Laboratório 9.8.1: Protocolo de Resolução de Endereços (ARP)

Diagrama de Topologia

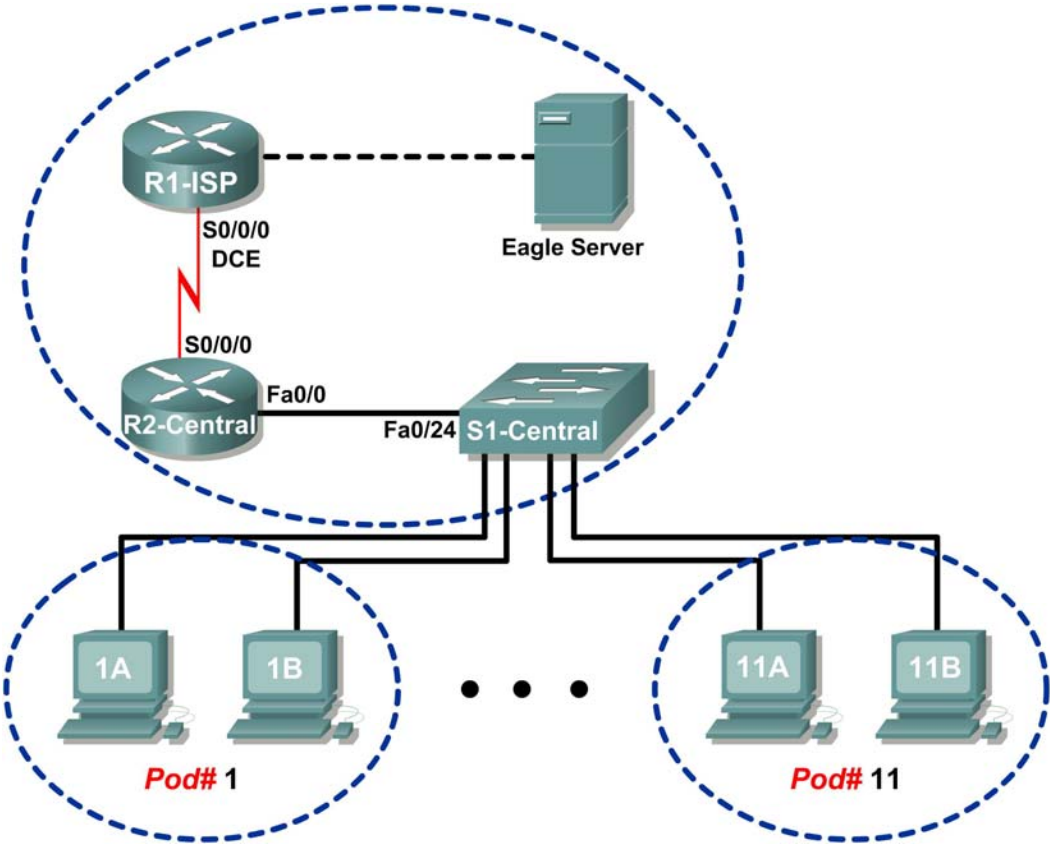

Tabela de Endereçamento

Dispositivo	Interface	Endereço IP	Máscara de Sub-Rede	Gateway Padrão
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	*N/A*
	Fa0/0	192.168.254.253	255.255.255.0	*N/A*
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	N/A
	Fa0/0	172.16.255.254	255.255.0.0	*N/A*
Eagle Server	*N/A*	192.168.254.254	255.255.255.0	192.168.254.253
	N/A	172.31.24.254	255.255.255.0	*N/A*
host*Pod#*A	*N/A*	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#*B	*N/A*	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	*N/A*	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos

Com a conclusão deste laboratório, você será capaz de:

- Usar o comando **arp** do Windows.
- Usar o Wireshark para examinar mudanças do ARP.

