Laboratório 9.8.3: Dispositivo Intermediário como um Dispositivo Final

Diagrama de Topologia

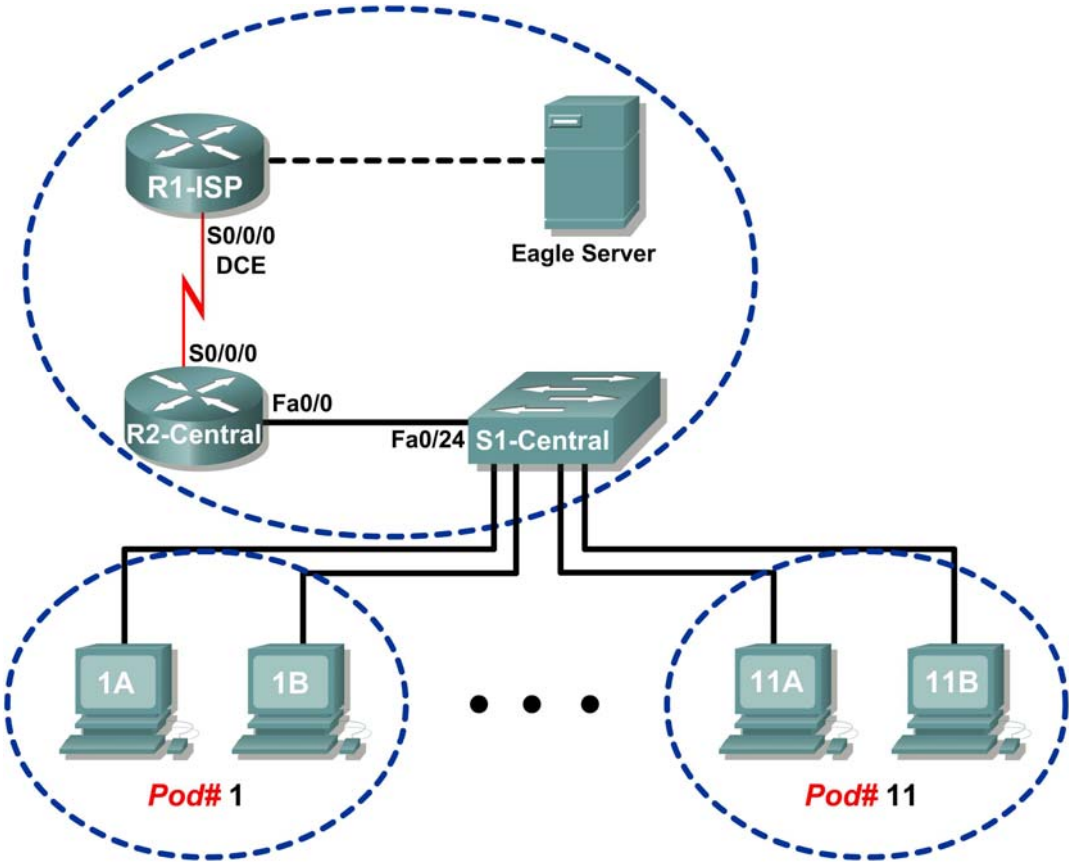

Tabela de Endereçamento

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 Wireshark para capturar e analisar quadros originados em nós de rede.
- Examinar a origem dos quadros em uma rede pequena.

Contexto

Um switch é usado para comutar quadros entre dispositivos de rede. Um switch não origina normalmente o quadro para dispositivos. Pelo contrário, um switch passa eficientemente o quadro de um dispositivo para outro na LAN.

Cenário

O Wireshark será usado para capturar e analisar quadros Ethernet. 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.

Em seu laboratório você executará ping em um computador vizinho.

Escreva o endereço IP e a porta de conexão de S1-Central para o computador vizinho:

Endereço IP: _____ Número da Porta em S1-Central: _____

Tarefa 1: Use o Wireshark para Capturar e Analisar Quadros Originários de Nós de Rede

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. Durante esta captura haverá provavelmente 200 capturas, tornando a análise um pouco tediosa. A conversação crítica de Telnet entre o computador e S1-Central será fácil de filtrar.

Etapa 2: Use o cliente Telnet do Windows para acessar S1-Central.

O S1-Central foi configurado com 11 contas de aluno, ccna1 até ccna11. Para fornecer acesso para cada aluno, use o userid que corresponde ao seu pod. Por exemplo, para computadores no pod 1, use userid ccna1. A menos que não determinado pelo seu instrutor, a senha é cisco.

1. A partir do terminal do Windows, execute o comando Telnet, **telnet** *destination-ip-address*:

   C:/> telnet 172.16.254.1

2. Digite o nome de usuário apropriado e senha, **cisco**.
   O prompt S1-Central deve ser exibido, S1-Central#.

Etapa 3: Limpe a tabela de endereços MAC.

1. Examine a tabela de endereço MAC do switch com o comando **show mac-address-table**. Além de várias entradas estáticas, deve haver numerosas entradas dinâmica na tabela de endereços.
2. Para limpar entradas dinâmicas na tabela de endereços MAC, use o comando **clear mac-address-table dynamic**.
3. Liste as entradas dinâmicas de endereço MAC:

Endereço MAC	Porta do Switch

4. Abra uma segunda janela de terminal. Execute o ping no endereço IP de seu vizinho, que foi gravado anteriormente:

   `C:>\ ping –n 1 ip-address`

5. O endereço MAC para este computador deve ser dinamicamente adicionado na tabela de endereços MAC de S1-Central.
6. Novamente liste as entradas dinâmicas de endereços MAC:

Endereço MAC	Porta do Switch

   Qual conclusão pode ser feita sobre como um switch aprende endereços MAC conectados às suas interfaces?

