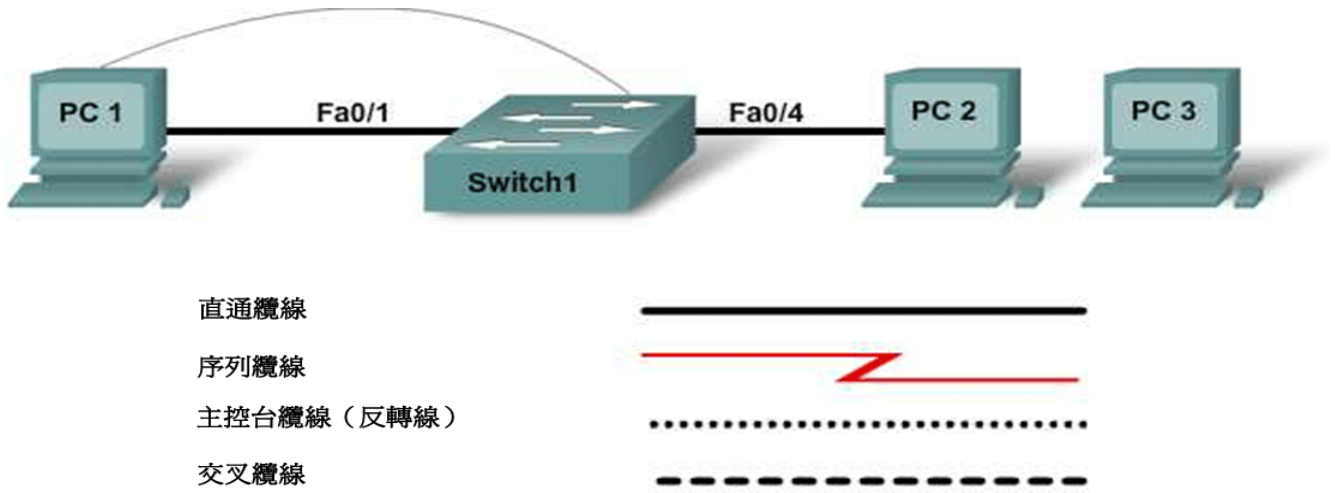
實驗 3.1.4 套用基本的交換器安全性



裝置編號	IP 位址	子網路遮罩	預設閘道	啓用加密密碼	vty 和主控台密碼
PC 1	192.168.1.3	255.255.255.0	192.168.1.1		
PC 2	192.168.1.4	255.255.255.0	192.168.1.1		
PC 3	192.168.1.5	255.255.255.0	192.168.1.1		
Switch1	192.168.1.2	255.255.255.0	192.168.1.1	class	cisco

目標

- 設定密碼以確保對 CLI 的存取受到保護。
- 移除交換器的 http 伺服器狀態，以確保安全。
- 設定連接埠安全性。
- 停用未使用的連接埠。
- 將未知主機連接到安全連接埠，以測試安全性設定。

背景/準備工作

參照拓撲圖，建立一個類似的網路。

本實驗需要以下資源：

- 一台 Cisco 2960 或同類交換器
- 兩台使用 Windows 系統的 PC，其中至少一台安裝有終端機模擬程式
- 至少一條 RJ-45 轉 DB-9 連接器主控台纜線

- 兩條直通乙太網路纜線（分別將 PC1 和 PC2 連接到交換器）
- 對 PC 命令提示字元的存取權
- 對 PC 網路 TCP/IP 設定的存取權

注意：請確保已清除交換器的啓動設定。有關清除交換器和路由器設定的說明，請參閱 Academy Connection 中 Tools（工具）部份的 Lab Manual（實驗手冊）。

