Práctica de laboratorio 9.8.1: Address Resolution Protocol (ARP)

Diagrama de topología

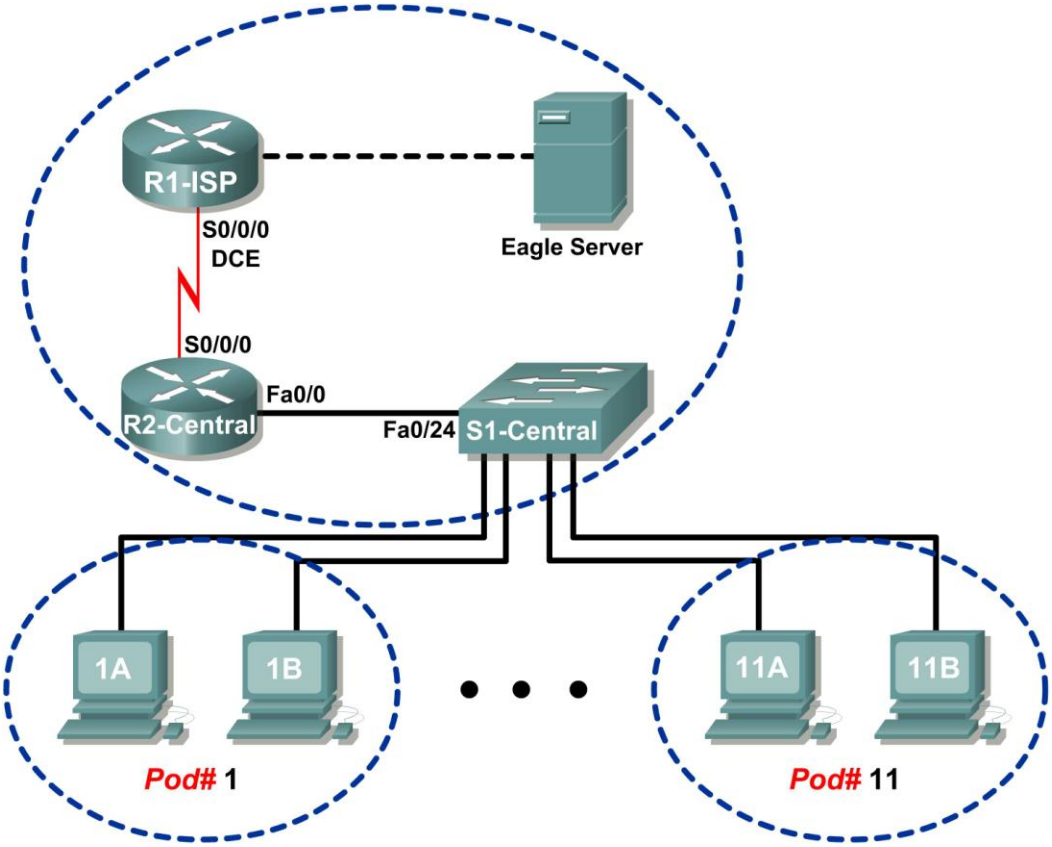

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	No aplicable
	Fa0/0	192.168.254.253	255.255.255.0	No aplicable
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	No aplicable
	Fa0/0	172.16.255.254	255.255.0.0	No aplicable
Eagle Server	No aplicable	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	No aplicable
host*Pod#***A**	No aplicable	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#***B**	No aplicable	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	No aplicable	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Usar el comando **arp** de Windows.
- Utilizar Wireshark para examinar los intercambios ARP.

Información básica

TCP/IP utiliza el Address Resolution Protocol (ARP) para asignar una dirección IP de Capa 3 a una dirección MAC de Capa 2. Cuando se coloca una trama en la red, debe tener una dirección MAC de destino. Para descubrir dinámicamente la dirección MAC al dispositivo de destino, se transmite una solicitud de ARP en la LAN. El dispositivo que tiene la dirección IP de destino responde y la dirección MAC es registrada en la caché ARP. Todos los dispositivos en la LAN tienen su propia caché ARP o un área más pequeña en la RAM que conserva los resultados ARP. Un temporizador de caché de ARP elimina las entradas ARP que no se hayan utilizado durante un determinado período de tiempo. l tiempo varía según el dispositivo. Por ejemplo, algunos sistemas operativos de Windows almacenan las entradas de caché de ARP durante 2 minutos. Si la entrada se utiliza nuevamente durante ese tiempo, el temporizador ARP para esa entrada se extiende a 10 minutos.

