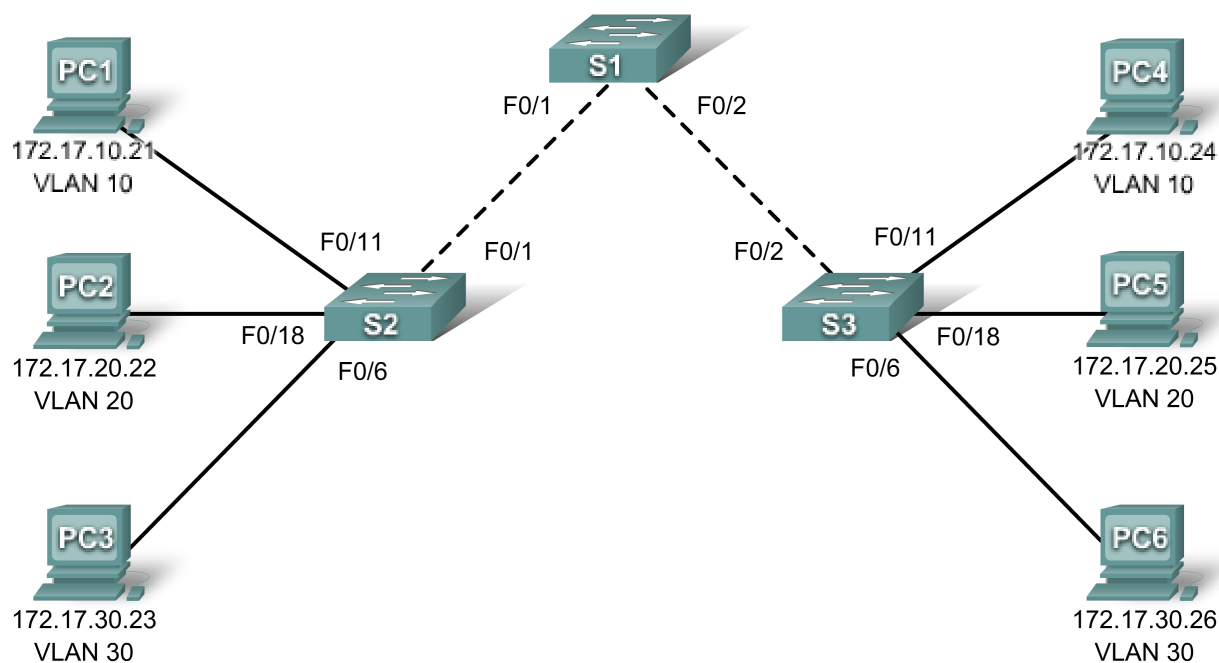


## Atividade PT 4.5.1: Desafio: Integração das habilidades no Packet Tracer

### Diagrama de topologia



### Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede	Gateway padrão
S1	VLAN 99	172.17.99.31	255.255.255.0	172.17.99.1
S2	VLAN 99	172.17.99.32	255.255.255.0	172.17.99.1
S3	VLAN 99	172.17.99.33	255.255.255.0	172.17.99.1
PC1	Placa de rede	172.17.10.21	255.255.255.0	172.17.10.1
PC2	Placa de rede	172.17.20.22	255.255.255.0	172.17.20.1
PC3	Placa de rede	172.17.30.23	255.255.255.0	172.17.30.1
PC4	Placa de rede	172.17.10.24	255.255.255.0	172.17.10.1
PC5	Placa de rede	172.17.20.25	255.255.255.0	172.17.20.1
PC6	Placa de rede	172.17.30.26	255.255.255.0	172.17.30.1

### Objetivos de aprendizagem:

- Configurar e verificar configurações básicas de dispositivo.
- Configurar e verificar a segurança da porta.
- Configurar VTP.

- Configurar o entroncamento.
- Configurar VLANs.
- Atribuir VLANs a portas.
- Verificar a conectividade fim-a-fim.

## Introdução

Nesta atividade, você irá configurar switches incluindo a configuração básica, a segurança de porta, o entroncamento e as VLANs. Você utilizará VTP para anunciar as configurações de VLAN a outros switches.

### Tarefa 1: Definir e verificar configurações básicas de dispositivo

#### Etapa 1. Configurar comandos básicos.

Configure cada switch usando os comandos básicos a seguir.

- Defina o nome de host para corresponder ao nome para exibição.
- Utilize **class** como a senha secreta de habilitação (enable secret password).
- Utilize **cisco** como a senha para as configurações de linha.
- Use a criptografia de serviço.

