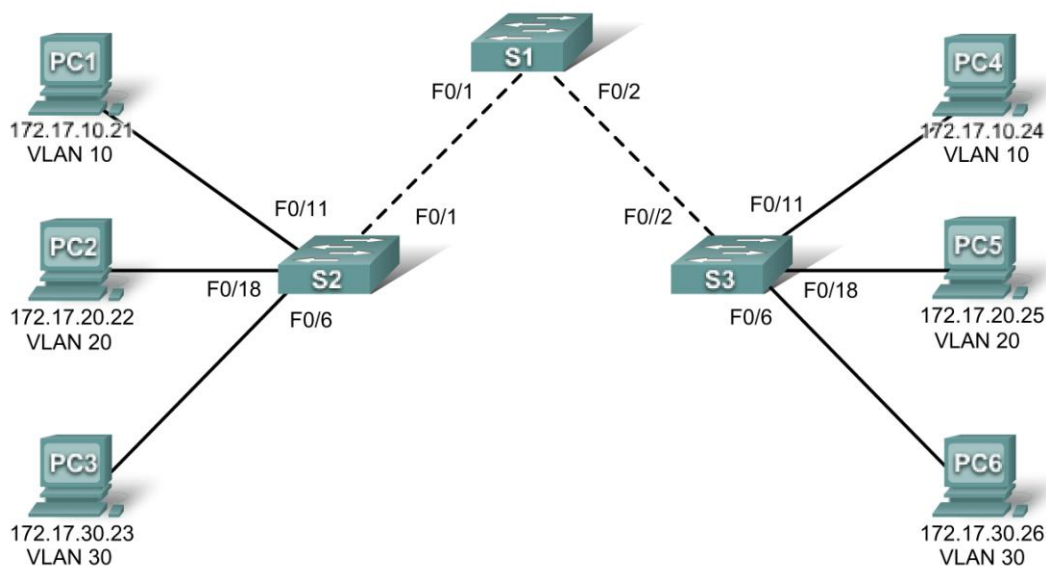


實驗 3.5.1：基本 VLAN 設定

拓樸圖



位址表

設備 (主機名稱)	介面	IP 位址	子網路遮罩	預設閘道
S1	VLAN 99	172.17.99.11	255.255.255.0	不適用
S2	VLAN 99	172.17.99.12	255.255.255.0	不適用
S3	VLAN 99	172.17.99.13	255.255.255.0	不適用
PC1	網卡	172.17.10.21	255.255.255.0	172.17.10.1
PC2	網卡	172.17.20.22	255.255.255.0	172.17.20.1
PC3	網卡	172.17.30.23	255.255.255.0	172.17.30.1
PC4	網卡	172.17.10.24	255.255.255.0	172.17.10.1
PC5	網卡	172.17.20.25	255.255.255.0	172.17.20.1
PC6	網卡	172.17.30.26	255.255.255.0	172.17.30.1

初始連接埠配置（交換器 2 和 3）

連接埠	配置	網路
Fa0/1 – 0/5	802.1q 主幹（原生 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

學習目標

完成本實驗後，你將能夠：

- 根據拓樸圖進行網路佈線
- 刪除交換器啟動設定並將其重載到預設狀態
- 執行交換器上的基本設定任務
- 新增 VLAN
- 配置交換器連接埠到 VLAN
- 增加、移動和更改連接埠
- 檢驗 VLAN 設定
- 對交換器間連接啟用主幹
- 檢驗主幹設定
- 儲存 VLAN 設定

任務 1：準備網路

步驟 1：根據拓樸圖所示完成網路電纜連線。

你可使用實驗室中現有的、具有拓樸所示介面的交換器。

注意：如果你使用的是 2900 或 2950 交換器，則螢幕輸出會略有差異。此外，你也可能無法使用某些命令，或命令的格式有所變化。

步驟 2：清除交換器上的所有現有設定，將所有連接埠置於關閉狀態。

如果需要，請參考實驗 2.5.1 的附錄 1，以瞭解清除交換器設定的方法。

要停用交換器上未使用的連接埠，較好的辦法是將這些連接埠設定為 shutdown。停用交換器上的所有連接埠。

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

任務 2：執行基本交換器設定

步驟 1：根據以下指導原則設定交換器。

- 設定交換器主機名稱。
- 停用 DNS 尋找。
- 將執行模式密碼設定為 **class**。
- 為控制台連接設定密碼 **cisco**。
- 為 vty 連接設定密碼 **cisco**。

