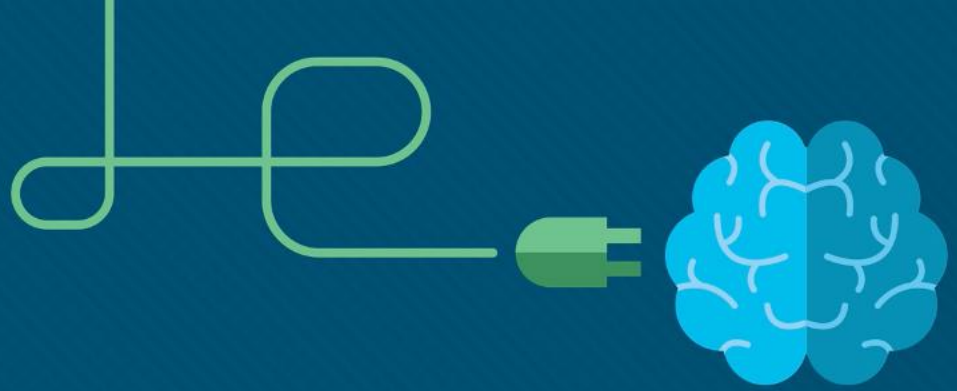


Módulo 24: Resolución de Direcciones

Fundamentos de Redes 3.0

Objetivos del Módulo

Título del Módulo: Resolución de Direcciones

Objetivo del Módulo: Explicar cómo ARP permite la comunicación en una red de área local.

Título del Tema	Objetivo del Tema
ARP	Describir el propósito de ARP.

24.1 ARP

Descripción General de ARP

- Si su red utiliza el protocolo de comunicaciones IPv4, necesita ARP 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:
  - **La dirección MAC de Destino** es la dirección MAC de 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 de la puerta de enlace predeterminada (es decir, el enrutador).
  - **La dirección MAC de Origen** es la dirección MAC de la NIC de Ethernet en el host de origen.

Descripción General de ARP (continuación)

- 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 nombre de dispositivo, pero se deben descubrir las direcciones MAC.

- Un dispositivo usa ARP para determinar la dirección MAC de destino de un dispositivo local cuando conoce su dirección IPv4, y ARP proporciona dos funciones principales:
  - Resolver direcciones IPv4 a direcciones MAC
  - Mantener una tabla de asignaciones de direcciones IPv4 a MAC

Funciones de 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 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.

Funciones de ARP (continuación)

- En cada entrada o fila de la tabla ARP, se enlaza una dirección IPv4 con una dirección MAC.
- La relación entre los dos valores se denomina asignación.
- Esto 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, utiliza su dirección MAC correspondiente como la dirección MAC de destino en la trama.
- El dispositivo envía una solicitud ARP si no encuentra una entrada.

Vídeo - Operación de ARP - Solicitud de ARP

- Cuando un dispositivo necesita determinar la dirección MAC asociada con una dirección IPv4, envía una solicitud ARP y no tiene una entrada para la dirección IPv4 en su tabla ARP.
- Los mensajes ARP se encapsulan directamente dentro de una trama Ethernet sin encabezado IPv4.
- La solicitud de ARP se encapsula en una trama de Ethernet con la siguiente información de encabezado:
  - **Dirección MAC de Destino** - 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 de ARP tienen un campo de tipo 0x806.
- Las solicitudes de ARP son de difusión, el conmutador las envía por todos los puertos, excepto el de recepción.
- Todas las NIC Ethernet de la LAN procesan difusiones 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.
- Solo un dispositivo en la LAN tendrá una dirección IPv4 que coincida con la dirección IPv4 de destino en la solicitud ARP, por lo que todos los demás dispositivos no responderán.
- Este vídeo cubrirá una solicitud ARP para una dirección MAC.