Contexto

Address Resolution Protocol (ARP) é usado pelo TCP/IP para mapear um endereço IP da Camada 3 para um endereço MAC da Camada 2. Quando um quadro é posicionado na rede, ele deve ter um endereço MAC de destino. Para descobrir dinamicamente o endereço MAC do dispositivo de destino, uma solicitação ARP é enviada em broadcast na LAN. O dispositivo que contém o endereço IP de destino responde, e o endereço MAC é gravado na cache ARP. Todo dispositivo na LAN mantém sua cache ARP própria, ou uma pequena área na RAM que armazena resultados ARP. Um temporizador da cache ARP remove entradas ARP que não foram usadas por certo período. Dependendo do dispositivo, o tempo difere. Por exemplo, alguns sistemas operacionais Windows mantêm entradas na cache ARP por 2 minutos. Se a entrada é usada novamente durante esse tempo, o temporizador ARP para essa entrada é estendido para 10 minutos.

O ARP é um excelente exemplo em desempenho de decisão. Sem cache, o ARP deve solicitar continuamente traduções de endereço cada vez que um quadro é colocado na rede. Isso acrescenta latência à comunicação e pode congestionar a LAN. Inversamente, tempos de espera ilimitados podem causar erros com dispositivos que foram removidos da rede ou sofreram alteração no endereço da Camada 3.

Um engenheiro de rede precisa estar atento ao ARP, mas pode não interagir com o protocolo regularmente. O ARP é um protocolo que permite que dispositivos de rede se comuniquem com o protocolo TCP/IP. Sem ARP, não há método eficiente para construir o datagrama do endereço de destino da Camada 2. Além disso, o ARP é um risco potencial à segurança. O ARP spoofing, ou ARP poisoning, é uma técnica usada por um atacante para inserir a associação de endereço MAC errado em uma rede. Um atacante falsifica o endereço MAC de um dispositivo, e quadros são enviados ao destino errado. A configuração manual estática de associações MAC é uma forma de prevenir ARP spoofing. Finalmente, uma lista de endereço MAC autorizada pode ser configurada para dispositivos Cisco para restringir o acesso à rede apenas para dispositivos autorizados.

Cenário

De um computador, use o comando **arp** do Windows para examinar e mudar entradas da cache ARP.

Na Tarefa 2, o Wireshark será usado para capturar e analisar mudanças do ARP entre dispositivos de rede. Se o Wireshark não foi instalado no computador, ele pode ser baixado da URL ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter9/, arquivo wireshark-setup-0.99.4.exe.

Tarefa 1: Use o Comando `arp` do Windows

Etapa 1: Acesse o terminal do Windows.

```
C:\> arp
Exibe e modifica as tabelas de tradução de endereço IP para Físico
usadas pelo 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          Exibe entradas ARP atuais apurando os dados atuais do
            protocolo. Se inet_addr for especificado, os endereços IP e
            Físico apenas para o computador especificado são exibidos.
```



```
             Se mais de uma interface de rede usa ARP, as entradas para
             cada tabela ARP são exibidas.
-g           Mesmo que -a.
inet_addr    Especifica um endereço de internet.
-N if_addr   Exibe as entradas ARP para a interface de rede especificada
             por if_addr.
-d           Exclui o host especificado por inet_addr. inet_addr pode
             ser o curinga com * excluir todos os hosts.
-s           Adiciona o host e associa o endereço de Internet inet_addr
             ao endereço Físico eth_addr.  O endereço Físico é dado como
             6 bytes hexadecimais separados por hífens. A entrada é
             permanente.
eth_addr     Especifica um endereço físico.
if_addr      Se presente, ele especifica o endereço de Internet da
             interface cuja tabela de tradução de endereços deve ser
             modificada. Se não está presente, a primeira interface
             aplicável será usada.
Example:
 > arp -s 157.55.85.212 00-aa-00-62-c6-09  .... Adiciona uma entrada
estática.
 > arp -a                                  .... Exibe uma tabela arp.
C:\ >
```

Figure 1. Sintaxe do Comando arp

1. Abra o terminal do Windows clicando **Start > Run**. Digite **cmd**, e clique em **OK**.
   Sem qualquer opção, o comando **arp** mostrará informações úteis de ajuda. Veja a Figura 1.
2. Execute o comando **arp** em um computador, e examine a saída.
3. Responda as seguintes questões sobre o comando **arp**:

   Qual comando seria usado para mostrar todas as entradas na cache ARP? _____

   Qual comando seria usado para apagar todas as entradas da cache ARP (limpar a memória da cache ARP)? _____

   Qual comando seria usado para apagar a entrada da cache ARP para 172.16.255.254?
   _____

Etapa 2: Use o com mando arp para examinar a cache ARP local.

```
C:\> arp -a
Nenhuma Entrada ARP Encontrada
C:\ >
```

Figura 2. Cache ARP Vazia

Sem comunicação de rede, a cache ARP deve estar vazia. Isto é o na Figura 2.

