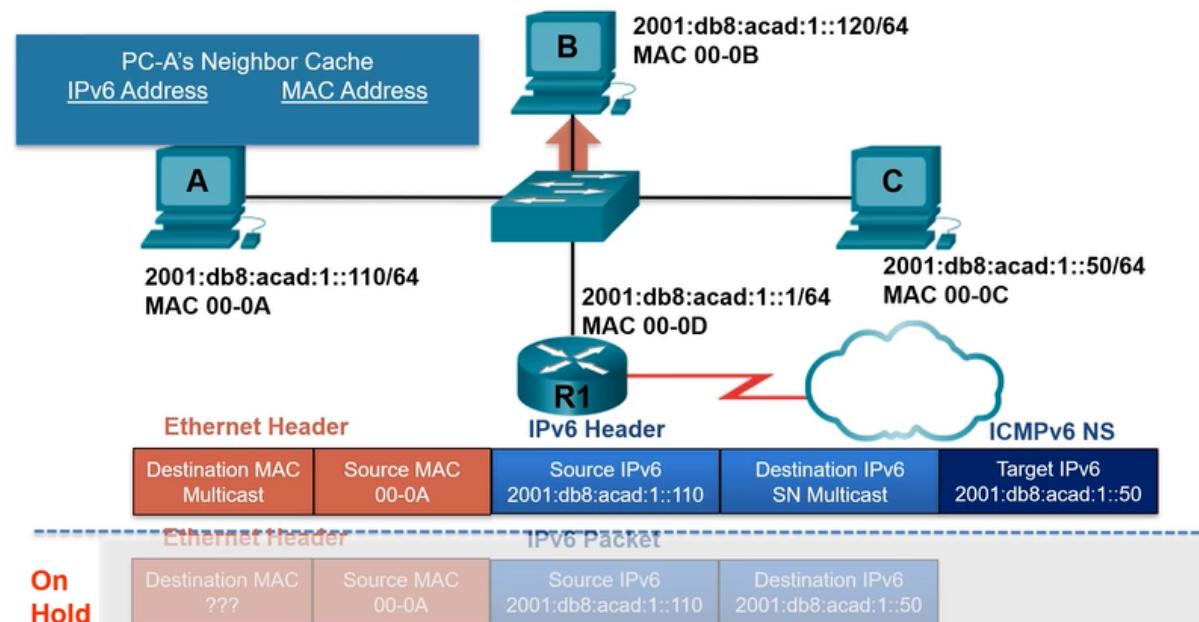


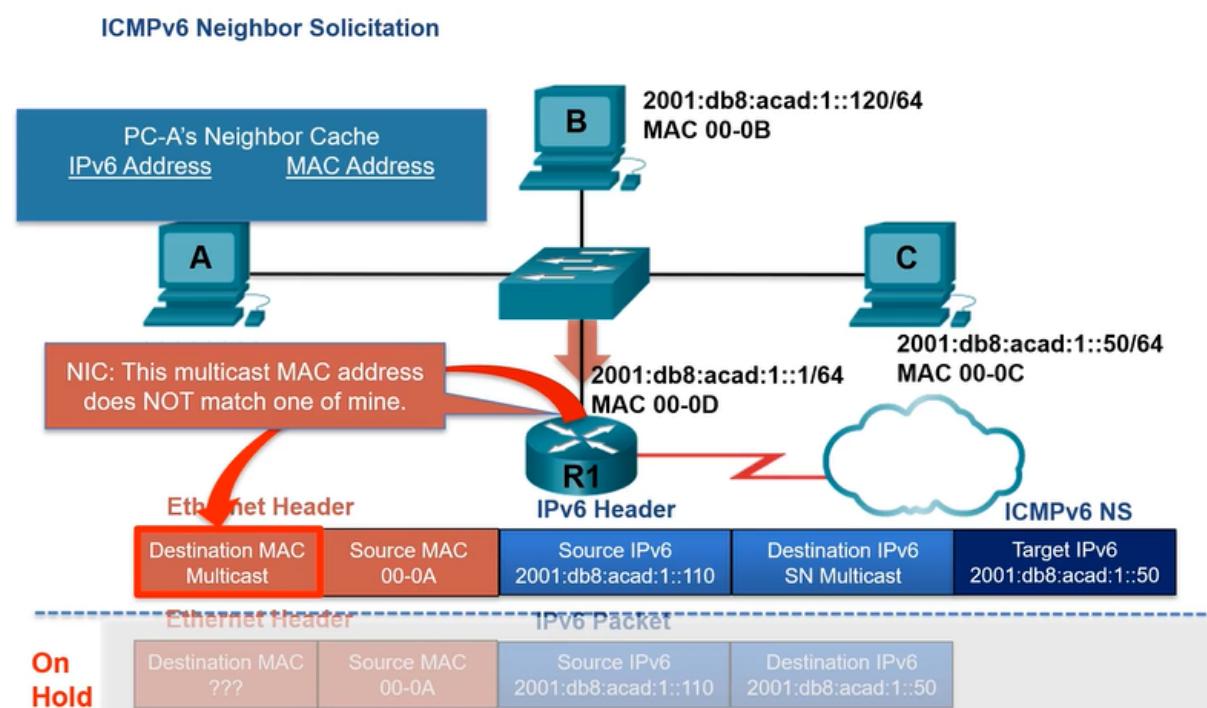
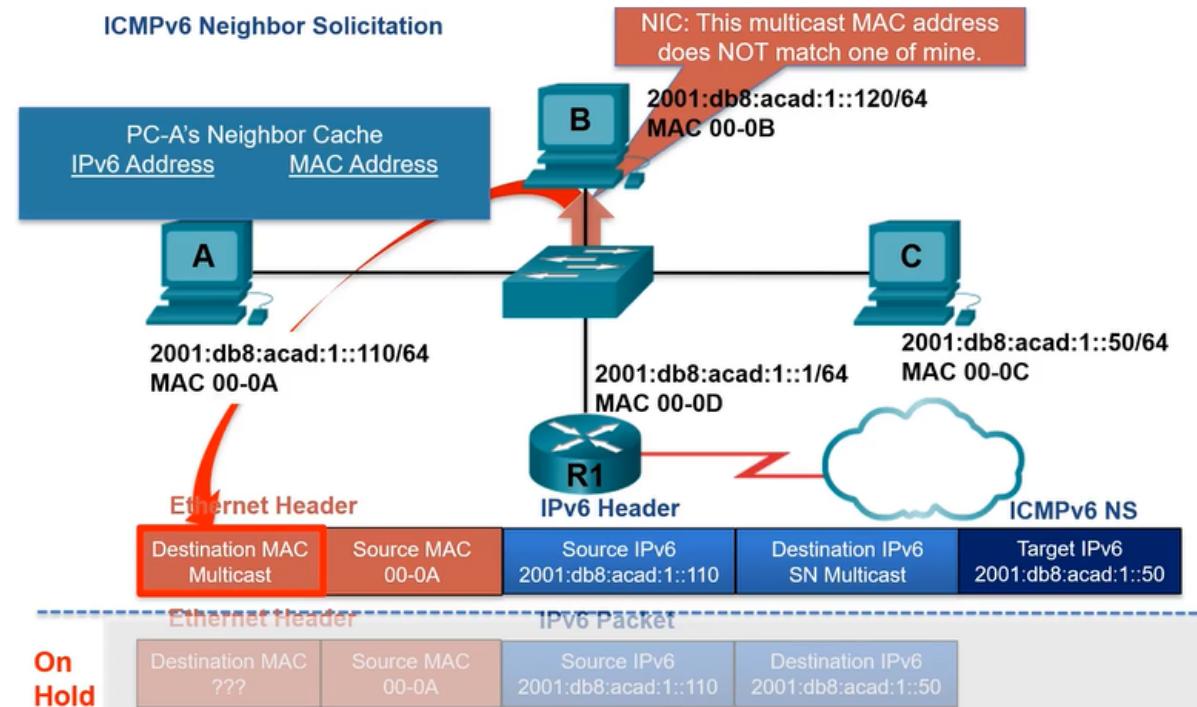


