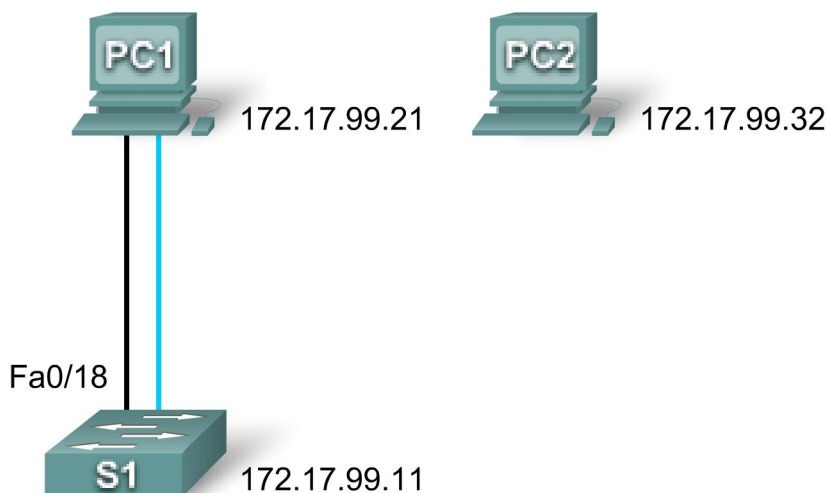


Atividade PT 2.5.1: Configuração básica do switch

Diagrama de topologia



NOTA PARA O USUÁRIO: Esta atividade é uma variação do Laboratório 2.5.1. O Packet Tracer pode não suportar todas as tarefas especificadas no laboratório prático. Esta atividade não deve ser considerada equivalente à conclusão do laboratório prático. O Packet Tracer não substitui um experimento em laboratório prático com equipamento real.

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede	Gateway padrão
PC1	Placa de rede	172.17.99.21	255.255.255.0	172.17.99.1
PC2	Placa de rede	172.17.99.22	255.255.255.0	172.17.99.1
S1	VLAN99	172.17.99.11	255.255.255.0	172.17.99.1

Objetivos de aprendizagem

- Apagar uma configuração existente em um switch.
- Verificar a configuração de switch padrão.
- Criar uma configuração básica de switch.
- Gerenciar a tabela de endereços MAC.
- Configurar a segurança de porta.

Introdução

Nesta atividade, você irá examinar e configurar um switch de rede local autônomo. Embora um switch execute funções básicas em sua condição padrão pronta para uso, há vários parâmetros que um administrador de rede deve modificar para assegurar otimizar uma LAN. Esta atividade apresenta os fundamentos da configuração do switch.

Tarefa 1: Apagar uma configuração existente em um switch

Etapa 1. Entrar no modo EXEC privilegiado, digitando o comando **enable**.

Clique em S1 e, em seguida, na guia **CLI**. Emita o comando **enable** para entrar no modo EXEC privilegiado.

```
Switch>enable  
Switch#
```

Etapa 2. Remover o arquivo de informações do banco de dados de VLAN.

As informações do banco de dados de VLAN são armazenadas em `vlan.dat` na memória flash, separadamente dos arquivos de configuração. Para remover o arquivo VLAN, emita o comando **delete flash:vlan.dat**.

```
Switch#delete flash:vlan.dat  
Delete filename [vlan.dat]? [Enter]  
Delete flash:vlan.dat? [confirm] [Enter]
```

Etapa 3. Remover o arquivo de configuração de inicialização da NVRAM do switch.

```
Switch#erase startup-config  
Erasing the nvram filesystem will remove all configuration files! Continue?  
[confirm] [Enter]  
[OK]  
Erase of nvram: complete
```

Etapa 4. Verificar se as informações de VLAN foram excluídas.

Verifique se a configuração de VLAN foi excluída utilizando o comando **show vlan**.

```
Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
10	VLAN10	active	
30	VLAN30	active	
1002	fddi-default	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

As informações de VLAN ainda estão no switch. Siga a próxima etapa para apagá-lo.

Etapa 5. Reiniciar o switch.

No prompt do modo EXEC privilegiado, digite o comando **reload** para começar o processo.

```
Switch#reload
Proceed with reload? [confirm] [Enter]
%SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.

<saída do comando omitida>

Press RETURN to get started! [Enter]

Switch>
```

Tarefa 2: Verificar a configuração de switch padrão

Etapa 1. Entrar no modo privilegiado.

Você pode acessar todos os comandos do switch no modo privilegiado. No entanto, como muitos dos comandos privilegiados configuram parâmetros operacionais, o acesso ao modo privilegiado deve ser protegido por senha para impedir a utilização sem autorização. O conjunto de comandos privilegiados inclui os comandos contidos no modo EXEC usuário, bem como o comando **configure** por meio do qual o acesso restante dos modos de comando é obtido.

