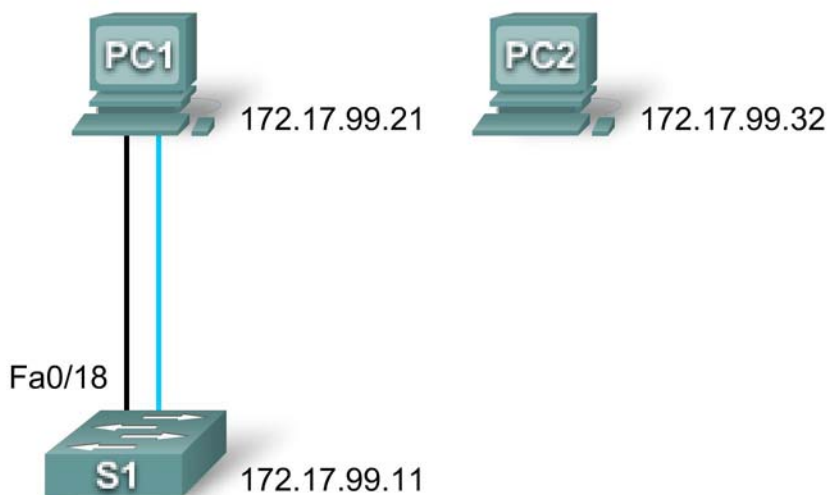


PT 练习 2.5.1：基本交换机配置

拓扑图



编址表

设备	接口	IP 地址	子网掩码	默认网关
PC1	网卡	172.17.99.21	255.255.255.0	172.17.99.11
PC2	网卡	172.17.99.22	255.255.255.0	172.17.99.11
S1	VLAN99	172.17.99.11	255.255.255.0	172.17.99.1

学习目标

- 清除交换机的现有配置
- 检验默认交换机配置
- 创建基本交换机配置
- 管理 MAC 地址表
- 配置端口安全性

简介

本练习中，您将检查并配置一台独立式 LAN 交换机。虽然交换机在出厂默认状态下能够执行基本功能，但为了保证 LAN 的安全并优化 LAN，网络管理员应当修改几个参数。本练习将向您介绍交换机配置的基本知识。

任务 1：清除交换机的现有配置

步骤 1. 键入 **enable** 命令进入特权执行模式。

单击 **S1**，然后单击 **CLI** 选项卡。发出 **enable** 命令，进入特权执行模式。

```
Switch>enable
Switch#
```

步骤 2. 删除 **VLAN** 数据库信息文件。

VLAN 数据库信息与配置文件分开存储，以 **vlan.dat** 文件名存储在闪存中。要删除 VLAN 文件，请发出命令 **delete flash:vlan.dat**

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]? [Enter]
Delete flash:vlan.dat? [confirm] [Enter]
```

步骤 3. 从 **NVRAM** 删除交换机启动配置文件。

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm] [Enter]
[OK]
Erase of nvram: complete
```

步骤 4. 确认 **VLAN** 信息已删除。

使用 **show vlan** 命令检查是否确实删除了 VLAN 配置。

```
Switch#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
10	VLAN10	active	
30	VLAN30	active	
1002	fddi-default	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN 信息仍在交换机上。执行下一步骤予以清除。

步骤 5. 重新加载交换机。

在特权执行模式提示符下，输入 **reload** 命令开始这一过程。

```
Switch#reload
Proceed with reload? [confirm] [Enter]
```

```
%SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
```

<output omitted>

Press RETURN to get started! [**Enter**]

Switch>

任务 2：检验默认交换机配置

步骤 1. 进入特权模式。

特权模式下，您可以使用全部交换机命令。不过，由于许多特权命令会配置操作参数，因此应使用口令对特权访问加以保护，防止未授权使用。特权命令集不仅包括用户执行模式所包含的那些命令，还包括 **configure** 命令，通过该命令可以访问其余命令模式。

