Entender o Proxy Address Resolution Protocol (ARP)

Contents

Introdução

Este documento descreve como o Proxy ARP ajuda as máquinas em uma sub-rede a alcançar sub-redes remotas sem a necessidade de configurar o roteamento ou um gateway padrão.

Pré-requisitos

Requisitos

Este documento requer uma compreensão do Proxy Address Resolution Protocol (ARP) e do ambiente Ethernet.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco IOS® Software, Versão 12.2(10b)
- Cisco 2500 Series Routers

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Este documento explica o conceito de Protocolo de resolução de endereço (ARP) do proxy. Proxy ARP é a técnica em que um host, geralmente um roteador, responde às solicitações de ARP destinadas a outra máquina. Se você falsificar sua identidade, o roteador aceitará a responsabilidade pelo roteamento de pacotes para o destino "real". O Proxy ARP pode ajudar máquinas em uma sub-rede a alcançar sub-redes remotas sem a necessidade de configurar o roteamento ou um gateway padrão. O proxy ARP é definido no RFC 1027.

Como o proxy ARP funciona?

Este é um exemplo de como o proxy ARP funciona:

Diagrama de Rede

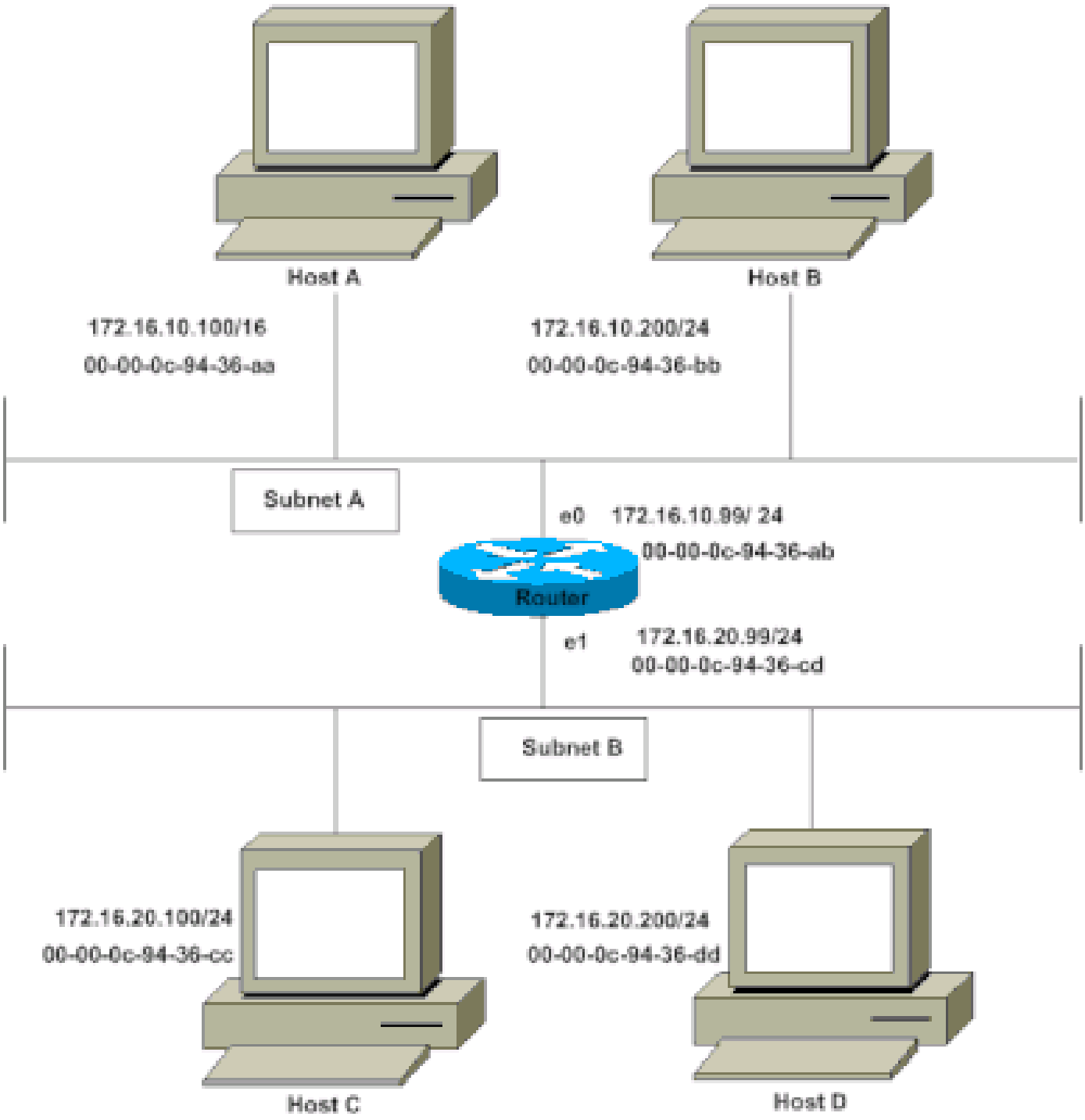


Diagrama de Rede

O host A (172.16.10.100) na sub-rede A precisa enviar pacotes ao host D (172.16.20.200) na sub-rede B. Como mostrado no diagrama, o host A tem uma máscara de sub-rede /16. Isso significa que o host A acredita que está diretamente conectado a toda a rede 172.16.0.0. Quando o host A precisa se comunicar com qualquer dispositivo que ele acredita estar conectado diretamente, ele envia uma solicitação ARP ao destino. Portanto, quando o Host A precisa enviar um pacote para o Host D, o Host A acredita que o Host D está conectado diretamente, então envia uma solicitação ARP para o Host D.

