



Módulo 8: Protocolo de resolução de endereço



CyberOps Associate v1.0

Prof. Clemilson Oliveira

clemilson.oliveira@edu.sc.senai.br



Objetivos do módulo

Título do Módulo: Protocolo de resolução de endereço

Objetivo do módulo: Analisar PDUs de protocolo de resolução de endereço em uma rede.

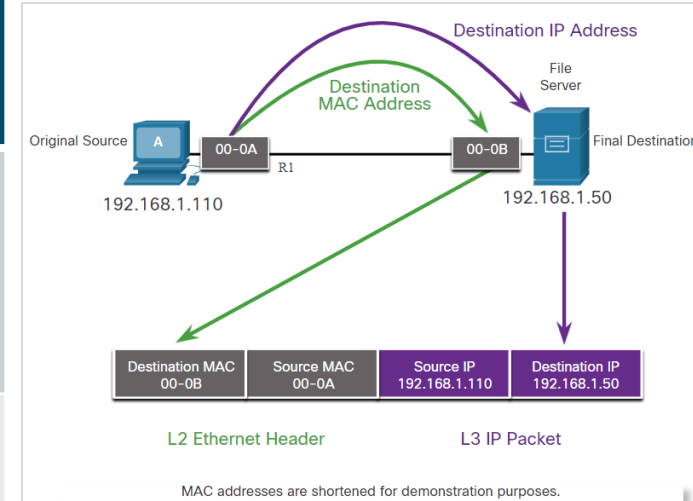
Título do Tópico	Objetivo do Tópico
MAC e IP	Comparar as funções do endereço MAC e do endereço IP.
ARP	Analisar o ARP examinando os quadros Ethernet.
Problemas do ARP	Explique como as solicitações ARP afetam o desempenho da rede e do host, bem como os riscos potenciais à segurança.

8.1 MAC e IP

Destino na mesma rede

- Os dois endereços principais atribuídos a um dispositivo em uma LAN Ethernet:

Endereços principais em LAN Ethernet	Descrição
Endereço físico (o endereço Mac)	<ul style="list-style-type: none">Usado para comunicações Ethernet NIC para Ethernet NIC na mesma rede.Se o endereço IP de destino estiver na mesma rede, o endereço MAC de destino será o do dispositivo de destino.
Endereço lógico (o endereço IP)	<ul style="list-style-type: none">Usado para enviar o pacote da fonte original ao destino final.O endereço IP de destino pode estar na mesma rede IP que a origem ou em uma rede remota.

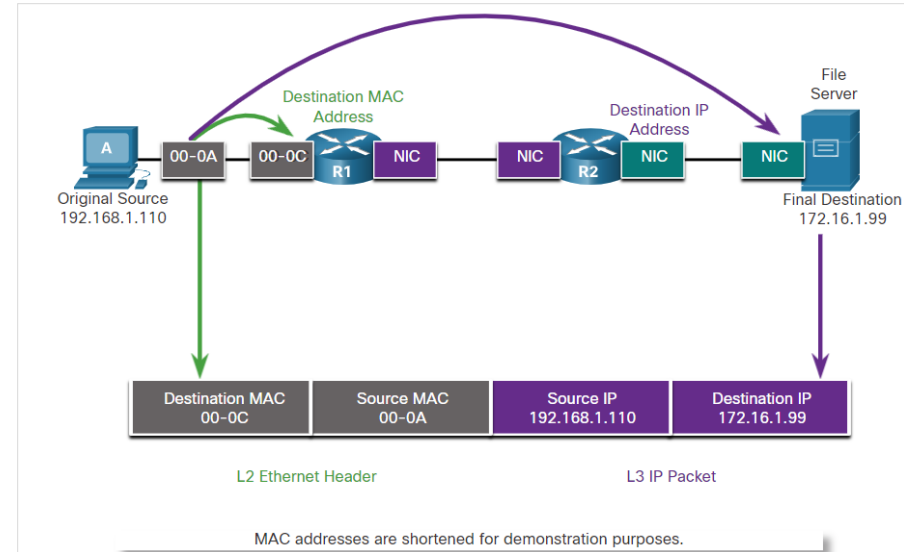


Comunicação em uma rede local

Nota: A maioria dos aplicativos usa o Domain Name System (DNS) para determinar o endereço IP quando recebe um nome de domínio como www.cisco.com.