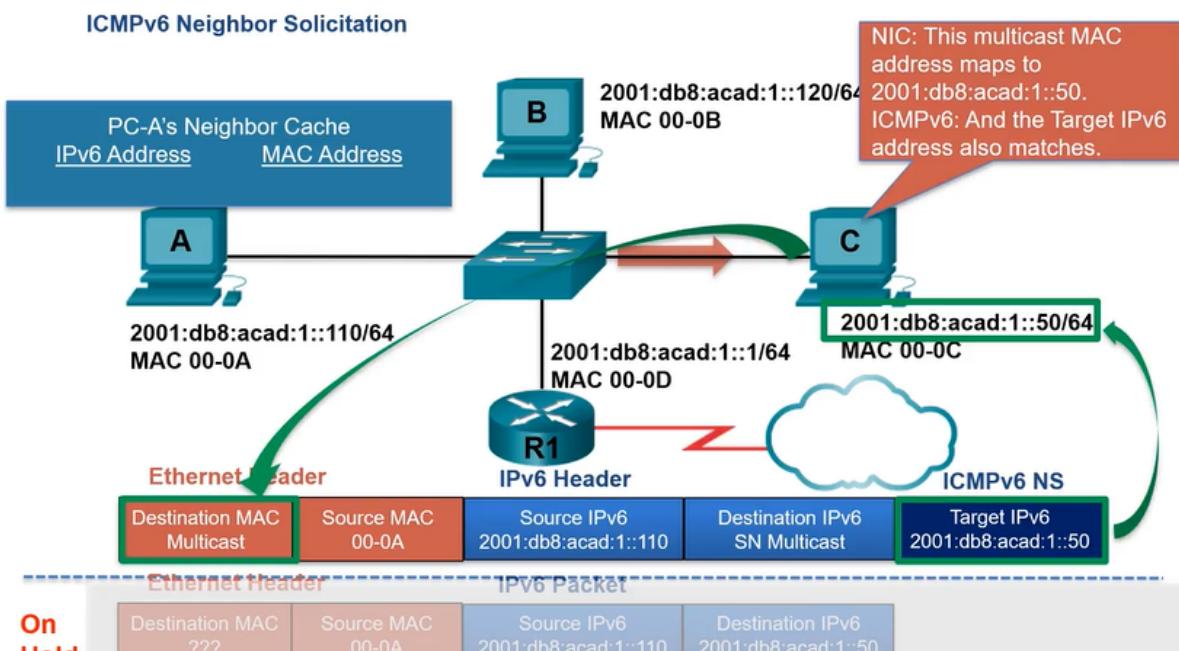
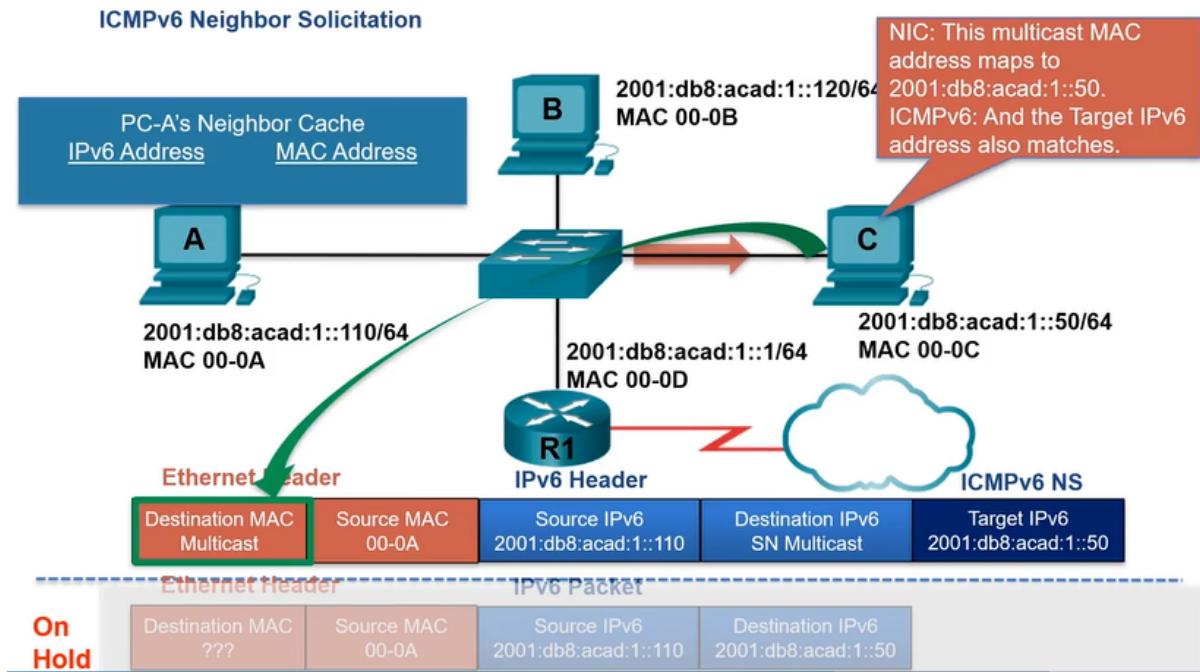
ICMPv6 Neighbor Solicitation

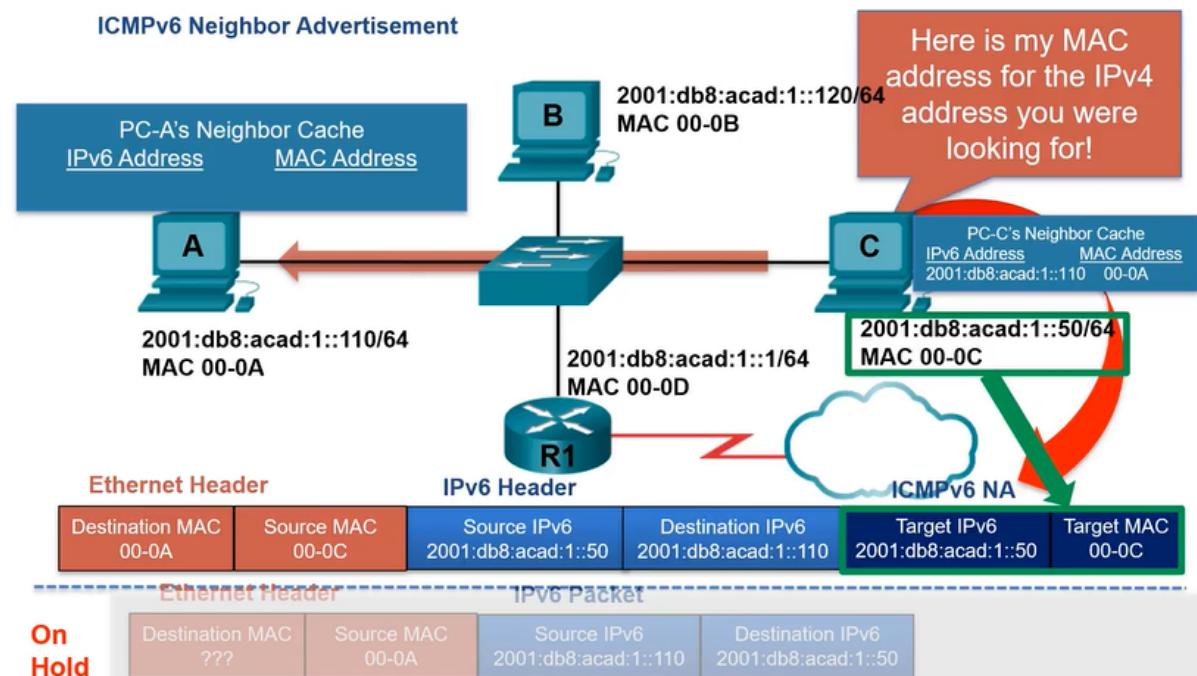
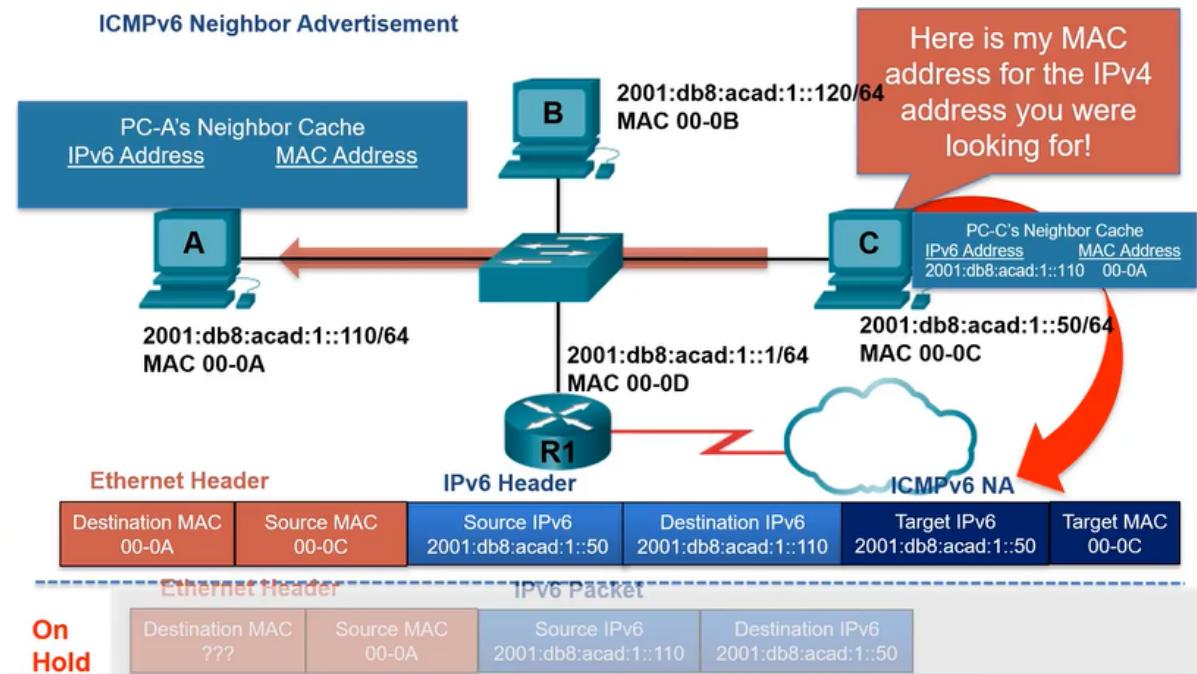


