

Proxy ARP

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[¿Cómo funciona ARP de representación?](#)

[Diagrama de la red](#)

[Ventajas de ARP de proxy](#)

[Desventajas de un proxy ARP](#)

[Información Relacionada](#)

Introducción

Este documento explica el concepto del Protocolo de resolución de direcciones (ARP) alternativo. ARP de representación es la técnica en la que un host, por lo general un router, responde las peticiones ARP dirigidas para otra máquina. "Falsificando" su identidad, el router acepta la responsabilidad de rutear los paquetes al destino "real". El ARP proxy puede ayudar a las máquinas de una subred a alcanzar subredes remotas sin la necesidad de configurar el ruteo o un gateway predeterminado. El ARP proxy se define en el [RFC 1027](#).

prerrequisitos

Requisitos

Este documento requiere la comprensión del entorno ARP y Ethernet.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 12.2(10b) del software del IOS® de Cisco
- Cisco 2500 Series Routers

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

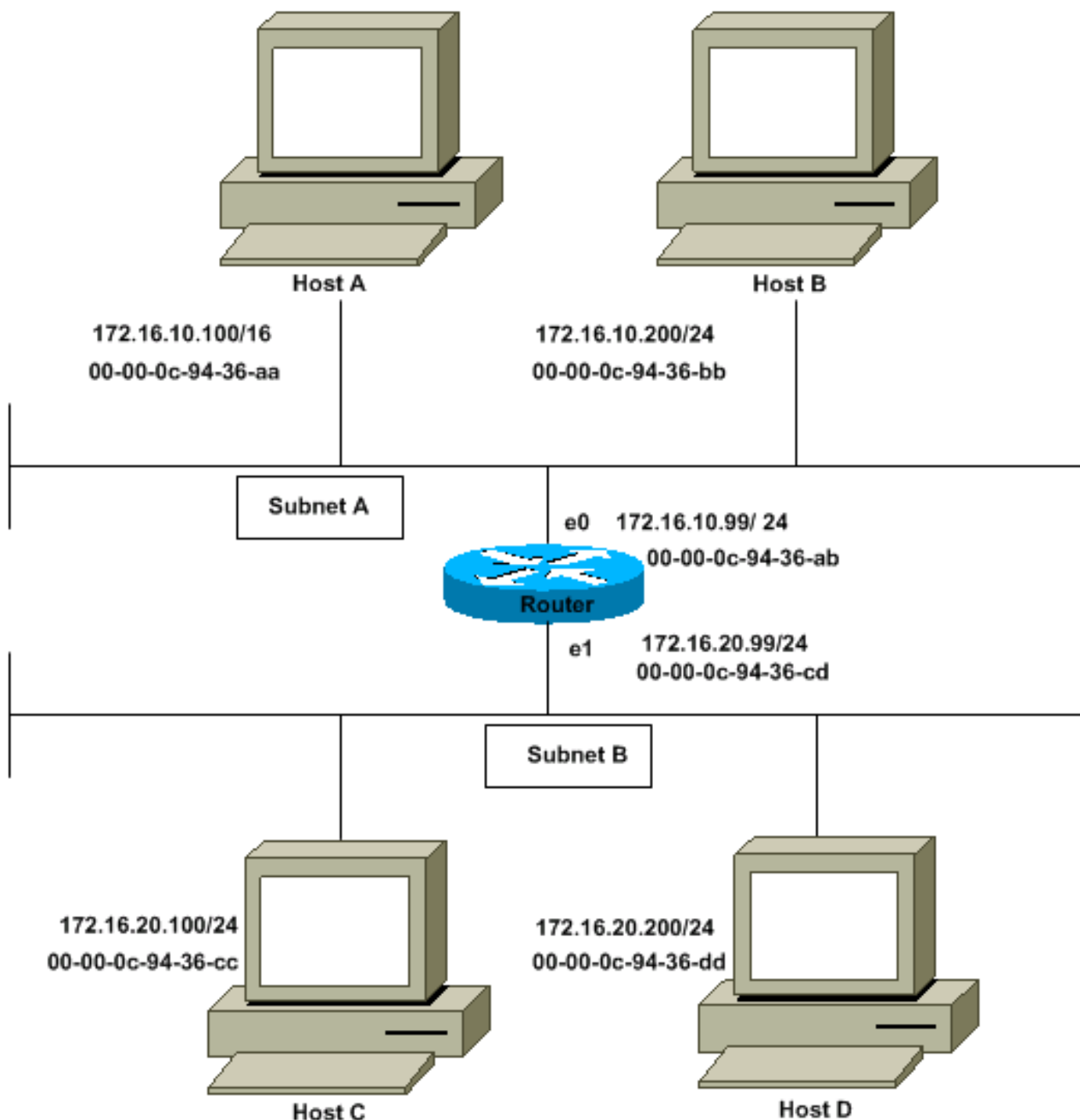
Convenciones

Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

¿Cómo funciona ARP de representación?

Éste es un ejemplo de cómo funciona el ARP proxy:

Diagrama de la red



El host A (172.16.10.100) de la Subred A necesita enviar paquetes al Host D (172.16.20.200) en la Subred B. Como se muestra en el diagrama, el Host A tiene una máscara de subred de /16. Lo

que significa es que el Host A cree que está directamente conectado a todas las 172.16.0.0. de la red. Cuando el Host A necesita comunicarse con cualquier dispositivo que cree que está conectado directamente, envía una solicitud ARP al destino. Por lo tanto, cuando el host A necesita enviar un paquete al host D, el host A cree que el host D está conectado directamente, entonces envía un pedido ARP al host D.