Destino em rede remota

- Quando o endereço IP de destino estiver em uma rede remota, o endereço MAC de destino será o endereço do gateway padrão do host. O processo na figura é como abaixo:
- Os roteadores examinam o endereço IPv4 de destino.
- Quando o roteador recebe o quadro Ethernet, ele desencapsula as informações da Camada 2.
- Usando o endereço IP de destino, o roteador determina o dispositivo do próximo salto e, a seguir, encapsula o pacote IP em um novo quadro de link de dados para a interface de saída.
- Se o dispositivo do próximo salto for o destino final, o endereço MAC de destino será o da NIC Ethernet do dispositivo.

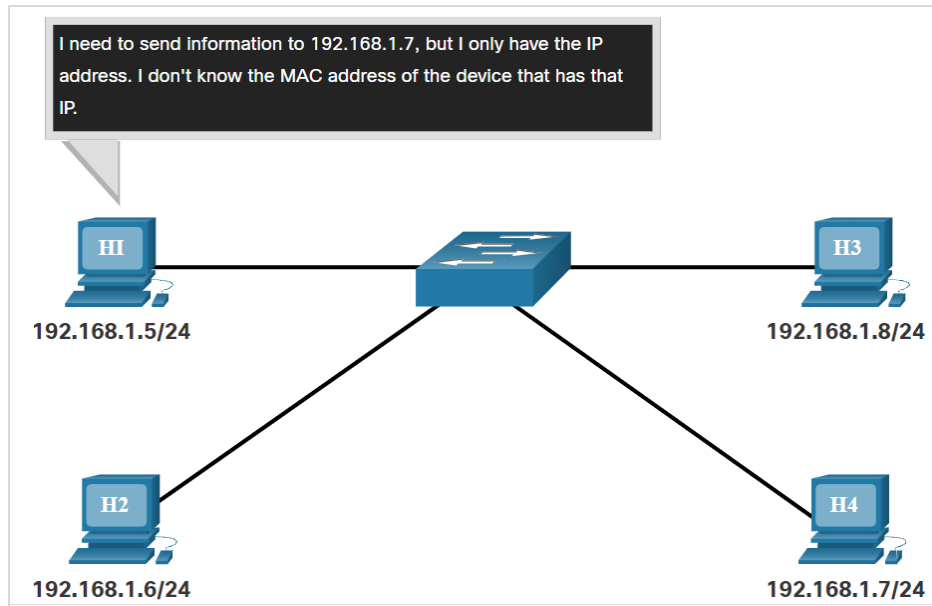


Comunicação em uma rede remota

8.2 ARP

ARP Visão geral

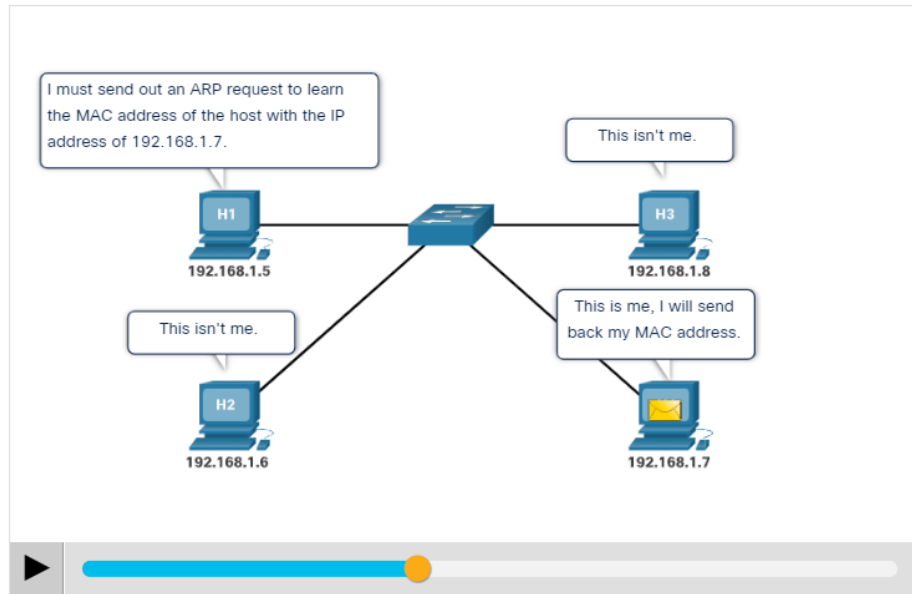
- A figura ilustra um problema ao enviar um pacote para outro host na mesma rede IPv4 local porque o endereço IP é conhecido, mas o endereço MAC do dispositivo é desconhecido.
- Um dispositivo utiliza o protocolo ARP (Address Resolution Protocol) para determinar o endereço MAC de destino de um dispositivo local quando conhece o endereço IPv4.
- O ARP fornece duas funções básicas:
 - Resolução de endereços IPv4 em endereços MAC
 - Mantendo uma tabela de mapeamentos de endereços IPv4 para MAC