步驟 2：啟用 S2 和 S3 上的用戶連接埠。

```
S2(config)#interface range fa0/6, fa0/11, fa0/18
```

```
S2(config-if-range)#switchport mode access
S2(config-if-range)#no shutdown
S3(config)#interface range fa0/6, fa0/11, fa0/18
S3(config-if-range)#switchport mode access
S3(config-if-range)#no shutdown
```

任務 3：設定並啟動乙太網介面

步驟 1：設定 PC。

執行本實驗可以只使用兩台 PC，只要根據要執行的測試相應地更改這兩台 PC 的 IP 位址即可。例如，如果你要測試 PC1 與 PC2 之間的連通性，那麼根據本實驗開頭部分的位址表為這兩台 PC 設定 IP 位址。或者你也可以為所有六台 PC 設定 IP 位址和預設閘道。

任務 4：在交換器上設定 VLAN

步驟 1：在交換器 S1 上新增 VLAN。

在全域設定模式下使用 **vlan vlan-id** 命令將 VLAN 增加到交換器 S1。本實驗需要設定四個 VLAN：VLAN 10 (faculty/staff)、VLAN 20 (students)、VLAN 30 (guest) 和 VLAN 99 (management)。新增 VLAN 之後，你將處於 vlan 設定模式，在該模式下可以使用 **name vlan name** 命令為 VLAN 指定名稱。

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

步驟 2：檢驗在 S1 上新增的 VLAN。

使用 **show vlan brief** 命令檢驗 VLAN 是否已成功新增。

```
S1#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	

步驟 3：在交換器 S2 和 S3 上設定並命名 VLAN。

使用步驟 1 中的命令在 S2 和 S3 上新增並命名 VLAN 10、20、30 和 99。使用 **show vlan brief** 命令檢驗設定是否正確。

目前哪些連接埠被配置到你所新增的四個 VLAN 中？_____

步驟 4：在 S2 和 S3 上將交換器連接埠配置給 VLAN。

請參考第 1 頁上的連接埠配置表。在介面設定模式下使用 **switchport access vlan vlan-id** 命令將連接埠配置給 VLAN。你可以單獨配置每個連接埠，或者也可按如下所示使用 **interface range** 命令來加快執行此任務的速度。以下僅顯示了 S3 上的命令，但你應在 S2 和 S3 上都執行類似的設定。完成後請儲存設定。

```
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]
```

步驟 5：確定已增加的連接埠。

在 S2 上使用 **show vlan id vlan-number** 命令查看哪些連接埠已配置給 VLAN 10。

哪些連接埠已配置給 VLAN 10？_____

注意：**show vlan name vlan-name** 可顯示相同的輸出。

你也可以使用 **show interfaces interface switchport** 命令查看 VLAN 配置資訊。

步驟 6：配置管理 VLAN。

管理 VLAN 是你設定用於存取交換器管理功能的 VLAN。如果你沒有特別指明使用其它 VLAN，那麼 VLAN 1 將作為管理 VLAN。你需要為管理 VLAN 配置 IP 位址和子網路遮罩。交換器可透過 HTTP、Telnet、SSH 或 SNMP 進行管理。因為 Cisco 交換器的出廠設定將 VLAN 1 作為預設 VLAN，所以將 VLAN 1 當作管理 VLAN 不是明智的選擇。你肯定不願意連接到交換器的任何用戶都預設連接到管理 VLAN。在本實驗前面的部分中，我們已經將管理 VLAN 設定為 VLAN 99。

在介面設定模式下，使用 **ip address** 命令為交換器配置管理 IP 位址。