```
Switch>enable  
Switch#
```

请注意特权执行模式下配置中提示符的变化。

步骤 2. 检查当前交换机配置。

发出 **show running-config** 命令，检查当前的运行配置。

交换机有多少个快速以太网接口？ _____

交换机有多少个千兆以太网接口？ _____

显示的 vty 线路值范围是什么？ _____

发出 **show startup-config** 命令，检查当前 NVRAM 的内容。

为什么交换机做出这样的响应？

发出 **show interface vlan1** 命令，检查虚拟接口 VLAN1 的特征。

交换机上设置了 IP 地址吗？ _____

虚拟交换机接口的 MAC 地址是什么？ _____

此接口打开了吗？ _____

现在使用 **show ip interface vlan1** 命令查看接口的 IP 属性。

你看到的输出是什么？ _____

步骤 3. 显示 Cisco IOS 信息。

使用 **show version** 命令显示 Cisco IOS 信息。

交换机运行的 Cisco IOS 版本是多少？ _____

系统图像文件名是什么？ _____

此交换机的基本 MAC 地址是什么？ _____

步骤 4. 检查快速以太网接口。

使用 **show interface fastethernet 0/18** 命令检查 PC1 所用快速以太网接口的默认属性。

```
Switch#show interface fastethernet 0/18
```

此接口是打开还是关闭的？ _____

什么事件会打开接口？ _____

接口的 MAC 地址是什么？ _____

该接口的速率和双工设置是什么？ _____

步骤 5. 检查 VLAN 信息。

使用 **show vlan** 命令检查交换机的默认 VLAN 设置。

VLAN 1 的名称是什么？ _____

此 VLAN 中有哪些端口？ _____

VLAN 1 是活动的吗？ _____

什么类型的 VLAN 是默认 VLAN？ _____

步骤 6. 检查闪存。

检查闪存的命令有两个：**dir flash:** 或 **show flash**。发出以上任一命令检查闪存目录中的内容。

发现了哪些文件或目录？

步骤 7. 检查并保存启动配置文件。

早在步骤 2 中，您已看到启动配置文件不存在。更改交换机的某项配置，然后保存配置。键入下列命令：

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#exit
S1#
```

要把运行配置文件的内容保存到非易失性 RAM (NVRAM)，请发出命令 **copy running-config startup-config**。

```
Switch#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
```

现在显示 NVRAM 的内容。当前配置已写入到 NVRAM。

任务 3：创建基本交换机配置

步骤 1. 为交换机指定名称。

进入全局配置模式。利用配置模式，您可以管理交换机。输入配置命令，每行一条。请注意命令行提示符的变化反应了当前的提示符和交换机名称。在前一任务的最后步骤中，您配置了主机名。下面是对所用命令的回顾。

```
S1#configure terminal
S1(config)#hostname S1
S1(config)#exit
```

步骤 2. 设置访问口令。

进入控制台线路配置模式。将登录口令设置为 **cisco**。另外，使用口令 **cisco** 配置 vty 线路 0 到 15。

```
S1#configure terminal
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)#exit
S1(config)#
```

为什么需要 **login** 命令？ _____

步骤 3. 设置命令模式口令。

将使能加密口令设置为 **class**。

```
S1(config)#enable secret class
```

步骤 4. 配置交换机的第 3 层地址。

在内部虚拟接口 VLAN 99 上将交换机的 IP 地址设置为 172.17.99.11，子网掩码为 255.255.255.0。首先必须在交换机上创建 VLAN，然后才能分配地址。

```
S1(config)#vlan 99
S1(config-vlan)#exit
S1(config)#interface vlan99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
```

步骤 5. 为交换机 VLAN 分配端口。

将 Fastethernet 0/1、0/8 和 0/18 端口分配给 VLAN 99。

```
S1(config)#interface fa0/1
S1(config-if)#switchport access vlan 99
S1(config-if)#exit
```

步骤 6. 设置交换机默认网关。

S1 是第 2 层交换机，因此它根据第 2 层报头做出转发决策。如果多个网络连到一台交换机，则需要明确交换机如何转发内部工作帧，因为路径必须在第 3 层确定。这就需要指定默认网关地址，它指向路由器或第 3 层交换机。虽然本练习没有包括外部 IP 网关，但可以假设您最终会把 LAN 连接到路由器进行外部访问。假设路由器上的 LAN 接口为 172.17.99.1，据此为交换机设置默认网关。

```
S1(config)#ip default-gateway 172.17.99.1
S1(config)#exit
```