ICMPv6 Neighbor Solicitation

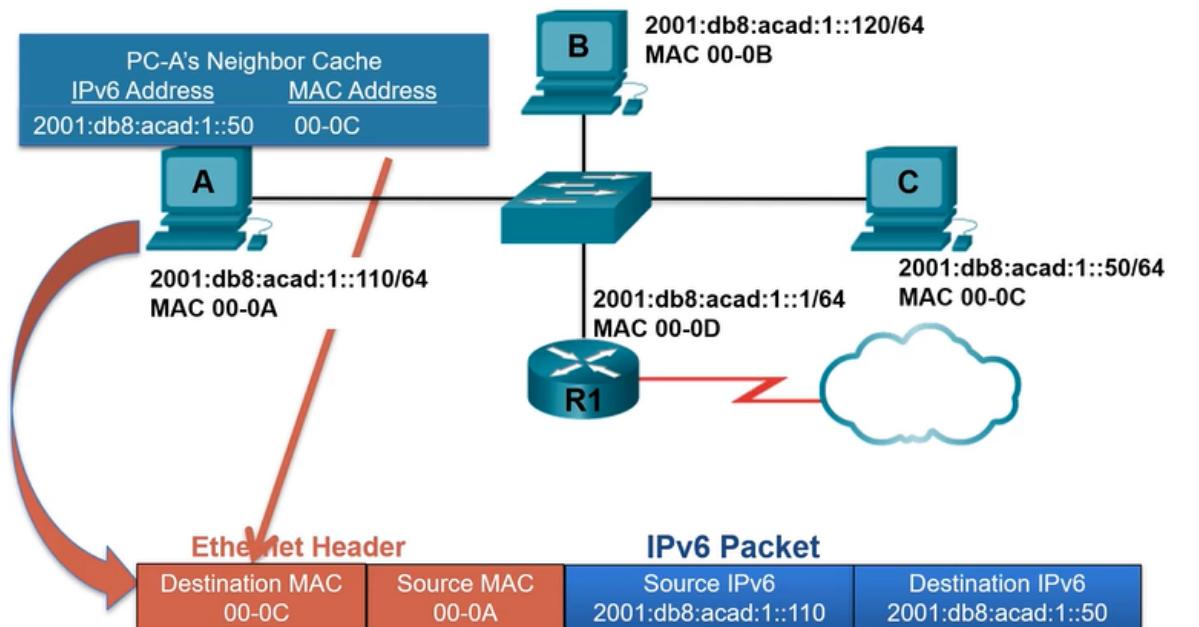
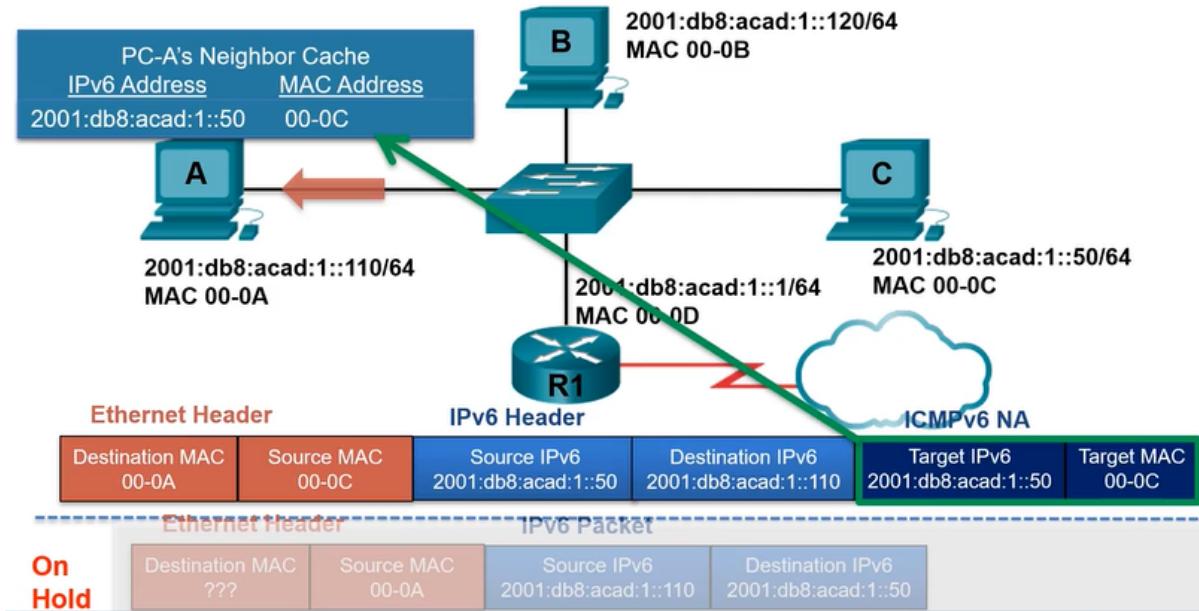


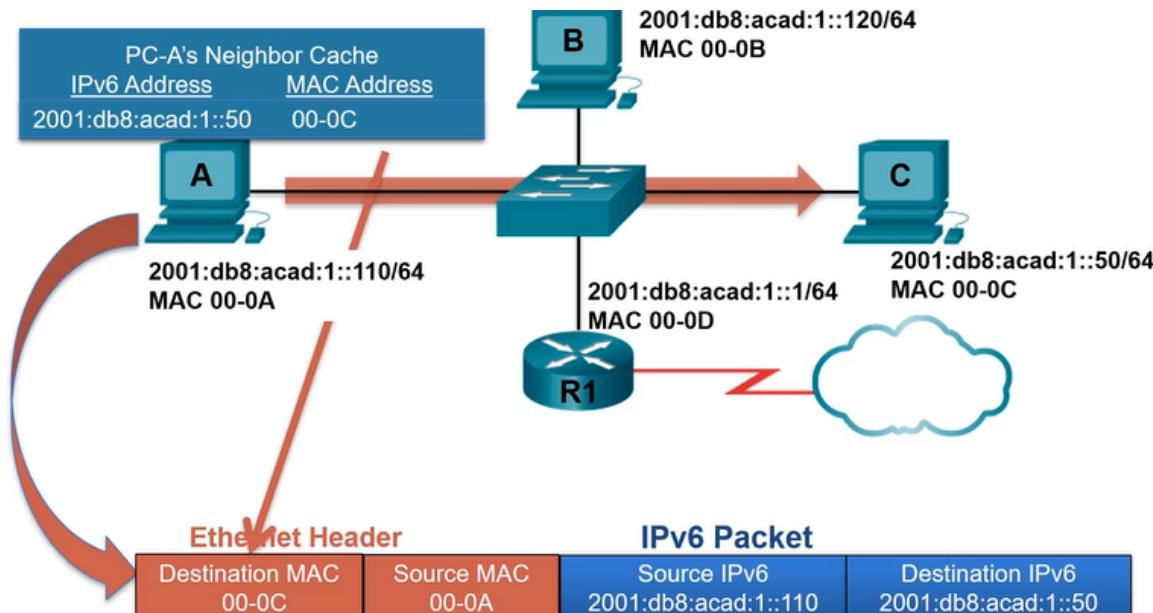






ICMPv6 Neighbor Advertisement





Mensajes de descubrimiento de vecinos IPv6

El protocolo IPv6 descubrimiento de vecinos se conoce a veces como ND o NDP. En este curso, nos referiremos a él como ND. ND proporciona servicios de resolución de direcciones, detección de routers y redirección para IPv6 mediante ICMPv6. ICMPv6 ND utiliza cinco mensajes ICMPv6 para realizar estos servicios:

- NS: Mensajes de solicitud de vecinos.
- NA: Mensaje de anuncio de vecino
- RS: Mensaje de solicitud del router
- RA: Mensajes de anuncio del router. Mensaje de* redirección

Los mensajes de solicitud de vecino y anuncio de vecino se utilizan para la mensajería de dispositivo a dispositivo, como la resolución de direcciones (similar a ARP para IPv4). Los dispositivos incluyen tanto equipos host como routers.

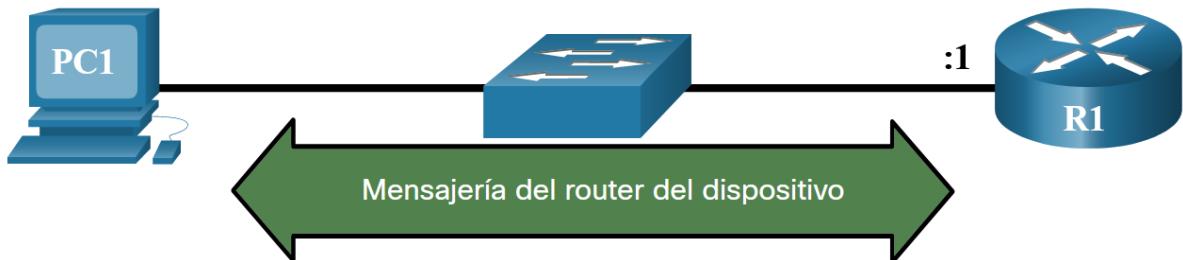
2001:db8:acad:1::/64



Los mensajes de solicitud de router y anuncio de router son para mensajes entre dispositivos y routers. Normalmente, la detección de routers se utiliza para la

asignación dinámica de direcciones y la configuración automática de direcciones sin estado (SLAAC).

