ARP y ND IPv6

Módulo 07

Los hosts y los enrutadores crean tablas de enrutamiento para garantizar que puedan enviar y recibir datos a través de las redes. Entonces, ¿cómo se crea esta información en una tabla de enrutamiento? Como administrador de red, puede ingresar estas direcciones MAC e IP manualmente. Pero eso llevaría mucho tiempo y la probabilidad de cometer algunos errores es excelente. ¿Está pensando que debe haber alguna forma de que esto pueda hacerse automáticamente, por los propios hosts y enrutadores? ¡Claro, tienes razón! Y a pesar de que es automático, aún debe comprender cómo funciona esto, ya que es posible que deba solucionar un problema, o peor, su red podría ser atacada por un actor de amenazas

Direccionamiento MAC e IP

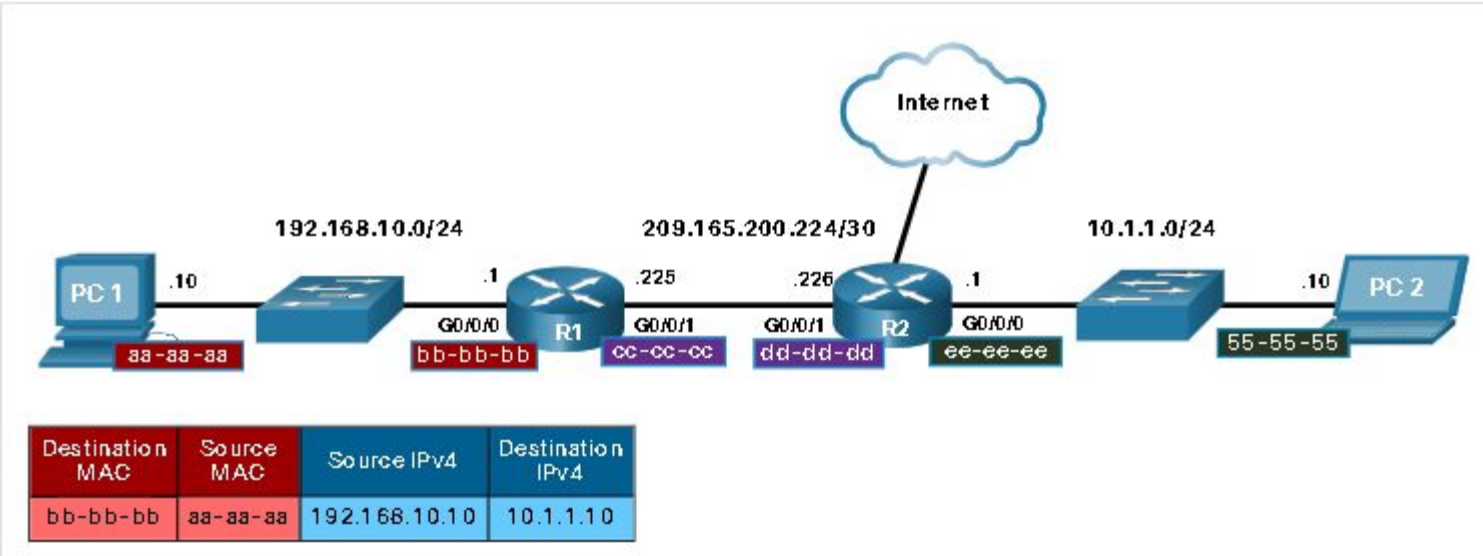
Dirección IPv4 en binario

Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

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.

Destino en red remota.