Execute o comando que mostra as entradas ARP. Quais são os resultados?

_____

_____

Etapa 3: Use o comando ping para adicionar dinamicamente entradas na cache ARP.

O comando **ping** pode ser usado para testar a conectividade de rede. Ao acessar outros dispositivos, associações ARP são dinamicamente adicionadas na cache ARP.

```
C:\> ping 172.16.1.2
Pinging 172.16.1.2 com 32 bytes de dados:
Resposta de 172.16.1.2: bytes=32 tempo<1ms TTL=128
Resposta de 172.16.1.2: bytes=32 tempo<1ms TTL=128
Resposta de 172.16.1.2: bytes=32 tempo<1ms TTL=128
Resposta de 172.16.1.2: bytes=32 tempo<1ms TTL=128
Estatísticas de ping para 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:\ >
```

Figure 3. Comando ping para um Computador

1. Use o comando **ipconfig /all** para verificar as informações da Camada 2 e da Camada 3 do computador.
2. Execute o comando **ping** para outro computador, o na Figura 3. A Figura 4 mostra a nova entrada da cache ARP.

```
C:\> arp -a
Interface: 172.16.1.1 --- 0x60004
  Endereço de Internet      Endereço Físico      Tipo
  172.16.1.2           00-10-a4-7b-01-5f     dinâmico
C:\ >
```

Figure 4. Exibição da Cache ARP

Como a entrada ARP foi adicionada na cache ARP? Dica: reveja a coluna Type.

_____

Qual é o endereço físico do computador de destino____.

Qual é o endereço físico do computador de destino?

Endereço IP	Endereço Físico	Como descobriu?

3. Não envie nenhum tráfego ao computador acessado previamente. Aguarde de 2 a 3 minutos, e verifique o cache ARP novamente. A entrada da cache ARP foi limpa? _Sim. Se a entrada não foi limpa, há algumas explicações possíveis. Primeiro, o aluno não esperou 2 minutos, que é o tempo que a cache ARP guarda uma entrada inicial. Ou o aluno acessou o dispositivo de destino mais de uma vez durante a janela de intervalo de 2 minutos, e causou um aumento no intervalo ARP para 10 minutos.
4. Execute o comando **ping** para o Gateway, R2-Central. Examine a entrada da cache ARP. Qual é o endereço físico do Gateway? _____

Endereço IP	Endereço Físico	Como descobriu?

5. Execute o comando **ping** para o Eagle Server, eagle-server.example.com. Examine a entrada da cache ARP. Qual é o endereço físico do Eagle Server?_____
_____
_____
_____
_____

Etapa 4: Ajuste manualmente as entradas na cache ARP.

Para apagar entradas no cache ARP, lance o comando **arp –d {inet-addr | *}**. Os endereços podem ser apagados individualmente ao especificar o endereço IP, ou todas as entradas podem ser apagadas com a opção *****.

Verifique que a cache ARP contém duas entradas: uma para o Gateway e uma para o computador de destino. Pode ser mais fácil efetuar um ping para ambos os dispositivos mais de uma vez, o que irá manter a cache por aproximadamente 10 minutos.

```
C:\> arp –a
Interface: 172.16.1.1 --- 0x60004
  Endereço de Internet      Endereço Físico      Tipo
  172.16.1.2            00-10-a4-7b-01-5f     dinâmico
  172.16.255.254        00-0c-85-cf-66-40     dinâmico
C:\ >
C:\>arp -d 172.16.255.254
C:\> arp -a
Interface: 172.16.1.1 --- 0x60004
  Endereço de Internet      Endereço Físico      Tipo
  172.16.1.2            00-10-a4-7b-01-5f     dinâmico
C:\ >
```

Figura 5. Removendo Manualmente uma Entrada da Cache ARP

Veja a Figura 5, que mostra como apagar manualmente uma entrada da cache ARP.