```
Switch>enable
Switch#
```

Observe que o prompt foi alterado na configuração para refletir o modo EXEC privilegiado.

Etapa 2. Examinar a configuração atual do switch.

- a. Examine a configuração atual em execução, emitindo o comando **show running-config**.
 1. Quantas interfaces Fast Ethernet o switch tem? _____
 2. Quantas interfaces Gigabit Ethernet o switch tem? _____
 3. Qual é o intervalo de valores mostrado para as linhas vty? _____
- b. Examine o conteúdo atual da NVRAM, emitindo o comando **show startup-config**.
 1. Por que o switch exibe esta resposta?

- c. Examine as características da interface virtual VLAN1, emitindo o comando **show interface vlan1**.
 1. Há um endereço IP configurado no switch? _____
 2. Qual é o endereço MAC desta interface virtual do switch? _____
 3. Esta interface está ativada? _____
- d. Agora exiba as propriedades IP da interface, utilizando o comando **show ip interface vlan1**.
 1. Que saída de dados você vê?

Etapa 3. Exibir informações do Cisco IOS.

- a. Exiba as informações do Cisco IOS, utilizando o comando **show version**.

1. Qual é a versão do Cisco IOS que o switch está executando? _____
2. Qual é o nome do arquivo de imagem do sistema? _____
3. Qual é o endereço MAC base deste switch? _____

Etapa 4. Examinar as interfaces Fast Ethernet.

- a. Examine as propriedades padrão da interface Fast Ethernet utilizada pelo PC1, utilizando o comando **show interface fastethernet 0/18**.

```
Switch#show interface fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
Hardware is Lance, address is 0060.5c36.4412 (bia 0060.5c36.4412)
MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s
```

<saída do comando omitida>

1. A interface está ativada ou desativada? _____
2. Que evento faria uma interface subir? _____
3. Qual é o endereço MAC da interface? _____
4. Qual é a velocidade e a configuração duplex da interface? _____

Etapa 5. Examinar informações de VLAN.

- a. Examine as configurações de VLAN do switch, utilizando o comando **show vlan**.

1. Qual é o nome da VLAN 1? _____
2. Quais portas estão nesta VLAN? _____
3. A VLAN 1 está ativa? _____
4. Qual tipo de VLAN é a VLAN padrão? _____

Etapa 6. Examinar a memória flash.

- a. Há dois comandos para examinar a memória flash: **dir flash:** ou **show flash**. Emita um dos comandos para examinar o conteúdo do diretório flash.

1. Quais arquivos ou diretórios são encontrados?

Etapa 7. Examinar e salvar o arquivo de configuração de inicialização.

Anteriormente, na etapa 2, você viu que não havia arquivo de configuração de inicialização. Faça uma alteração na configuração do switch e salve-a. Digite os comandos a seguir:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#exit
S1#
```

Para salvar o conteúdo do arquivo de configuração em execução na NVRAM (RAM não volátil), emita o comando **copy running-config startup-config**.

```
Switch#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
```

Agora exiba o conteúdo da NVRAM. A configuração atual foi gravada na NVRAM.

Tarefa 3: Criar uma configuração básica de switch

Etapa 1. Atribuir um nome ao switch.

Entre no modo de configuração global. O modo de configuração permite gerenciar o switch. Insira os comandos de configuração, um por linha. Observe que o prompt da linha de comando é alterado para refletir o prompt atual e o nome do switch. Na última etapa da tarefa anterior, você configurou o hostname. Aqui está uma revisão dos comandos usados.

```
S1#configure terminal
S1(config)#hostname S1
S1(config)#exit
```

Etapa 2. Definir as senhas de acesso.

Entre no modo **config-line** da console. Defina a senha de login como **cisco**. Também configure as linhas vty de 0 a 15 usando a senha **cisco**.

```
S1#configure terminal
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

Por que o comando **login** é necessário? _____

Etapa 3. Definir as senhas no modo de comando.

Defina a enable secret password como class.

```
S1(config)#enable secret class
```

Etapa 4. Configurar o endereço da Camada 3 do switch.

Defina o endereço IP do switch como 172.17.99.11 com uma máscara de sub-rede 255.255.255.0 na interface virtual interna VLAN 99. Para que o endereço seja atribuído, a VLAN deve primeiro ser criada no switch.

```
S1(config)#vlan 99
S1(config-vlan)#exit
S1(config)#interface vlan99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
```

Etapa 5. Atribuir portas à VLAN do switch.

Atribua a Fastethernet 0/1, a 0/8 e a 0/18 à VLAN 99.