步驟 1：將 PC1 連接到交換器

a. 將 PC1 連接到高速乙太網路交換器連接埠 Fa0/1。使用表中所示的 IP 位址、遮罩和閘道設定 PC1。

b. 建立從 PC1 到交換器的終端機模擬會談。

步驟 2：將 PC2 連接到交換器

a. 將 PC2 連接到高速乙太網路交換器連接埠 Fa0/4。

b. 使用表中所示的 IP 位址、遮罩和閘道設定 PC2。

步驟 3：設定 PC3 但不連接

本實驗還需要第三台主機。

a. 使用 IP 位址 192.168.1.5、子網路遮罩 255.255.255.0 和預設閘道 192.168.1.1 設定 PC3。

b. 暫時不要將此 PC 連接到交換器，因爲它要用來測試安全性。

步驟 4：在交換器上執行初始設定

a. 將交換器的主機名稱設定爲 **Switch1**。

```
Switch>enable
Switch#config terminal
Switch(config)#hostname Switch1
```

b. 將特權執行模式密碼設定爲 **cisco**。

```
Switch1(config)#enable password cisco
```

c. 將特權執行模式加密密碼設定爲 **class**。

```
Switch1(config)#enable secret class
```

d. 設定主控台和虛擬終端機線路的密碼，並且要求在登入時輸入密碼。

```
Switch1(config)#line console 0
Switch1(config-line)#password cisco
Switch1(config-line)#login
Switch1(config-line)#line vty 0 15
Switch1(config-line)#password cisco
Switch1(config-line)#login
Switch1(config-line)#end
```

e. 退出主控台會談，然後重新登入。

進入特權執行模式需要輸入什麼密碼？_____

爲什麼？

_____

步驟 5：設定 VLAN 1 上的交換器管理介面

a. 進入 VLAN 1 的介面設定模式。

```
Switch1(config)#interface vlan 1
```

b. 爲管理介面設定 IP 位址、子網路遮罩和預設閘道。

```
Switch1(config-if)#ip address 192.168.1.2 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config-if)#exit
Switch1(config)#ip default-gateway 192.168.1.1
Switch1(config)#end
```

爲什麼介面 VLAN 1 需要此 LAN 中的 IP 位址？

_____

預設閘道有何作用？

_____

步驟 6：驗證管理 LAN 設定

a. 驗證交換器 VLAN 1 上管理介面的 IP 位址與 PC1 及 PC2 的 IP 位址是否在同一區域網路中。使用 **show running-config** 命令檢視交換器的 IP 位址設定。

b. 驗證 VLAN 1 上的介面設定。

```
Switch1#show interface vlan 1
```

此介面的頻寬是多少？_____

VLAN 狀態是什麼？

VLAN 1 爲 _____，線路協定爲_____。

步驟 7：暫停交換器成爲 http 伺服器

關閉交換器用作 http 伺服器的功能。

```
Switch1(config)#no ip http server
```

步驟 8：驗證連通性

a. 要驗證主機和交換器的設定是否正確，請從主機 ping 交換器 IP 位址。

ping 是否成功？_____

如果 ping 命令失敗，則重新驗證設定和連接。確保使用了正確的纜線，而且連接固定好。檢查主機和交換器設定。

b. 儲存設定。

步驟 9：記錄主機 MAC 位址

確定並記錄 PC 網路介面卡的第 2 層位址。在每台電腦的命令提示字元視窗中輸入 **ipconfig /all**。

PC1 _____

PC2 _____

PC3 _____

步驟 10：確定交換器獲知哪些 MAC 位址

在特權執行模式提示字元下，使用 **show mac-address-table** 命令來確定交換器到底獲知了哪些 MAC 位址。

```
Switch1#show mac-address-table
```

一共有多少個動態位址？_____

現在表中一共有多少個 MAC 位址？_____

這些 MAC 位址是否與主機 MAC 位址相符？_____

步驟 11：檢視 show mac-address-table 選項

檢視 **show mac-address-table** 命令提供的選項。

```
Switch1(config)#show mac-address-table ?
```

可以使用哪些選項？_____

_____

步驟 12：設定靜態 MAC 位址

在 FastEthernet 0/4 介面上設定靜態 MAC 位址。使用在步驟 9 中記錄的 PC2 的位址。MAC 位址 00e0.2917.1884 僅做範例說明用。

```
Switch1(config)#mac-address-table static 00e0.2917.1884 vlan 1
interface fastethernet 0/4
```