Para alcançar o Host D (172.16.20.200), o Host A precisa do endereço MAC do Host D.

Portanto, o Host A envia uma solicitação ARP por broadcast na Sub-rede A, como mostrado:

Endereço MAC do remetente	Endereço IP do remetente	Endereço MAC de destino	Endereço IP de destino
00-00-0c-94-36-aa	172.16.10.100	00-00-00-00-00-00	172.16.20.200

Nesta solicitação ARP, o Host A (172.16.10.100) solicita que o Host D (172.16.20.200) envie seu endereço MAC. O pacote de solicitação ARP é encapsulado em um quadro Ethernet com o endereço MAC do Host A como o endereço de origem e um broadcast (FFFF.FFFF.FFFF) como o endereço de destino. Como a solicitação ARP é um broadcast, ela alcança todos os nós na Sub-rede A, que inclui a interface e0 do roteador, mas não alcança o Host D. O broadcast não chega ao Host D porque os roteadores, por padrão, não encaminham broadcasts.

Como o roteador sabe que o endereço de destino (172.16.20.200) está em outra sub-rede e pode acessar o Host D, ele responde com seu próprio endereço MAC para o Host A.

Endereço MAC do remetente	Endereço IP do remetente	Endereço MAC de destino	Endereço IP de destino
00-00-0c-94-36-ab	172.16.20.200	00-00-0c-94-36-aa	172.16.10.100

Esta é a resposta Proxy ARP que o roteador envia ao Host A. O pacote de resposta proxy ARP é encapsulado em um quadro Ethernet com o endereço MAC do roteador como o endereço de origem e o endereço MAC do Host A como o endereço de destino. As respostas ARP são sempre unicast para o solicitante original.

