Atividade PT 4.4.1: Configuração básica de VTP

Diagrama de topologia

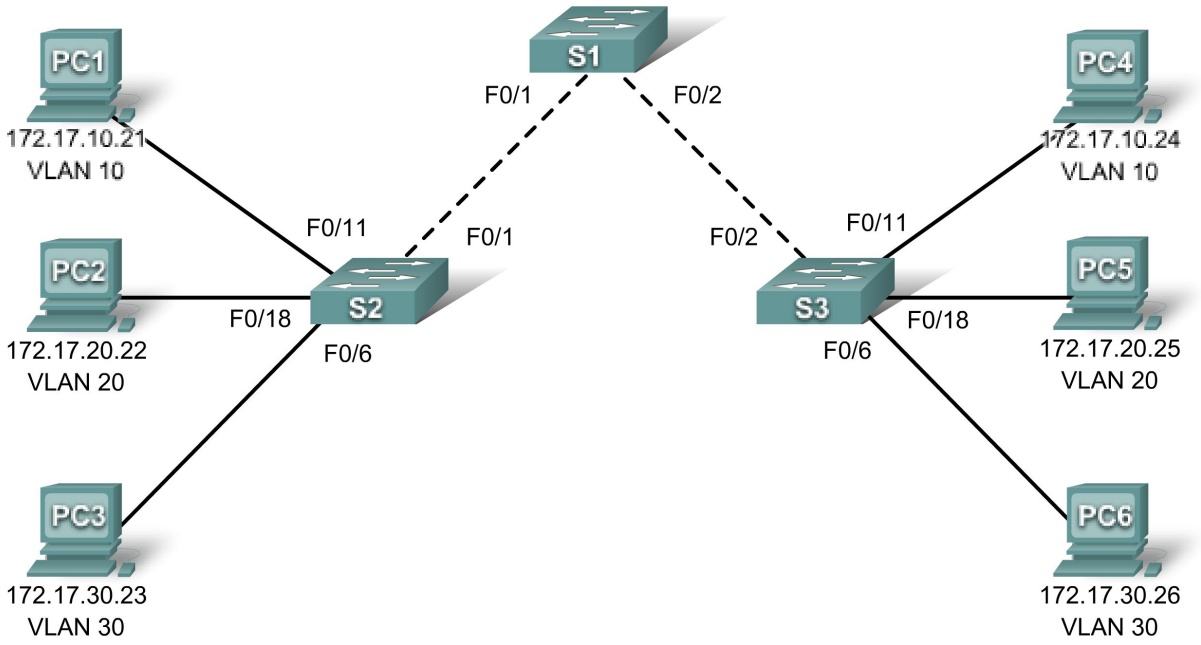

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede	Gateway padrão
S1	**VLAN 99**	172.17.99.11	255.255.255.0	N/A
S2	**VLAN 99**	172.17.99.12	255.255.255.0	N/A
S3	**VLAN 99**	172.17.99.13	255.255.255.0	N/A
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

Designações de porta (S2 e S3)

Portas	Atribuição	Rede
Fa0/1 - 0/5	802.1q Troncos (VLAN 99 nativa)	172.17.99.0 /24
Fa0/6 - 0/10	VLAN 30 - Convidado (Padrão)	172.17.30.0 /24
Fa0/11 - 0/17	VLAN 10 - Corpo docente/administração	172.17.10.0 /24
Fa0/18 - 0/24	VLAN 20 - Alunos	172.17.20.0 /24

Objetivos de aprendizagem

- Executar as configurações básicas de switch.
- Configurar as interfaces Ethernet nos PCs de host.
- Configurar o VTP e a segurança nos switches.

Introdução

Nesta atividade, você irá realizar configurações de switch básicas, configurar VTP, entroncamento, aprender modos VTP, criar e distribuir informações de VLAN e atribuir portas a VLANs. A rede inicial é aberta em um estado seguro com todas as portas desativadas administrativamente.

Tarefa 1: Realizar configurações básicas de switch

Configure os switches S1, S2 e S3 de acordo com as seguintes diretrizes e salve todas as suas configurações:

- Configure o nome de host do switch conforme indicado na topologia.
- Desabilite a pesquisa DNS.
- Configure uma senha criptografada **class** no modo EXEC privilegiado.
- Configure uma senha **cisco** para as conexões de console.
- Configure uma senha **cisco** para as conexões vty.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#no ip domain-lookup
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)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```


Seu percentual de conclusão deve ser 7%. Do contrário, solucione o problema e corrija todos os erros.

