Atividade PT 2.6.1: Desafio: Integração das habilidades no Packet Tracer

Diagrama de topologia

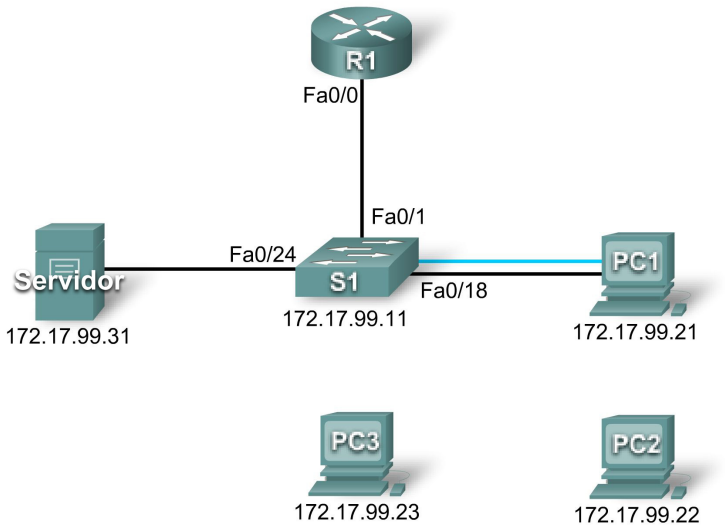

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede
R1	**Fa0/0**	172.17.99.1	255.255.255.0
S1	**Fa0/1**	172.17.99.11	255.255.255.0
PC1	**Placa de rede**	172.17.99.21	255.255.255.0
PC2	**Placa de rede**	172.17.99.22	255.255.255.0
Servidor	**Placa de rede**	172.17.99.31	255.255.255.0

Objetivos

- Estabelecer uma conexão de console com o switch.
- Configurar o nome de host e a VLAN99.
- Configurar a hora.
- Modificar o buffer de histórico.
- Configurar senhas de console/acesso Telnet.
- Configurar banners de login.
- Configurar o roteador.
- Configurar a seqüência de inicialização.
- Resolver uma incompatibilidade entre duplex e velocidade.

- Gerenciar a tabela de endereços MAC.
- Configurar a segurança de porta.
- Assegurar portas não usadas.
- Gerenciar o arquivo de configuração do switch.

Introdução

Nesta Atividade avançada de integração das habilidades no Packet Tracer, você irá configurar o gerenciamento de switch básico, incluindo comandos de manutenção gerais, senhas e segurança de porta. Esta atividade fornece uma oportunidade de revisar habilidades previamente adquiridas.

Tarefa 1: Estabelecer uma conexão de console com um switch

Etapa 1: Conectar um cabo de console a S1.

Para esta atividade, o acesso direto às guias **Config** e **CLI** de S1 está desabilitado. Você deve estabelecer uma sessão de console através do PC1. Conecte um cabo de console do PC1 para S1.

Etapa 2: Estabelecer uma sessão de terminal.

No PC1, abra uma janela **Terminal** e utilize a **Terminal Configuration** padrão. Agora você deve ter acesso à CLI de S1.

Etapa 3: Verificar resultados.

Seu percentual de conclusão deve ser de 6%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 2: Configurar o nome de host e a VLAN 99

Etapa 1: Configurar o nome de host do switch como S1.

Etapa 2: Configurar a porta Fa0/1 e a interface VLAN 99.

Atribua a VLAN 99 à FastEthernet 0/1 e defina o modo de acesso. Esses comandos serão discutidos no próximo capítulo.

```
S1(config)#interface fastethernet 0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 99
```

Configure a conectividade IP em S1 usando a VLAN 99.

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

Etapa 3: Configurar o gateway padrão de S1.

Configure o gateway padrão e teste a conectividade. S1 deve ser capaz de executar ping em R1.

Etapa 4: Verificar os resultados.

Seu percentual de conclusão deve ser 26%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos. Também verifique se a interface VLAN 99 está ativa.

Tarefa 3: Configurar a hora utilizando o recurso de Ajuda

Etapa 1: Configurar a hora segundo a hora atual.