2001:db8:acad:1::/64

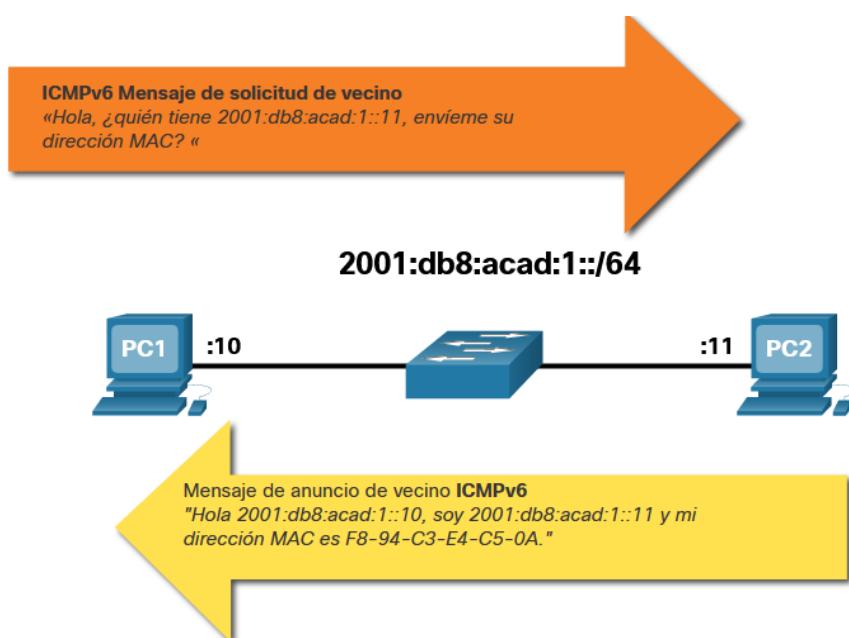


Nota: El quinto mensaje ICMPv6 ND es un mensaje de redirección que se utiliza para una mejor selección de siguiente salto.

Descubrimiento de vecinos IPv6: resolución de direcciones

Al igual que ARP para IPv4, los dispositivos IPv6 utilizan IPv6 ND para determinar la dirección MAC de un dispositivo que tiene una dirección IPv6 conocida.

Los mensajes ICMPv6 Solicitud de vecino y Anuncio de vecino se utilizan para la resolución de la dirección MAC. Esto es similar a las solicitudes ARP y las respuestas ARP utilizadas por ARP para IPv4. Por ejemplo, supongamos que PC1 desea hacer ping a PC2 en la dirección IPv6 **2001:db8:acad:1::11**. Para determinar la dirección MAC de la dirección IPv6 conocida, PC1 envía un mensaje de solicitud de vecino ICMPv6 como se ilustra en la figura.



Los mensajes de solicitud de vecinos ICMPv6 se envían utilizando direcciones multibroadcast Ethernet e IPv6 especiales. Esto permite que la NIC Ethernet del dispositivo receptor determine si el mensaje de solicitud de vecino es para sí mismo sin tener que enviarlo al sistema operativo para su procesamiento.

PC2 responde a la solicitud con un mensaje ICMPv6 Neighbor Advertisement que incluye su dirección MAC.

Mensajes ICMPv4 e ICMPv6

Protocolo de mensaje de control de Internet (ICMP Internet Control Message Protocols).

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.

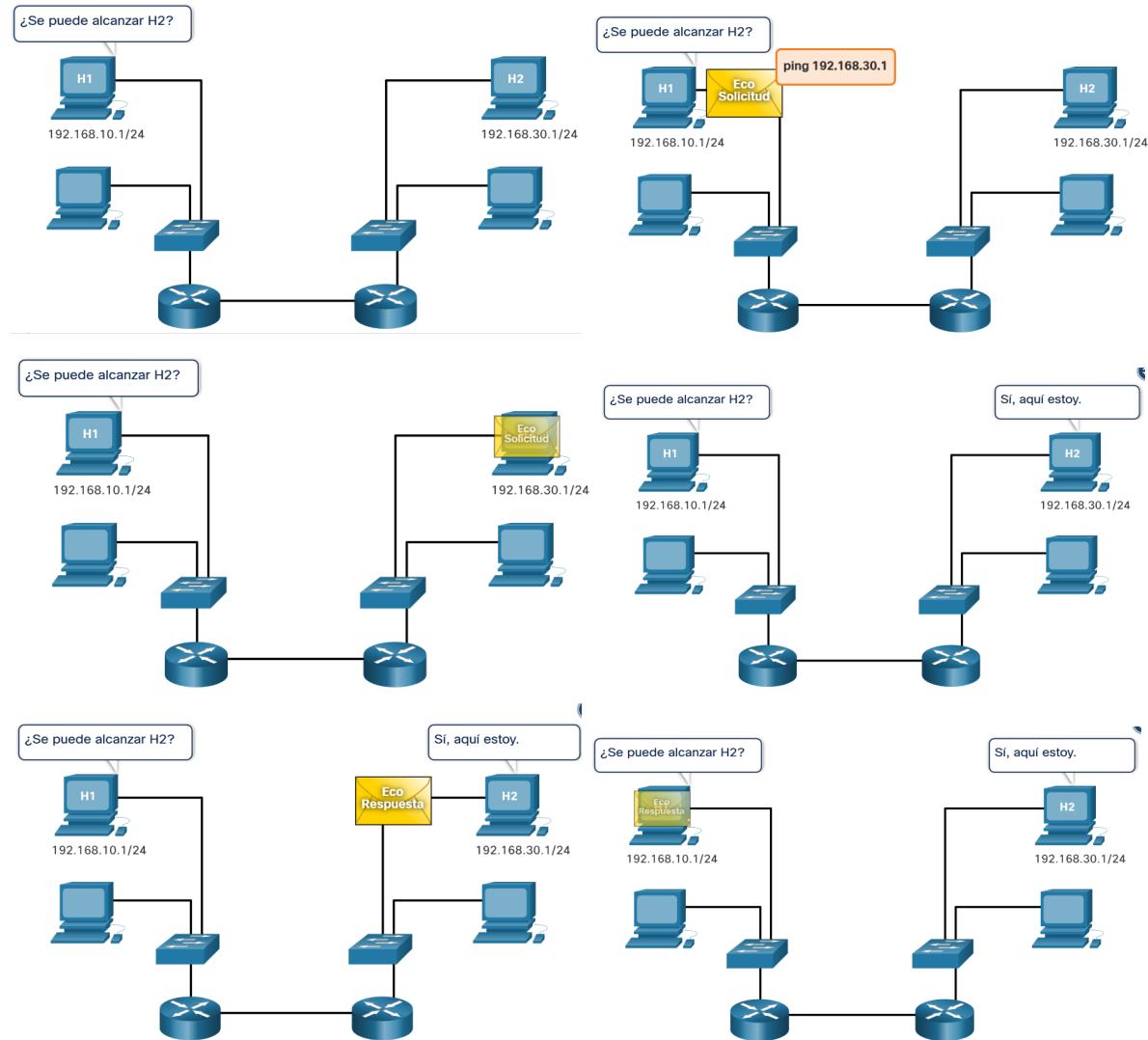
El protocolo ICMP está disponible tanto para IPv4 como para IPv6. El protocolo de mensajes para IPv4 es ICMPv4. ICMPv6 proporciona estos mismos servicios para IPv6, pero incluye funcionalidad adicional. En este curso, el término ICMP se utilizará para referirse tanto a ICMPv4 como a ICMPv6.

Los tipos de mensajes ICMP y las razones por las que se envían son extensos. Los mensajes ICMP comunes a ICMPv4 e ICMPv6 y discutidos en este módulo incluyen:

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

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 **ping** utilidad.



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

Algunos de los códigos de destino inalcanzable para ICMPv6 son los siguientes:

- 0 - No hay ruta para el destino

- 1 - La comunicación con el destino está prohibida administrativamente (por ejemplo, firewall)
- 2 — Más allá del alcance de la dirección de origen
- 3 - No se puede alcanzar la dirección
- 4 – Puerto inalcanzable

Nota: ICMPv6 tiene códigos similares pero ligeramente diferentes para los mensajes de destino inalcanzable.

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.

ICMPv6 también envía un mensaje de tiempo superado si el router no puede reenviar un paquete IPv6 debido a que el paquete caducó. En lugar del campo TTL de IPv4, ICMPv6 usa el campo Límite de salto de IPv6 para determinar si el paquete ha expirado.

La **Nota:** herramienta utiliza los mensajes de **traceroute** tiempo excedido.

Mensajes 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).

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 Router Solicitation)
- Mensaje de anuncio de router (RA Router Advertisement)

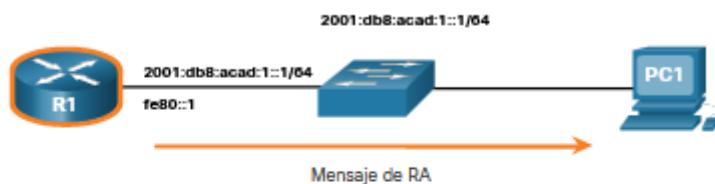
Los mensajes entre dispositivos IPv6, incluida la detección de direcciones duplicadas y la resolución de direcciones, son los siguientes:

- Mensaje de solicitud de vecino (NS Neighbor Solicitation)
- Mensaje de anuncio de vecino (NA Neighbor Advertisement)

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

Mensaje RA

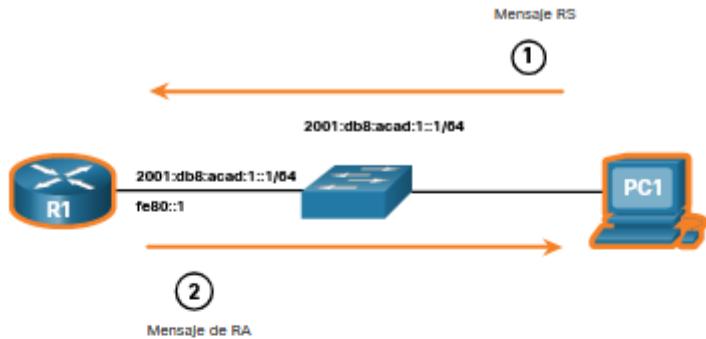
Los enruteadores habilitados para IPv6 envían mensajes de RA cada 200 segundos para proporcionar información de direccionamiento a los hosts habilitados para IPv6. El mensaje RA puede incluir información de direccionamiento para el host, como el prefijo, la longitud del prefijo, la dirección DNS y el 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.



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.

Mensaje 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.