1. Em seu computador, verifique primeiramente se as duas entradas estão presentes. Caso negativo, execute o ping para a entrada ausente.
2. Em seguida, apague a entrada para o computador.
3. Finalmente, verifique a mudança.
4. Registre as duas entradas da cache ARP:

Dispositivo	Endereço IP	Endereço Físico	Como descobriu?

5. Escreva o comando que apagará a entrada para o computador: _____

6. Execute o comando em seu computador. Registre a entrada da cache ARP remanescente:

Dispositivo	Endereço IP	Endereço Físico	Como descobriu?

7. Simule a remoção de todas as entradas. Escreva o comando que apagará todas as entradas na cache ARP: _____
8. Execute o comando em seu computador, e examine a cache ARP com o comando **arp -a**. Todas as entradas devem ser removidas. _____

9. Considere um ambiente seguro onde o Gateway controla o acesso ao servidor web que contém informações super secretas. Qual é uma opção de segurança que pode ser aplicada às entradas da cache ARP que podem ajudar no combate ao ARP spoofing?
   _____
10. Escreva o comando que adicionará uma entrada ARP estática para o Gateway na cache ARP:
    _____
11. Examine a cache ARP novamente, e preencha a seguinte tabela:

Endereço IP	Endereço Físico	Tipo

Para a próxima tarefa, o Wireshark será usado para capturar e examinar uma alteração do ARP. Não feche o terminal Windows—ele será usado para visualizar a cache ARP.

Tarefa 2: Use o Wireshark para Examinar Alterações do ARP

Etapa 1: Configure o Wireshark para capturas de pacote.

Prepare o Wireshark para capturas.

1. Clique em **Capture > Options**.
2. Selecione a Interface que corresponde à LAN.
3. Verifique a caixa Update list de pacotes em tempo real.
4. Clique em **Start**.

Isto iniciará a captura do pacote.

Etapa 2: Prepare o computador para capturas ARP.

1. Se ainda não foi feito, abra a janela de terminal do Windows clicando em **Start > Run**. Digite **cmd**, e clique em **OK**.
2. Limpe a cache ARP, que irá solicitará ao ARP redescobrir mapas de endereço. Escreva o comando que você usou: _____

Etapa 3: Capture e avalie a comunicação ARP.

Nesta etapa, uma solicitação ping será enviada ao Gateway, e outra ao Eagle Server. Depois, a captura do Wireshark será interrompida e a comunicação ARP avaliada.

1. Envie uma solicitação ping ao Gateway, usando o comando **ping** –**n 1 172.16.255.254.**
2. Envie uma solicitação ping ao Eagle Server, usando o comando **ping** –**n 1 192.168.254.254**.