Funções do ARP

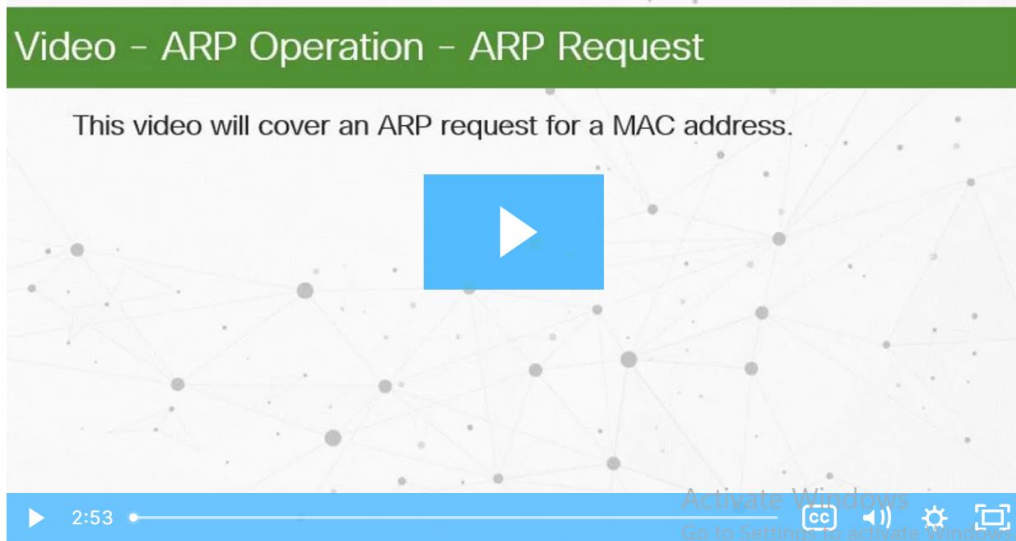
- Quando um pacote é enviado para a camada de enlace de dados para ser encapsulado em um quadro Ethernet, o dispositivo consulta uma tabela chamada **tabela ARP** ou cache ARP em sua memória RAM para encontrar o endereço MAC mapeado para o endereço IPv4.
- O dispositivo de envio pesquisará em sua tabela ARP um endereço IPv4 de destino e um endereço MAC correspondente, se o endereço IPv4 de destino do pacote estiver na mesma rede que o endereço IPv4 de origem.
- Se o dispositivo localizar o endereço IPv4, o endereço MAC correspondente será usado como o endereço MAC destino no quadro.

Clique em reproduzir na figura para ver uma animação da função ARP.



