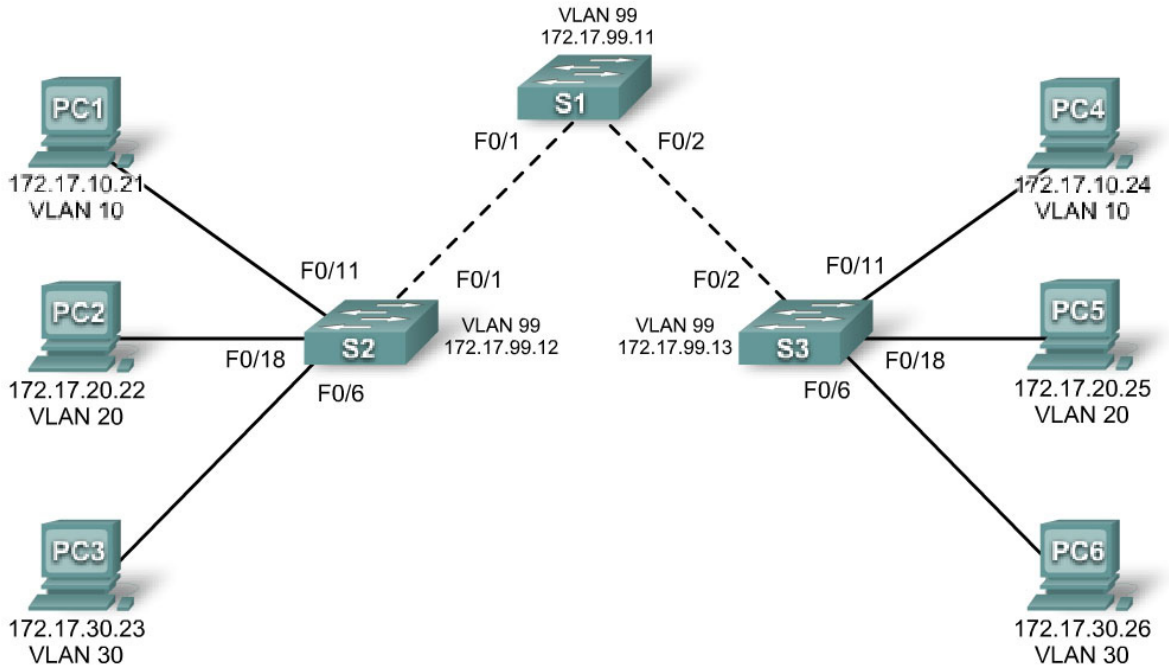
# Laboratório 4.4.1: Configuração básica de VTP

## Diagrama de topologia




## Tabela de endereçamento

| Dispositivo (Nome do host) | 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 (switches 2 e 3)

| Portas | Atribuição | Rede |
|---|---|---|
| Fa0/1 – 0/5 | 802.1q Trunks (Native VLAN 99) | 172.17.99.0 /24 |
| Fa0/6 – 0/10 | VLAN 30 – Guest (Default) | 172.17.30.0 /24 |
| Fa0/11 – 0/17 | VLAN 10 – Faculty/Staff | 172.17.10.0 /24 |
| Fa0/18 – 0/24 | VLAN 20 – Students | 172.17.20.0 /24 |

## Objetivos de aprendizagem

Após concluir este laboratório, você será capaz de:

- Cabear a rede de acordo com o diagrama de topologia
- Apagar a configuração de inicialização e recarregar o estado padrão de um switch
- Executar tarefas de configuração básica em um switch
- Configurar o protocolo VTP (VLAN Trunking Protocol) em todos os switches
- Habilitar o entroncamento (trunk) em conexões inter-switch
- Verificar a configuração do tronco (trunk)
- Modificar os modos VTP e observar o impacto
- Criar VLANs no servidor VTP e distribuir essas informações de VLAN para switches na rede
- Explicar as diferenças no funcionamento entre os modos VTP: transparente, servidor e cliente
- Atribuir portas de switch a VLANs
- Salvar a configuração VLAN
- Habilitar o VTP pruning na rede
- Explicar como o pruning reduz o tráfego de broadcast desnecessário na rede local

### Tarefa 1: Preparar a rede

**Etapa 1: Cabear uma rede de maneira semelhante à presente no diagrama de topologia.**

Você pode utilizar qualquer switch atual em seu laboratório contanto que ele tenha as interfaces exigidas mostradas na topologia. A saída de dados mostrada neste laboratório tem por base switches 2960. Outros tipos de switch podem gerar uma saída diferente. Se você estiver usando switches mais antigos, alguns comandos podem ser diferentes ou estarem indisponíveis.

Você irá observar na Tabela de endereçamento se os PCs foram configurados com um endereço IP de gateway padrão. Esse seria o endereço IP do roteador local não incluído no cenário deste laboratório. O gateway padrão, o roteador, seria necessário para PCs em diferentes VLANs, para que possa haver comunicação. Isso será discutido em um capítulo posterior.

Configure conexões de console para todos os três switches.

**Etapa 2: Limpar todas as configurações existentes nos switches.**

Se necessário, consulte o Laboratório 2.5.1, Apêndice 1, quanto ao procedimento para limpar as configurações do switch e as VLANs. Use o comando **show vlan** para confirmar se existem apenas VLANs padrão e se todas as portas estão atribuídas à VLAN 1.

```
Switch#show vlan

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
```

**Etapa 3: Desabilitar todas as portas utilizando o comando shutdown.**
Repita estes comandos em todos os switches da topologia.

```
Switch(config)#interface range fa0/1-24
Switch(config-if-range)#shutdown
Swtich(config-if-range)#interface range gi0/1-2
Swtich(config-if-range)#shutdown
```

## Tarefa 2: Realizar configurações básicas de switch

**Etapa 1: Concluir a configuração básica dos switches S1, S2 e S3.**

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 a senha do modo EXEC como **class**.
- Configure a senha para as conexões de console como **cisco**.
- Configure a senha **cisco** para as conexões vty.