ARP es un excelente ejemplo del equilibrio del rendimiento. Sin caché, ARP debe solicitar continuamente traducciones de direcciones cada vez que se coloca una trama en la red. Esto agrega latencia a la comunicación y podría congestionar la LAN. Por el contrario, los tiempos de espera ilimitados podrían provocar errores con dispositivos que dejan la red o cambiar la dirección de la Capa 3.

Un ingeniero de redes debe estar al tanto del ARP, pero es posible que no interactúe con el protocolo regularmente. El ARP es un protocolo que permite que los dispositivos de la red se comuniquen con el protocolo TCP/IP. Sin ARP, no hay un método eficiente para construir el datagrama de la dirección de destino de Capa 2. Pero también representa un riesgo para la seguridad. El spoofing de ARP, también conocido como ARP poisoning, es una técnica que utilizan los atacantes para introducir la asociación de la dirección MAC incorrecta en una red. El individuo falsifica la dirección MAC de un dispositivo y las tramas se envían a la dirección equivocada. Una manera de evitar el ARP spoofing es configurar asociaciones de ARP estáticas manualmente. Por último, se puede configurar una lista de direcciones MAC autorizadas en los dispositivos Cisco para restringir el acceso sólo a los dispositivos aprobados.

Escenario

Con un equipo de computadora host del módulo, utilice el comando utilitario de Windows **arp** para evaluar y cambiar las entradas de caché del ARP.

En la Tarea 2 se emplea Wireshark para capturar y analizar el intercambio ARP entre los dispositivos de la red. Si no se cargó Wireshark en la computadora host del módulo, lo puede descargar desde el URL ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter9/, archivo `wireshark-setup-0.99.4.exe`.

Tarea 1: Uso del comando **arp** de Windows.

Paso 1: Acceder al terminal de Windows.

```
C:\> arp
Muestra y modifica las tablas de traducción de direcciones de IP
a física utilizadas en el address resolution protocol (ARP).
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]
-a          Muestra las entradas de ARP actuales al interrogar los
            datos del protocolo actual. Si se especifica inet_addr,
            se muestran las direcciones IP y física sólo en las
            computadoras especificadas. Si más de una interfaz de red
            utiliza ARP, se muestran las entradas de cada tabla ARP.
-g          Igual que -a.
inet_addr   Especifica una dirección de Internet.
-N if_addr  Muestra las entradas de ARP de la interfaz de red
            especificadas por if_addr.
-d          Elimina el host especificado mediante inet_addr. Es posible
            utilizar inet_addr como wildcard con * para eliminar todos
            los hosts.
-s          Agrega el host y asocia la dirección de Internet inet_addr
            con la dirección física eth_addr.  La dirección física
            tiene 6 bytes hexadecimales separados por guiones.
            La entrada es permanente.
eth_addr    Especifica una dirección física.
if_addr     Si está presente, identifica la dirección de Internet
            de la interfaz cuya tabla de traducción de direcciones se
            debe modificar. Si no está presente, se utiliza la primera
            interfaz aplicable.
Ejemplo:
 > arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Agrega una entrada
estática. Muestra la tabla ARP.
C:\>
```

Figura 1. Sintaxis del comando arp

1. Abra un terminal de Windows haciendo clic en **Inicio> Ejecutar**. Ingrese: **cmd** y haga clic en **Aceptar**. Sin opciones, el comando **arp** muestra la información de ayuda útil. Vea la Figura 1.
2. Emita el comando **arp** en el equipo de la computadora host y examine el resultado.
3. Responda las siguientes preguntas sobre el comando **arp**:

   ¿Qué comando se usaría para mostrar las entradas en la caché de ARP?

   _____

   ¿Qué comando se usaría para eliminar todas las entradas de la caché ARP (purgar la caché ARP)?

   _____

   ¿Qué comando se usaría para eliminar la entrada de la caché ARP para 172.16.255.254?

