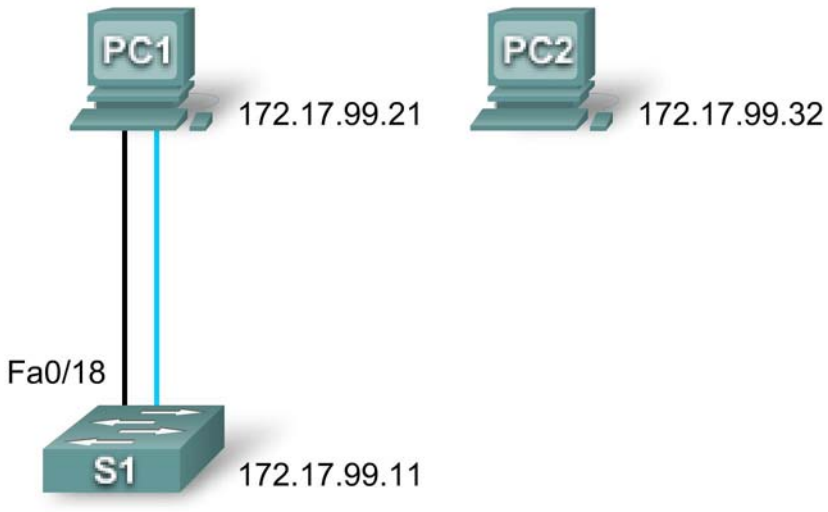
PT 练习 2.4.7：配置交换机安全性

拓扑图



编址表

设备	接口	IP 地址	子网掩码
S1	**VLAN99**	172.17.99.11	255.255.255.0
PC1	**网卡**	172.17.99.21	255.255.255.0
PC2	**网卡**	172.17.99.32	255.255.255.0

学习目标

- 配置基本交换机管理
- 配置动态端口安全性
- 测试动态端口安全性
- 保护未使用端口的安全

任务 1：配置基本交换机管理

步骤 1：从 PC1 建立到 S1 的控制台连接。

- 单击 **PC1**，然后单击 **Desktop（桌面）**选项卡。选择桌面选项卡中的 **Terminal（终端）**。
- 保留终端配置的下列默认设置不变，然后单击 **OK（确定）**：

  Bits Per Second（每秒位数）= 9600

Data Bits（数据位）= 8
Parity（奇偶校验）= None（无）
Stop Bits（停止位）= 1
Flow Control（流量控制）= None（无）

- 现在已建立到 S1 的控制台连接。按 Enter 进入交换机提示符。

步骤 2：变更到特权执行模式。

要使用特权执行模式，键入 **enable** 命令。提示符从 **>** 变为 **#**。

```
S1>enable
S1#
```

注意您是如何能够不提供口令而进入特权执行模式的。为什么缺少特权执行模式口令是一个安全威胁？

_____

_____

_____

步骤 3：变更到全局配置模式配置特权执行模式口令。

- 在特权执行模式下，您可以使用 **configure terminal** 命令访问全局配置模式。
- 使用 **enable secret** 命令设置口令。对于本练习，请将口令设置为 **class**。

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#enable secret class
S1(config)#
```

注：PT 不会给 **enable secret** 命令评分。

步骤 4：配置虚拟终端和控制台的口令并要求用户通过口令登录。

访问控制台线路应当需要口令。即使最基本的用户执行模式也能给恶意用户提供重要信息。另外，vty 线路必须有口令，用户从远程访问交换机时必须先输入口令。

- 使用 **line console 0** 命令进入控制台提示符。
- 使用 **password** 命令将控制台和 vty 线路的口令配置为 **cisco**。注：这种情况下，PT 不会给 **password cisco** 命令评分。
- 然后输入 **login** 命令，它要求用户先输入口令，然后才能进入用户执行模式。
- 对 vty 线路重复上述过程。使用 **line vty 0 15** 命令进入正确的提示符。
- 键入 **exit** 命令，返回全局配置提示符。

```
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)#
```

步骤 5：配置口令加密

特权执行口令已经加密。要对刚才配置的线路口令加密，请在全局配置模式下输入 **service password-encryption** 命令。

```
S1(config)#service password-encryption
S1(config)#
```

步骤 6：配置并测试 MOTD 标语。

配置当天消息 (MOTD)，文本使用 **Authorized Access Only（仅限授权访问）**。标语文本区分大小写。请勿在标语文本前后添加空格。在标语文本前后使用定界符指示文本从何处开始，到何处结束。下例中使用的定界符为 **&**，但是您可以使用标语文本中未使用的任何字符。配置完 MOTD 后，从交换机注销，然后再次登录，检查是否显示了上述标语。

```
S1(config)#banner motd &Authorized Access Only&
S1(config)#end [or exit]
S1#exit

S1 con0 is now available

Press RETURN to get started.

