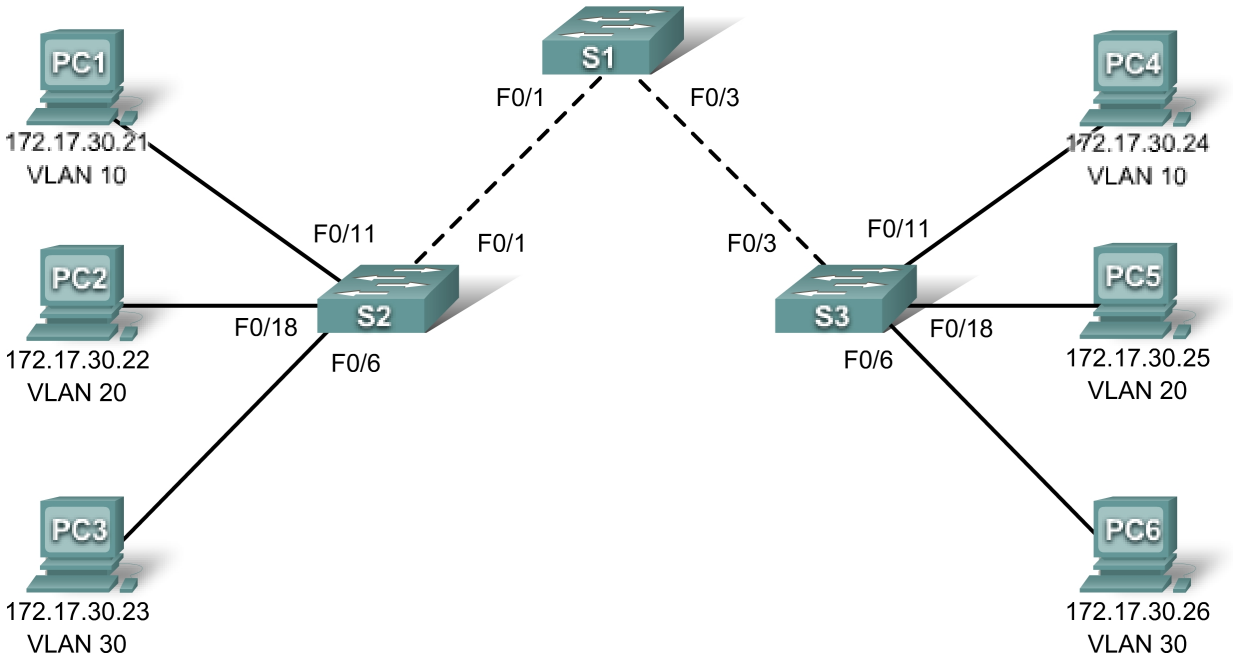
Atividade PT 4.3.3: Configurar VTP

Diagrama de topologia



Objetivos de aprendizagem

- Investigar a configuração atual.
- Configurar S1 como servidor VTP.
- Configurar S2 e S3 como clientes VTP.
- Configurar VLANs em S1.
- Configurar troncos em S1, S2 e S3.
- Verificar o status de VTP em S1, S2 e S3.
- Atribuir VLANs a portas em S2 e S3.
- Verificar a implementação da VLAN e testar a conectividade

Introdução

Nesta atividade, você irá praticar a configuração de VTP. Quando o Packet Tracer abre pela primeira vez, os switches já contêm uma configuração parcial. A senha EXEC do usuário é **cisco** e a senha EXEC privilegiada é **class**.

Tarefa 1: Investigar a configuração atual

Etapa 1. Verificar a configuração de execução atual nos switches.

Quais configurações já estão presentes nos switches?

_____

_____

_____

Etapa 2. Exibir as VLANs atuais em cada switch.

Existe alguma VLAN presente? As VLANs foram criadas pelo usuário ou são VLANs padrão?

_____

```
S1#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
                                           Gig1/1, Gig1/2
1002 fddi-default                 active
1003 token-ring-default           active
1004 fddinet-default              active
1005 trnet-default                active
```

A conclusão deve estar em 0% ao final desta tarefa.