```
S1(config)#interface fa0/1
S1(config-if)#switchport access vlan 99
S1(config-if)#interface fa0/8
S1(config-if)#switchport access vlan 99
S1(config-if)#interface fa0/18
S1(config-if)#switchport access vlan 99
S1(config-if)#exit
```

Etapa 6. Definir o gateway padrão do switch.

Como S1 é um switch de camada 2, ele faz encaminhamento com base no cabeçalho da Camada 2. Se várias redes forem conectadas a um switch, você precisará especificar como o switch encaminha os quadros de redes interconectadas, porque o caminho deve ser determinado na Camada três. Isso é feito especificando-se um endereço de gateway padrão que aponta para um roteador ou um switch Camada 3. Embora esta atividade não inclua um gateway de IP externo, consideremos que você acabe precisando conectar a rede local a um roteador para acesso externo. Supondo que a interface LAN do roteador seja 172.17.99.1, defina o gateway padrão para o switch.

```
S1(config)#ip default-gateway 172.17.99.1
S1(config)#exit
```

Etapa 7. Verificar as configurações de rede local de gerenciamento.

Verifique as configurações da interface na VLAN 99 com o comando **show interface vlan 99**.

```
S1#show interface vlan 99
Vlan99 is up, line protocol is up
  Hardware is CPU Interface, address is 0060.47ac.1eb8 (bia 0060.47ac.1eb8)
  Internet address is 172.17.99.11/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
<saída do comando omitida>
```

Qual é a largura de banda nesta interface? _____

Qual é a estratégia de fila? _____

Etapa 8. Configurar o endereço IP e o gateway padrão do PC1.

Defina o endereço IP do PC1 para 172.17.99.21, com uma máscara de sub-rede 255.255.255.0. Configure o gateway padrão como sendo o endereço 172.17.99.11. Clique no PC1, em sua guia **Desktop** e na configuração IP para inserir os parâmetros de endereçamento.

Etapa 9. Verificar a conectividade.

Para verificar se o host e o switch estão configurados corretamente, execute ping no switch a partir do PC1.

Se o ping não tiver êxito, solucione problemas no switch e na configuração do host. Observe que isso pode exigir algumas tentativas para que haja êxito dos pings.

Etapa 10. Configurar a velocidade de porta e as configurações duplex para uma interface Fast Ethernet.

Defina as configurações duplex e de velocidade na Fast Ethernet 0/18. Use o comando **end** para retornar ao modo EXEC privilegiado quando terminar.

```
S1#configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#speed 100
S1(config-if)#duplex full
S1(config-if)#end
```

A autodetecção é padrão na interface Ethernet do switch. Desse modo, ela negocia automaticamente as configurações ideais. Você só deverá definir duplex e velocidade manualmente se uma porta precisar funcionar a uma determinada velocidade e em modo duplex. Configurar manualmente as portas pode acarretar incompatibilidades bidirecionais, o que pode diminuir significativamente o desempenho.

Observe como o link entre o PC1 e S1 foi desativado. Remova os comandos **speed 100** e **duplex full**. Agora verifique as configurações na interface Fast Ethernet com o comando **show interface fa0/18**.

```
S1#show interface fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Lance, address is 0060.5c36.4412 (bia 0060.5c36.4412)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
<saída do comando omitida>
```

Etapa 11. Salvar a configuração de VLAN.

Você concluiu a configuração básica do switch. Agora faça o backup do arquivo de configuração em execução na NVRAM para assegurar que as alterações feitas não sejam perdidas caso o sistema seja reinicializado ou desligado.

```
S1#copy running-config startup-config

Destination filename [startup-config]?[Enter]
Building configuration...
[OK]
S1#
```

Etapa 12. Examinar o arquivo de configuração de inicialização.

Para ver a configuração armazenada na NVRAM, emita o comando **show startup-config** no modo EXEC privilegiado (enable mode).

Todas as alterações inseridas foram registradas no arquivo?

Tarefa 4: Gerenciar a tabela de endereços MAC

Etapa 1. Registrar os endereços MAC dos hosts.

Determine e registre os endereços de Camada 2 (endereço físico) das placas de interface de rede do PC utilizando as seguintes etapas:

- Clique no PC.
- Selecione a guia **Desktop**.
- Clique em **Command Prompt**.
- Digite o comando **ipconfig /all**.

Etapa 2. Determinar os endereços MAC que o switch aprendeu.

Visualize os endereços MAC usando o comando **show mac-address-table** no modo EXEC privilegiado. Se não houver nenhum endereço MAC, execute ping do PC1 em S1 e verifique novamente.

```
S1#show mac-address-table
```

Etapa 3. Limpar a tabela de endereços MAC.

Para remover os endereços MAC existentes, utilize o comando **clear mac-address-table dynamic** no modo EXEC privilegiado.

```
S1#clear mac-address-table dynamic
```

Etapa 4. Verificar os resultados.

Verificar se a tabela de endereços MAC foi apagada.

