Atividade PT 2.4.7: Configurar a segurança do switch

Diagrama de topologia

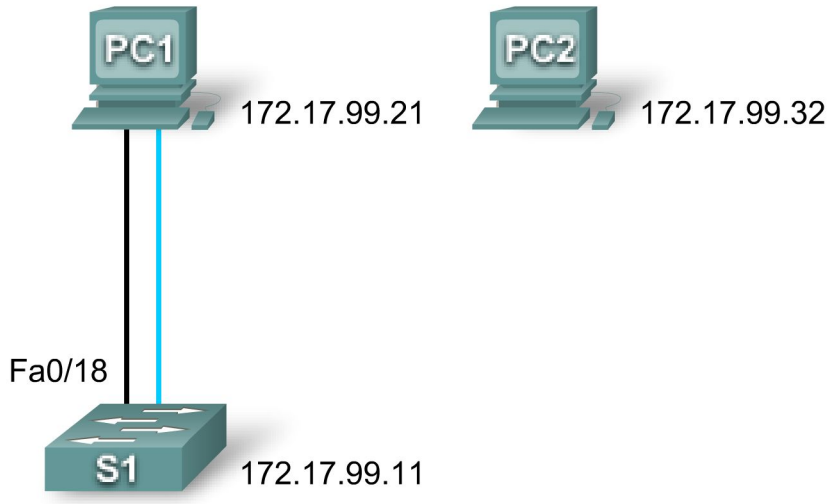

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede
S1	**VLAN99**	172.17.99.11	255.255.255.0
PC1	**Placa de rede**	172.17.99.21	255.255.255.0
PC2	**Placa de rede**	172.17.99.32	255.255.255.0

Objetivos de aprendizagem

- Configurar o gerenciamento básico de switch.
- Configurar segurança dinâmica da porta.
- Testar a segurança dinâmica da porta.
- Proteger portas não utilizadas

Tarefa 1: Configurar gerenciamento básico de switch

Etapa 1: Em PC1, acessar a conexão da console a S1.

- Clique em PC1 e na guia **Desktop**. Selecione **Terminal** na guia **Desktop**.
- Mantenha estas configurações padrão para **Terminal Configuration** e clique em **OK**:

  Bits por segundo = 9600
  Bits de dados = 8
  Paridade = nenhuma

Bits de parada = 1
Controle de fluxo = nenhum

- Você agora está conectado ao S1 através de um console. Pressione Enter para obter o prompt do switch.

Etapa 2: Alternar para modo EXEC privilegiado.

Para acessar o modo EXEC privilegiado, digite o comando **enable**. O prompt é alterado de **>** para **#**.

```
S1>enable
S1#
```

Observe como você conseguiu entrar no modo EXEC privilegiado sem fornecer uma senha. Por que a falta de uma senha de modo EXEC privilegiado é uma ameaça de segurança?

_____

_____

_____

Etapa 3: Alterar para modo de configuração global e configurar a senha no modo EXEC privilegiado.

- Ainda no modo EXEC privilegiado, você pode acessar o modo de configuração global, utilizando o comando **configure terminal**.
- Utilize o comando **enable secret** para definir a senha. Para esta atividade, defina a senha como **class**.

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#enable secret class
S1(config)#
```

Nota: PT não utilizará o comando **enable secret**.

Etapa 4: Configurar senhas de terminal virtual e de console e exigir que os usuários façam login.

Uma senha deve ser obrigatória para acessar a linha de console. Mesmo o modo EXEC usuário básico pode fornecer informações significativas para um usuário mal-intencionado. Além disso, as linhas vty devem ter uma senha para que os usuários possam acessar o switch remotamente.

- Acesse o prompt de console utilizando o comando **line console 0**.
- Utilize o comando **password** para configurar as linhas de console e vty com **cisco** como a senha. Nota: PT não utilizará o comando **password cisco** nesse caso.
- Em seguida, digite o comando **login**, que exige aos usuários digitar uma senha para obter acesso ao modo EXEC do usuário.
- Repita o processo usando as linhas vty. Utilize o comando **line vty 0 15** para acessar o prompt correto.
- Digite o comando **exit** para retornar ao prompt de configuração global.

```
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)#
```


Etapa 5: Configurar criptografia de senha.

A senha no modo EXEC privilegiado já está criptografada. Para criptografar as senhas de linha que você acabou de configurar, digite o comando **service password-encryption** no modo de configuração global.

```
S1(config)#service password-encryption
S1(config)#
```

Etapa 6: Configurar e testar o banner MOTD.

Configure a mensagem do dia (MOTD), utilizando **Authorized Access Only** como o texto. O texto do banner faz distinção entre maiúsculas e minúsculas. Verifique se você não adicionou nenhum espaço antes ou depois do texto do banner. Utilize um caractere delimitador antes e depois do texto do banner para indicar onde o texto começa e termina. O caractere delimitador utilizado no exemplo abaixo é **&**, mas você pode utilizar qualquer caractere não usado no texto do banner. Depois de configurar o MOTD, faça logout do switch para verificar se o banner é exibido quando você volta a fazer login.

```
S1(config)#banner motd &Authorized Access Only&
S1(config)#end [or exit]
S1#exit

S1 con0 is now available

Press RETURN to get started.

[Enter]

Authorized Access Only

User Access Verification

Password:
```

- O prompt de senha agora exige uma senha para entrar no Modo EXEC do usuário. Digite a senha **cisco**.
- Entre no modo EXEC privilegiado com a senha **class** e retorne ao modo de configuração global com o comando **configure terminal**.

```
Password: [cisco] !Nota: A senha não é exibida quando você a digita.