步骤 7. 检验管理 LAN 设置。

使用 **show interface vlan 99** 命令检验 VLAN 99 上的接口设置。

```
S1#show interface vlan 99
Vlan99 is up, line protocol is up
  Hardware is CPU Interface, address is 0060.47ac.1eb8 (bia 0060.47ac.1eb8)
  Internet address is 172.17.99.11/24
```

```
MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,  
    reliability 255/255, txload 1/255, rxload 1/255  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00  
Last input 21:40:21, output never, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
<省略部分输出>
```

此接口的带宽是多少？ _____

排队策略是什么？ _____

步骤 8. 配置 PC1 的 IP 地址和默认网关。

将 PC1 的 IP 地址设置为 172.17.99.21，子网掩码设置为 255.255.255.0。配置默认网关为 172.17.99.11。单击 PC1 -> Desktop（桌面）选项卡 -> IP 配置，输入上述编址参数。

步骤 9. 检验连通性。

要检验主机和交换机的配置是否正确，请从 PC1 ping 交换机。

如果 ping 不成功，请排除交换机和主机的配置故障。请注意，可能需要尝试好几次才能 ping 成功。

步骤 10. 配置快速以太网接口的端口速率和双工设置。

配置 FastEthernet 0/18 的双工和速率设置。完成后，使用 **end** 命令返回特权执行模式。

```
S1#configure terminal  
S1(config)#interface fastethernet 0/18  
S1(config-if)#speed 100  
S1(config-if)#duplex full  
S1(config-if)#end
```

交换机以太网接口的默认设置是自动检测，因此它会自动采用最佳设置。只有当一个端口必须以某一速率和双工模式运作时，才需要手动设置双工模式和速率。手动配置端口可能会导致双工不匹配，从而显著降低性能。

请注意 PC1 与 S1 之间的链路是如何关闭的。删除 **speed 100** 和 **duplex full** 命令。现在使用 **show interface fa0/18** 命令检验快速以太网接口的设置。

```
S1#show interface fastethernet 0/18  
FastEthernet0/18 is up, line protocol is up (connected)  
    Hardware is Lance, address is 0060.5c36.4412 (bia 0060.5c36.4412)  
    MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,  
        reliability 255/255, txload 1/255, rxload 1/255  
    Encapsulation ARPA, loopback not set  
    Keepalive set (10 sec)  
    Full-duplex, 100Mb/s  
<省略部分输出>
```

步骤 11. 保存配置。

您已经完成交换机的基本配置。现在将运行配置文件备份到 NVRAM，确保所做的变更不会因系统重启或断电而丢失。

```
S1#copy running-config startup-config

Destination filename [startup-config]?[Enter]
Building configuration...
[OK]
S1#
```

步骤 12. 检查启动配置文件。

要查看 NVRAM 中存储的配置，请在特权执行（enable 模式）下发出 **show startup-config** 命令。

文件中记录了之前输入的所有变更吗？

任务 4：管理 MAC 地址表

步骤 1. 记录主机的 MAC 地址。

通过下列步骤确定并记录 PC 网络接口卡的第 2 层（物理）地址：

- 单击 PC。
- 选择 Desktop（桌面）选项卡。
- 单击 Command Prompt（命令提示符）。
- 键入 **ipconfig /all**

步骤 2. 确定交换机已学习的 MAC 地址。

在特权执行模式下使用 **show mac-address-table** 命令显示 MAC 地址。如果没有显示 MAC 地址，请从 PC1 ping S1，然后再次检查。

```
S1#show mac-address-table
```

步骤 3. 清除 MAC 地址表。

要删除现有 MAC 地址，请在特权执行模式下使用 **clear mac-address-table dynamic** 命令。

```
S1#clear mac-address-table dynamic
```