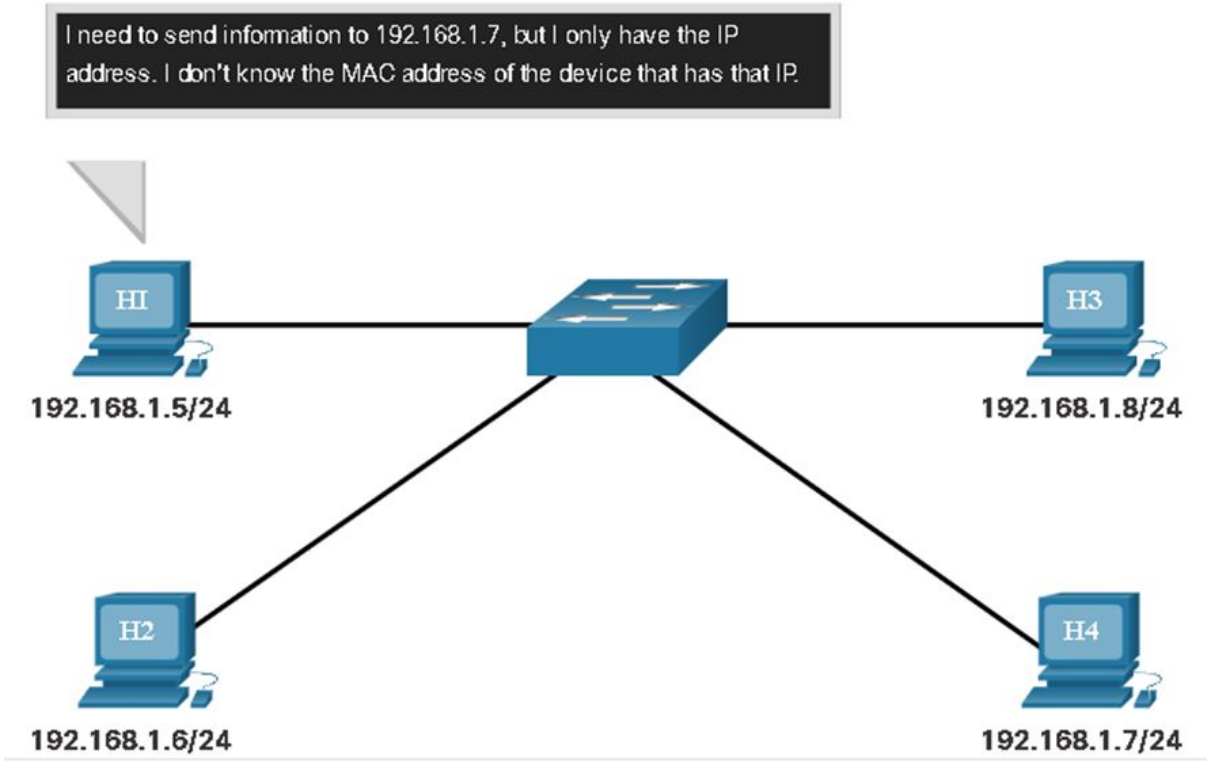
Cuando la dirección IP de destino (IPv4 o IPv6) está en una red remota, la dirección MAC de destino será la dirección de la puerta de enlace predeterminada del host (es decir, la interfaz del enrutador).



ARP

Protocolo ARP

- Si su red está utilizando el protocolo de comunicaciones IPv4, el Protocolo de resolución de direcciones, o ARP, es lo que necesita para asignar direcciones IPv4 a direcciones MAC.

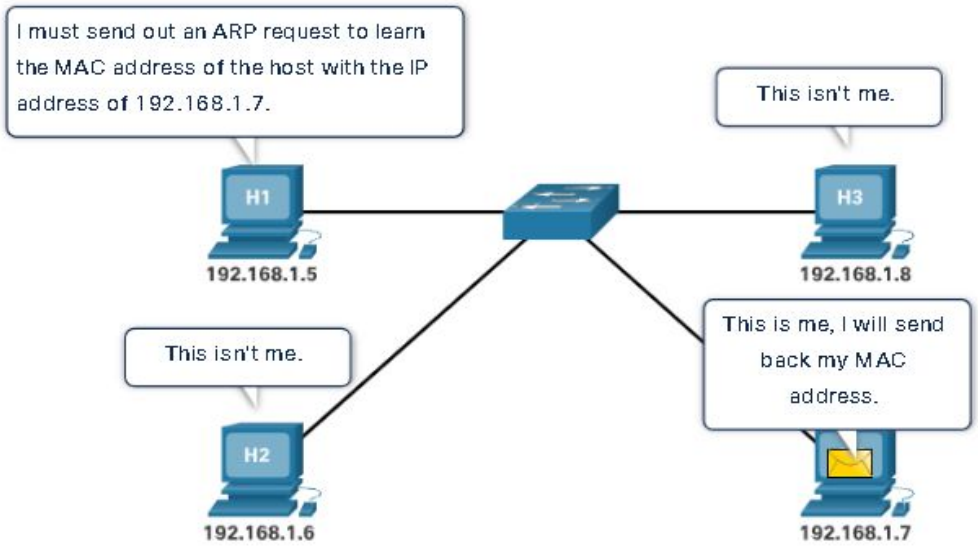


Funciones del protocolo ARP.