   _____

   _____

7. Feche a captura do Wireshark.

   A captura será analisada na próxima tarefa.

Tarefa 2: Examine a Origem de Quadros em uma Rede Pequena

Etapa 1: Examine uma sessão Telnet para S1-Central.

1. Destaque um dos pacotes de sessão Telnet. No menu do Wireshark, clique em **Analyze | Follow TCP Stream**. Uma janela de conteúdo de fluxo abrirá, no padrão ASCII. Se o nome do usuário e senhas não forem visíveis, mude para HEX Dump.
2. Verifique o nome do usuário e senha que você digitou:
   Nome do usuário: _____ Senha: _____
3. Feche a janela de conteúdo de fluxo.

Etapa 2: Examine informações do comando show mac-address-table.

1. Abra o Notepad. Dados capturados serão transferidos para o Notepad para análise. Pode haver numerosos pacotes que foram capturados.
2. No painel superior do Wireshark Packet List, role para baixo para a solicitação ICMP capturada. Se a janela inferior Packet Byte do Wireshark não estiver visível, clique em **View** > **Packet bytes**.

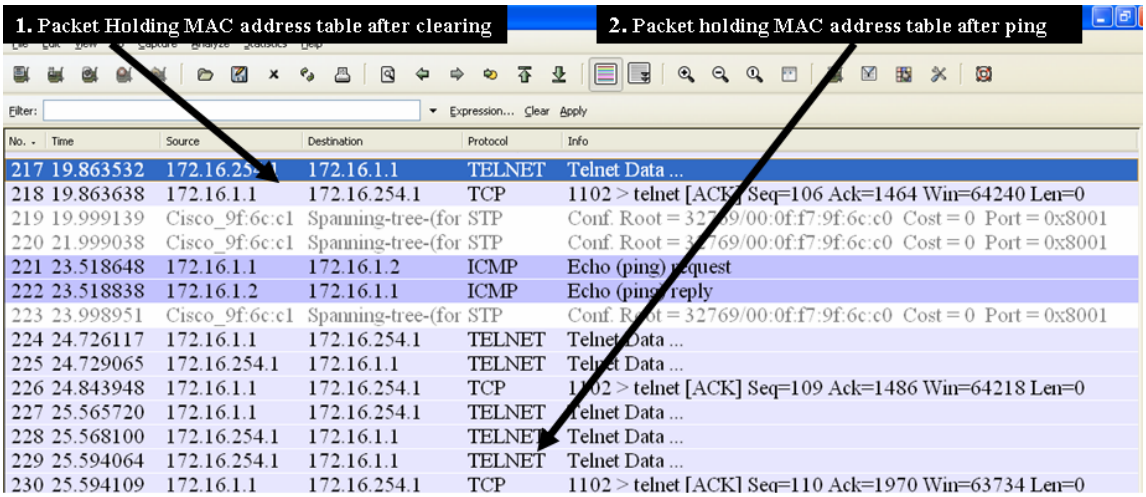

Figura 1. Captura Wireshark de Telnet

Veja a Figura 1, temos uma saída parcial da captura do Wireshark:

1 Selecione o último pacote de dados Telnet de S1-Central antes do comando **ping**. Em seguida, selecione o Packet byte correspondente. Clique com o botão direito em Packet byte e clique em **Copy** > **Text only**. No Bloco de Notas, clique em **Edit > Paste**. Os mapeamentos dinâmicos devem ser similares aos seguintes:

```
{_lEMaNL;RPC          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000f.f79f.6cc0    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0010.a47b.015f    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 5
S1-Central#
```

3. Escreva o endereço MAC e o Número da porta exibidos na saída. A porta do switch corresponde ao seu computador? _____

Endereço MAC	Tipo	Porta

Por que o mapeamento do seu computador está ainda na tabela de endereços MAC, apesar de ter sido limpa?

_____

_____

2 Selecione o último pacote de dados Telnet imediatamente após a resposta do ping. Em seguida, selecione o Packet byte correspondente. Clique com o botão direito em Packet byte e clique em **Copy** > **Text only**. No Bloco de Notas, clique em **Edit > Paste**. Mapeamentos dinâmicos devem ser similares à seguinte ação:

```
{_lEPaNM;VP          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000f.f79f.6cc0    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0010.a47b.015f    DYNAMIC     Fa0/1
   1    0016.76ac.a76a    DYNAMIC     Fa0/2
Total Mac Addresses for this criterion: 6
S1-Central#
```

4. Escreva o endereço MAC e o número da Porta para a segunda entrada dinâmica exibida na saída. A porta do switch corresponde ao seu computador? _____

Endereço MAC	Tipo	Porta

Tarefa 3: Reflexão

A captura Wireshark de uma sessão entre um computador e S1-Central foi analisada para mostra como um switch aprende dinamicamente sobre nós diretamente conectados a ele.

Tarefa 4: Desafio

Use o Wireshark para capturar e analisar sessões entre o computador e o switch Cisco. Use a opção do menu do Wireshark **Analyze > Follow TCP Stream** para visualizar o nome do usuário e a senha de acesso. Quão seguro é o protocolo Telnet protocolo? O que pode ser feito para tornar a comunicação com dispositivos Cisco mais segura?

_____

_____

_____

_____

_____

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 **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.

