Modulo 9 resolucion de direccion

9.0 Introducción

Desplázate para empezar

9.0.1 ¿Por qué debería tomar este módulo?

¡Bienvenido a Resolución de Direcciones!

Tanto los hosts como los routers crean tablas de enrutamiento para garantizar que pueden 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 introducir estas direcciones MAC e IP manualmente. Pero eso llevaría mucho tiempo y la probabilidad de cometer algunos errores es grande. ¿Está pensando que debe haber alguna manera de que esto pueda hacerse automáticamente, por los propios hosts y routers? ¡Por supuesto, tiene razón!. Y aunque sea automático, debe entender cómo funciona esto, porque puede que tenga que solucionar un problema o, peor aún, su red podría ser amenazada por un atacante. ¿Está listo para obtener información sobre la resolución de direcciones?. Este módulo tiene varios videos muy buenos para ayudar a explicar los conceptos, así como tres actividades Packet Tracer para consolidar su comprensión. ¿Por qué esperar?

9.0.2 ¿Qué aprenderé en este módulo?

Título del módulo: Resolución de dirección

Objetivos del módulo: Explique cómo ARP y ND permiten la comunicación en una red.

9.1 MAC e IP

Desplázate para empezar

9.1.1 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.

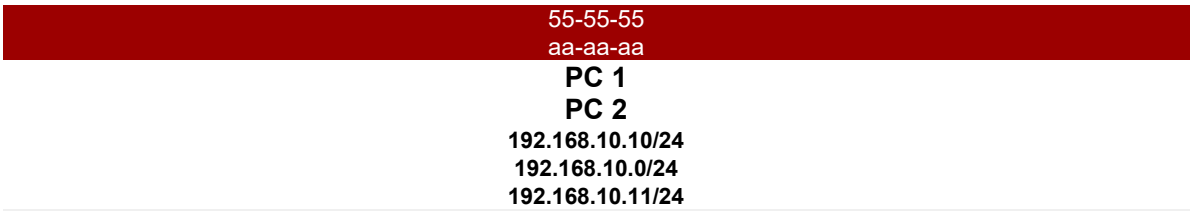
Hay dos direcciones primarias asignadas a un dispositivo en una LAN Ethernet:

- **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.

La imagen es un diagrama de red con PC 1 en IP 192.168.10.10/24 con MAC simplificado aa-aa-aa, conectado a un switch en IP 192.168.10.0/24, conectado a PC 2 en IP 192.168.10.11/24 con MAC simplificado 55-55. Debajo del diagrama hay cuatro cuadros que leen de izquierda a derecha: Destino MAC 55-55, MAC de origen aa-aa-aa, IPv4 192.168.10.10 y Destino IPv4 192.168.10.11.



En este ejemplo, PC1 desea enviar un paquete a PC2. La figura muestra las direcciones MAC de origen y destino de Capa 2 y el direccionamiento IPv4 de Capa 3 que se incluirían en el paquete enviado desde PC1.

La trama Ethernet de capa 2 contiene lo siguiente:

- **Dirección MAC de destino:** esta es la dirección MAC simplificada de PC2, 55-55.
- **Dirección MAC de origen:** es la dirección MAC simplificada de la NIC Ethernet en PC1, aa-aa-aa.

El paquete IP de capa 3 contiene lo siguiente:

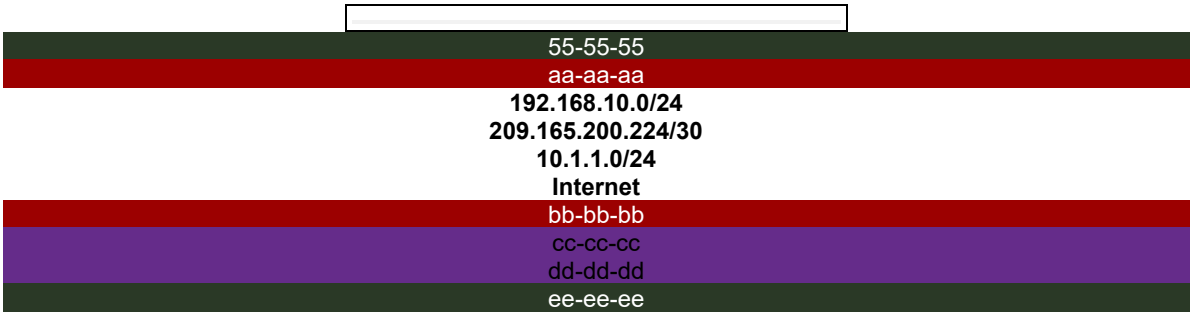
- **Dirección IPv4 de origen:** esta es la dirección IPv4 de PC1, 192.168.10.10.
- **Dirección IPv4 de destino:** esta es la dirección IPv4 de PC2, 192.168.10.11.