- Cuando se envía un paquete a la capa de enlace de datos para ser encapsulado en una trama de Ethernet, el dispositivo hace referencia a una tabla en su memoria para encontrar la dirección MAC que se asigna a la dirección IPv4. Esta tabla se almacena temporalmente en la memoria RAM y se denomina tabla ARP o caché ARP.

- Si la dirección IPv4 de destino del paquete está en la misma red que la dirección IPv4 de origen, el dispositivo buscará en la tabla ARP la dirección IPv4 de destino.

- Cada entrada o fila de la tabla ARP enlaza una dirección IPv4 con una dirección MAC.

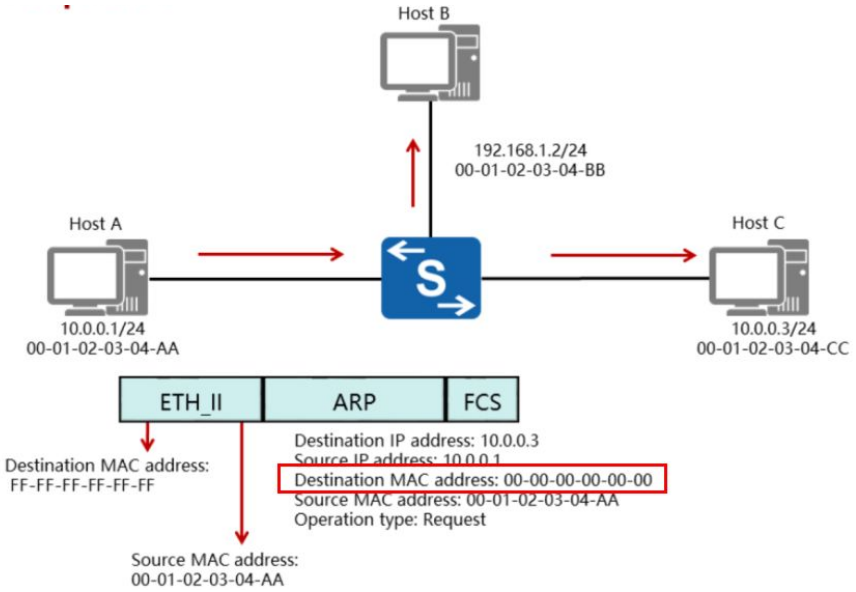


ARP Request

- 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 ARP se encapsulan directamente dentro de una trama Ethernet. No hay encabezado IPv4. La solicitud ARP se encapsula en una trama Ethernet utilizando la siguiente información de encabezado:

- Dirección MAC de destino: esta es una dirección de difusión FF-FF-FF-FF-FF-FF que requiere que todas las NIC de Ethernet en la LAN acepten y procesen la solicitud 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 0x806. Esto informa a la NIC receptora que la porción de datos de la trama debe pasar al proceso ARP.



ARP Reply

- Only the device with the target IPv4 address associated with the ARP request will respond with an ARP reply. The ARP reply is encapsulated in an Ethernet frame using the following header information:

- Destination MAC address – This is the MAC address of the sender of the ARP request.
- Source MAC address – This is the MAC address of the sender of the ARP reply.
- Type - ARP messages have a type field of 0x806. This informs the receiving NIC that the data portion of the frame needs to be passed to the ARP process.