Tarefa 2: Configurar as interfaces Ethernet nos PCs de host.

Configure as interfaces Ethernet de PC1, PC2, PC3, PC4, PC5 e PC6 com os endereços IP e os gateways padrão indicados na tabela de endereçamento.

Seu percentual de conclusão deve ser 20%. Do contrário, solucione o problema e corrija todos os erros.

Tarefa 3: Configurar VTP e segurança nos switches

Etapa 1. Habilitar as portas de usuário em S2 e S3.

Configure as portas de usuário no modo de acesso. Consulte o diagrama de topologia para determinar que portas estão conectadas a dispositivos de usuário final.

```
S2(config)#interface fa0/6
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/11
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/18
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
```

Etapa 2. Verificar as configurações VTP atuais em três switches.

Utilize o comando show vtp status para determinar o modo operacional VTP para todos os três switches.

```
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Server
Nome de domínio de VTP          :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

S2#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Server
Nome de domínio de VTP          :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```



```
Local updater ID is 0.0.0.0 (no valid interface found)
S3#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Server
Nome de domínio de VTP          :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

O VTP permite que o administrador de rede controle as instâncias de VLANs na rede, criando domínios de VTP. Dentro de cada domínio de VTP, são configurados um ou mais switches como servidores de VTP. Dessa forma, as VLANs são criadas no servidor VTP e enviadas para os demais switches do domínio. As tarefas de configuração VTP estão definindo o modo operacional, o domínio e a senha. Observe que todos os três switches estão no modo de servidor. Modo de servidor é o modo VTP padrão da maioria dos switches Catalyst. Nesta atividade, você irá utilizar S1 como o servidor VTP, com S2 e S3 configurados como clientes VTP ou no modo transparente de VTP.

Etapa 3. Configurar o modo operacional, o nome de domínio e a senha VTP em todos os três switches.

Defina o nome de domínio VTP como Lab4 e a senha VTP como cisco em todos os três switches. Configure S1 no modo servidor, S2 no modo cliente e S3 no modo transparente.

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#vtp domain Lab4
Changing VTP domain name from NULL to Lab4
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#end

S2(config)#vtp mode client
Setting device to VTP CLIENT mode
S2(config)#vtp domain Lab4
Changing VTP domain name from NULL to Lab4
S2(config)#vtp password cisco
Setting device VLAN database password to cisco
S2(config)#end

S3(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
S3(config)#vtp domain Lab4
Changing VTP domain name from NULL to Lab4
S3(config)#vtp password cisco
Setting device VLAN database password to cisco
S3(config)#end
```


Nota: O nome de domínio do VTP pode ser aprendido por um switch de cliente a partir de um switch de servidor, mas somente se o domínio de switch do cliente estiver no estado nulo. Ele não conhecerá um novo nome se já houver um definido. Por esse motivo, trata-se de uma prática recomendada configurar o nome de domínio manualmente em todos os switches para assegurar que o nome de domínio seja configurado corretamente. Os switches em domínios VTP diferentes não trocam nenhuma informação VLAN.

Etapa 4. Configurar o entroncamento e a VLAN nativa para as portas de entroncamento em todos os três switches.

Em todos os switches, configure o entroncamento e a VLAN nativa para as interfaces FastEthernet 0/1 a 5. Apenas os comandos para fa0/1 em cada switch são mostrados abaixo.

```
S1(config)#interface fa0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#no shutdown
S1(config-if)#interface fa0/2
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#no shutdown
S1(config-if)#end

S2(config)#interface fa0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 99
S2(config-if)#no shutdown
S2(config-if)#end

S3(config)#interface fa0/2
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 99
S3(config-if)#no shutdown
S3(config-if)#end
```

Etapa 5. Configurar a segurança de porta nos switches da camada de acesso S2 e S3.

Configure as portas fa0/6, fa0/11 e fa0/18 para que elas permitam apenas um host único e aprendam o endereço MAC do host dinamicamente.

