Labview a tabela de endereços MAC do switch

Topologia

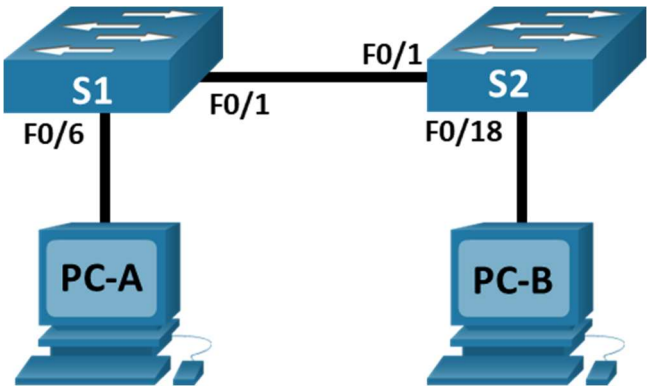

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede
S1	VLAN 1	192.168.1.11	255.255.255.0
S2	VLAN 1	192.168.1.12	255.255.255.0
PC-A	NIC	192.168.1.1	255.255.255.0
PC-B	NIC	192.168.1.2	255.255.255.0

Objetivos

Parte 1: Criar e Configurar a Rede

Parte 2: Examinar a Tabela de Endereços MAC do Switch

Histórico/Cenário

O objetivo de um switch LAN de Camada 2 é entregar quadros Ethernet a dispositivos host na rede local. O switch registra os endereços MAC do host que estão visíveis na rede e os mapeia para suas próprias portas Ethernet. Esse processo é chamado de criação da tabela de endereços MAC. Quando um switch recebe um quadro de um PC, ele examina os endereços MAC de origem e de destino do quadro. O endereço MAC de origem é gravado e mapeado para a porta do switch em que chegou. O endereço MAC de destino é pesquisado na tabela de endereços MAC. Se o endereço MAC de destino for um endereço conhecido, o quadro será enviado pela porta do switch associada ao endereço MAC. Se o endereço MAC for desconhecido, o quadro será transmitido por todas as portas do switch, exceto aquela em que ele chegou. É importante observar e entender a função de um switch e como ele realiza a entrega de dados na rede. O modo como um switch opera tem implicações para administradores de rede cujo trabalho é garantir a comunicação segura e confiável da rede.

Os switches são usados para interconectar e entregar informações a computadores em redes locais. Os switches entregam quadros Ethernet a dispositivos host identificados por endereços MAC da placa de interface de rede.

Na Parte 1, você criará uma topologia com vários switches e um tronco que conecta os dois switches. Na Parte 2, você fará ping em vários dispositivos e observará como os dois switches criam suas tabelas de endereços MAC.

Nota: Os swithcs usados são o Cisco Catalyst 2960s com Cisco IOS Release 15.2 (2) (imagem lanbasek9). Podem ser usados outros switches e outras versões do Cisco IOS. De acordo com o modelo e da versão do Cisco IOS, os comandos disponíveis e a saída produzida poderão variar em relação ao que é mostrado nos laboratórios.

Nota: Verifique se os switches foram apagados e se não há configurações de inicialização. Se estiver em dúvida, entre em contato com o instrutor.

Recursos necessários

- 2 comutadores (Cisco 2960 com imagem lanbasek9 do Cisco IOS Release 15.2 (2) ou comparável)
- 2 PCs (Windows com programa de emulação terminal, como o Tera Term)
- Cabos de console para configurar os dispositivos Cisco IOS por meio das portas de console
- Cabos ethernet conforme mostrado na topologia

Nota: As interfaces Fast Ethernet nos comutadores Cisco 2960 são de detecção automática e um cabo direto Ethernet pode ser usado entre os comutadores S1 e S2. Se estiver usando outro modelo de switch da Cisco, pode ser necessário usar um cabo Ethernet cruzado.

Instruções

Parte 1: Criar e Configurar a Rede

Etapa 1: Instale a rede de acordo com a topologia.

Etapa 2: Configure os PCs hosts.

Etapa 3: Inicialize e recarregue os switches, conforme necessário.

Etapa 4: Defina as configurações básicas de cada switch.

a. Configure o nome do dispositivo conforme mostrado na topologia.

b. Configure o endereço IP conforme listado na Tabela de Endereçamento.

c. Atribua **cisco** como o console e senhas vty.

d. Atribua **class** como a senha do EXEC privilegiado.

Parte 2: Examinar a Tabela de Endereços MAC do Switch

Um switch reconhece endereços MAC e cria a tabela de endereços MAC, enquanto os dispositivos de rede iniciam a comunicação na rede.

Etapa 1: Registre os endereços MAC do dispositivo de rede.

a. Abra um prompt de comando no PC-A e PC-B e digite **ipconfig /all**.

Quais são os endereços físicos do adaptador de Ethernet?

Endereço MAC PC-A: 0010.119D.7DB0

Endereço MAC PC-B: 0060.5CBE.CB69

b. Use o console para se conectar aos switches S1 e S2 e digite o comando **show interface F0/1** em cada switch.