R1 responde a la RS con un mensaje de RA.

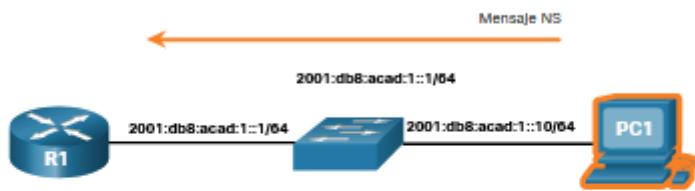
1. PC1 envía un mensaje RS, «Hola, acabo de arrancar. ¿Hay un enrutador IPv6 en la red? Necesito saber cómo obtener la información de mi dirección IPv6 de forma dinámica».
2. R1 responde con un mensaje de RA. «Hola a todos los dispositivos habilitados para IPv6. Soy R1 y puedes usar SLAAC para crear 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. »

Mensaje 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 duplicate address detection) 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, como se muestra en la figura.

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.

Nota: No se requiere DAD, pero RFC 4861 recomienda que DAD se realice en direcciones unicast.



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?»

Mensaje 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.

En la figura, R1 envía un mensaje NS a 2001:db8:acad:1::10 pidiendo su dirección MAC.

Ping: Prueba de Conectividad

Ping es una utilidad de prueba de IPv4 e IPv6 que utiliza la solicitud de eco ICMP y los mensajes de respuesta de eco para probar la conectividad entre los hosts.

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.

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

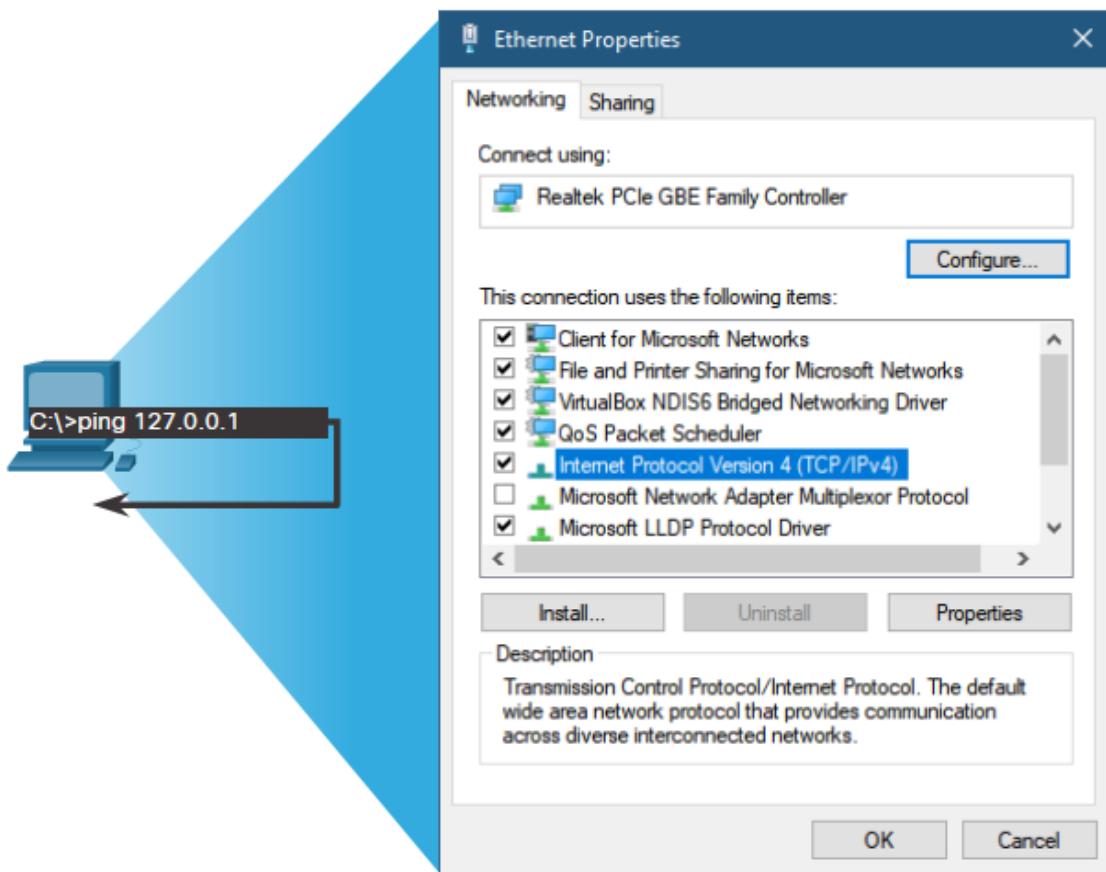
Los tipos de pruebas de conectividad que se realizan con **ping** son los siguientes:

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

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.



- Hacer ping al host local permite confirmar que el protocolo TCP/IP se encuentra instalado en el host y que funciona.
- Hacer ping a 127.0.0.1 ocasiona que un dispositivo se haga ping a sí mismo.

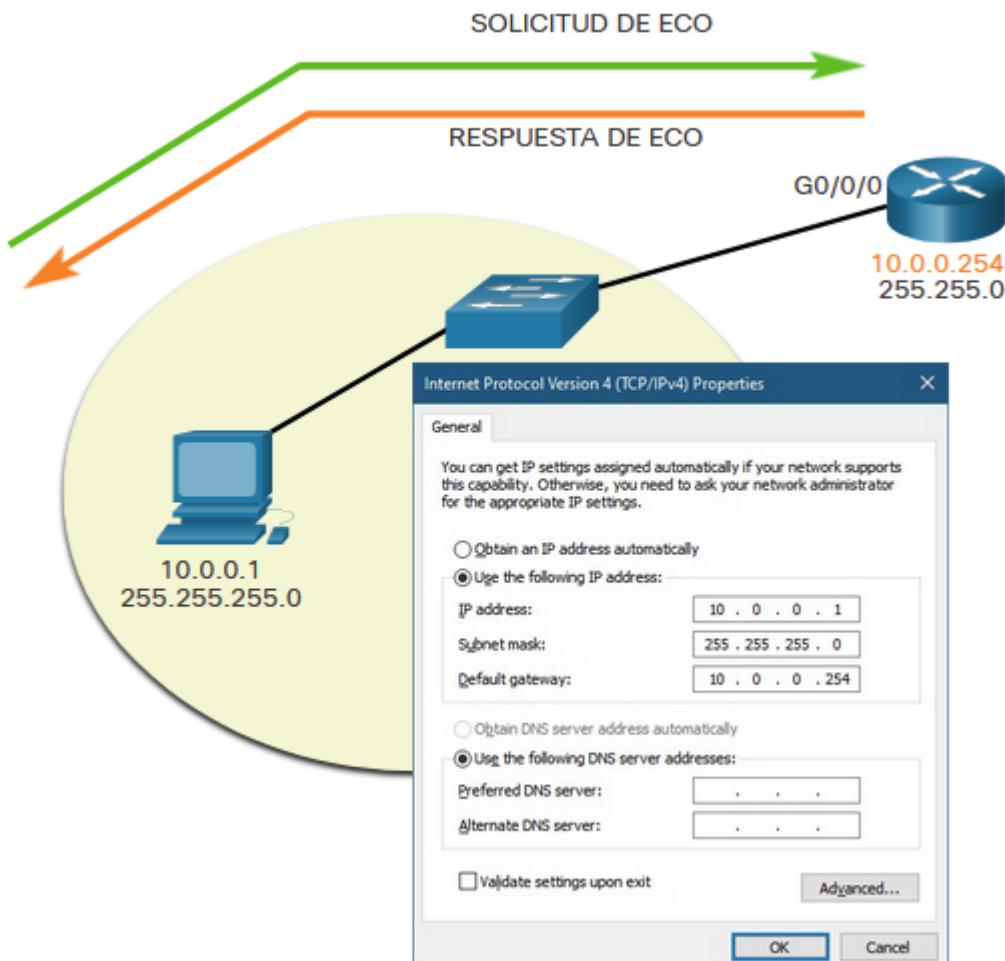
Hacer ping al gateway predeterminado

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 en la **ping** 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.

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.