Vídeo- Operação ARP - Solicitação ARP

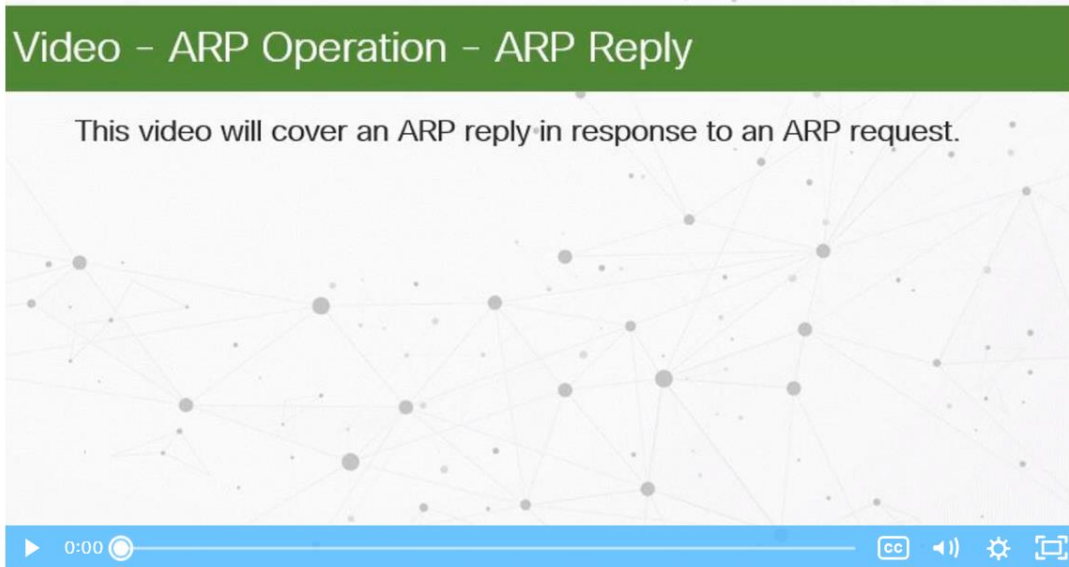
- Quando um dispositivo precisa determinar o endereço MAC mapeado para o endereço IPv4 e nenhuma entrada é encontrada para o endereço IPv4 em sua tabela ARP, uma solicitação ARP é enviada.
- Clique em Reproduzir para ver uma demonstração de uma solicitação ARP para um endereço IPv4 de destino que está na rede local.



Vídeo - Operação ARP - Resposta ARP

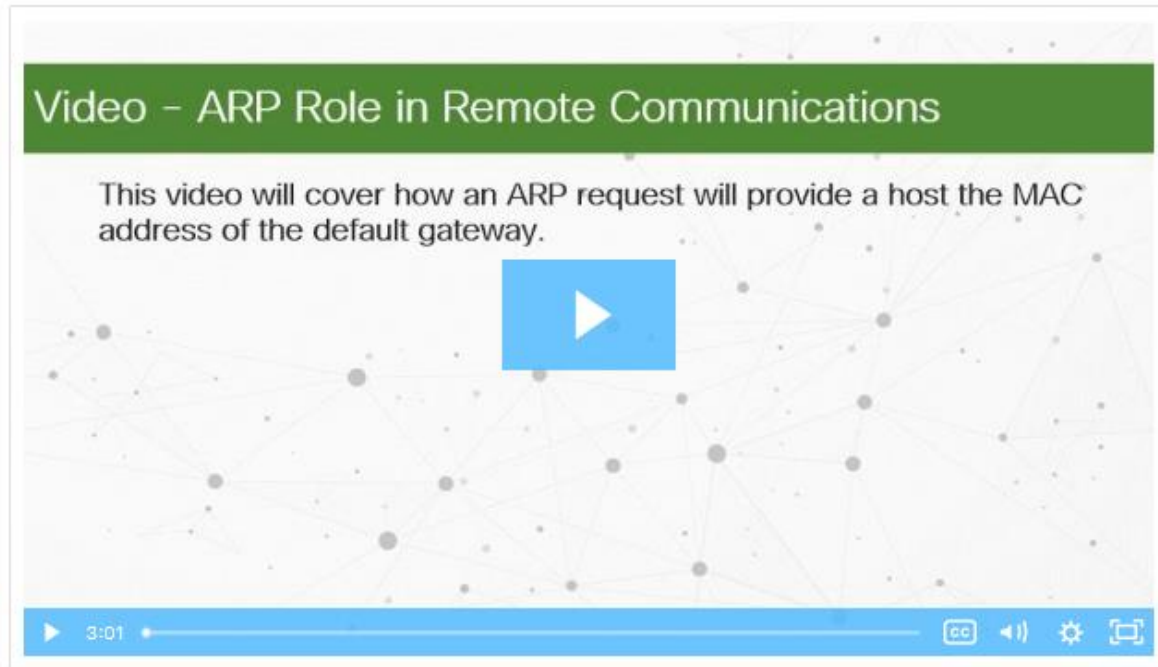
- Somente o dispositivo com o endereço IPv4 de destino associado à solicitação ARP responderá com uma resposta ARP.
- Clique em Reproduzir na figura para ver uma demonstração de uma resposta ARP.