ARP REPLY		
L2 Header	SMAC	**B**
	DMAC	**A**
	TYPE	**0x0806**
ARP HEADER	OpCode	**Reply**
	Sender MAC Address	**B**
	Sender IP Address	**10.1.1.2**
	Target MAC Address	**A**
	Target IP Address	**10.1.1.1**

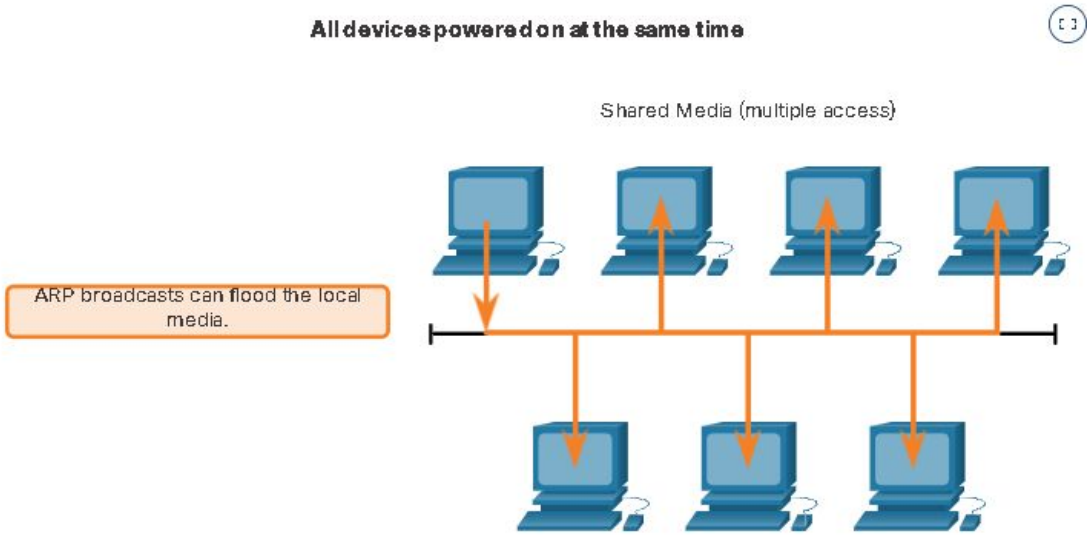
Tablas ARP en dispositivos de red

```
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>
```

Problemas en ARP

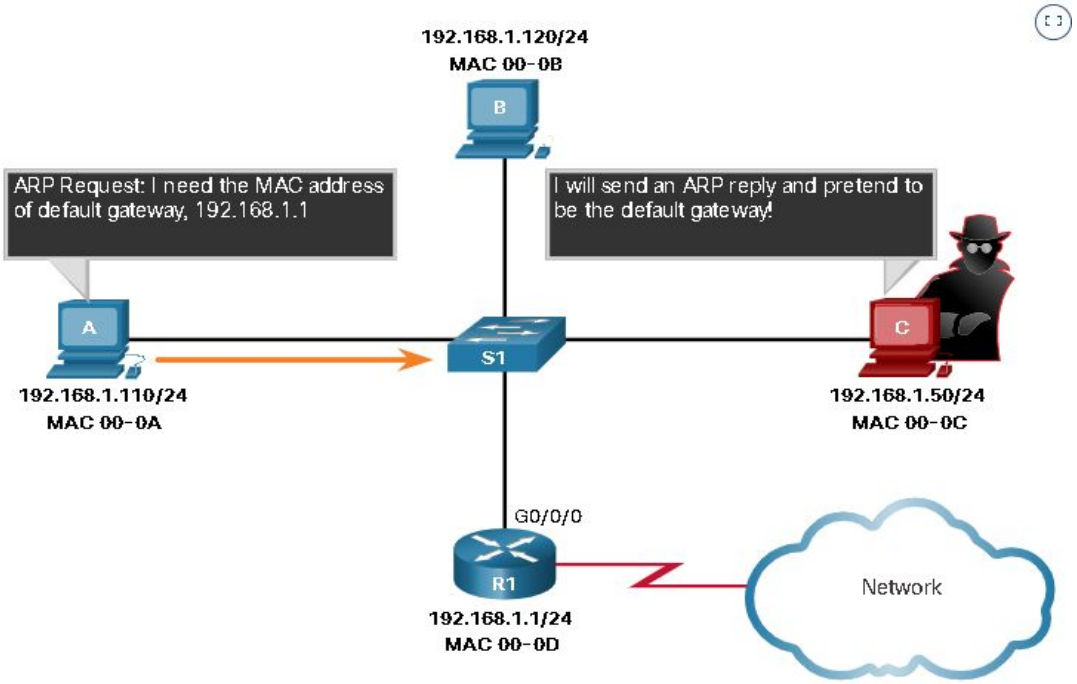
ARP Broadcoast

Como trama de difusión, todos los dispositivos de la red local reciben y procesan una solicitud ARP. En una red comercial típica, estas transmisiones probablemente tendrían un impacto mínimo en el rendimiento de la red. Sin embargo, si un gran número de dispositivos se encendieran y todos comenzaran a acceder a los servicios de red al mismo tiempo, podría haber una reducción en el rendimiento durante un corto período de tiempo,