步驟 13：驗證結果

a. 驗證 MAC 位址表條目。

```
Switch1#show mac-address-table
```

現在表中有多少個動態 MAC 位址？_____

現在表中有多少個靜態 MAC 位址？_____

b. 從 MAC 位址表中移除靜態項目。

```
Switch1(config)#no mac-address-table static 00e0.2917.1884 vlan 1
interface fastethernet 0/4
```

步驟 14：列出連接埠安全選項

a. 確定用於在 FastEthernet 0/4 介面上設定連接埠安全的選擇性的參數有哪些。

```
Switch1(config)#interface fastethernet 0/4
Switch1(config-if)#switchport port-security ?
```

可以使用哪些選擇性的參數？_____

b. 設定連接埠安全，使交換器連接埠 FastEthernet 0/4 只接受一台裝置。

```
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport port-security
Switch1(config-if)#switchport port-security mac-address sticky
```

c. 退出設定模式並檢查連接埠安全設定。

```
Switch1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
--------------------------------------------------------------------------
      Fa0/4        1            0                0            Shutdown
--------------------------------------------------------------------------
```

如果 PC2 以外的主機嘗試連接到 Fa0/4，會發生什麼情況？

_____

步驟 15：限制每個連接埠的主機數目

a. 在 FastEthernet 0/4 介面上，將連接埠安全最大 MAC 數設定為 1。

```
Switch1(config-if)#switchport port-security maximum 1.
```

b. 拔除連接到 FastEthernet 0/4 介面的 PC，將 PC3 連接到 FastEthernet 0/4 介面。PC3 已經獲得 IP 位址 192.168.1.5，並且尚未連接到交換器。可能必須 ping 交換器位址 192.168.1.2 來產生一些流量。

記錄觀察到的任何情況。_____

_____

步驟 16：設定連接埠，如果發生違反安全規則時關閉該連接埠

a. 介面應在發生違反安全規則時關閉。為使連接埠因安全性問題而自動關閉，請輸入以下命令：

```
Switch1(config-if)#switchport port-security violation shutdown
```

連接埠安全還可以使用哪些操作選項？_____

_____

b. 如有必要，請從 PC3 192.168.1.5 ping 交換器位址 192.168.1.2。此電腦現已連接到 FastEthernet 0/4 介面，這就確保從 PC 到交換器可以通訊。

c. 記錄觀察到的任何情況。

_____

_____

d. 檢查連接埠安全設定。

```
Switch1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
--------------------------------------------------------------------------
      Fa0/4        1            1                0            Shutdown
--------------------------------------------------------------------------
```

步驟 17：顯示 0/4 埠 的設定資訊

如果只想檢視高速乙太網路埠 0/4 的設定資訊，在特權執行模式提示字元下輸入 **show interface fastethernet 0/4**。

```
Switch1#show interface fastethernet 0/4
```

介面的狀態是什麼？

FastEthernet0/4 為 _____，線路通訊協定為 _____。

步驟 18：重新啟動連接埠

a. 如果連接埠因違反安全規則而關閉，則使用 **shutdown / no shutdown** 命令來重新啟動它。

b. 在帶有原埠 0/4 的主機和新的主機間切換使用，多次嘗試重新啟動此連接埠。插上原主機，對介面套用 **no shutdown** 命令，然後使用命令提示字元執行 ping 操作。

ping 必須重複多次；或者使用 **ping 192.168.1.2 –n 200** 命令。此命令將 ping 封包的數量從 4 個變更為 200 個。然後更換主機並重試。

步驟 19：停用未使用的連接埠

停用交換器上所有未使用的連接埠。

```
Switch1(config)#interface range Fa0/5 - 24
Switch1(config-if-range)#shutdown

Switch1(config)#interface range gigabitethernet0/1 - 2
Switch1(config-if-range)#shutdown
```

步驟 20：思考

a. 為什麼要在交換器上啟用連接埠安全？_____

_____

b. 為什麼要停用交換器上未使用的連接埠？_____

_____