Nota: O IPv6 usa um processo semelhante ao ARP para IPv4, conhecido como ICMPv6 Neighbour Discovery (ND). O IPv6 usa mensagens de requisição e de anúncio de vizinho, semelhantes a solicitações ARP e respostas ARP no IPv4.



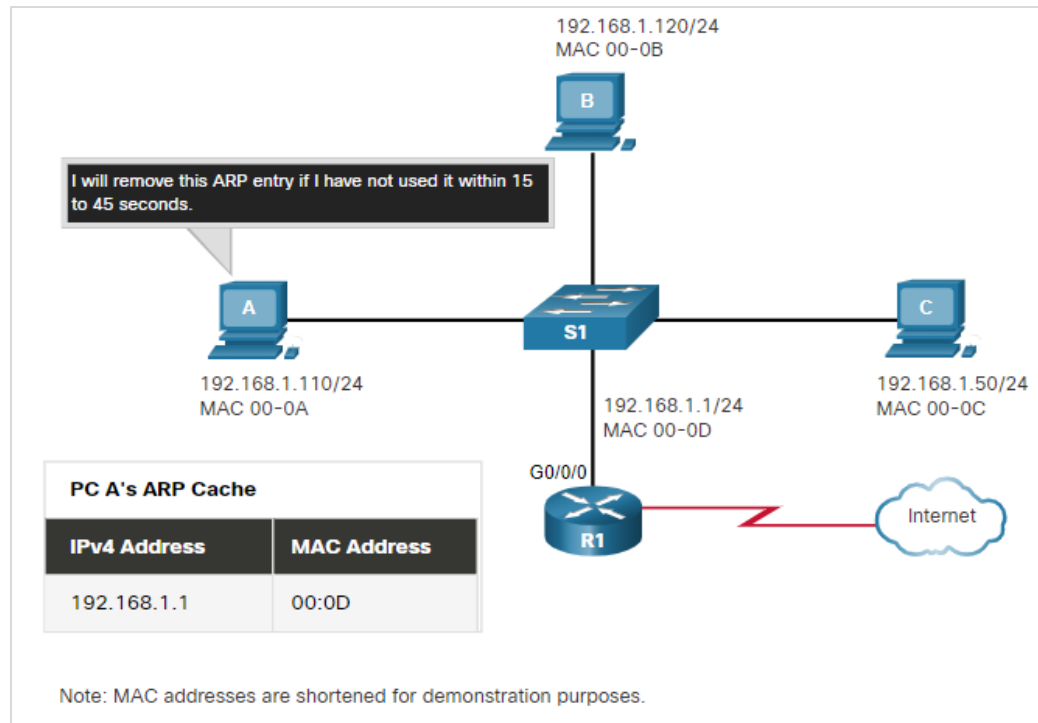
Vídeo - Função ARP na comunicação remota

- Clique em Reproduzir para ver uma demonstração de uma requisição ARP e de uma resposta ARP associadas ao gateway padrão.



Remoção de entradas de uma tabela ARP

- Para cada dispositivo, um temporizador de cache ARP remove as entradas ARP que não foram usadas por um período de tempo especificado.
- Os horários diferem dependendo do sistema operacional do dispositivo.
- Os comandos também podem ser usados para remover manualmente algumas ou todas as entradas na tabela ARP.
- Após a remoção de uma entrada, o processo de envio de uma requisição ARP e de recebimento de uma resposta ARP deve ocorrer novamente para inserir o mapa na tabela ARP.



Tabelas ARP em dispositivos de rede

Em um roteador Cisco, o comando **show ip arp** é usado para exibir a tabela ARP.

```
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#
```

Em um PC Windows 10, o comando **arp -a** é usado para exibir a tabela ARP.

```
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>
```

Laboratório - Wireshark para examinar frames Ethernet

Neste laboratório, você fará o seguinte:

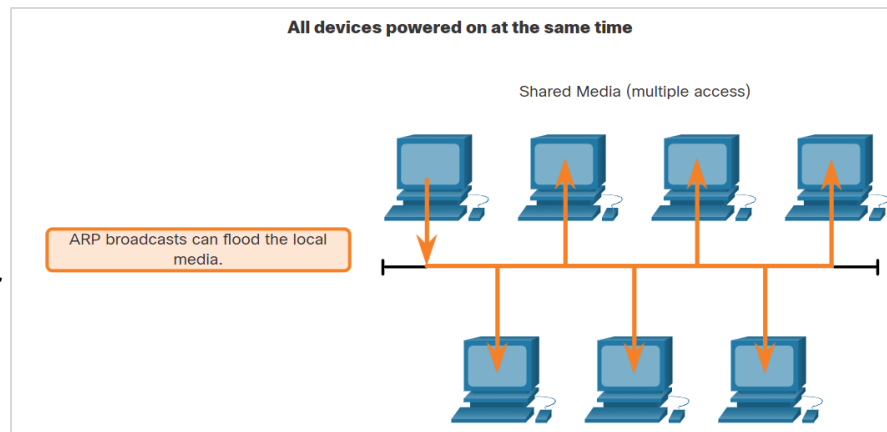
- Use o Wireshark para capturar e visualizar quadros Ethernet para investigar o endereçamento ARP e IP e MAC.
- Capture e analise quadros ICMP.

8.3 Problemas do ARP

Problemas de ARP - transmissões ARP e spoofing de ARP

Broadcasts ARP

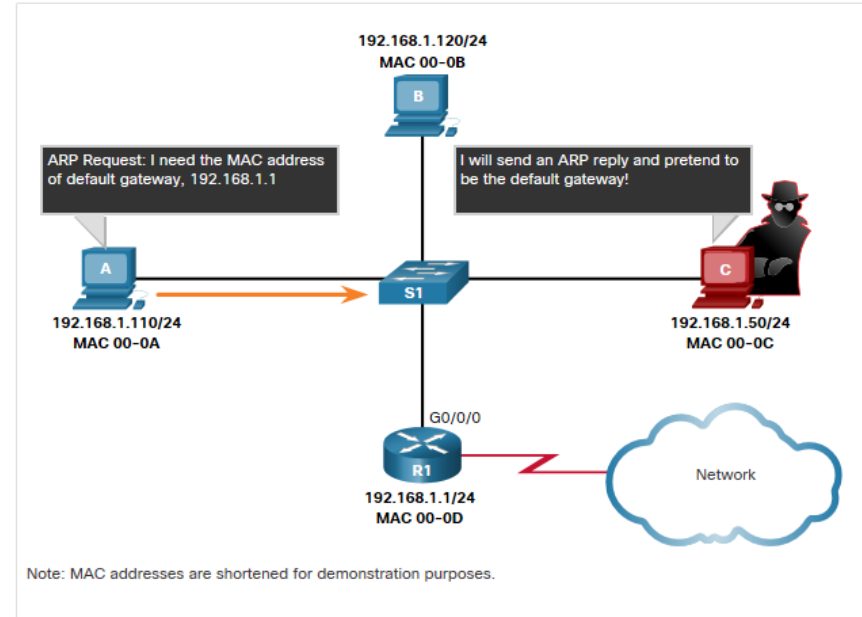
- Como um quadro broadcast, uma requisição ARP é recebida e processada por todos os dispositivos na rede local.
- Em uma rede comercial típica, essas transmissões teriam um impacto mínimo no desempenho da rede.
- Se muitos dispositivos começarem a acessar serviços de rede ao mesmo tempo, pode haver redução no desempenho por um curto período de tempo.
- Depois que os dispositivos enviarem os broadcasts ARP iniciais e tiverem reconhecido os endereços MAC necessários, qualquer impacto na rede será minimizado.



Problemas de ARP - Transmissões ARP e spoofing de ARP (cont.)