Video - Operación de ARP - Respuesta de ARP

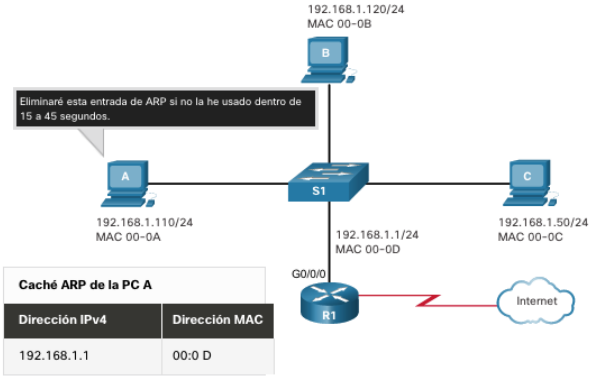
- Solo el dispositivo con la dirección IPv4 de destino asociada con la solicitud ARP responderá con una respuesta ARP.
- La respuesta ARP se encapsula en una trama de Ethernet con la siguiente información de encabezado:
  - **Dirección MAC de destino** - Es la dirección MAC del remitente de la solicitud de ARP.
  - **Dirección MAC de origen** - Esta es la dirección MAC del remitente de la respuesta ARP.
  - **Tipo** - Los mensajes de ARP tienen un campo de tipo 0x806.
- Solo el dispositivo que envió originalmente la solicitud ARP recibirá la respuesta ARP de unidifusión y agregará 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.
- Descarta el paquete si ningún dispositivo responde a la solicitud ARP porque no se puede crear una trama.
- Las entradas en la tabla ARP tienen una marca de tiempo, por lo que si un dispositivo no recibe una trama de un dispositivo en particular antes de que caduque la marca de tiempo, la tabla ARP elimina la entrada para este dispositivo.
- Además, las entradas de mapas estáticos se pueden ingresar en una tabla ARP (rara vez se hace), pero no caducan con el tiempo y deben eliminarse manualmente.
- Este vídeo cubrirá una respuesta de ARP en respuesta a una solicitud de ARP.

Video - El Rol de 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 a su puerta de enlace predeterminada (la interfaz del enrutador 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 configuración IPv4 de los hosts almacena la dirección IPv4 de la puerta de enlace predeterminada.
- Cuando un host crea un paquete para un destino, compara la dirección IPv4 de destino y su dirección IPv4 para determinar si la ubicación de las dos direcciones IPv4 está 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 de la puerta de enlace predeterminada.
- Si no hay una entrada, utiliza el proceso ARP para determinar la dirección MAC del gateway predeterminado.
- Este video cubrirá cómo una solicitud ARP proporcionará a un host con la dirección MAC de la puerta de enlace predeterminada.

Eliminar Entradas de una Tabla de ARP

- Para cada dispositivo que no usa ARP durante un período específico, un temporizador de caché ARP lo elimina.
- 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.
- El uso de comandos también puede eliminar manualmente algunas o todas las entradas de la tabla ARP.
- Después de eliminar una entrada, el proceso para enviar una solicitud ARP y recibir una respuesta ARP debe ocurrir nuevamente para ingresar el mapa en la tabla ARP.



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

Tablas de ARP en Dispositivos

- El comando **show ip arp** se usa en un enrutador Cisco para mostrar la tabla ARP, como se muestra en la figura.

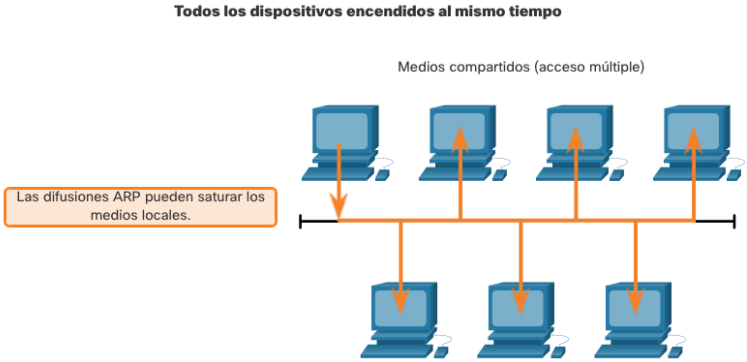
```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type  Interface
Internet  192.168.10.1            -  a0e0.af0d.e140  ARPA  GigabitEthernet0/0/0
Internet  209.165.200.225          -  a0e0.af0d.e141  ARPA  GigabitEthernet0/0/1
Internet  209.165.200.226          1  a03d.6fe1.9d91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

- El comando **arp -a** en una PC con Windows 10 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>
```