9.1.2 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.

La imagen es un diagrama de red que muestra el direccionamiento MAC e IPv4 de origen y destino para el primer salto cuando la información se envía desde un PC en una red a un destino en una red remota. La descripción que sigue son los nombres, conexiones y direcciones de los dispositivos de izquierda a derecha. PC 1 está conectado a un switch que está conectado al router R1 interfaz G0/0/0 en la red 192.168.10.0/24. PC 1 tiene una IP de 192.168.10.10 y MAC de aa-aa-aa. La interfaz G0/0/0 en R1 tiene una IP de 192.168.10.1 y MAC de bb-bb-bb. R1 tiene una interfaz G0/0/1 conectada a la interfaz del router R2 G0/0/1 en la red 209.165.200.224/30. La interfaz G0/0/1 en R1 tiene una IP de 209.165.200.225 y MAC cc-cc-cc. La interfaz G0/0/1 en R2 tiene una IP de 209.165.200.226 y MAC dd-dd-dd. R2 tiene una interfaz G0/0/0 conectada a un switch conectado al PC 2 en la red 10.1.1.0/24. La interfaz G0/0/0 en R2 tiene una IP de 10.1.1.1 y MAC ee-ee-ee. PC 2 tiene una IP de 10.10.10.10 y MAC 55-55. R2 también tiene una conexión en la parte superior que conduce a la nube de Internet. Debajo del diagrama en la red 192.168.10.0/24 hay cuatro cuadros que leen de izquierda a derecha: MAC de destino bb-bb-bb, MAC de origen aa-aa-aa, IPv4 192.168.10.10 y Destino IPv4 10.1.1.10. R1R2PC 2 PC 1.10.1.225.226.1.10G0/0/1G0/0/1G0/0/0G0/0/0



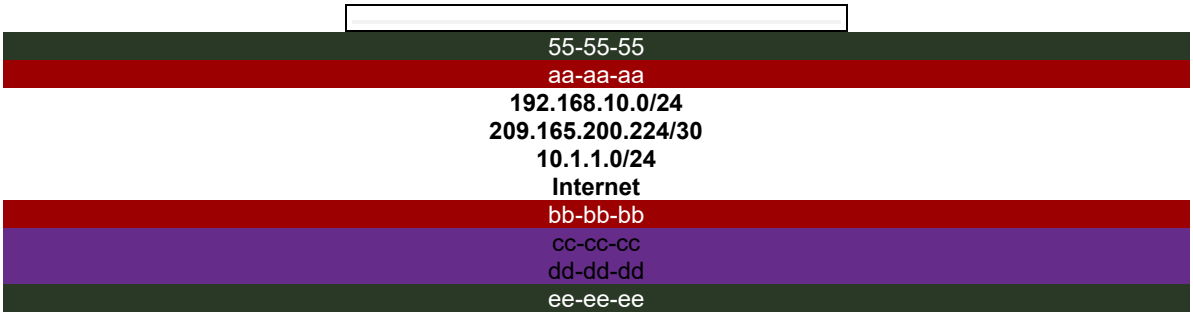
En este ejemplo, PC1 desea enviar un paquete a PC2. PC2 se encuentra en una red remota. Dado que la dirección IPv4 de destino no está en la misma red local que PC1, la dirección MAC de destino es la del gateway predeterminado local en el router.

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.