Na segunda linha da saída do comando, quais são os endereços de hardware (ou bia [burned-in address, endereço gravado na ROM])?

S1 Fast Ethernet 0/1 MAC Address:

0006.2a78.d501

S2 Fast Ethernet 0/1 MAC Address:

0005.5ec1.9201

Etapa 2: Exiba a tabela de endereços MAC do switch.

Use o console para se conectar ao switch S2 e visualize a tabela de endereços MAC antes e depois de executar os testes de comunicação de rede com ping.

a. Estabeleça uma conexão de console com S2 e entre no modo EXEC privilegiado.

b. No modo EXEC privilegiado, digite o comando **show mac address-table** e pressione Enter.

```
S2# show mac address-table
```

Mesmo que não haja comunicação de rede iniciada pela rede (isto é, nenhum uso de ping), é possível que o switch tenha reconhecido os endereços MAC da sua conexão com o PC e com o outro switch.

Existe algum endereço MAC gravado na tabela de endereços MAC?

Sim

Quais endereços MAC estão registrados na tabela? Em que portas do switch eles estão mapeados e a que dispositivos pertencem? Ignore os endereços MAC que estão mapeados para a CPU.

1 0006.2a78.d502 DYNAMIC Fa0/2, pertence ao S1

Se você não havia gravado anteriormente os endereços MAC dos dispositivos de rede na Etapa 1, como você poderia dizer a quais dispositivos os endereços MAC pertencem, usando apenas a saída do comando **show mac address-table**? Isso funciona em todos os cenários?
Embora o comando show mac address-table possa fornecer algumas informações úteis, ele não é suficiente para identificar de forma confiável todos os dispositivos em uma rede.
Usando em conjunto um software de gerenciamento de rede, análise de tráfego de rede e ou a documentação da rede pode ajudar a identificar os hosts dos endereços MAC.

Etapa 3: Limpe a tabela de endereços MAC de S2 e exiba a tabela de endereços MAC novamente.

a. No modo EXEC privilegiado, digite o comando dinâmico **clear mac address-table** e pressione **Enter**.

```
S2# clear mac address-table dynamic
```

b. Digite rapidamente o comando **show mac address-table** novamente.

A tabela de endereços MAC tem algum endereço para VLAN 1? Há outros endereços MAC listados?

Tem 1 endereço listado apenas

Aguarde 10 segundos, digite o comando **show mac address-table** e pressione Enter. Há novos endereços na tabela de endereços MAC?

Não

Etapa 4: Em PC-B, faça ping nos dispositivos da rede e observe a tabela de endereços MAC do switch.

a. No PC-B, abra um prompt de comando e digite **arp -a**.

Não incluindo endereços de difusão seletiva ou difusão, quantos pares de endereços IP para MAC do dispositivo foram aprendidos pelo ARP?

No ARP Entries Found

b. No prompt de comando de PC-B, faça ping em PCA-A, S1 e S2.

Todos os dispositivos tiveram respostas bem-sucedidas? Em caso negativo, verifique o cabeamento e as configurações de IP.

Sim, todos tiveram respostas positivas.

c. De uma conexão de console ao S2, digite o comando **show mac address-table**.

O switch adicionou outros endereços MAC à tabela de endereços MAC? Em caso afirmativo, que endereços e dispositivos?

Adicionou mais 3 endereços.

1	0010.119d.7db0	DYNAMIC	Fa0/2
1	0090.0c67.a863	DYNAMIC	Fa0/2
1	00d0.ffe3.e7ea	DYNAMIC	Fa0/1

No PC-B, abra um prompt de comando e digite novamente **arp -a**.

A cache ARP de PC-B tem entradas adicionais para todos os dispositivos de rede que receberam pings?

Internet Address	Physical Address	Type
192.168.1.1	0010.119d.7db0	dynamic
192.168.1.11	0090.0c67.a863	dynamic
192.168.1.12	0090.2bb7.c564	dynamic

Perguntas para reflexão

Em redes Ethernet, os dados são entregues a dispositivos baseados em seus endereços MAC. Para que isso aconteça, switches e computadores criam dinamicamente caches ARP e tabelas de endereços MAC. Com apenas alguns computadores na rede, esse processo parece muito fácil. Quais seriam alguns dos desafios em redes maiores?

Escalabilidade:
Em redes com muitos dispositivos, as tabelas ARP e de endereços MAC pode consumir recursos de memória nos switches e computadores, o processamento das tabelas podem gerar latência e sobrecarregar os dispositivos de rede.

Segurança:
Dependendo da configuração pode tornar vulnerável a ataques de envenenamento ou falsificação de ARP, nos onde um invasor pode associar seu próprio endereço MAC a um endereço IP legítimo.
Isso pode permitir que o invasor intercepte, modifique, desvie o tráfego de rede ou até inundar um switch com um grande número de endereços MAC falsos, sobrecarregando a tabela de endereços MAC do switch.