```
S1#show mac-address-table
```

Etapa 5. Examinar a tabela MAC novamente.

Observe novamente a tabela de endereços MAC no modo EXEC privilegiado. A tabela não foi alterada, execute ping em S1 a partir do PC1 e verifique novamente.

Etapa 6. Definir um endereço MAC estático.

Para especificar as portas às quais um host pode se conectar, uma opção é criar um mapeamento estático do endereço MAC do host para uma porta.

Defina um endereço MAC estático na interface Fast Ethernet 0/18 utilizando o endereço que foi gravado para o PC1 na Etapa 1 desta tarefa, 0002.16E8.C285.

```
S1(config)#mac-address-table static 0002.16E8.C285 vlan 99 interface  
fastethernet 0/18  
S1(config)#end
```

Etapa 7. Verificar os resultados.

Verificar as entradas da tabela de endereços MAC.

```
S1#show mac-address-table
```


Etapa 8. Remover a entrada MAC estática.

Entre no modo de configuração e remova o MAC estático, colocando um **no** na frente da cadeia de caracteres do comando.

```
S1(config)#no mac-address-table static 0002.16E8.C285 vlan 99 interface
fastethernet 0/18
S1(config)#end
```

Etapa 9. Verificar os resultados.

Verifique se o endereço MAC estático foi limpo com o comando **show mac-address-table static**.

Tarefa 5: Configurando a segurança de porta

Etapa 1. Configurar um segundo host.

Um segundo host é necessário para esta tarefa. Defina o endereço IP do PC2 para 172.17.99.22, com uma máscara de sub-rede 255.255.255.0 e um gateway padrão 172.17.99.11. Não conecte ainda este PC ao switch.

Etapa 2. Verificar a conectividade.

Verifique se o PC1 e o switch ainda estão configurados corretamente, executando ping no endereço IP da VLAN 99 do switch a partir do host. Se os pings não tiverem êxito, solucione os problemas nas configurações do host e do switch.

Etapa 3. Determinar quais endereços MAC o switch aprendeu.

Visualize os endereços MAC aprendidos usando o comando **show mac-address-table** no modo EXEC privilegiado.

Etapa 4. Listar as opções de segurança de porta.

Explore as opções para definir a segurança de porta na interface Fast Ethernet 0/18.

```
S1# configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#switchport port-security ?
    mac-address      Secure mac address
    maximum          Max secure addresses
    violation         Security violation mode
    <cr>
```

Etapa 5. Configurar a segurança de porta em uma porta de acesso.

Configure a porta Fast Ethernet 0/18 do switch para aceitar dois dispositivos, para aprender os endereços MAC desses dispositivos dinamicamente e para desligar a porta em caso de uma violação.

```
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 2
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#switchport port-security violation shutdown
S1(config-if)#exit
```

Etapa 6. Verificar os resultados.

Mostre as configurações de segurança de porta usando o comando **show port-security interface fa0/18**.

Quantos endereços seguros são permitidos na Fast Ethernet 0/18?
Qual é a ação de segurança para esta porta?

Etapa 7. Examinar o arquivo de configuração em execução.

S1#**show running-config**

Há instruções listadas que refletem diretamente a implementação de segurança da configuração em execução?

Etapa 8. Modificar as configurações de segurança de porta em uma porta.

Na interface Fast Ethernet 0/18, altere a contagem de endereços MAC máxima da segurança de porta para 1.

```
S1(config-if)#switchport port-security maximum 1
```

Etapa 9. Verificar os resultados.

Mostre as configurações de segurança de porta usando o comando **show port-security interface fa0/18**.

As configurações de segurança de porta foram alteradas para refletir as modificações feitas na Etapa 8?

Execute ping no endereço da VLAN 99 do switch a partir do PC1 para verificar a conectividade e atualizar a tabela de endereços MAC.

Etapa 10. Introduzir um host invasor.

Desconecte o PC conectado a Fast Ethernet 0/18 do switch. Conecte o PC2, que recebeu o endereço IP 172.17.99.22 para a porta Fast Ethernet 0/18. Execute ping no endereço da VLAN 99 172.17.99.11 a partir do novo host.

O que aconteceu quando você tentou executar ping em S1?

Nota: A convergência pode demorar um minuto. Alterne os modos **Simulation** e **Realtime** para agilizar a convergência.

Etapa 11. Reativar a porta.

Como o host invasor está conectado a Fast Ethernet 0/18, nenhum tráfego pode passar entre o host e o switch. Reconecte o PC1 a Fast Ethernet 0/18 e digite os seguintes comandos no switch para reativar a porta:

```
S1#configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#no shutdown
S1(config-if)#end
```

Etapa 12. Verificar a conectividade.

Depois da convergência, o PC1 deve ser capaz de executar ping em S1 novamente.

Etapa 13. Verificar os resultados.

O percentual de conclusão deve ser de 100%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.