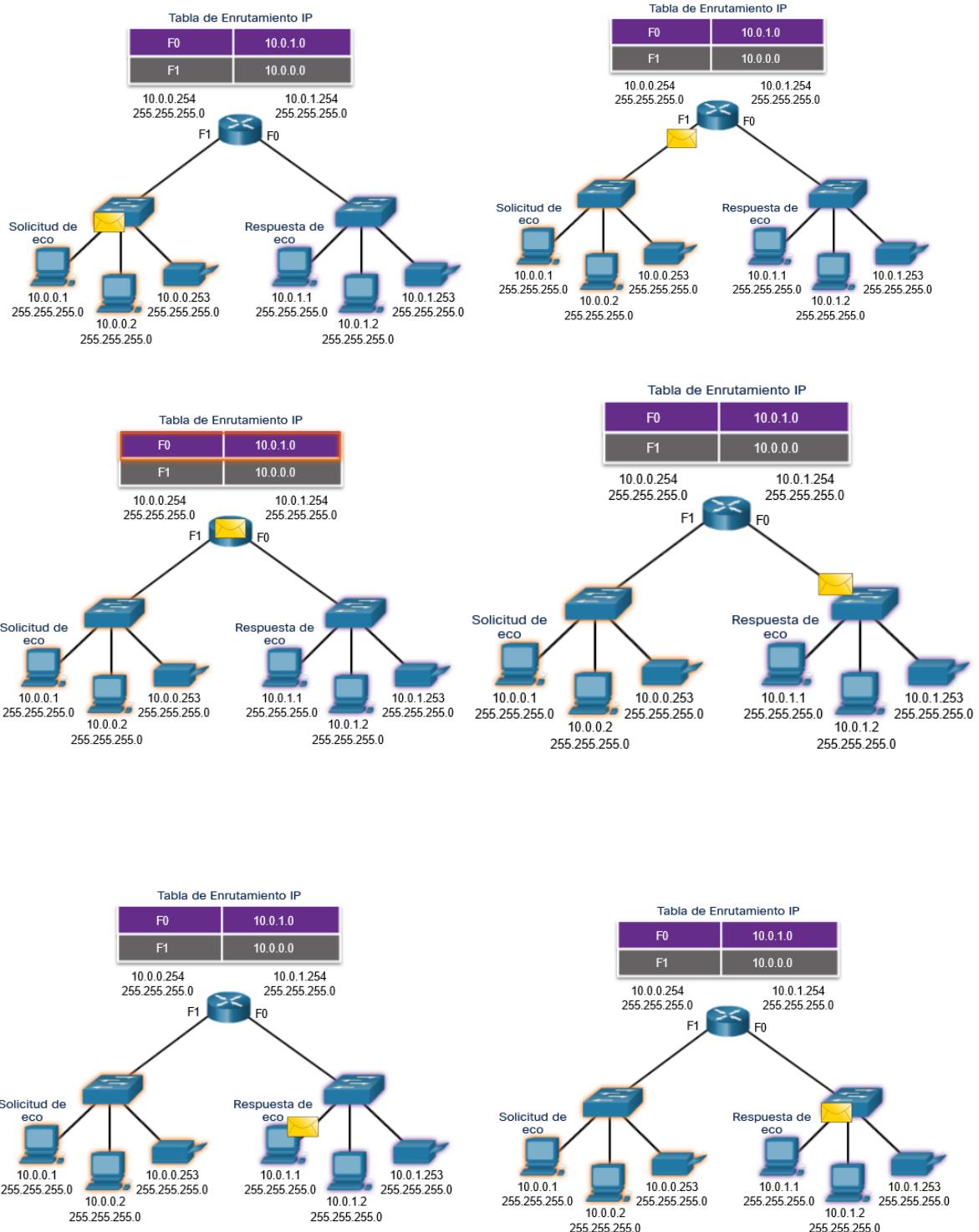
Hacer ping a un Host Remoto

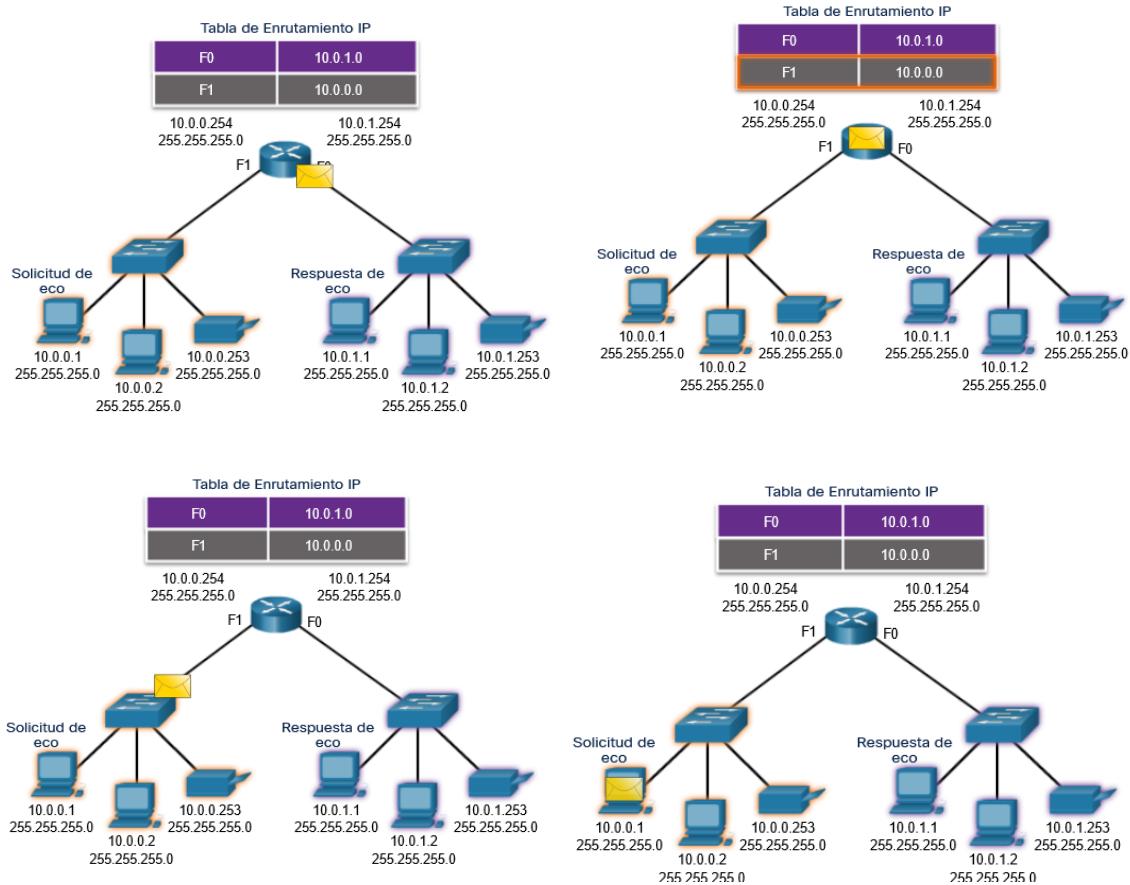
También se puede utilizar el comando ping para probar la capacidad de un host local para comunicarse en una interconexión de redes. El host local puede hacer ping a un host IPv4 operativo de una red remota, como se muestra en la ilustración. El router utiliza su tabla de enruteamiento IP para reenviar los paquetes.

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

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

Nota: Muchos administradores de red limitan o prohíben la entrada de mensajes ICMP en la red corporativa; **ping** por lo tanto, la falta de respuesta podría deberse a restricciones de seguridad.





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.

Tiempo de ida y vuelta (RTT)

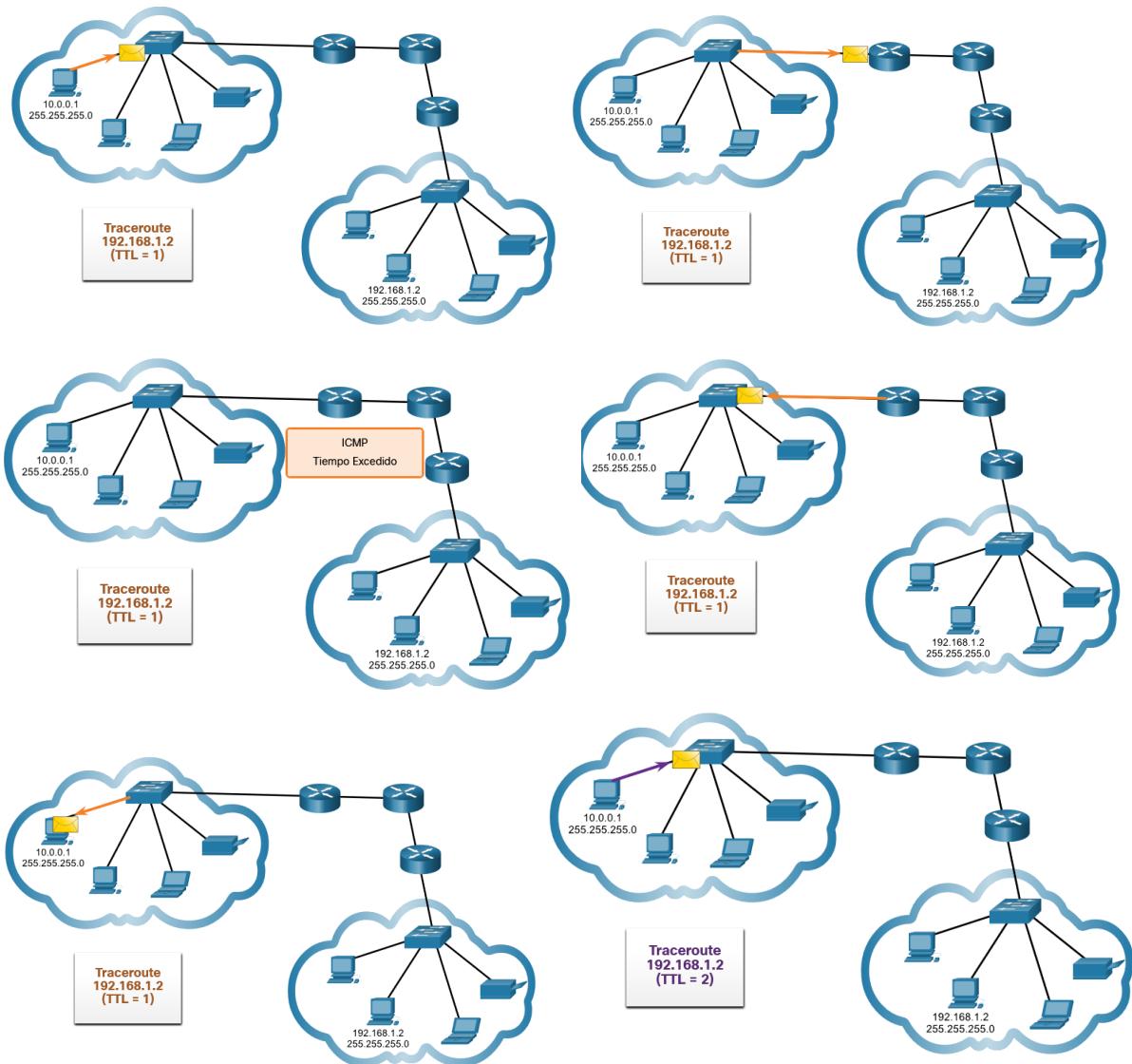
El uso de traceroute proporciona tiempo de ida y vuelta para cada salto a lo largo del camino e indica si un salto no responde. El tiempo de ida y vuelta es el tiempo que tarda un paquete en llegar al host remoto y que la respuesta del host regrese. Se utiliza un asterisco (*) para indicar un paquete perdido o no respondido.