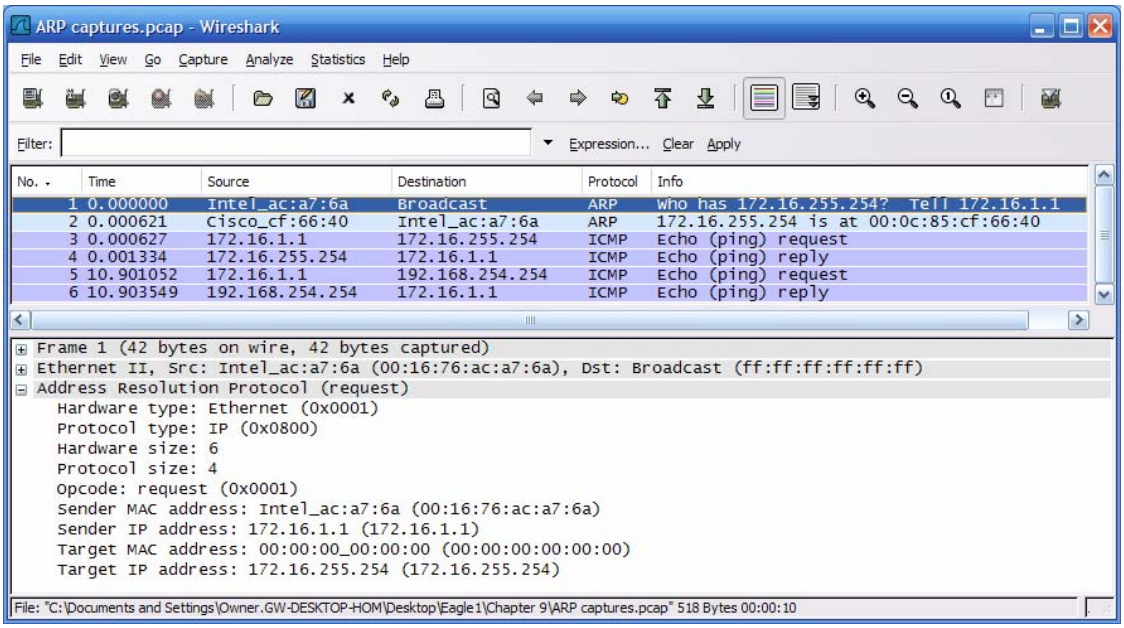

Figura 6. Captura do Wireshark da Comunicação ARP

3. Interrompa o Wireshark e avalie a comunicação. Você deve ver uma tela do Wireshark similar à tela a na Figura 6. A Janela Packet list do Wireshark mostra o número de pacotes capturados. A Janela Packet Details mostra conteúdos do protocolo ARP.

4. Usando sua captura Wireshark, responda as seguintes perguntas:

   Qual foi o primeiro pacote ARP? _____

   Qual foi o segundo pacote ARP? _____

   Preencha a seguinte tabela com informações sobre o primeiro pacote ARP:

Campo	Valor
Endereço MAC do Emissor	
Endereço IP do Emissor	
Endereço MAC do Alvo	
Endereço IP do Alvo	

   Preencha a seguinte tabela com informações sobre o segundo pacote ARP:

Campo	Valor
Endereço MAC do Emissor	
Endereço IP do Emissor	
Endereço MAC do Alvo	
Endereço IP do Alvo	

   Se o quadro Ethernet II para uma solicitação ARP for de broadcast, por que o endereço MAC do Alvo contém somente **0**s? _____

   Por que não houve solicitação ARP para o ping para o Eagle Server?

   _____

   _____

   _____

Quanto tempo deve o mapeamento do Gateway ser guardado na cache ARP do computador? Por quê?

_____

_____

Tarefa 3: Reflexão

O protocolo ARP mapeia os endereços IP da Camada 3 para os endereços MAC da Camada 2. Se um pacote deve se mover através das redes, o endereço MAC da Camada 2 se modifica com cada salto através de um roteador, mas o endereço da Camada 3 nunca se modifica.

A cache ARP guarda mapeamentos ARP. Se a entrada foi aprendida dinamicamente, será eventualmente apagada da cache. Se a entrada foi inserida manualmente, é uma entrada estática e permanecerá até o computador ser desligado ou a cache ARP ser manualmente limpa.

Tarefa 4: Desafio

Usando fontes externas, realize uma busca sobre ARP spoofing. Discuta várias técnicas usadas para combater este tipo de ataque.

A maioria dos roteadores sem fio suporta acesso de rede sem fio. Usando esta técnica, endereços MAC que possuem permissão de acesso à rede sem fio são manualmente adicionados ao roteador sem fio. Usando fontes externas, discuta as vantagens de configurar o acesso de rede sem fio. Discuta modos que atacantes podem usar para burlar esta segurança.

Tarefa 5: Limpeza

O Wireshark foi instalado no computador. Se o Wireshark precisar ser desinstalado, clique em **Iniciar> Painel de Controle.** Abra **Adicionar ou Remover Programas**. Selecione o Wireshark, e clique em **Remover**.

Remova quaisquer arquivos criados no computador durante o laboratório.

A menos que não solicitado pelo instrutor, desligue os computadores. Remova qualquer coisa que tenha sido trazida ao laboratório e deixe a sala pronta para a próxima aula.