La imagen es un diagrama de red que muestra el direccionamiento MAC e IPv4 de origen y destino cuando la información se pasa entre dos routers a medida que se envía desde un PC en una red a un destino en una red remota. La descripción que sigue son los nombres, conexiones y direcciones de los dispositivos de izquierda a derecha. PC 1 está conectado a un switch que está conectado al router R1 interfaz G0/0/0 en la red 192.168.10.0/24. PC 1 tiene una IP de 192.168.10.10 y MAC de aa-aa-aa. La interfaz G0/0/0 en R1 tiene una IP de 192.168.10.1 y MAC de bb-bb-bb. R1 tiene una interfaz G0/0/1 conectada a la interfaz del router R2 G0/0/1 en la red 209.165.200.224/30. La interfaz G0/0/1 en R1 tiene una IP de

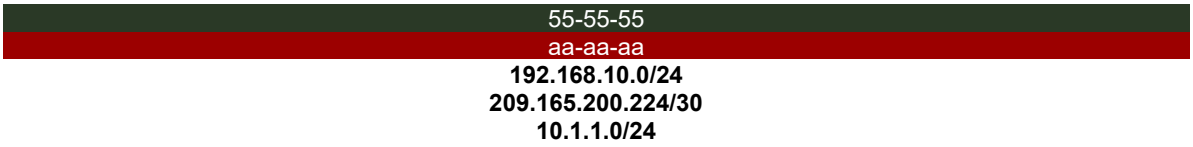
209.165.200.225 y MAC cc-cc-cc. La interfaz G0/0/1 en R2 tiene una IP de 209.165.200.226 y MAC dd-dd-dd. R2 tiene una interfaz G0/0/0 conectada a un switch conectado al PC 2 en la red 10.1.1.0/24. La interfaz G0/0/0 en R2 tiene una IP de 10.1.1.1 y MAC ee-ee-ee. PC 2 tiene una IP de 10.10.10.10 y MAC 55-55. R2 también tiene una conexión en la parte superior que conduce a la nube de Internet. Debajo del diagrama en red 209.165.200.224/30 hay cuatro cuadros que leen de izquierda a derecha: Destino MAC dd-dd-dd, MAC de origen cc-cc-cc, IPv4 192.168.10.10 y Destino IPv4 10.1.1.10.
R1R2PC 2 PC 1.10.1.225.226.1.10G0/0/1G0/0/1G0/0/0G0/0/0



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.

La imagen es un diagrama de red que muestra el direccionamiento MAC e IPv4 de origen y destino cuando la información sale de un router al destino final a medida que se envía desde un PC en una red a un destino en una red remota. La descripción que sigue son los nombres, conexiones y direcciones de los dispositivos de izquierda a derecha. PC 1 está conectado a un switch que está conectado al router R1 interfaz G0/0/0 en la red 192.168.10.0/24. PC 1 tiene una IP de 192.168.10.10 y MAC de aa-aa-aa. La interfaz G0/0/0 en R1 tiene una IP de 192.168.10.1 y MAC de bb-bb-bb. R1 tiene una interfaz G0/0/1 conectada a la interfaz del router R2 G0/0/1 en la red 209.165.200.224/30. La interfaz G0/0/1 en R1 tiene una IP de 209.165.200.225 y MAC cc-cc-cc. La interfaz G0/0/1 en R2 tiene una IP de 209.165.200.226 y MAC dd-dd-dd. R2 tiene una interfaz G0/0/0 conectada a un switch conectado al PC 2 en la red 10.1.1.0/24. La interfaz G0/0/0 en R2 tiene una IP de 10.1.1.1 y MAC ee-ee-ee. PC 2 tiene una IP de 10.10.10.10 y MAC 55-55. R2 también tiene una conexión en la parte superior que conduce a la nube de Internet. Debajo del diagrama en la red 10.1.1.0/24 hay cuatro cuadros que leen de izquierda a derecha: Destino MAC 55-55, MAC de origen ee-ee-ee, IPv4 192.168.10.10 y Destino IPv4 10.1.1.10.
R1R2PC 2 PC 1.10.1.225.226.1.10G0/0/1G0/0/1G0/0/0G0/0/0



¿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).

9.2 ARP

Desplázate para empezar

9.2.1 Descripción general de ARP

Si su red utiliza el protocolo de comunicaciones IPv4, el protocolo de resolución de direcciones o ARP es lo que necesita para asignar direcciones IPv4 a direcciones MAC. En este tema se explica cómo funciona ARP.

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.

Cuatro hosts, H1, H2, H3 y H4, están conectados al mismo switch. H1 tiene una IP de 192.168.1.5/24, H2 tiene una IP de 192.168.1.6/24, H3 tiene una IP de 192.168.1.8/24 y H4 tiene una IP de 192.168.1.7/24. H1 tiene un enunciado que dice: Necesito enviar información a 192.168.1.7, pero solo tengo la dirección IP. No conozco la dirección MAC del dispositivo que tiene esa dirección IP.

