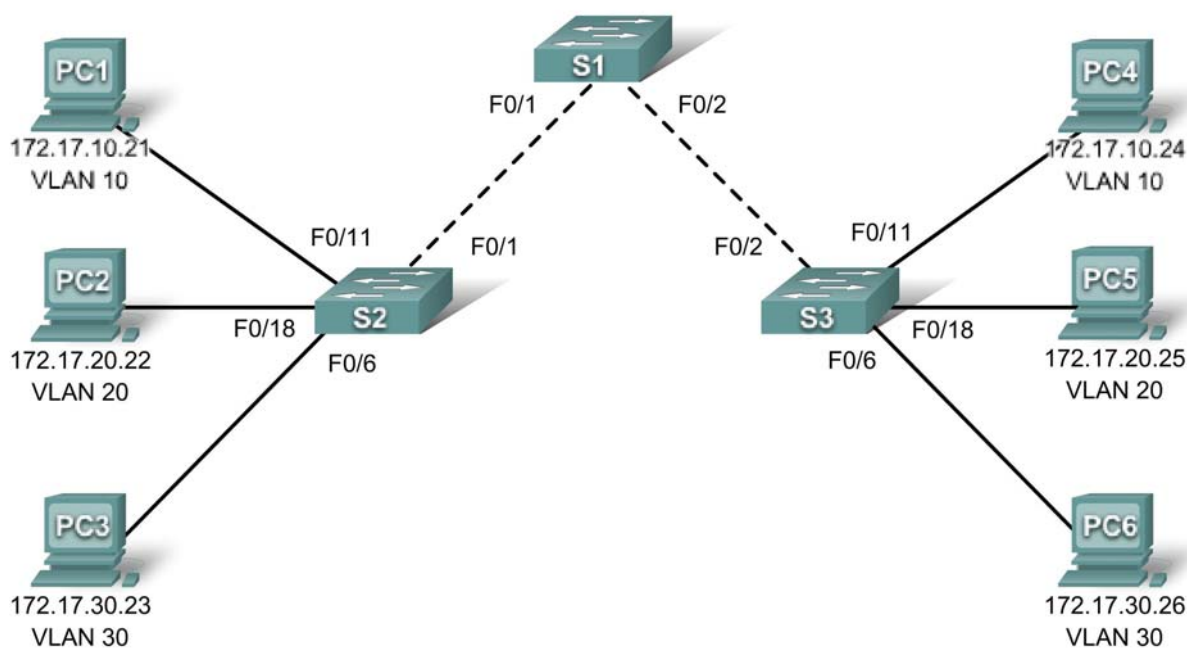


PT 练习 4.4.1：基本 VTP 配置

拓扑图



地址表

设备	接口	IP 地址	子网掩码	默认网关
S1	VLAN 99	172.17.99.11	255.255.255.0	不适用
S2	VLAN 99	172.17.99.12	255.255.255.0	不适用
S3	VLAN 99	172.17.99.13	255.255.255.0	不适用
PC1	网卡	172.17.10.21	255.255.255.0	172.17.10.1
PC2	网卡	172.17.20.22	255.255.255.0	172.17.20.1
PC3	网卡	172.17.30.23	255.255.255.0	172.17.30.1
PC4	网卡	172.17.10.24	255.255.255.0	172.17.10.1
PC5	网卡	172.17.20.25	255.255.255.0	172.17.20.1
PC6	网卡	172.17.30.26	255.255.255.0	172.17.30.1

端口分配 (S2 和 S3)

端口	分配	网络
Fa0/1 - 0/5	802.1q 中继 (本征 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

学习目标

- 执行基本交换机配置
- 配置主机 PC 上的以太网接口
- 在交换机上配置 VTP 和安全功能

简介

在本练习中, 您的任务包括: 执行基本的交换机配置、配置 VTP 和中继、了解 VTP 模式、创建和分发 VLAN 信息以及将端口分配给 VLAN。本练习开始时, 网络处于安全状态, 所有端口都已管理性关闭。

任务 1: 执行基本交换机配置

根据以下原则配置交换机 S1、S2 和 S3 并保存配置:

- 按照拓扑所示配置交换机主机名。
- 禁用 DNS 查找。
- 将执行模式口令配置为 **class**。
- 为控制台连接配置口令 **cisco**。
- 为 vty 连接配置口令 **cisco**。

```
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]
```

任务 2: 配置主机 PC 上的以太网接口

使用地址表中的 IP 地址和默认网关配置 PC1、PC2、PC3、PC4、PC5 和 PC6 的以太网接口。

任务 3: 在交换机上配置 VTP 和安全功能

步骤 1. 启用 S2 和 S3 上的用户端口。

将用户端口配置为接入模式。请参阅拓扑图来确定哪些端口连接到最终用户设备。

```
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
```