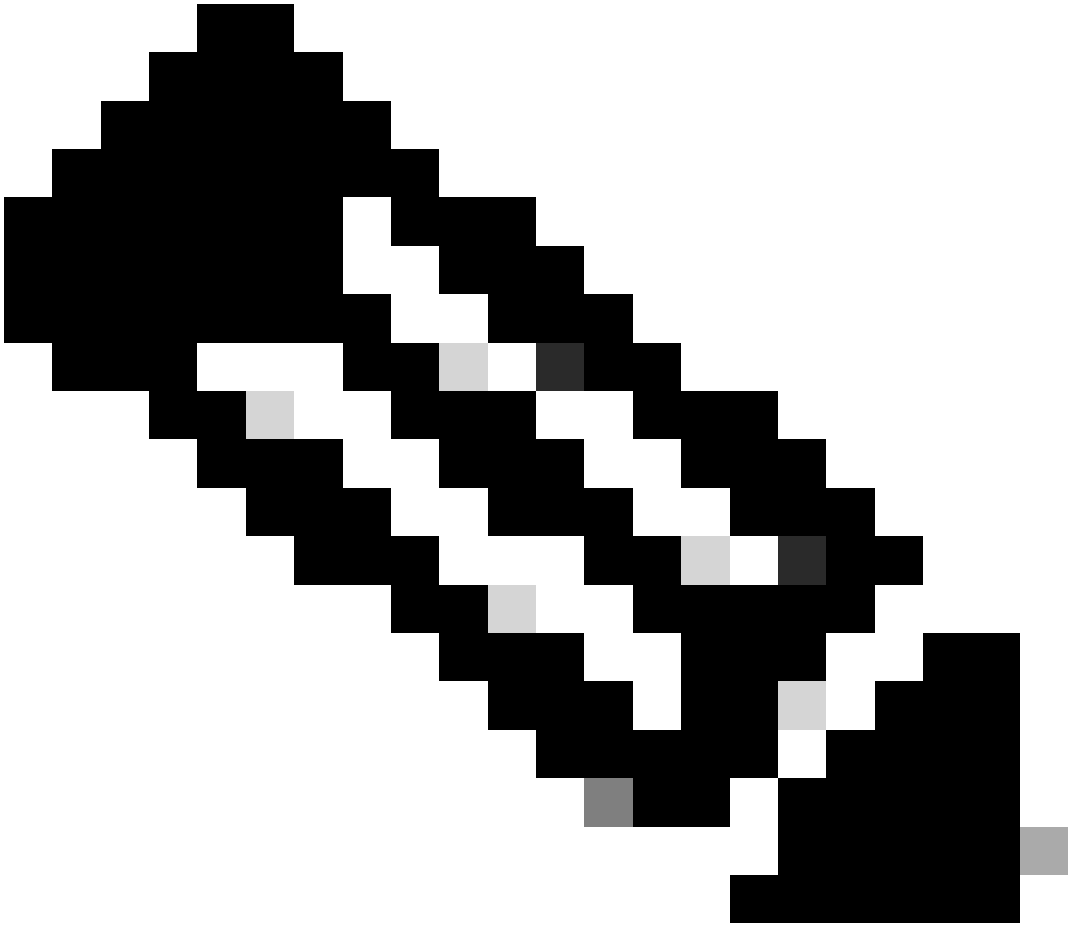
Ao receber esta resposta ARP, o Host A atualiza sua tabela ARP, como mostrado:

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

A partir de agora, o Host A encaminha todos os pacotes que deseja alcançar 172.16.20.200 (Host D) para o endereço MAC 00-00-0c-94-36-ab (roteador). Como o roteador sabe como atingir o Host D, ele encaminha o pacote para o Host D. O cache ARP nos hosts da sub-rede A é preenchido com o endereço MAC do roteador para todos os hosts da sub-rede B. Portanto, todos os pacotes destinados à sub-rede B são enviados para o roteador. O roteador encaminha esses pacotes aos hosts na Sub-rede B.

O cache ARP do Host A é mostrado nesta tabela:

IP Address	Endereço 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



Observação: vários endereços IP são mapeados para um único endereço MAC, o endereço MAC desse roteador, que indica que o proxy ARP está em uso.

A interface do Cisco deve ser configurada para aceitar e responder ao proxy ARP. Iss está habilitado por padrão. O **no ip proxy-arp**comando deve ser configurado na interface do roteador conectado ao roteador do ISP. O Proxy ARP pode ser desativado em cada interface individualmente com o comando**no ip proxy-arp** de configuração de interface, como mostrado:

<#root>

Router#

configure terminal

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

```
 interface ethernet 0
```

```
Router(config-if)#
```