[Enter]

Authorized Access Only

User Access Verification

Password:
```

- 现在口令提示符要求输入口令才能进入用户执行模式。输入口令 **Cisco**。
- 使用口令 **class** 进入特权执行模式，然后使用 **configure terminal** 命令返回全局配置模式。

```
Password:[cisco] !注：键入口令时，口令将会自动隐藏。

S1>enable
Password:[class] !注：键入口令时，口令将会自动隐藏。
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
```

步骤 7：检查结果。

完成百分比应当为 40%。如果不是，请单击 **Check Results（检查结果）**，查看哪些需要的组件尚未完成。

任务 2：配置动态端口安全性

步骤 1：启用 VLAN99。

Packet Tracer 启动时，VLAN 99 接口处在关闭状态，但实际的交换机并不是这样运作。必须使用 **no shutdown** 命令启用 VLAN 99，然后该接口在 Packet Tracer 中才变为活动状态。

```
S1(config)#interface vlan 99
S1(config-if)#no shutdown
```

步骤 2：进入 FastEthernet 0/18 的接口配置模式并启用端口安全性。

首先必须启用端口安全性，才能在接口上使用其它端口安全性命令。

```
S1(config-if)#interface fa0/18
S1(config-if)#switchport port-security
```

请注意，无需退回到全局配置模式便可进入 fa0/18 的接口配置模式。

步骤 3：配置 MAC 地址的最大数量。

要配置端口使其只允许学习一个 MAC 地址，请将 **maximus** 设置为 1：

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

注：PT 不会给 **switchport port-security maximum 1** 命令评分，但此命令对配置端口安全性非常重要。

步骤 4：配置端口将 MAC 地址添加到运行配置中。

可以把端口学习的 MAC 地址添加（“粘滞”）到端口的运行配置中。

```
S1(config-if)#switchport port-security mac-address sticky
```

注：PT 不会给 **switchport port-security mac-address sticky** 命令评分，但此命令对配置端口安全性非常重要。

步骤 5：配置端口在发生端口安全违规事件时自动关闭。

如果不配置以下命令，则 S1 只会将违规事件登记在端口安全性统计信息中，而不会关闭端口。

```
S1(config-if)#switchport port-security violation shutdown
```

注：PT 不会给 **switchport port-security violation shutdown** 命令评分，但此命令对配置端口安全性非常重要。

步骤 6：确认 S1 已学习到 PC1 的 MAC 地址。

从 PC1 ping S1。

确认 S1 现在的 MAC 表中有 PC1 的静态 MAC 地址：

```
S1#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  99    0060.5c5b.cd23    STATIC      Fa0/18
```

该 MAC 地址现已“粘滞”到运行配置。

```
S1#show running-config
<output omitted>
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0060.5C5B.CD23
<省略部分输出>
S1#
```

步骤 7：检查结果。

完成百分比应当为 70%。如果不是，请单击 **Check Results（检查结果）**，查看哪些需要的组件尚未完成。

任务 3：测试动态端口安全性

步骤 1：拆除 PC1 与 S1 之间的连接，将 PC2 与 S1 相连。

- 要测试端口安全性，请拆除 PC1 与 S1 之间的以太网连接。如果不小心拆除了控制台电缆连接，只需重新连上。
- 将 PC2 连接到 S1 的 Fa0/18。等待琥珀色链路指示灯变绿，然后从 PC2 ping S1。端口随后应当自动关闭。

步骤 2：确认端口安全性是导致端口关闭的原因。

要确认端口关闭的原因与端口安全性有关，请输入命令 **show interface fa0/18**。

```
S1#show interface fa0/18
FastEthernet0/18 is down, line protocol is down (err-disabled)
  Hardware is Lance, address is 0090.213e.5712 (bia 0090.213e.5712)
<省略部分输出>
```

由于交换机端口从不同于已学习到的 MAC 地址接收到帧而发生错误 (err)，致使线路协议关闭，因而 Cisco IOS 软件关闭了 (disabled) 该端口。

也可以使用 **show port-security interface fa0/18** 命令检验安全违规事件。

```
S1#show port-security interface fa0/18
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 00E0.F7B0.086E:99
Security Violation Count   : 1
```

请注意端口状态为 **secure-shutdown**，并且安全违规事件计数为 **1**。

步骤 3：恢复 PC1 与 S1 之间的连接并重置端口安全性。

拆除 PC2 与 S1 之间的连接。将 PC1 重新连接到 S1 上的 Fa0/18 端口。

请注意，尽管您已重新连上端口允许的 PC，但是端口仍处在关闭状态。对于发生安全违规事件的端口，必须手动将其激活。关闭端口，然后使用 **no shutdown** 命令激活端口。

```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface fa0/18
S1(config-if)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to
administratively down
S1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
S1(config-if)#exit
S1(config)#
```

步骤 4：从 PC1 ping S1，测试其间的连通性。

从 PC1 应当能成功 ping 通 S1。

此任务结束时，完成百分比仍应是 70%。

任务 4：保护未使用端口的安全

为了防止未经授权访问网络，许多管理员使用的一个简单方法是禁用网络交换机上的所有未使用端口。

步骤 1：禁用 S1 上的接口 Fa0/17。

进入 FastEthernet 0/17 的接口配置模式，关闭该端口。

```
S1(config)#interface fa0/17
S1(config-if)#shutdown
```

步骤 2：将 PC2 连接到 S1 上的 Fa0/17，测试该端口。

将 PC2 连接到 S1 上的 Fa0/17 接口。请注意链路指示灯为红色。PC2 无权访问网络。

步骤 3：检查结果。

完成百分比应当为 100%。如果不是，请单击 **Check Results（检查结果）**，查看哪些需要的组件尚未完成。