   _____

Paso 2: Usar el comando arp para examinar la caché ARP local.

```
C:\> arp -a
No se encontraron entradas de ARP
C:\>
```

Figura 2. Caché ARP vacía

Si no se cuenta con comunicación de red, la caché de ARP debe estar vacía. Esto se muestra en la Figura 2.

Ejecute el comando para mostrar las entradas de ARP. ¿Cuáles son los resultados?

_____

_____

Paso 3: Usar el comando `ping` para agregar de manera dinámica entradas en la caché ARP.

El comando **`ping`** se utiliza para verificar la conectividad de la red. Al acceder a otros dispositivos, las asociaciones de ARP se agregan de manera dinámica a la caché ARP.

```
C:\> ping 172.16.1.2
Pinging 172.16.1.2 with 32 bytes of data:
Reply from 172.16.1.2: bytes=32 time<10ms TTL=128
Reply from 172.16.1.2: bytes=32 time<10ms TTL=128
Reply from 172.16.1.2: bytes=32 time<10ms TTL=128
Reply from 172.16.1.2: bytes=32 time<10ms TTL=128
Ping statistics for 172.16.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Figura 3. Comando `ping` a una computadora host del módulo

1. Utilice el comando **`ipconfig /all`** para verificar la información de la Capa 2 y la Capa 3 de la computadora host del módulo.
2. Emita el comando **`ping`** hacia otra computadora host del módulo, como se muestra en la Figura 3. En la Figura 4 se muestra la nueva entrada de caché de ARP.

```
C:\> arp -a
Interfaz: 172.16.1.1 --- 0x60004
  Dirección de Internet    Dirección física   Tipo
  172.16.1.2               00-10-a4-7b-01-5f  dinámica
C:\>
```

Figura 4. Pantalla de la caché de ARP

¿Cómo se agregó la entrada ARP a la caché de ARP? Ayuda: revise la columna Tipo.

_____

¿Cuál es la dirección física de la computadora host del módulo de destino?

_____

¿Cuál es la dirección física de la computadora host del módulo de destino?

Dirección IP	Dirección física	¿De qué manera se obtuvo?

3. No envíe tráfico a la computadora a la que accedió previamente. Espere entre 2 y 3 minutos y verifique nuevamente la caché de ARP. ¿Se eliminó la entrada de caché de ARP? _____
4. Emitir el comando **ping** al Gateway, R2-Central. Examine la entrada de caché de ARP. ¿Cuál es la dirección física del Gateway? _____

Dirección IP	Dirección física	¿De qué manera se obtuvo?

5. Emita el comando **ping** a Eagle Server, eagle-server.example.com. Examine la entrada de caché de ARP. ¿Cuál es la dirección física de Eagle Server? _____

_____

_____

Paso 4: Ajustar las entradas de caché de ARP manualmente.

Para eliminar las entradas en la caché ARP, emita el comando **arp –d {inet-addr | *}**. Las direcciones se pueden eliminar de manera individual al especificar la dirección IP, o bien todas juntas con el wildcard *****.

Verifique que la caché ARP contenga dos entradas: una para el Gateway y otra para la computadora host de destino del módulo. Puede resultar más fácil hacer ping en ambos dispositivos más de una vez; de esta manera se retiene la entrada a caché durante 10 minutos aproximadamente.