No prompt do EXEC privilegiado, digite **clock ?**. Use o recurso de Ajuda para descobrir cada etapa adicional necessária para definir a hora atual. Como o Packet Tracer não classifica esse comando, o percentual de conclusão não é alterado.

Etapa 2: Verificar se a hora está certa em relação à hora atual.

Utilize o comando **show clock** para verificar se o relógio agora está certo em relação à hora atual. O Packet Tracer talvez não simule corretamente o momento da inserção.

Tarefa 4: Modificar o buffer de histórico

Etapa 1: Definir o buffer de histórico como 50 para a linha de console.

Etapa 2: Definir o buffer de histórico como 50 para as linhas vty.

Etapa 3: Verificar os resultados.

Seu percentual de conclusão deve ser de 32%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 5: Configurar senhas e console/acesso Telnet

Etapa 1: Configurar a senha do modo EXEC privilegiado.

Utilize a forma criptografada da senha no modo EXEC privilegiado e defina a senha como **class**.

Etapa 2: Configurar as senhas para console e Telnet.

Defina a console e a senha vty como **cisco** e exija que os usuários façam o login.

Etapa 3: Criptografar senhas.

Exibir a configuração atual em S1. Observe que as senhas de linha são mostradas em texto não criptografado. Insira o comando para criptografar essas senhas.

Etapa 4: Verificar os resultados.

Seu percentual de conclusão deve ser de 41%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 6: Configurar o banner de login

Se você não digitar o texto do banner exatamente como especificado, o Packet Tracer não usará o comando corretamente. Esses comandos diferenciam maiúsculas de minúsculas. Também certifique-se de não incluir nenhum espaço antes de ou depois do texto.

Etapa 1: Configurar o banner de mensagem do dia em S1.

Configure a mensagem do dia como **Authorized Access Only.**

Etapa 2: Verificar os resultados.

Seu percentual de conclusão deve ser de 44%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 7: Configurar o roteador

Etapa 1: Configurar o roteador com os mesmos comandos básicos utilizados em S1.

Roteadores e switches compartilham muitos comandos. Acesse a CLI de R1, clicando no dispositivo. Faça o seguinte em R1:

- Configure o hostname.
- Defina o buffer de histórico como 50 para console e vty.
- Configure a forma criptografada da senha no modo EXEC privilegiado e defina a senha como **class**.
- Defina a senha de console e vty como **cisco** e exija que os usuários façam o login.
- Criptografe as senhas de console e vty.
- Configure a mensagem do dia como **Acesso somente autorizado.**
- Mova o cabo de console para reconectar o PC1 a S1.

Etapa 2: Verificar os resultados.

Seu percentual de conclusão deve ser de 65%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 8: Configurar a seqüência de inicialização

Etapa 1: Exibir arquivos atualmente armazenados na memória flash.

Em S1, digite o comando **show flash**. Você deve ver os seguintes arquivos listados:

```
S1#show flash
Directory of flash:/

    1  -rw-     4414921          <sem data>  c2960-lanbase-mz.122-25.FX.bin
    3  -rw-     4670455          <sem data>  c2960-lanbase-mz.122-25.SEE1.bin
    2  -rw-         616          <sem data>  vlan.dat

32514048 bytes total (23428056 bytes free)
```

Etapa 2: Configurar S1 para inicializar utilizando a segunda imagem listada.

Verifique se o comando inclui o sistema de arquivos, que é **flash**.

Nota: O Packet Tracer não mostra esse comando na configuração em execução. Além disso, se você reiniciar o switch, o Packet Tracer não carregará a imagem especificada.

Etapa 3: Verificar os resultados.

Seu percentual de conclusão deve ser de 68%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 9: Resolver uma incompatibilidade de duplex e velocidade

Etapa 1: Alterar o duplex e velocidade em S1.

O PC1 e o servidor atualmente não têm acesso via S1 porque existe uma incompatibilidade entre duplex e velocidade. Insira comandos em S1 para resolver esse problema.

Etapa 2: Verificar conectividade.

O PC1 e o Servidor agora devem ser capazes de executar ping em S1, R1 e entre si.

Etapa 3: Verificar os resultados.

Seu percentual de conclusão deve ser de 74%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 10: Gerenciar a tabela de endereços MAC

Etapa 1: Exibir a tabela de endereços MAC atual.