步骤 4. 确认结果。

确认 MAC 地址表已清除。

```
S1#show mac-address-table
```

步骤 5. 再次检查 MAC 表。

在特权执行模式下再次查看 MAC 地址表。如果地址表没有变化，请从 PC1 ping S1，然后再次检查。

步骤 6. 设置静态 MAC 地址。

要指定主机可以连接到哪些接口，一个方法是创建主机 MAC 地址与端口的静态映射表。

使用本任务步骤 1 中为 PC1 记录的地址 0002.16E8.C285 设置快速以太网接口 0/18 的静态 MAC 地址。

```
S1(config)#mac-address-table static 0002.16E8.C285 vlan 99 interface
fastethernet 0/18
```

步骤 7. 确认结果。

检查 MAC 地址表条目。

```
S1#show mac-address-table
```

步骤 8. 删除静态 MAC 条目。

进入配置模式，在命令串前加上 **no** 以删除静态 MAC。

```
S1(config)#no mac-address-table static 0002.16E8.C285 vlan 99 interface
fastethernet 0/18
```

步骤 9. 确认结果。

使用 **show mac-address-table static** 命令确认静态 MAC 地址已删除。

任务 5：配置端口安全性

步骤 1. 配置第二台主机。

本任务需要第二台主机。将 PC2 的 IP 地址设置为 172.17.99.22，子网掩码为 255.255.255.0，默认网关为 172.17.99.11。暂时不要将此 PC 连接到交换机。

步骤 2. 检验连通性。

从主机 ping 交换机的 VLAN 99 IP 地址，检验 PC1 和交换机的配置是否仍然正确。如果 ping 不成功，请排除主机和交换机的配置故障。

步骤 3. 确定交换机已学习了哪些 MAC 地址。

在特权执行模式下使用 **show mac-address-table** 命令显示已学习的 MAC 地址。

步骤 4. 列出端口安全选项。

研究用于在快速以太网接口 0/18 上设置端口安全的选项有哪些。

```
S1# configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#switchport port-security ?
    mac-address      Secure mac address
    maximum          Max secure addresses
    violation         Security violation mode
    <cr>
```

步骤 5. 在接入端口上配置端口安全性。

配置交换机端口 FastEthernet 0/18 仅接受两台设备，动态学习这些设备的 MAC 地址，并在发生安全违规事件时关闭端口。

```
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 2
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#switchport port-security violation shutdown
S1(config-if)#exit
```


步骤 6. 确认结果。

使用 **show port-security interface fa0/18** 命令显示端口安全性设置。

FastEthernet 0/18 上允许多少安全地址？

对此端口的安全操作是什么？

步骤 7. 检查运行配置文件。

```
S1#show running-config
```

所列语句是否直接反映了运行配置安全的实施情况？

步骤 8. 在端口上修改端口安全设置。

在快速以太网接口 0/18 上，将端口安全最大 MAC 地址计数更改为 1。

```
S1(config-if)#switchport port-security maximum 1
```

步骤 9. 确认结果。

使用 **show port-security interface fa0/18** 命令显示端口安全性设置。

端口安全设置是否已更改为步骤 8 中的配置？

从 PC1 ping 交换机的 VLAN 99 地址，检验连通性并刷新 MAC 地址表。

步骤 10. 引入一台流氓主机。

断开连接到交换机快速以太网接口 0/18 的 PC。将分配有 IP 地址 172.17.99.22 的 PC2 连接到端口 FastEthernet 0/18。从新主机 ping VLAN 99 地址 172.17.99.11。

尝试 ping S1 时发生了什么情况？

注：网络收敛可能需要一些时间。切换仿真模式和实时模式可加快收敛。

步骤 11. 重新激活端口。

只要流氓主机与 FastEthernet 0/18 相连，主机与交换机之间便不会有流量通过。重新连接 PC1 与 FastEthernet 0/18，在交换机上输入下列命令以重新激活该端口：

```
S1#configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#no shutdown
S1(config-if)#exit
```

步骤 12. 检验连通性。

网络收敛后，PC1 应能再次 ping 通 S1。