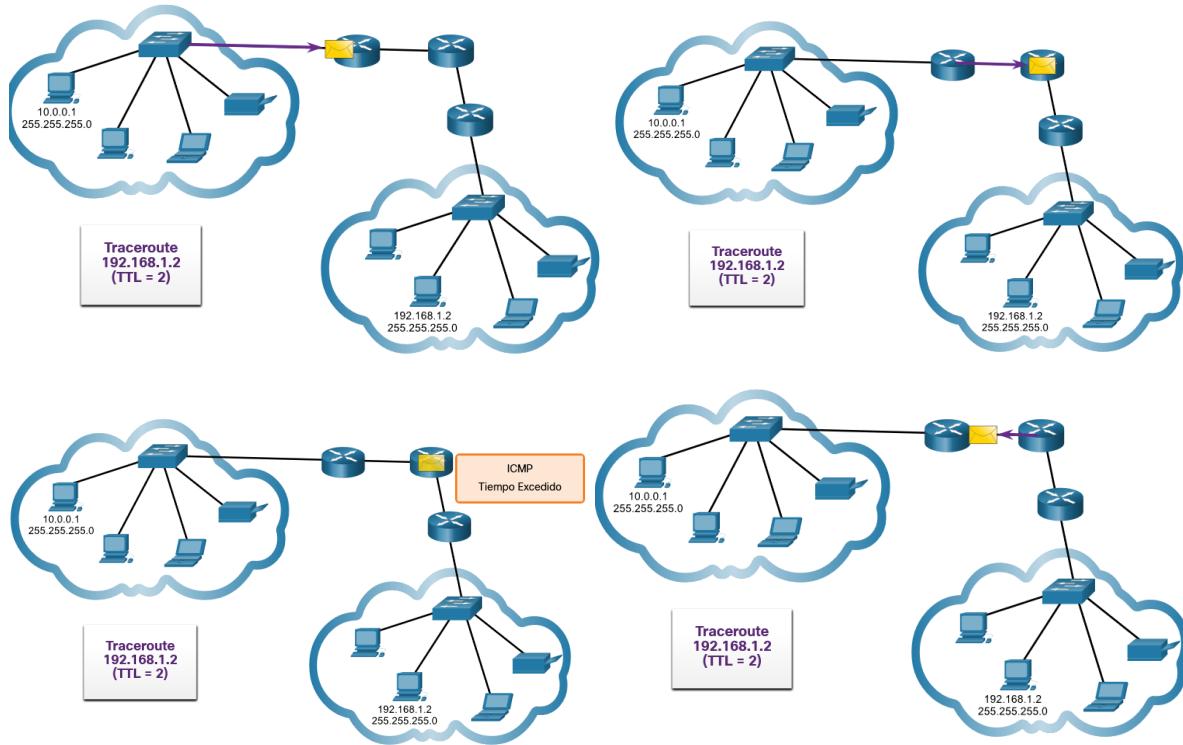
Esta información se puede usar para localizar un enrutador problemático en la ruta o puede indicar que el enrutador está configurado para no responder. Si en la pantalla

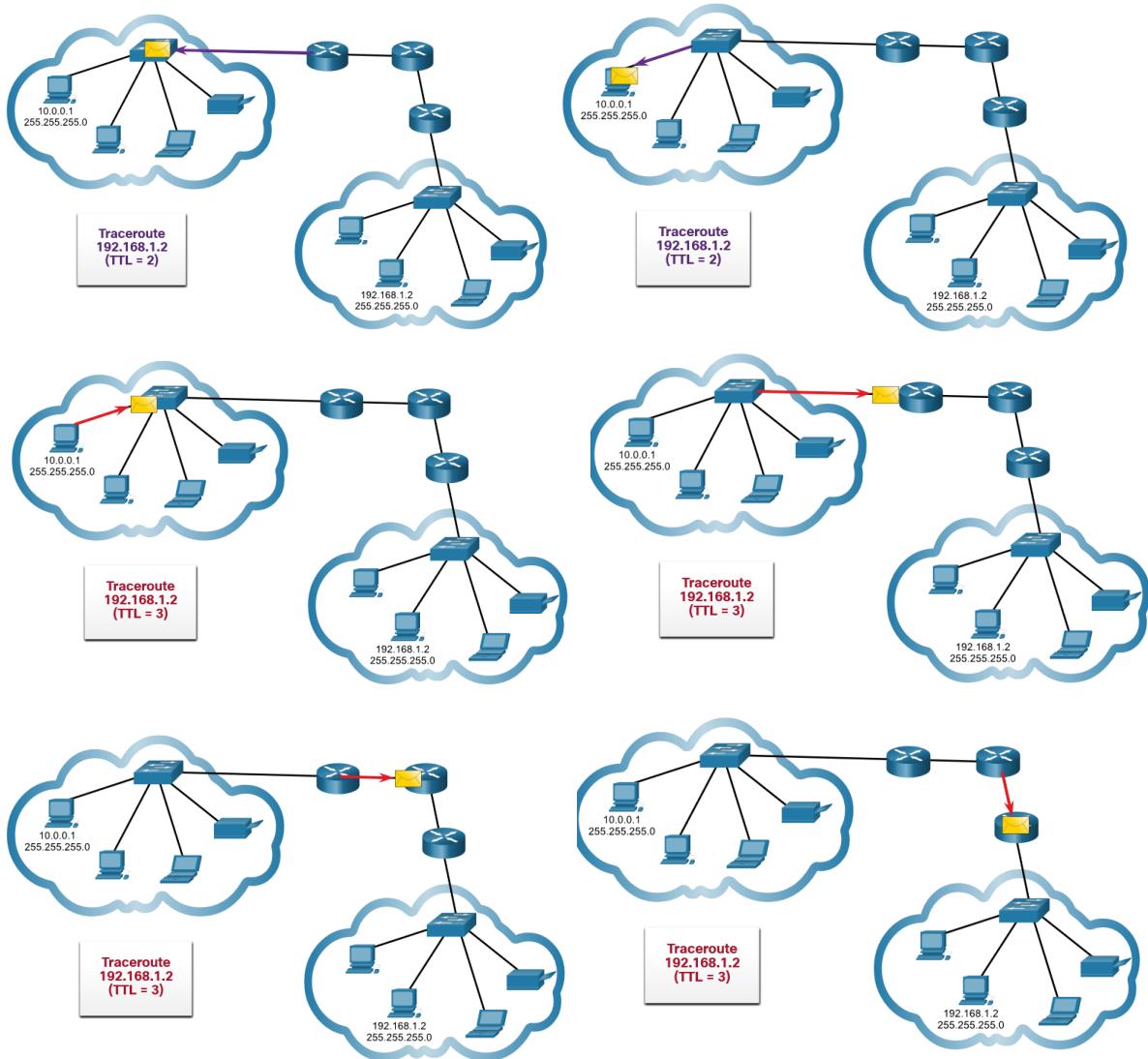
se muestran tiempos de respuesta elevados o pérdidas de datos de un salto en particular, esto constituye un indicio de que los recursos del router o sus conexiones pueden estar sobrecargados.