```
C:\> arp –a
Interfaz: 172.16.1.1 --- 0x60004
  Dirección de Internet   Dirección física      Tipo
  172.16.1.2              00-10-a4-7b-01-5f     dinámica
  172.16.255.254          00-0c-85-cf-66-40     dinámica
C:\>
C:\>arp -d 172.16.255.254
C:\> arp -a
Interfaz: 172.16.1.1 --- 0x60004
  Dirección de Internet   Dirección física      Tipo
  172.16.1.2              00-10-a4-7b-01-5f     dinámica
C:\>
```

Figura 5. Eliminar manualmente una entrada a la caché de ARP

Consulte la Figura 5, donde se muestra cómo eliminar manualmente una entrada a caché ARP.

1. En la computadora, primero verifique que estén las dos entradas. Si no están, haga ping en la entrada faltante.
2. A continuación, elimine la entrada de la computadora host del módulo.
3. Por ultimo, verifique el cambio que realizó.

4. Registre las dos entradas en la caché ARP.

Dispositivo	Dirección IP	Dirección física	¿De qué manera se obtuvo?

5. Escriba el comando que sirve para eliminar la entrada de la computadora host del módulo:
_____

6. Emita el comando en la computadora host del módulo. Registre la entrada en la caché ARP restante:

Dispositivo	Dirección IP	Dirección física	¿De qué manera se obtuvo?

7. Simule que elimina todas las entradas. Escriba el comando que sirve para eliminar todas las entradas de la caché ARP:
_____

8. Emita el comando en la computadora host del módulo y examine la caché ARP con el comando **`arp -a`**. Todas las entradas deben haber sido eliminadas.
_____

9. Considere un entorno seguro donde el Gateway controla el acceso al servidor Web que contiene información confidencial. ¿Cuál es la capa de seguridad que se puede aplicar a las entradas de la caché ARP que ayudaría a contrarrestar el ARP spoofing?
_____

10. Escriba el comando que sirve para agregar una entrada ARP estática en la caché ARP para el Gateway:
_____

11. Examine la caché ARP nuevamente y complete la siguiente tabla:

Dirección IP	Dirección física	Tipo

En la siguiente tarea, se utiliza Wireshark para capturar y examinar el intercambio ARP. No cierre el terminal de Windows: lo usará para ver la caché ARP.

Tarea 2: Utilizar Wireshark para examinar los intercambios ARP.

Paso 1: Configurar Wireshark para las capturas de paquetes.

Prepare Wireshark para las capturas.

1. Haga clic en **Captura > Opciones**.
2. Seleccione la interfaz que corresponda a la LAN.
3. Marque la casilla para Actualizar la lista de paquetes en tiempo real.
4. Haga clic en **Inicio**.

Con esta acción se inicia la captura de paquetes.

Paso 2: Preparar la computadora host del módulo para las capturas de ARP.

1. Si aún no lo hizo, abra una ventana del terminal de Windows haciendo clic en **Inicio > Ejecutar**. Ingrese: **cmd** y haga clic en **Aceptar**.
2. Purgue la caché ARP, que requiere que el ARP vuelva a descubrir los mapas de direcciones. Escriba el comando que utilizó: _____

Paso 3: Capturar y evaluar la comunicación del ARP.

En este paso se envía una solicitud de ping al Gateway y otra solicitud de ping a Eagle Server. Luego la captura de Wireshark se detiene y se evalúa la comunicación ARP.