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

9.2.2 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.

Haga clic en Reproducir en la figura para ver una animación de la función ARP.

Esta animación ilustra cómo un host utilizará ARP para descubrir la dirección MAC de una dirección IP conocida. El host H1 debe enviar cierta información a un host con la dirección IP 192 dot 168 dot 1 dot 7. Sin embargo, H1 no tiene la dirección MAC para esa dirección. Por lo tanto, envía una solicitud A R P a la dirección IP 192.168.1.7. Todos los hosts de la red recibirán la solicitud ARP. Sin embargo, solo el host H4 con la dirección IP 192.168.1.7 enviará una respuesta ARP que contenga su dirección MAC. Luego, H1 puede enviar un sobre al switch que va directamente a H4.

Debo enviar una solicitud de ARP para descubrir la dirección MAC del host con la dirección IP 192.168.1.7.

No soy yo.
No soy yo.
Soy yo. Enviaré mi dirección MAC.
Ahora tengo la dirección MAC. Puedo enviar mi información.
Gracias. La recibí.

play_circle_filled

9.2.3 Video - 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.

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.

Haga clic en Reproducir para ver una demostración de una solicitud de ARP para una dirección IPv4 de destino que está en la red local.

9.2.4 Vídeo - Funcionamiento de ARP - 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.

Haga clic en Reproducir en la ilustración para ver una demostración de una respuesta de ARP.

9.2.5 Video - 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.

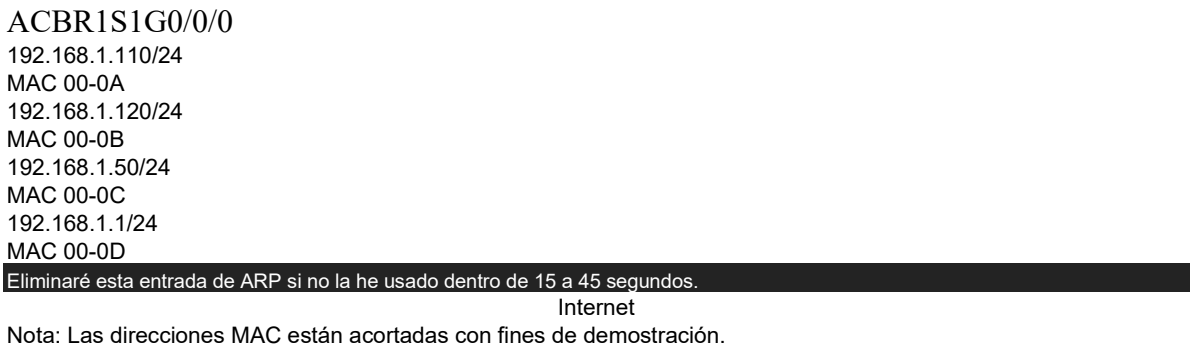
La dirección IPv4 de la dirección del gateway predeterminado se almacena en la configuración IPv4 de los hosts. Cuando un host crea un paquete para un destino, compara la dirección IPv4 de destino con la propia para determinar si ambas están ubicadas en la misma red de capa 3. Si el host de destino no 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.

Haga clic en Reproducir para ver una demostración de una solicitud de ARP y una respuesta de ARP asociadas con el gateway predeterminado.

9.2.6 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.

9.2.7 Tablas ARP en dispositivos de red

En un router Cisco, el **show ip arp** comando se utiliza para mostrar la tabla ARP, como se muestra en la figura.

```
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#
```

En una PC con Windows 10, el **arp -a** comando se usa para mostrar la tabla ARP, como se muestra en la figura.

```
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>
```

9.2.8 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.

El diagrama muestra siete dispositivos en medios compartidos (acceso múltiple) todos encendidos al mismo tiempo. Un cuadro de texto dice: las difusiones ARP pueden inundar los medios locales.

Todos los dispositivos encendidos al mismo tiempo

Las difusiones ARP pueden saturar los medios locales.

Medios compartidos (acceso múltiple)

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.