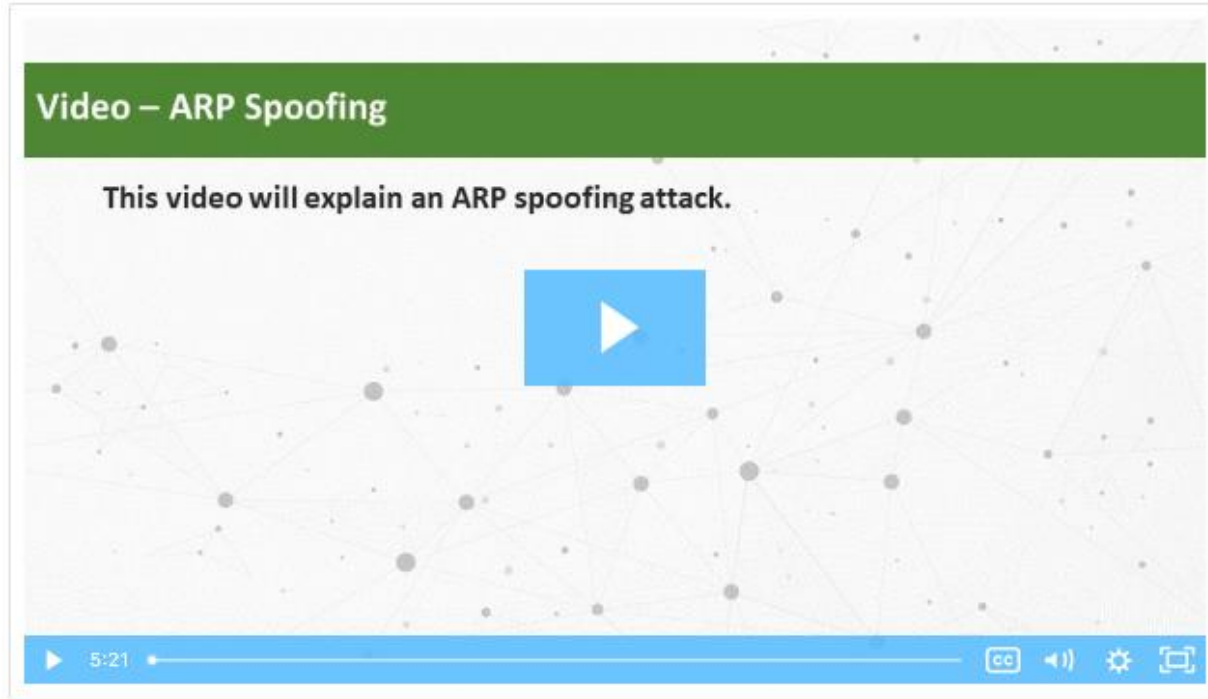
Falsificação ARP (ARP Spoofing)

- O uso de ARP pode levar a um risco potencial de segurança em alguns casos.
- Um agente de ameaça usa ARP spoofing para realizar um ataque de envenenamento ARP.
 - É uma técnica usada por um agente de ameaça para responder a uma solicitação ARP de um endereço IPv4 pertencente a outro dispositivo, como o gateway padrão.
 - O agente da ameaça envia uma resposta ARP com seu próprio endereço MAC. O receptor da resposta do ARP adicionará o endereço MAC errado à sua tabela ARP e enviará esses pacotes ao agente da ameaça.



Vídeo - ARP Spoofing

- Clique em Play na figura para visualizar um vídeo sobre falsificação de ARP.



8.4 Resumo do protocolo ARP

O que aprendi neste módulo?

- Os endereços IP são usados para identificar o endereço do dispositivo de origem original e o dispositivo de destino final.
- Os endereços MAC são usados para entregar o quadro de link de dados com o pacote IP encapsulado de um NIC para outro NIC na mesma rede.
- ARP é usado para mapear o endereço IPv4 lógico com o endereço MAC da Camada 2.
- O ARP fornece duas funções básicas: resolver endereços IPv4 para endereços MAC e manter uma tabela de mapeamentos de endereços IPv4 para MAC.
- Quando o endereço IPv4 de destino está na mesma rede que a origem, o processo ARP envia o endereço IPv4 para todos os hosts na rede para que o host com o endereço IPv4 correspondente possa responder com o endereço MAC correspondente
- Se o endereço IPv4 destino do pacote estiver na mesma rede que o endereço IPv4 origem, o dispositivo pesquisará o endereço IPv4 destino na tabela ARP.

O que eu aprendi neste módulo? (Continuação)

- Se não houver entrada para o endereço IPv4 em sua tabela ARP, o dispositivo de envio enviará uma solicitação ARP para determinar o endereço MAC de destino.
- Somente o dispositivo com o endereço IPv4 de destino associado à solicitação ARP responderá com uma resposta ARP.
- No IPv6, ICMPv6 Neighbor Discovery (ND) é usado.
- Como um quadro broadcast, uma requisição ARP é recebida e processada por todos os dispositivos na rede local.
- Um agente de ameaça pode usar ARP spoofing para executar um ataque de envenenamento ARP respondendo a uma solicitação ARP para um endereço IPv4 pertencente a outro dispositivo, como o gateway padrão.