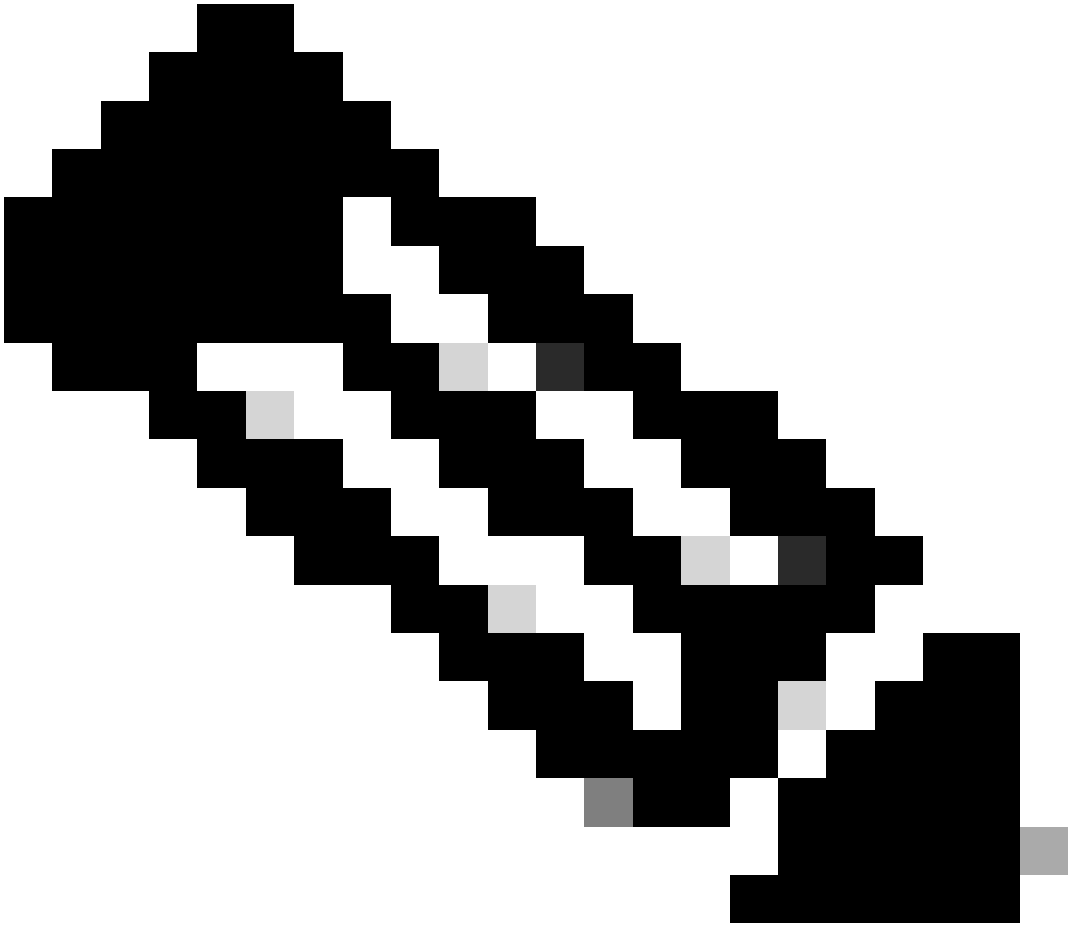
```
 no ip proxy-arp
```

```
Router(config-if)#
```

```
^Z
```

```
Router#
```

Para habilitar o proxy ARP em uma interface, execute o comando de configuração de **ip proxy-arp**interface.



Observação: quando o Host B (172.16.10.200/24) na Sub-rede A tenta enviar pacotes ao Host D (172.16.20.200) de destino na Sub-rede B, ele examina sua tabela de roteamento IP e roteia o pacote de acordo. O host B (172.16.10.200/24) não usa o ARP para o endereço IP 172.16.20.200 do host D porque ele pertence a uma sub-rede diferente da configurada na interface Ethernet 172.16.20.200/24 do host B.

Vantagens do Proxy ARP

A principal vantagem do proxy ARP é que ele pode ser adicionado a um único roteador em uma rede e não perturba as tabelas de roteamento de outros roteadores na rede.

O Proxy ARP deve ser usado na rede onde os hosts IP não estão configurados com um gateway padrão ou não têm nenhuma inteligência de roteamento.

Desvantagens de ARP do proxy

Os hosts não têm ideia dos detalhes físicos de sua rede e assumem que é uma rede linear na qual podem alcançar qualquer destino se enviarem uma solicitação ARP. Quando você usa o ARP para tudo, há desvantagens. Estas são algumas das desvantagens:

- Aumenta a quantidade de tráfego ARP no segmento.
- Os hosts precisam de tabelas ARP maiores para lidar com mapeamentos de endereços IP para MAC.
- A segurança pode ser comprometida. Uma máquina pode declarar ser outra a fim de interceptar pacotes, um ato chamado spoofing (falsificação).
- Isso não funciona para redes que não usam ARP para a resolução de endereços.
- Ele não se generaliza para todas as topologias de rede. Por exemplo, mais de um roteador que conecta duas redes físicas.

Informações Relacionadas

- **Recursos de suporte IP**
- **Página de suporte de NAT**
- **Ferramentas e recursos**
- **Suporte técnico e downloads da Cisco**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.