Para alcanzar el Host D (172.16.20.200), el Host A necesita la dirección MAC del Host D.

Por lo tanto, el Host A transmite una solicitud ARP en la Subred A, como se muestra:

Dirección MAC del remitente	Dirección IP del remitente	Dirección MAC objetivo	Dirección de IP objetivo
00-00-0c-94-36-aa	172.16.10.100	00-00-00-00-00-00	172.16.20.200

En esta solicitud ARP, el Host A (172.16.10.100) solicita que el Host D (172.16.20.200) envíe su dirección MAC. El paquete de solicitud ARP se encapsula entonces en una trama Ethernet con la dirección MAC del Host A como dirección de origen y un broadcast (FFFF.FFFF.FFFF) como dirección de destino. Puesto que la solicitud ARP es un broadcast, alcanza todos los nodos de la Subred A, que incluye la interfaz e0 del router, pero no alcanza el Host D. El broadcast no alcanza el Host D porque los routers, de forma predeterminada, no remiten broadcasts.

Puesto que el router sabe que la dirección de destino (172.16.20.200) está en otra subred y puede alcanzar el Host D, responde con su propia dirección MAC al Host A.

Dirección MAC del remitente	Dirección IP del remitente	Dirección MAC objetivo	Dirección de IP objetivo
00-00-0c-94-36-ab	172.16.20.200	00-00-0c-94-36-aa	172.16.10.100

Ésta es la respuesta ARP proxy que el router envía al Host A. El paquete de respuesta ARP proxy se encapsula en una trama Ethernet con la dirección MAC del router como dirección de origen y la dirección MAC del Host A como dirección de destino. Las respuestas ARP son siempre unicast para el solicitante original.

Tras la recepción de esta respuesta ARP, el Host A actualiza su tabla ARP, como se muestra:

IP Address	Dirección MAC
172.16.20.200	00-00-0c-94-36-ab

De ahora en adelante, el Host A remite todos los paquetes que desea que alcancen 172.16.20.200 (Host D) a la dirección MAC 00-00-0c-94-36-ab (router). Dado que el router sabe cómo llegar al Host D, le reenvía el paquete. La memoria caché ARP de los hosts de la Subred A se llena con la dirección MAC del router para todos los hosts de la Subred B. En consecuencia, todos los paquetes destinados a la Subred B se envían al router. El router remite esos paquetes a los hosts de la Subred B.

La memoria caché ARP del Host A se muestra en esta tabla:

IP Address	Dirección MAC
172.16.20.200	00-00-0c-94-36-ab
172.16.20.100	00-00-0c-94-36-ab
172.16.10.99	00-00-0c-94-36-ab
172.16.10.200	00-00-0c-94-36-bb

Note: Múltiples direcciones IP se asignan a una única dirección MAC, la dirección MAC de este router, lo que indica que el ARP proxy está en uso.

La interfaz de Cisco se debe configurar para que acepte y responda al ARP proxy. Esto se activa como opción predeterminada. El comando **no ip proxy-arp** se debe configurar en la interfaz del router conectado al router del ISP. El ARP proxy se puede inhabilitar en cada interfaz individualmente con el comando de configuración de la interfaz **no ip proxy-arp**, como se muestra:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface ethernet 0
Router(config-if)# no ip proxy-arp
Router(config-if)# ^Z
Router#
```

Para habilitar el ARP proxy en una interfaz, emita el comando de configuración de la interfaz **ip proxy-arp**.

Note: Cuando el Host B (172.16.10.200/24) de la Subred A intenta enviar paquetes al Host D(172.16.20.200) de destino en la Subred B, mira en su tabla de ruteo IP y rutea el paquete en consecuencia. El Host B (172.16.10.200/24) no hace ARP para la dirección IP 172.16.20.200 del Host D porque pertenece a una subred diferente de la configurada en la interfaz Ethernet 172.16.20.200/24 del Host B.

[Ventajas de ARP de proxy](#)

La ventaja principal del ARP proxy es que se puede agregar a un único router de una red y no perturba las tablas de ruteo de los otros routers de la red.

El ARP proxy se debe utilizar en la red donde los hosts IP no estén configurados con un gateway predeterminado o no tengan ninguna inteligencia de ruteo.

[Desventajas de un proxy ARP](#)

Los host desconocen los detalles físicos de su red y suponen que es una red plana en la que pueden alcanzar cualquier destino simplemente al enviar una solicitud ARP. No obstante, la utilización de ARP para todo tiene desventajas. Éstas son algunas de las desventajas:

- Aumenta el tráfico ARP de su segmento.
- Los hosts necesitan tablas ARP mayores para gestionar las asignaciones de direcciones IP a MAC.
- La seguridad se puede socavar. Una máquina puede pretender ser otra para interceptar paquetes, un acto llamado "spoofing".
- No funciona para las redes que no utilizan ARP para la resolución de la dirección.

- No se generaliza a todas las topologías de red. Por ejemplo, más de un router que conecta dos redes físicas.

Refiérase a la sección [Habilitación de ARP Proxy](#) de [Configuración del Direccionamiento IP](#) para obtener más información sobre la configuración de ARP proxy.

[Información Relacionada](#)

- [Recursos de Soporte de IP](#)
- [Página de Soporte de NAT](#)
- [Herramientas y Recursos](#)
- [Soporte Técnico - Cisco Systems](#)