Tarefa 2: Configurar S1 como servidor VTP

Etapa 1. Configurar o comando no modo VTP.

S1 será o servidor de VTP. Defina S1 como o modo de servidor.

```
S1(config)#vtp mode servidor
Device mode already VTP SERVER.
S1(config)#
```

Observe que o switch já está definido por padrão como modo de servidor. No entanto, é importante que você configure esse comando explicitamente para verificar se o switch está no modo de servidor.

Etapa 2. Configurar o nome de domínio VTP.

Configure S1 com **CCNA** como o nome de domínio VTP. Lembre-se de que os nomes de domínio VTP diferenciam maiúsculas de minúsculas.

```
S1(config)#vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S1(config)#
```


Etapa 3. Configurar a senha de domínio VTP.

Configure S1 com **cisco** como a senha de domínio VTP. Lembre-se de que as senhas de domínio VTP diferenciam maiúsculas de minúsculas.

```
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#
```

Etapa 4. Confirmar alterações feitas na configuração.

Utilize o comando **show vtp status** em S1 para confirmar que o modo VTP e o domínio sejam configurados corretamente.

```
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Servidor
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8C 0x29 0x40 0xDD 0x7F 0x7A 0x63
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Para verificar a senha do VTP, use o comando **show vtp password**.

```
S1#show vtp password
VTP Password: cisco
S1#
```

Etapa 5. Verificar os resultados.

O percentual de conclusão deve ser 8%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 3: Configurar S2 e S3 como clientes VTP

Etapa 1. Configurar o comando no modo VTP.

S2 e S3 serão clientes VTP. Defina esses dois switches como o modo de cliente.

Etapa 2. Configurar o nome de domínio VTP.

Para que aceitem anúncios VTP de S1, S2 e S3 devem pertencer ao mesmo domínio VTP. Configure S2 e S3 com **CCNA** como o nome de domínio VTP. Lembre-se de que os nomes de domínio VTP diferenciam maiúsculas de minúsculas.

Etapa 3. Configurar a senha de domínio VTP.

S2 e S3 também devem usar a mesma rede antes de aceitar anúncios VTP do servidor VTP. Configure S2 e S3 com **cisco** como a senha de domínio VTP. Lembre-se de que as senhas de domínio VTP diferenciam maiúsculas de minúsculas.

Etapa 4. Confirmar alterações feitas na configuração.

Utilize o comando **show vtp status** em todos os switches para confirmar que o modo VTP e o domínio sejam configurados corretamente. A saída de S3 é mostrada aqui.

```
S3#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8C 0x29 0x40 0xDD 0x7F 0x7A 0x63
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Observe que o número de revisão da configuração é 0 em todos os três switches. Por quê?

_____

_____

_____

Para verificar a senha do VTP, use o comando **show vtp password**.

```
S3#show vtp password
VTP Password: cisco
S3#
```

Etapa 5. Verificar os resultados.

O percentual de conclusão deve ser 31%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 4: Configurar VLANs em S1

As VLANs podem ser criadas no servidor VTP e distribuídas a outros switches do domínio do VTP. Nesta tarefa, você irá criar 4 novas VLANs no servidor VTP, S1. Essas VLANs serão distribuídas ao S2 e ao S3 por VTP.

Etapa 1. Criar as VLANs.

Para fins de classificação no Packet Tracer, os nomes de VLAN diferenciam maiúsculas de minúsculas.

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

Etapa 2. Verificar as VLANs.