```
S2(config)#interface fa0/6
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#interface fa0/11
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#interface fa0/18
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#end
```



```
S3(config)#interface fa0/6
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#interface fa0/11
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#interface fa0/18
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#end
```

Etapa 6. Configurar as VLANs no servidor VTP.

Há quatro VLANs obrigatórias neste laboratório:

- VLAN 99 (gerenciamento)
- VLAN 10 (corpo docente/administração)
- VLAN 20 (alunos)
- VLAN 30 (convidado)

Configure-os no servidor VTP. A classificação do Packet Tracer diferencia maiúsculas e minúsculas.

```
S1(config)#vlan 99
S1(config-vlan)#name gerenciamento
S1(config-vlan)#exit
S1(config)#vlan 10
S1(config-vlan)#name corpo docente/administração
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name alunos
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name convidado
S1(config-vlan)#exit
```

Verificar se as VLANs foram criadas no S1 com o comando show vlan brief.

Etapa 7. Verificar se as VLANs criadas em S1 foram distribuídas para S2 e S3.

Utilize o comando show vlan brief em S2 e S3 para determinar se o servidor VTP usou sua configuração VLAN em todos os switches.

```
S2#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, 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, Gi0/1
                                                 Gi0/2
10   corpo docente/administração       active
20   alunos                            active
30   convidado                         active
```



```
99   gerenciamento                  active
S3#show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, 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
```

As mesmas VLANs são configuradas em todos os switches? _____

Por que S2 e S3 têm configurações de VLAN diferentes neste momento?

Etapa 8. Criar uma nova VLAN em S2 e S3.

```
S2(config)#vlan 88
%VTP VLAN configuration not allowed when device is in CLIENT mode.

S3(config)#vlan 88
S3(config-vlan)#name test
S3(config-vlan)#
```

Por que você é impedido de criar uma nova VLAN em S2 mas não em S3?

Exclua a VLAN 88 de S3.

```
S3(config)#no vlan 88
```

Etapa 9. Configurar manualmente VLANs.

Configure as quatro VLANs identificadas na Etapa 6 no switch S3.

```
S3(config)#vlan 99
S3(config-vlan)#name gerenciamento
S3(config-vlan)#exit
S3(config)#vlan 10
S3(config-vlan)#name corpo docente/administração
S3(config-vlan)#exit
S3(config)#vlan 20
S3(config-vlan)#name alunos
S3(config-vlan)#exit
S3(config)#vlan 30
S3(config-vlan)#name convidado
S3(config-vlan)#exit
```

Aqui você vê uma das vantagens de VTP. A configuração manual é entediante e propensa a erros, e qualquer erro apresentado aqui pode impedir a comunicação entre VLANs. Além disso, esses tipos de erros podem ser difíceis de solucionar.

Etapa 10. Configurar o endereço da interface de gerenciamento em todos os três switches.

```
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
S2(config)#interface vlan 99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown
S3(config)#interface vlan 99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
S3(config-if)#no shutdown
```

Verificar se os switches estão configurados corretamente executando ping entre si. Em S1, execute ping na interface de gerenciamento em S2 e S3. Em S2, execute ping na interface de gerenciamento em S3.

Os pings obtiveram sucesso? Do contrário, solucione os problemas das configurações do switch e tente novamente.

Etapa 11. Atribuir portas de switch a VLANs.

Consulte a tabela de atribuição de portas no início da atividade para atribuir portas às VLANs. As designações de porta não são configuradas via VTP. As designações de porta devem ser configuradas em cada switch manual ou dinamicamente usando um servidor VMPS. Os comandos são mostrados apenas para S3, mas os switches S2 e S3 devem ser configurados da mesma forma. Salve a configuração quando você tiver terminado.

```
S3(config)#interface range fa0/6 – fa0/10
S3(config-if-range)#switchport access vlan 30
S3(config-if-range)#interface range fa0/11 – fa0/17
S3(config-if-range)#switchport access vlan 10
S3(config-if-range)#interface range fa0/18 – fa0/24
S3(config-if-range)#switchport access vlan 20
S3(config-if-range)#end
S3#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
S3#
```

O percentual de conclusão deve ser 100%. Utilize o botão **Check Results** para verificar se todos os componentes estão completos.