步骤 2. 检查三台交换机上的当前 VTP 配置。

使用 show vtp status 命令确定所有三台交换机的 VTP 工作模式。

```
S1#show vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 64
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                  : 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
VTP Domain Name             :
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
VTP Domain Name              :
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)
```

VTP 可让网络管理员通过创建 VTP 域来控制网络上的 VLAN 实例。在每个 VTP 域中, 可以将一台或多台交换机配置为 VTP 服务器。然后可以在 VTP 服务器上创建 VLAN, 并将这些 VLAN 传送给域中的其它交换机。常见的 VTP 配置任务是设置工作模式、域和口令。请注意, 三台交换机均处于服务器模式。服务器模式是大多数 Catalyst 交换机的默认 VTP 模式。在本练习中, 您将使用 S1 作为 VTP 服务器, S2 和 S3 则配置为 VTP 客户端或 VTP 透明模式。

步骤 3. 在所有三台交换机上配置工作模式、域名和 VTP 口令。

在三台交换机上, 全部将 VTP 域名设置为 Lab4, VTP 口令设置为 cisco。将 S1 配置为服务器模式, S2 配置为客户端模式, S3 配置为透明模式。

```
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
```

注意: 客户端交换机可从服务器交换机处获知 VTP 域名, 但前提是客户端交换机的域为空。如果客户端交换机已设置有域名, 则不会获知新的域名。因此, 最好是在所有交换机上手动配置域名, 以确保域名配置正确。位于不同 VTP 域中的交换机不会交换 VLAN 信息。

步骤 4. 为所有三台交换机上的中继端口配置中继和本征 VLAN。

在所有交换机上, 为 FastEthernet 接口 0/1-5 配置中继和本征 VLAN。以下仅提供了每台交换机的 fa0/1 接口的配置命令。

```
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
```

步骤 5. 在 **S2** 和 **S3** 接入层交换机上配置端口安全功能。

配置端口 fa0/6、fa0/11 和 fa0/18, 使它们只支持一台主机, 并且动态获知该主机的 MAC 地址。

```
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
```

步骤 6. 在 VTP 服务器上配置 VLAN。

本实验需要四个 VLAN:

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

在 VTP 服务器上配置这些 VLAN。Packet Tracer 评分时会区分大小写。

```
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
```

使用 `show vlan brief` 命令检查 S1 上是否创建了这些 VLAN。

步骤 7. 检查 S1 上创建的 VLAN 是否已分发给 S2 和 S3。

在 S2 和 S3 上使用 `show vlan brief` 命令检查 VTP 服务器是否已将其 VLAN 配置传送给所有的交换机。

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, Fa0/3, 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
```

所有交换机上配置的 VLAN 都相同吗? _____

为什么 S2 和 S3 具有不同的 VLAN 配置?

步骤 8. 在 S2 和 S3 上创建新的 VLAN。

```
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)#
```

为什么您不能在 S2 上创建新的 VLAN, 但在 S3 上可以?

从 S3 上删除 VLAN 88。

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

步骤 9. 手动配置 VLAN。

在交换机 S3 上配置步骤 6 中提到的四个 VLAN。

```
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
```

此时您能体会到 VTP 的一项优点。手动配置费时又容易出错, 并且此处所犯的任何错误都可能阻碍 VLAN 内的通信。此外, 此类错误也难以排查。

步骤 10. 在所有三台交换机上配置管理接口地址。

```
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
```

在交换机之间执行 ping 操作, 检查这些交换机是否都已得到正确配置。从 S1 ping S2 和 S3 的管理接口。
从 S2 ping S3 的管理接口。

ping 是否成功? 若不成功, 则排除交换机配置故障, 然后重试。

步骤 11. 分配交换机端口给 VLAN。

请参阅本练习开头的端口分配表，将端口分配给 VLAN。由于 Packet Tracer 4.11 不支持 `interface range` 命令，因此只需为每个 VLAN 配置第一个接口。端口分配不是通过 VTP 完成的。必须在每台交换机上以手动方式或使用 VMPS 服务器动态执行端口分配。下面只显示了 S3 上的端口分配命令，但是交换机 S2 和 S3 的配置方法相似。完成后保存配置。

```
S3(config)#interface fa0/6
S3(config-if-range)#switchport access vlan 30
S3(config-if-range)#interface fa0/11
S3(config-if-range)#switchport access vlan 10
S3(config-if-range)#interface fa0/18
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#
```