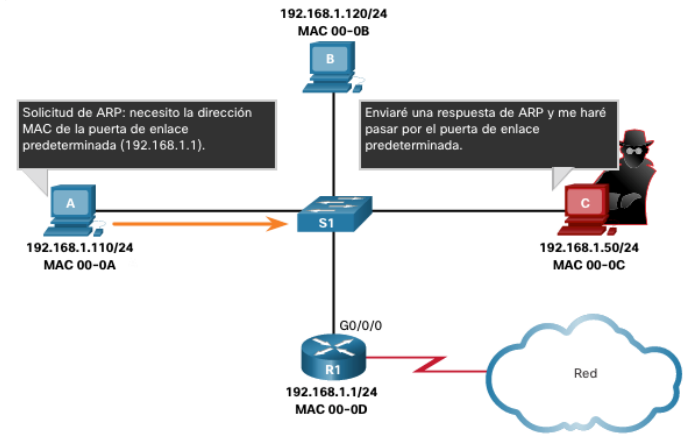
Problemas de ARP - Difusiones de ARP y Suplantación de Identidad de ARP

- Como una trama de difusión, cada dispositivo de la red local recibe y procesa una solicitud ARP.
- En una red comercial típica, estas difusiones tendrían, probablemente, un efecto mínimo en el rendimiento de la red.
- Suponga que se encienden varios dispositivos y todos comienzan a acceder a los servicios de red simultáneamente. En ese caso, podría haber alguna reducción en el rendimiento durante un período breve, como se muestra en la figura.
- Después de que los dispositivos envían las difusiones ARP iniciales y obtienen las direcciones MAC necesarias, se minimiza cualquier efecto en la red.



Problemas de ARP - Difusiones de ARP y Suplantación de Identidad de ARP (continuación)

- En algunos casos, usar ARP puede conducir a un riesgo potencial de seguridad.
- Un atacante puede usar la suplantación de identidad ARP (ARP spoofing) para realizar un ataque de envenenamiento ARP.
- 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 conmutadores de nivel empresarial incluyen técnicas de mitigación conocidas como inspección dinámica de ARP (DAI).



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

Packet Tracer - Examinar la Tabla ARP

En esta actividad de Packet Tracer, completará los siguientes objetivos:

- Examinar una Solicitud de ARP
- Examinar una tabla de direcciones MAC del switch
- Examinar el proceso ARP en comunicaciones remotas

Práctica de Laboratorio - Ver Tráfico ARP en Wireshark

En esta actividad, cumplirá los siguientes objetivos:

- Parte 1 : Capturar y analizar datos de ARP en Wireshark
- Parte 2 : Ver las entradas de caché ARP en la PC

24.2 Resumen de Resolución de Direcciones

¿Qué Aprendí en este Módulo?

- 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.
- Un dispositivo utiliza ARP para determinar la dirección MAC de destino de un dispositivo local cuando conoce su dirección IPv4.
- ARP proporciona dos funciones esenciales: resolver direcciones IPv4 a direcciones MAC y mantener una tabla de asignaciones de direcciones IPv4 a MAC.
- 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.
- De lo contrario, el dispositivo buscará en la tabla ARP la dirección IPv4 de la puerta de enlace predeterminada.
- Cada entrada o fila de la tabla ARP, se enlaza una dirección IPv4 con una dirección MAC.
- La solicitud ARP se encapsula en una trama Ethernet utilizando la siguiente información de encabezado: dirección MAC de destino (dirección de transmisión FF-FF-FF-FF-FF-FF), dirección MAC de origen (dirección MAC del remitente de la solicitud ARP) y tipo (0x806).
- Las solicitudes de ARP son de difusión, el conmutador las envía por todos los puertos, excepto el de recepción.
- Sólo el dispositivo con la dirección IPv4 de destino asociada con la solicitud ARP responderá con una respuesta ARP.

¿Qué Aprendí en este Módulo? (continuación)

- Después de recibir la respuesta ARP, el dispositivo agregará 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 a su puerta de enlace predeterminada (la interfaz del enrutador 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 configuración IPv4 de los hosts almacena la dirección IPv4 de la puerta de enlace predeterminada.
- 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 hay una entrada, utiliza el proceso ARP para determinar la dirección MAC de la puerta de enlace predeterminada.
- Para cada dispositivo, un temporizador de caché ARP elimina las entradas ARP que no utilizan un dispositivo durante un período específico.
- El comando show ip arp se usa en un enrutador Cisco para mostrar la tabla ARP.
- El comando arp -a en una PC con Windows 10 se usa para mostrar la tabla ARP.
- Como una trama de difusión, cada dispositivo de la red local recibe y procesa una solicitud ARP.
- En algunos casos, el uso de ARP puede generar un riesgo de seguridad potencial porque un actor de amenazas puede usar la suplantación de identidad de ARP para realizar un ataque de envenenamiento de ARP.