#### Etapa 2. Configurar a interface VLAN de gerenciamento em S1, S2 e S3.

Crie e habilite uma VLAN 99 de interface em cada switch. Use a tabela de endereçamento para a configuração do endereço.

#### Etapa 3. Verificar se os PCs na mesma sub-rede podem executar ping um no outro.

Os PCs já estão configurados com endereçamento correto. Crie PDUs simples para testar a conectividade entre dispositivos na mesma sub-rede:

#### Etapa 4. Verificar os resultados.

Seu percentual de conclusão deve ser 15%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

### Tarefa 2: Configurar e verificar segurança de porta

#### Etapa 1. Configurar todos os links de acesso com a segurança de porta.

Normalmente, você configura a segurança de porta em todas as portas de acesso ou desliga a porta se ela não estiver em uso. Use a política a seguir para estabelecer a segurança de porta apenas nas portas usadas pelos PCs.

- Defina a porta como modo de acesso.
- Habilite a segurança da porta.
- Permita apenas 1 endereço MAC.
- Configure o primeiro endereço MAC aprendido para "aderir" à configuração.
- Defina a porta para desativar se houver uma violação de segurança.
- Force os switches a aprenderem os endereços MAC enviando pings em todos os três switches.

**NOTA:** Apenas a habilitação da segurança de porta é usada pelo Packet Tracer. No entanto, todas as tarefas de segurança de porta listadas acima são necessárias para concluir esta atividade.

### **Etapa 2. Testar segurança de porta.**

- Conecte PC2 à porta de PC3 e conecte PC3 à porta de PC2.
- Envie pings entre os PCs na mesma sub-rede.
- As portas para o PC2 e o PC3 devem ser fechadas.

**Etapa 3. Verificar se as portas estão "err-disabled" e se uma violação de segurança foi registrada em log.**

### **Etapa 4. Reconectar os PCs à porta correta e limpar as violações de segurança da porta.**

- Conecte PC2 e PC3 à porta correta.
- Limpe a violação de segurança da porta.
- Verificar se o PC2 e o PC3 já podem enviar pings em todo o S2.

### **Etapa 5. Verificar os resultados.**

O percentual de conclusão deve ser 55%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

## **Tarefa 3: Configurar VTP**

### **Etapa 1. Configurar o modo VTP em todos os três switches.**

Configure S1 como o servidor. Configure S2 e S3 como clientes.

### **Etapa 2. Configurar o nome de domínio VTP em todos os três switches.**

Use **CCNA** como o nome de domínio de VTP.

### **Etapa 3. Configurar a senha de domínio VTP em todos os três switches.**

Use **cisco** como a senha de domínio de VTP.

### **Etapa 4. Verificar os resultados.**

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

## **Tarefa 4: Configurar entroncamento**

### **Etapa 1. Configurar o entroncamento em S1 S2 e S3.**

Configure as interfaces apropriadas no modo de entroncamento e atribua VLAN 99 como a VLAN nativa.

### **Etapa 2. Verificar os resultados.**

O percentual de conclusão deve ser 83%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

## Tarefa 5: Configurar VLANs

### Etapa 1. Criar as VLANs em S1.

Crie e nomeie as seguintes VLANs apenas em S1. O VTP anunciará as novas VLANs para o S1 e o S2.

- VLAN 10 **Corpo docente/administração**
- VLAN 20 **Alunos**
- VLAN 30 **Convidado(Padrão)**
- VLAN 99 **Gerenciamento&Nativo**

### Etapa 2. Verificar se as VLANs foram enviadas para S2 e S3.

Use os comandos apropriados para verificar se o S2 e o S3 já têm as VLANs que você criou no S1. Pode demorar alguns minutos para o Packet Tracer simular os anúncios VTP.

### Etapa 3. Verificar os resultados.

O percentual de conclusão deve ser 90%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

## Tarefa 6: Atribuir VLANs a portas

### Etapa 1. Atribuir VLANs a portas de acesso em S2 e S3.

Atribua portas de acesso PC a VLANs:

- VLAN 10: PC1 e PC4
- VLAN 20: PC2 e PC5
- VLAN 30: PC3 e PC6

### Etapa 2. Verificar a implementação VLAN.

Use o comando apropriado para verificar a implementação da VLAN.

### Etapa 3. Verificar os resultados.

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

## Tarefa 7: Verificar conectividade fim-a-fim

**Etapa 1. Verificar se PC1 e PC4 podem executar ping um no outro.**

**Etapa 2. Verificar se PC2 e PC5 podem executar ping um no outro.**

**Etapa 3. Verificar se PC3 e PC6 podem executar ping um no outro.**

**Etapa 4. PCs em VLANs diferentes não devem ser capazes de executar ping um no outro.**