La imagen es un diagrama de red que muestra dos hosts, Host A con IP 192.168.1.110/24 y MAC 00-0A y Host B con IP 192.168.1.120/24 y MAC 00-0B, conectados al switch S1 que está conectado al router R1 en el puerto G0/0/0 (el gateway predeterminado con IP 192.168.1.1/24 y MAC 00-0D) que está conectado a la nube de Internet. También está conectado a S1 un atacante en el host C con IP 192.168.1.50/24 y MAC 00-0C. El host A tiene un enunciado que dice: Solicitud ARP: Necesito la dirección MAC del gateway predeterminado, 192.168.1.1. El atacante anfitrión C tiene un enunciado que dice: ¡Enviaré una respuesta ARP y fingiré ser la gateway predeterminado! Nota: Las direcciones MAC están acortadas con fines de demostración.
ABS1R1CA192.168.1.110/24MAC 00-0A192.168.1.120/24MAC 00-0B192.168.1.50/24MAC 00-0C192.168.1.1/24MAC 00-0DG0/0/0
Red
Nota: Las direcciones MAC están acortadas con fines de demostración.

9.3 Detección de vecinos IPv6

Desplázate para empezar

9.3.1 Video - 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.

Haga clic en Reproducir en la figura para ver una demostración de Descubrimiento de vecinos IPv6.

9.3.2 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.

:11:102001:db8:acad:1::/64PC1PC2

Mensajería de dispositivo a dispositivo

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).

:12001:db8:acad:1::/64PC1R1

Mensajería del router del dispositivo

Nota: El quinto mensaje ICMPv6 ND es un mensaje de redirección que se utiliza para una mejor selección de siguiente salto. Esto está fuera del alcance de este curso.

IPv6 ND se define en IETF RFC 4861.

9.3.3 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: :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.

El diagrama muestra PC1 y PC2 conectados al mismo switch en la red 2001:db8:acad:1: :/64. PC1 tiene una dirección IPv6 2001:db8:acad:1: :10 y PC2 tiene una dirección IPv6 2001:db8:acad:1: :11. PC1 está enviando un mensaje de solicitud de vecino ICMPv6 que dice: Hola, ¿quién tiene 2001: db8: acad: 1:: 11, envíeme su dirección MAC? PC2 está respondiendo con un mensaje de anuncio de vecino ICMPv6 que dice: Hola 2001:db8:acad:1::10, soy 2001:db8:acad:1::11 y mi dirección MAC es F8-94-C3-E4-C5-0A.

:11:102001:db8:acad:1::/64PC1PC2

Mensaje de anuncio de vecino **ICMPv6**

"Hola 2001:db8:acad:1::10, soy 2001:db8:acad:1::11 y mi dirección MAC es F8-94-C3-E4-C5-0A."

ICMPv6 Mensaje de solicitud de vecino

«Hola, ¿quién tiene 2001:db8:acad:1::11, envíeme su dirección MAC? «

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.

9.4 Módulo de Práctica y Prueba

Desplázate para empezar

9.4.1 ¿Qué aprendió en este módulo?

MAC e IP

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. 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). 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 es la de la NIC Ethernet del dispositivo. ¿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 ARP. Para los paquetes IPv6, el proceso es ICMPv6 ND.

ARP

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 y dirección MAC de origen. Un dispositivo utiliza ARP para determinar la dirección MAC de destino de un dispositivo local cuando conoce su dirección IPv4. ARP proporciona dos funciones básicas: resolver direcciones IPv4 a direcciones MAC y mantener una tabla de asignaciones de direcciones IPv4 a MAC. La solicitud ARP se encapsula en una trama Ethernet utilizando esta información de encabezado: direcciones MAC de origen y destino y tipo. 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. La respuesta ARP contiene los mismos campos de encabezado que la solicitud. 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. 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. Para cada dispositivo, un temporizador de memoria caché ARP elimina las entradas de ARP que no se hayan utilizado durante un período especificado. Los comandos también se pueden usar para eliminar manualmente algunas o todas las entradas de la tabla ARP. Como una trama de difusión, todos los dispositivos de la red local reciben y procesan una solicitud ARP, lo que podría hacer que la red se desacelere. Un atacante puede usar la ARP spoofing para realizar un ataque de ARP poisoning.

Detección de Vecinos

IPv6 no utiliza ARP, utiliza el protocolo ND para resolver direcciones MAC. 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: solicitud de vecino, anuncio de vecino, solicitud de router, anuncio de router y redirección. Al igual que ARP para IPv4, los dispositivos IPv6 utilizan IPv6 ND para resolver la dirección MAC de un dispositivo en una dirección IPv6 conocida.