Utilize o comando **show vlan brief** para verificar as VLANs e seus nomes.

```
S1#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
                                                 Gig1/1, Gig1/2
10   Corpo docente/administração       active
20   Alunos                            active
30   Convidado(Padrão)                 active
99   Gerenciamento&Nativo              active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Se inserir o mesmo comando em S2 e S3, você notará que as VLANs não estão em seu banco de dados de VLAN? Por que não?

_____

_____

Etapa 4. Verificar os resultados.

Seu percentual de conclusão deve ser 46%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 5: Configurar troncos em S1, S2 e S3

Utilize o comando **switchport mode trunk** a fim de definir o modo de tronco para cada link de tronco. Utilize o comando **switchport trunk native vlan 99** para definir VLAN 99 como a VLAN nativa.

Etapa 1. Configurar FastEthernet 0/1 e FastEthernet 0/3 em S1 para entroncamento.

Insira os comandos apropriados para configurar o entroncamento e defina VLAN 99 como a VLAN nativa.

Depois de configurado, o DTP (Dynamic Trunking Protocol) ativará os links de tronco. Você pode verificar se S2 e S3 agora estão em entroncamento, digitando o comando **show interface fa0/1 switchport** em S2 e o comando **show interface fa0/3 switchport** em S3.

Se você aguardar alguns minutos até o Packet Tracer simular todos os processos, S1 anunciará a configuração de VLAN para S2 e S3. Ele pode ser verificado em S2 ou S3 com os comandos **show vlan brief** e **show vtp status**.

No entanto, é uma prática recomendada para configurar ambas as extremidades dos links de tronco no modo **on**.

Etapa 2. Configurar Fast Ethernet 0/1 em S2 para entroncamento.

Insira os comandos apropriados para configurar o entroncamento e defina VLAN 99 como a VLAN nativa.

Etapa 3. Configurar Fast Ethernet 0/3 em S3 para entroncamento.

Insira os comandos apropriados para configurar o entroncamento e defina VLAN 99 como a VLAN nativa.

Etapa 4. Verificar os resultados.

O percentual de conclusão deve ser 77%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 6: Verificar status VTP

Utilizando os comandos **show vtp status** e **show vlan brief**, verifique o seguinte.

- S1 deve mostrar o status de servidor.
- S2 e S3 devem mostrar o status de cliente.
- S2 e S3 devem ter VLANs de S1.

Nota: Os anúncios VTP são inundados em todo o domínio de gerenciamento a cada cinco minutos ou sempre que ocorrer uma alteração em configurações VLAN. Para agilizar esse processo, você pode alternar entre os modos em tempo real e de simulação até a próxima rodada de atualizações. No entanto, talvez você precise fazer isso várias vezes porque ele só encaminhará o relógio do Packet Tracer dez segundos por vez. Como alternativa, você pode alterar um dos switches do cliente para o modo transparente e retornar ao modo cliente. (A numeração de revisão da configuração pode ser diferente em roteadores reais em comparação com roteadores no Packet Tracer. Esta atividade não está classificando os números de revisão de configuração.)

Qual é o número de revisão de configuração? _____

O número de revisão da configuração é mais alto que o número de VLANs que você criou?

_____

_____

Qual é o número atual das VLANs existentes? _____

Por que há mais VLANs existentes do que as quatro que você criou?

_____

A conclusão ainda deve estar em 77% ao término desta tarefa.

Tarefa 7: Atribuir VLANs a portas

Utilize o comando **switchport mode access** para definir o modo de acesso segundo os links de acesso. Utilize o comando **switchport access vlan** *vlan-id* para atribuir uma VLAN a uma porta de acesso.

Etapa 1. Atribuir VLANs a portas em S2.

- Fa0/11 em VLAN 10
- Fa0/18 em VLAN 20
- Fa0/6 em VLAN 30

Etapa 2. Atribuir VLANs a portas em S3.

- Fa0/11 em VLAN 10
- Fa0/18 em VLAN 20
- Fa0/6 em VLAN 30

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 8: Verificar implementação da VLAN e testar conectividade

Etapa 1. Verificar a configuração VLAN e as atribuições de porta.

Utilize o comando **show vlan brief** para verificar a configuração VLAN e as atribuições de porta em todos os switches. Compare a sua saída com a topologia.

Etapa 2. Testar conectividade entre PCs.

Deve haver êxito nos pings entre PCs na mesma VLAN, devendo haver falha nos pings entre PCs nas VLANs diferentes.

Em PC1, execute ping em PC4.

Em PC2, execute ping em PC5.

Em PC3, execute ping em PC6.