Que comando você utilizaria para mostrar a tabela de endereço MAC?

```
S1#_________________________________________
          Mac Address Table
-------------------------------------------

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

  99    0001.637b.b267    DYNAMIC     Fa0/24
  99    0004.9a32.8e01    DYNAMIC     Fa0/1
  99    0060.3ee6.1659    DYNAMIC     Fa0/18
```

A lista de endereços MAC em sua saída de dados pode ser diferente, dependendo do tempo decorrido desde que você enviou pacotes através do switch.

Etapa 2: Configurar um endereço MAC estático.

A política de rede pode determinar que todos os endereços de servidor são configurados estaticamente. Insira o comando para configurar estaticamente o endereço MAC do servidor.

Etapa 3: Verificar os resultados.

Seu percentual de conclusão deve ser 76%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 11: Configurar a segurança de porta

Etapa 1: Configurar a segurança de porta no PC1.

Use a política a seguir para estabelecer a segurança de porta na porta usada pelo PC1:

- Habilitar a segurança de porta
- Permitir apenas um endereço MAC
- Configurar o primeiro endereço MAC aprendido para "aderir" à configuração
- Definir a porta para desativar se houver uma violação de segurança

Nota: Apenas a etapa da habilitação da segurança de porta é usada pelo Packet Tracer e contabilizada no percentual de conclusão. No entanto, todas as tarefas de segurança de porta listadas acima são necessárias para concluir esta atividade.

Etapa 2: Verificar a segurança de porta.

Verificar se a segurança de porta está habilitada para Fa0/18. Sua saída de dados deve ter a aparência a seguir. Observe que S1 ainda não aprendeu um endereço MAC para essa interface.

Qual comando gerou a seguinte saída de dados?

```
S1#_____________________________________
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Etapa 3: Forçar S1 a aprender o endereço MAC do PC1.

Envie um ping do PC1 ao S1. Em seguida, verifique se S1 adicionou o endereço MAC do PC1 à configuração em execução.

```
!
interface FastEthernet0/18
 <saída do comando omitida>
 switchport port-security mac-address sticky 0060.3EE6.1659
 <saída do comando omitida>
!
```

Etapa 4: Testar a segurança de porta.

Remova a conexão FastEthernet entre S1 e o PC1. Conecte o PC2 a Fa0/18. Espere até que todas as luzes do link fiquem verdes. Se necessário, envie um ping do PC2 para S1 para desativar a porta. A segurança de porta deve mostrar os seguintes resultados:

```
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   : 00D0.BAD6.5193:99
Security Violation Count   : 1
```

A exibição da interface Fa0/18 mostra **line protocol is down (err-disabled)**, o que também indica uma violação à segurança.

```
S1#show interface fa0/18
FastEthernet0/18 is down, line protocol is down (err-disabled)
<saída do comando omitida>
```


Etapa 5: Reconectar o PC1 e reabilitar a porta.

Para reativar a porta, desconecte o PC2 da Fa0/18 e conecte o PC1 novamente. A interface Fa0/18 deve ser configurada manualmente antes de voltar ao estado ativo.

Etapa 6: Verificar os resultados.

Seu percentual de conclusão deve ser de 82%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 12: Proteger as portas não utilizadas

Etapa 1: Desabilitar todas as portas não utilizadas em S1.

Desabilite todas as portas que não são usadas atualmente em S1. O Packet Tracer classifica o status das seguintes portas: Fa0/2, Fa0/3, Fa0/4, Gig 1/1 e Gig 1/2.

Etapa 2: Verificar os resultados.

Seu percentual de conclusão deve ser 97%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 13: Gerenciar o arquivo de configuração do switch

Etapa 1: Salvar a configuração atual na NVRAM para R1.

Etapa 2: Fazer backup dos arquivos de configuração de inicialização de S1 e R1 no servidor.

Faça o backup do arquivo de configuração de inicialização de S1 e R1, carregando-os no servidor. Depois de concluir, verifique se o servidor tem os arquivos **R1-confg** e **S1-confg**.

Mova o cabo de console para reconectar o PC1 a S1

Etapa 3: Verificar os resultados.

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