(Mostrada saída de S1)

```
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]
```

**Etapa 2: Reabilitar 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

S3(config)#interface fa0/6
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
S3(config-if)#interface fa0/11
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
S3(config-if)#interface fa0/18
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
```

**Etapa 3: Reabilitar as portas de tronco em S1, S2 e S3.**

```
S1(config)#interface fa0/1
S1(config-if)#no shutdown
S1(config)#interface fa0/2
S1(config-if)#no shutdown

S2(config)#interface fa0/1
S2(config-if)#no shutdown

S3(config)#interface fa0/2
S3(config-if)#no shutdown
```

## Tarefa 3: Configurar as interfaces Ethernet nos PCs.

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 no início do laboratório.

Verifique se PC1 pode executar um ping em PC4, se PC2 pode executar um ping em PC5 e se PC3 pode executar um ping em PC6.

## Tarefa 4: Configurar VTP nos switches

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 comuns de configuração VTP são: definir o modo de operação, domínio e senha. Neste laboratório, você irá utilizar S1 como o servidor VTP, S2 e S3 configurados como clientes VTP ou no modo transparente de VTP.

### Etapa 1: Verificar as configurações VTP atuais em três switches.

```
S1#show vtp status

VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
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 : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
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 : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Observe que todos os três switches estão no modo de servidor. Modo de servidor é o modo VTP padrão da maioria dos switches Catalyst.

**Etapa 2: 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 3: Configurar o entroncamento (trunking) e a VLAN nativa para as portas de entroncamento (trunking) em todos os três switches.**

Use o comando **interface range** no modo de configuração global para simplificar essa tarefa.

```
S1(config)#interface range fa0/1-5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end

S2(config)# interface range fa0/1-5
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end

S3(config)# interface range fa0/1-5
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end
```

**Etapa 4: Configurar 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 5: Configurar VLANs no servidor VTP.**

Há quatro VLANs adicionais neste laboratório:

- VLAN 99 (management)
- VLAN 10 (faculty/staff)
- VLAN 20 (students)
- VLAN 30 (guest)

Configure-as no servidor VTP.

```
S1(config)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#exit
S1(config)#vlan 10
S1(config-vlan)#name faculty/staff
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name students
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#exit
```

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

**Etapa 6: 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   faculty/staff                    active
20   students                         active
30   guest                            active
99   management                       active

S3#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
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

As mesmas VLANs são configuradas em todos os switches? _____

Explique por que S2 e S3 têm configurações de VLAN diferentes neste momento. _____

_____

_____

**Etapa 7: Criar uma nova VLAN nos switches 2 e 3.**

```
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 8: Configurar manualmente as VLANs.**

Configure as quatro VLANs identificadas na Etapa 5 no switch S3.

```
S3(config)#vlan 99
S3(config-vlan)#name management
S3(config-vlan)#exit
S3(config)#vlan 10
S3(config-vlan)#name faculty/staff
S3(config-vlan)#exit
S3(config)#vlan 20
S3(config-vlan)#name students
S3(config-vlan)#exit
S3(config)#vlan 30
S3(config-vlan)#name guest
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 9: 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 um ping entre si. Em S1, execute um ping para a interface de gerenciamento de S2 e S3. Em S2, execute um ping para a interface de gerenciamento em S3.

Os pings obtiveram sucesso? _____

Do contrário, solucione problemas nas configurações do switch e tente novamente.

**Etapa 10: Atribuir portas de switch a VLANs.**

Consulte a tabela de designação de porta no início do laboratório para atribuir portas às VLANs. Use o comando **interface range** para simplificar essa tarefa. 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 fa0/6-10
S3(config-if-range)#switchport access vlan 30
S3(config-if-range)#interface range fa0/11-17
S3(config-if-range)#switchport access vlan 10
S3(config-if-range)#interface range fa0/18-24
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#
```

## Tarefa 5: Configurar VTP pruning nos switches

O VTP pruning permite que um servidor VTP anule o tráfego de transmissão de IP de VLANs específicas para switches que não têm nenhuma porta nessa VLAN. Por padrão, todos o unicasts desconhecidos e broadcasts em uma VLAN inundam toda a VLAN. Todos os switches na rede recebem todos os broadcasts, até mesmo em situações nas quais poucos usuários são conectados nessa VLAN. O VTP pruning é utilizado para eliminar ou cortar esse tráfego desnecessário. Pruning economiza largura de banda da LAN porque os broadcasts não precisam ser enviados para switches que não precisam deles.

O pruning é configurado no switch que opera no modo servidor com o comando **vtp pruning** no modo de configuração global. A configuração é enviada para switches cliente.

Confirme a configuração do VTP Pruning em cada switch utilizando o comando **show vtp status**. O modo VTP Pruning deve ser habilitado em todos os switches.

```
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 17
Maximum VLANs supported locally : 255
Number of existing VLANs        : 9
VTP Operating Mode              : Server
VTP Domain Name                 : Lab4
VTP Pruning Mode                : Enabled
<saída do comando omitida>
```

## Tarefa 6: Limpar

Apague as configurações e recarregue os switches. Desconecte e guarde o cabeamento. Para os PCs normalmente conectados a outras redes (como a rede local escolar ou a Internet), reconecte o cabeamento apropriado e restaure as configurações TCP/IP.