```
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
```

配置管理位址後，交換器之間便可透過 IP 通信。此外，任何主機只要連接到已配置給 VLAN 99 的連接埠，這些主機便能連接到交換器。因為 VLAN 99 設定為管理 VLAN，所以任何配置到該 VLAN 的連接埠都應視為管理連接埠，並且應該對這些連接埠實施安全保護，控制可以連接到這些連接埠的設備。

步驟 7：為所有交換器上的主幹連接埠設定主幹和原生 VLAN。

主幹是交換器之間的連接，它允許交換器交換所有 VLAN 的資訊。預設情況下，主幹連接埠屬於所有 VLAN，而接取連接埠則僅屬於一個 VLAN。如果交換器同時支援 ISL 和 802.1Q VLAN 封裝，則主幹必須指定使用哪種方法。因為 2960 交換器僅支援 802.1Q 主幹，所以在本實驗中無需指定使用何種方法。

原生 VLAN 配置給 802.1Q 主幹連接埠。在拓樸中，原生 VLAN 是 VLAN 99。802.1Q 主幹連接埠支援來自多個 VLAN 的流量（已標記流量），也支援來源不是 VLAN 的流量（無標記流量）。802.1Q 主幹連接埠會將無標記流量發送到原生 VLAN。產生無標記流量的電腦連接到設定有原生 VLAN 的交換器連接埠。在有關原生 VLAN 的 IEEE 802.1Q 規範中，其中一項的作用便是維護無標記流量的向下相容性，這種流量在傳統 LAN 方案中十分常見。對於本練習而言，原生 VLAN 的作用是充當主幹鏈路兩端的通用識別符號。最佳做法是使用 VLAN 1 以外的 VLAN 作為原生 VLAN。

在全域設定模式下使用 **interface range** 命令可簡化設定主幹的操作。

```
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
```

使用 **show interface trunk** 命令檢驗主幹的設定情況。

```
S1#show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	99
Fa0/2	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Fa0/1	1-4094
Fa0/2	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,30,99
Fa0/2	1,10,20,30,99

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,10,20,30,99
Fa0/2	1,10,20,30,99

步驟 8：檢驗交換器之間是否能夠通信。

從 S1 ping S2 和 S3 的管理位址。

```
S1#ping 172.17.99.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms

S1#ping 172.17.99.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.13, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

步驟 9：從 PC2 ping 其它主機。

從主機 PC2 ping 主機 PC1 (172.17.10.21)。ping 是否成功？_____

從主機 PC2 ping 交換器 VLAN 99 IP 位址 172.17.99.12。ping 是否成功？_____

因為這些主機處於不同的子網中，而且在不同的 VLAN 內，所以如果沒有第 3 層設備提供各個子網之間的路由，這些主機將無法通信。

從主機 PC2 ping 主機 PC5。ping 是否成功？_____

因為 PC2 與 PC5 在相同的 VLAN 以及相同的子網中，所以能夠 ping 通

步驟 10：將 PC1 移到與 PC2 相同的 VLAN 中。

連接到 PC2 的連接埠 (S2 Fa0/18) 已配置到 VLAN 20，而連接到 PC1 的連接埠 (S2 Fa0/11) 已配置到 VLAN 10。將 S2 Fa0/11 連接埠重新配置到 VLAN 20。要更改連接埠所屬的 VLAN，無需將連接埠先從原有的 VLAN 中刪除。為連接埠重新配置新的 VLAN 之後，該連接埠將自動從以前的 VLAN 中刪除。

```
S2#configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
S2(config)#interface fastethernet 0/11
S2(config-if)#switchport access vlan 20
S2(config-if)#end
```

從主機 PC2 ping 主機 PC1。ping 是否成功？_____

儘管 PC1 和 PC2 使用的連接埠在同一個 VLAN 中，它們仍然位於不同的子網內，所以不能直接通信。

步驟 11：更改 PC1 的 IP 位址和網路。

將 PC1 的 IP 位址更改為 172.17.20.21。子網路遮罩和預設閘道可以保留不變。使用新配置的 IP 位址再次從主機 PC2 ping 主機 PC1。

ping 是否成功？_____

為什麼這次會成功？

任務 5：記錄交換器設定

在每台交換器上，擷取執行設定並儲存成文字檔，以供將來參考。

任務 6：課後清理

刪除設定，然後重新啟動交換器。拆下纜線並放回儲存處。對於通常連接到其它網路（例如學校 LAN 或 Internet）的 PC 主機，請重新連接相應的纜線並恢復原有的 TCP/IP 設定。