1. Envíe una solicitud de ping al Gateway, con el comando **ping –n 1 172.16.255.254.**
2. Envíe una solicitud de ping a Eagle Server, con el comando **ping –n 1.192,168.254,254.**

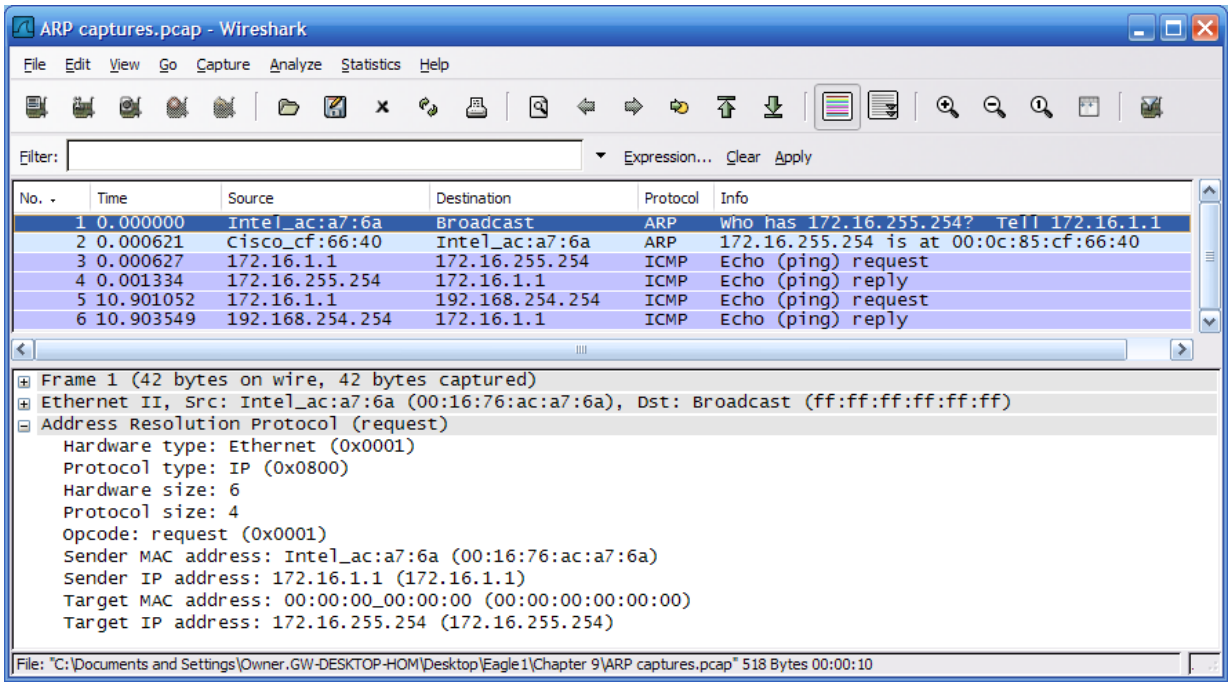

Figura 6. Captura Wireshark de la comunicación ARP

3. Detenga Wireshark y evalúe la comunicación. Debe ver una pantalla de Wireshark similar a la que se muestra en la Figura 6. En la ventana que contiene la lista de paquetes de Wireshark se muestra la cantidad de paquetes capturados. En la ventana de detalles del paquete se muestra el contenido del protocolo ARP.
4. A partir de la captura de Wireshark, responda las siguientes preguntas:

   ¿Cuál fue el primer paquete de ARP? _____

   ¿Cuál fue el segundo paquete de ARP? _____

Complete la siguiente taba con información sobre el primer paquete de ARP:

Campo	Valor
Dirección MAC del emisor	
Dirección IP del emisor	
Dirección MAC de destino	
Dirección IP de destino	

Complete la siguiente tabla con información sobre el segundo paquete de ARP:

Campo	Valor
Dirección MAC del emisor	
Dirección IP del emisor	
Dirección MAC de destino	
Dirección IP de destino	

Si la trama de Ethernet II de una solicitud ARP es un broadcast, ¿por qué la dirección MAC contiene sólo **0**? _____

¿Por qué no hubo una solicitud ARP para el ping a Eagle Server? _____

_____

_____

¿Por cuánto tiempo se debe guardar la asignación del gateway en la caché ARP en la computadora host del módulo? ¿Por qué? _____

_____

Tarea 3: Reflexión

El protocolo ARP asigna direcciones IP de Capa 3 a las direcciones MAC de Capa 2. Si un paquete se debe mover por las redes, la dirección MAC de Capa 2 cambia con cada salto que hace en el router, pero la dirección de Capa 3 nunca cambia.

En la caché de ARP se guardan las asignaciones de las direcciones de ARP. Si se obtuvo la entrada de manera dinámica, eventualmente se eliminará de la caché. Si se insertó de forma manual en la caché de ARP, se trata de una entrada estática que permanecerá en la computadora hasta que se apague o se purgue manualmente la caché ARP.

Tarea 4: Desafío

Con recursos externos, realice una búsqueda sobre ARP spoofing. Analice las distintas técnicas que se utilizan para contrarrestar este tipo de ataque.

La mayoría de los routers inalámbricos admiten acceso inalámbrico a las redes. Con esta técnica, las direcciones MAC que tienen acceso permitido a la red inalámbrica se agregan manualmente al router inalámbrico. Utilizando recursos externos, evalúe las ventajas de configurar un acceso a la red inalámbrica. Debata las maneras en que se puede violar esta seguridad.

Tarea 5: Limpieza

Se instaló Wireshark en la computadora host del módulo. Si debe desinstalarlo, haga clic en **Inicio > Panel de control**. Abra **Agregar o quitar programas**. Marque Wireshark y haga clic en **Quitar**.

Elimine todos los archivos creados durante la práctica de laboratorio en la computadora host del módulo.

A menos que el instructor le indique lo contrario, apague las computadoras host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.