S1>enable
Password: [class] !Nota: A senha não é exibida quando você a digita.
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
```

Etapa 7: Verificar os resultados.

Seu percentual de conclusão deve ser 40%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 2: Configurar segurança dinâmica de porta

Etapa 1: Habilitar VLAN99.

O Packet Tracer é aberto com a interface VLAN 99 no estado desativado, no qual um switch real não costuma funcionar. Você deve habilitar VLAN 99 com o comando **no shutdown** antes da interface ficar ativa no Packet Tracer.


```
S1(config)#interface vlan 99
S1(config-if)#no shutdown
```

Etapa 2: Entrar no modo de configuração da interface de FastEthernet 0/18 e habilitar a segurança de porta.

Antes da configuração de outros comandos de segurança de porta na interface, a segurança de porta deve ser habilitada.

```
S1(config-if)#interface fa0/18
S1(config-if)#switchport port-security
```

Observe que você não precisa sair novamente do modo de configuração global antes de entrar no modo de configuração da interface de fa0/18.

Etapa 3: Configurar o número máximo de endereços MAC.

Para configurar a porta para aprender apenas um endereço MAC, defina **maximum** como **1**:

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

Nota: PT não usa o comando **switchport port-security maximum 1**, mas esse comando é essencial na configuração da segurança de porta.

Etapa 4: Configurar a porta para adicionar o endereço MAC à configuração de execução.

O endereço MAC aprendido na porta pode ser adicionado (“preso”) à configuração de execução da porta.

```
S1(config-if)#switchport port-security mac-address sticky
```

Nota: PT não usa o comando **switchport port-security mac-address sticky**, mas esse comando é essencial na configuração da segurança de porta.

Etapa 5: Configurar a porta para ser desligada automaticamente se a segurança da porta for violada.

Se você não configurar o comando a seguir, S1 só registrará a violação nas estatísticas de segurança da porta, mas não a desligará.

```
S1(config-if)#switchport port-security violation shutdown
```

Nota: PT não usa o comando **switchport port-security violation shutdown**, mas esse comando é essencial na configuração da segurança de porta.

Etapa 6: Confirmar se S1 aprendeu o endereço MAC de PC1.

Ping entre PC1 para S1.

Confirme se S1 agora tem uma entrada de endereço MAC estática para PC1 na tabela MAC:

```
S1#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  99    0060.5c5b.cd23    STATIC      Fa0/18
```

O endereço MAC agora está “preso” à configuração de execução.

```
S1#show running-config
<saída do comando omitida>
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0060.5C5B.CD23
<saída do comando omitida>
S1#
```

Etapa 7: Verificar os resultados.

Seu percentual de conclusão deve ser 70%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 3: Testar segurança dinâmica de porta

Etapa 1: Remover a conexão entre PC1 e S1 e conectar PC2 a S1.

- Para testar a segurança da porta, exclua a conexão Ethernet entre o PC1 e o S1. Se você excluir a conexão do cabo de console acidentalmente, basta reconectá-lo.
- Conecte PC2 a Fa0/18 em S1. Aguarde a luz do link âmbar ficar verde e, em seguida, execute ping de PC2 em S1. Em seguida, a porta deve ser fechada automaticamente.

Etapa 2: Verificar se a segurança de porta é a razão do desligamento da porta.

Para verificar se a segurança da porta a desligou, digite o comando **show interface fa0/18**.

```
S1#show interface fa0/18
FastEthernet0/18 is down, line protocol is down (err-disabled)
  Hardware is Lance, address is 0090.213e.5712 (bia 0090.213e.5712)
<saída do comando omitida>
```

Como o protocolo de linha está desativado por conta de um erro (**err**) ao aceitar um quadro com um endereço MAC diferente do endereço MAC aprendido, o software Cisco IOS desativa (**disabled**) a porta.

Você também pode verificar uma violação à segurança com o comando **show port-security interface fa0/18**.

```
S1#show port-security interface fa0/18
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 00E0.F7B0.086E:99
Security Violation Count   : 1
```

Observe que o status da porta é **secure-shutdown** e a contagem de violação à segurança, **1**.

Etapa 3: Restaurar a conexão entre PC1 e S1 e redefinir a segurança de porta.

Remova a conexão entre PC2 e S1. Reconecte PC1 à porta Fa0/18 em S1.

Observe que a porta continua desativada, mesmo você reconectando o PC permitido na porta. Uma porta no estado desativado por conta de uma violação à segurança deve ser reativada manualmente. Desative a porta e, em seguida, ative-a com **no shutdown**.

```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface fa0/18
S1(config-if)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to
administratively down
S1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
S1(config-if)#exit
S1(config)#
```

Etapa 4: Testar conectividade, executando ping em S1 de PC1.

O ping do PC1 para o S1 deve ter êxito.

Seu percentual de conclusão ainda deve ser 70% ao fim desta tarefa.

Tarefa 4: Proteger portas não utilizadas

Um método simples usado por muitos administradores para ajudar na proteção de sua rede contra o acesso não autorizado é desabilitar todas as portas não usadas em um switch de rede.

Etapa 1: Desabilitar interface Fa0/17 em S1.

Acesse o modo de configuração da interface de FastEthernet 0/17 e desligue a porta.

```
S1(config)#interface fa0/17
S1(config-if)#shutdown
```

Etapa 2: Testar a porta, conectando PC2 a Fa0/17 em S1.

Conecte PC2 à interface Fa0/17 em S1. Observe que as luzes do link estão vermelhas. PC2 não tem acesso à rede.

Etapa 3: Verificar os resultados.

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