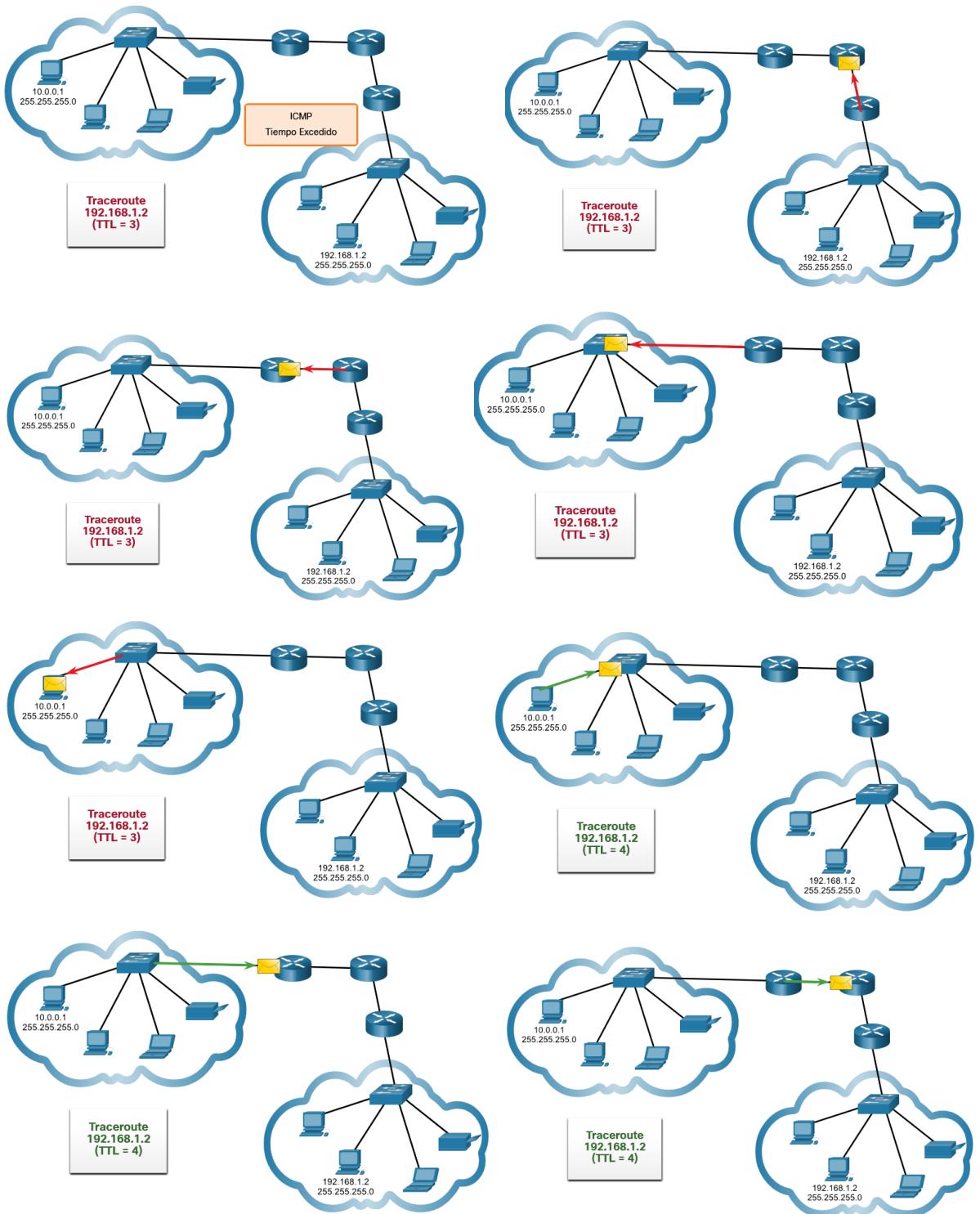
TTL de IPv4 y Límite de Saltos en IPv6

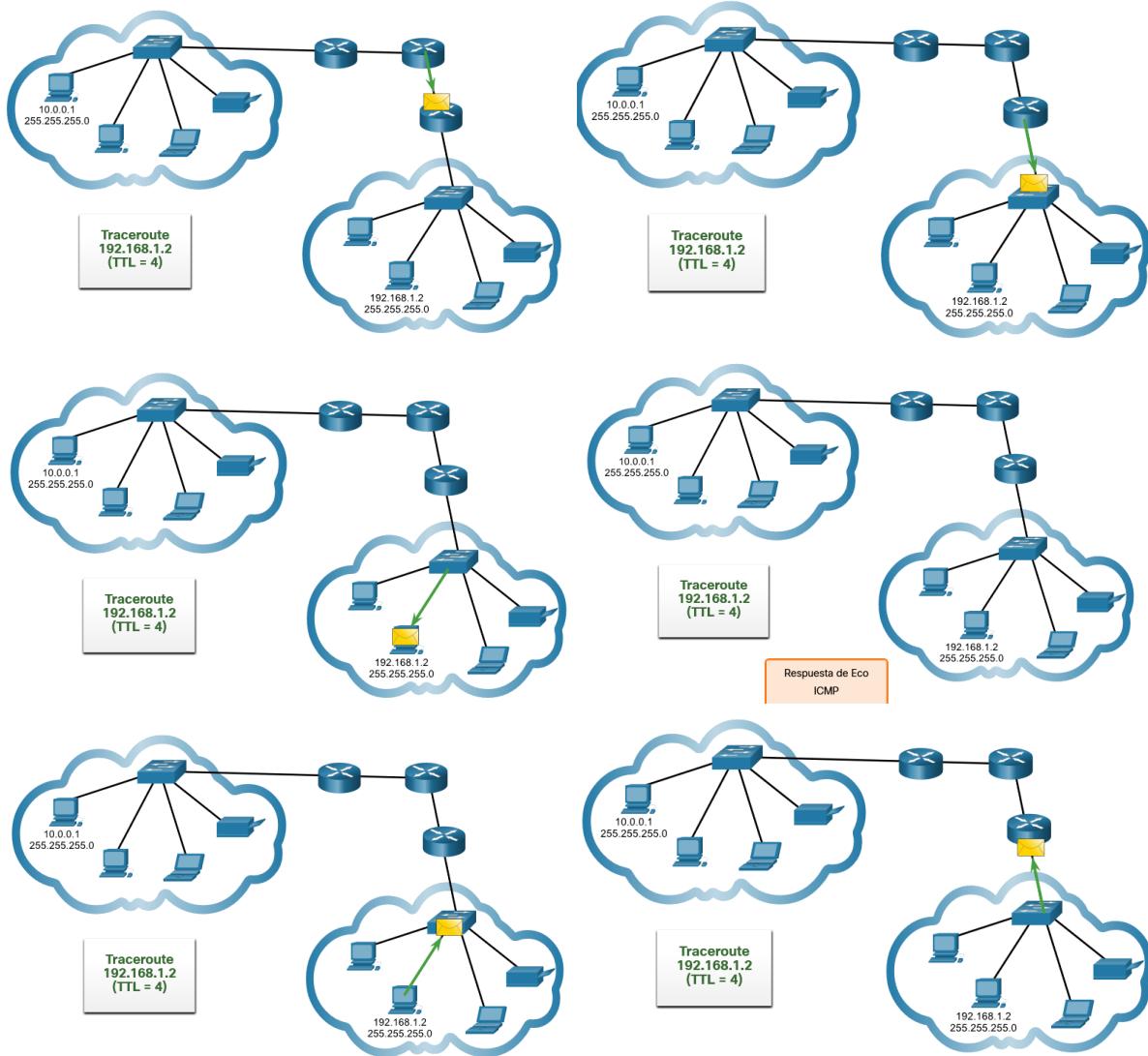
Traceroute utiliza una función del campo TTL en IPv4 y el campo Límite de salto en IPv6 en los encabezados de Capa 3, junto con el mensaje ICMP Time Exceeded.

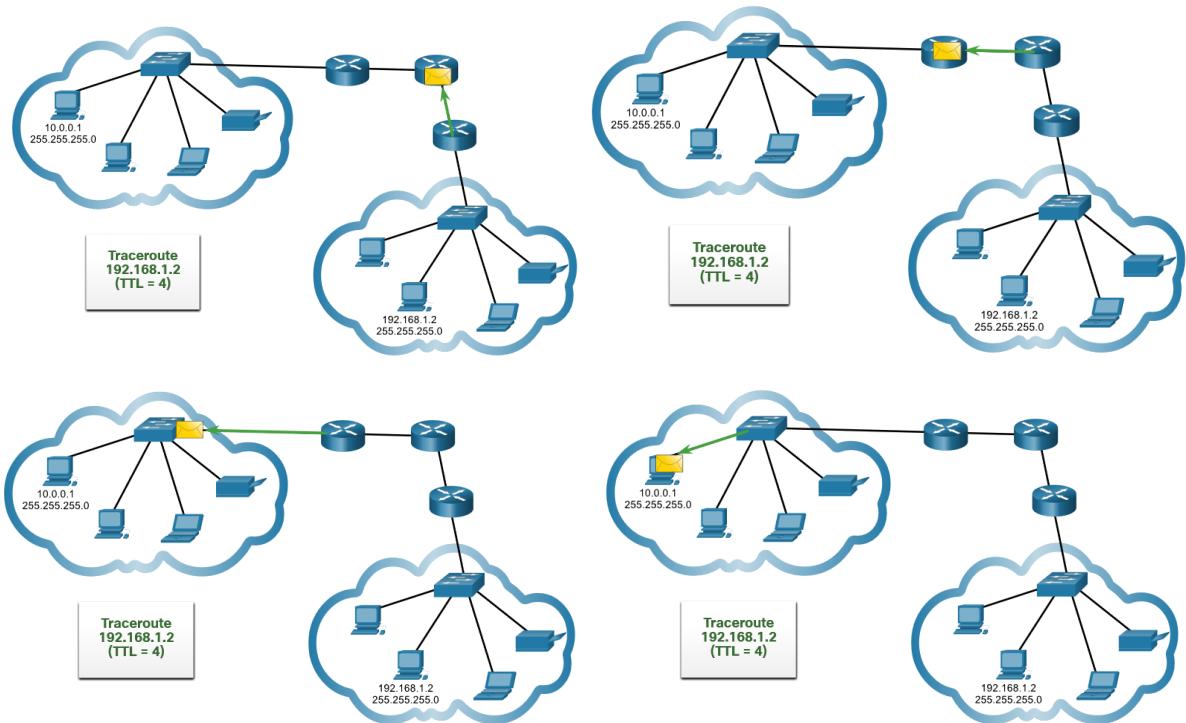












La primera secuencia de mensajes enviados desde traceroute tiene un valor de 1 en el campo TTL. Esto hace que el TTL agote el tiempo de espera del paquete IPv4 en el primer router. Este enrutador responde con un mensaje ICMPv4 Tiempo excedido. Traceroute ahora tiene la dirección del primer salto.

A continuación, Traceroute incrementa progresivamente el campo TTL (2, 3, 4...) para cada secuencia de mensajes. Esto proporciona el rastro con la dirección de cada salto a medida que los paquetes caducan más adelante en la ruta. El campo TTL sigue aumentando hasta que se alcanza el destino, o se incrementa a un máximo predefinido.

Una vez que se alcanza el destino final, el host responde con un mensaje de puerto inalcanzable ICMP o un mensaje de respuesta de eco ICMP en lugar del mensaje de tiempo excedido ICMP.