ARP Spoofing

En algunos casos, el uso de ARP puede conducir a un riesgo potencial de seguridad. Un actor de amenaza puede usar la suplantación de ARP para realizar un ataque de envenenamiento por ARP. Esta es una técnica utilizada por un actor de amenazas para responder a una solicitud ARP de una dirección IPv4 que pertenece a otro dispositivo, como la puerta de enlace predeterminada.

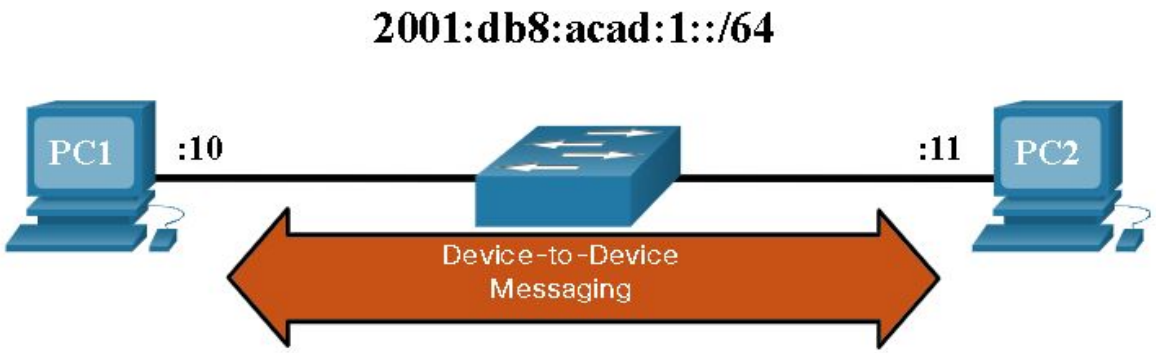


Descubrimiento de vecinos en IPv6

Mensajes de descubrimiento de vecinos IPv6

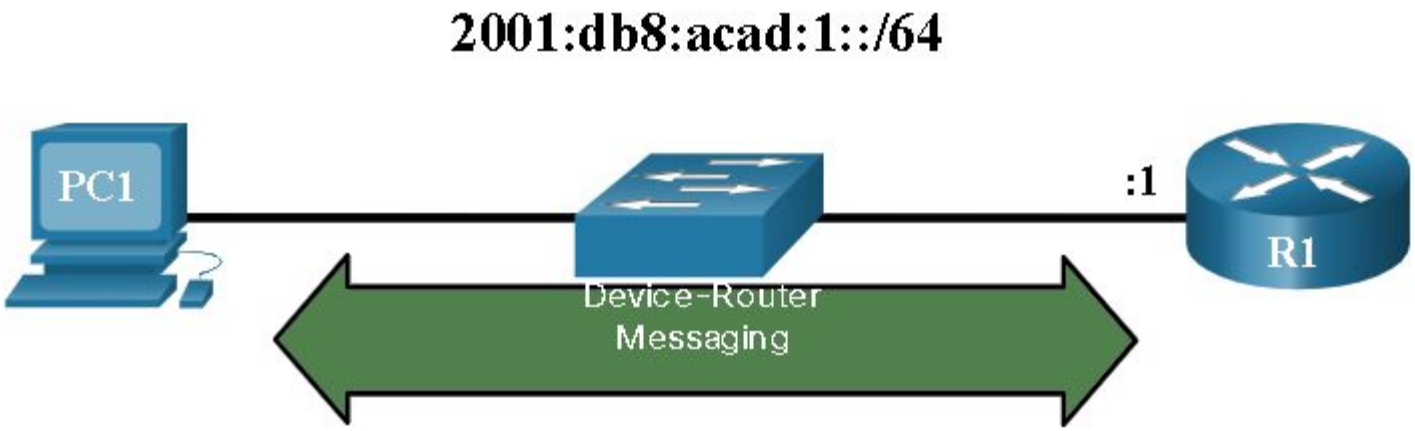
El protocolo de descubrimiento de vecinos IPv6 a veces se denomina ND o NDP. ND proporciona resolución de direcciones, descubrimiento de enrutadores y servicios de redireccionamiento para IPv6 utilizando ICMPv6. ICMPv6 ND utiliza cinco mensajes ICMPv6 para realizar estos servicios:

- Mensajes de solicitud de vecinos
- Mensajes de anuncio de vecinos
- Mensajes de solicitud de enrutador
- Mensajes de anuncio de enrutador
- Redirigir mensaje



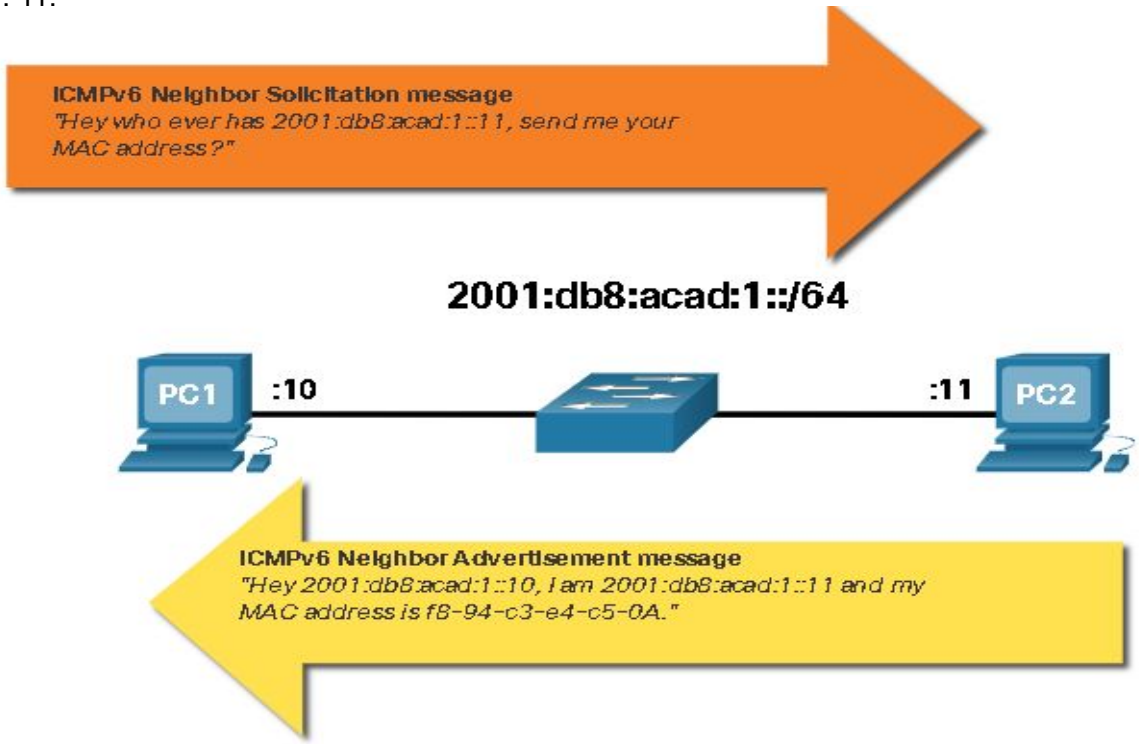
Solicitud de enrutador y anuncio de enrutador

Los mensajes son para mensajes entre dispositivos y enrutadores. Normalmente, el descubrimiento de enrutadores se utiliza para la asignación dinámica de direcciones y la configuración automática de direcciones sin estado (SLAAC).



Descubrimiento de vecinos IPv6: resolución de direcciones

Al igual que ARP para IPv4, los dispositivos IPv6 usan 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, suponga que PC1 quiere hacer ping a PC2 en la dirección IPv6 2001: db8: acad :: 11.



Laboratorio

Módulo 07

¡Muchas gracias!

¡Sigamos trabajando!