

今天網管人員希望讓有連接使用端(PC-PT)之 Switch，無法任意增減 Vlan，且能夠接收(Switch1 或 Switch4)並更新 Vlan 資訊。另外，也希望 Switch1 之 Vlan 能夠在 PVST 內擔任所有 Vlan 之 Root，而且不允許有新 Switch 加入參與此架構之 PVST。最後，必須確定整個網路架構圖，是否完整能夠彼此相互連通。

實作檢查測試：

1. 將 Switch5 任意連接至架構圖中之 Switch 的介面卡。
2. 在 Switch2 底下加入一台 PC，並將 PC 配置至考官指定之 Vlan 編號。
3. 任意 PC 能 Ping 至此架構圖中之有 IP 的任意設備。

設備密碼：CCNA

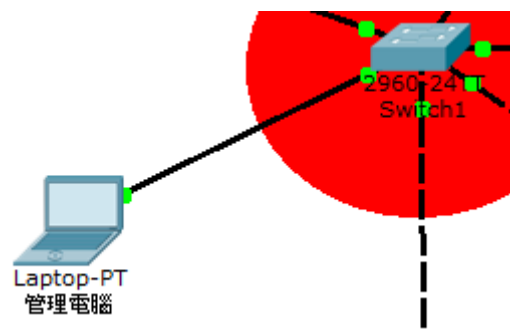
管理 IP：

Switch 1 Vlan 1 192.168.0.1

Switch 4 Vlan 1 192.168.0.2

無法任意增減 Vlan，且能夠接收並更新 Vlan 資訊，屬於 VTP (Vlan Trunk protocol) 之功能，所以現在必須先將架構圖中之 Switch 都設定 VTP。(p.11-6)

首先參考管理 IP 資訊，挑一台能夠 Telnet 進入的 Switch，將 PC 連接至該臺 Switch(圖一)。



(圖一)

連接完畢後，使用 Command Telnet 進入至所連接之 Switch(圖二)。

```
PC>telnet 192.168.0.1
Trying 192.168.0.1 ...Open

User Access Verification

Password:
Switch1>en
Switch1>enable
Password:
Switch1#
```

(圖二)

進入到特權模式(Enable)後，先查看 VTP 是否有無相關設定(圖三)。

```
Switch1#show vtp status
VTP Version                : 2
Configuration Revision      : 4
Maximum VLANs supported locally : 255
Number of existing VLANs    : 7
VTP Operating Mode          : Server
VTP Domain Name             : TestVlan
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0xA9 0x42 0x5E 0x2C 0xA4 0x91 0x2F 0xEB
Configuration last modified by 0.0.0.0 at 3-1-93 00:28:59
Local updater ID is 192.168.0.1 on interface Vl1 (lowest numbered VLAN interface found)
```

(圖三)

查看後，發現有設定 VTP Domain Name 為 TestValn，並且此台設備為 Server。而 VTP 要正常運作，**VTP 必須設定名稱以及密碼**。所以可以檢查是否有無設定密碼，或是直接新設定 VTP 密碼(圖四)。

```
Switch1#show vtp password
VTP Password: CCNA
Switch1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)#vtp password 輸入想要的密碼
```

(圖四)

接下來，必須確認架構圖中**每一台 Switch VTP 之設定名稱使否相同，與密碼是否有無設定**。因此需要找出其它 Switch 之管理 IP，才能夠 Telnet 進入到 Switch 查看以及更改

找尋設備的方式有：

1. show cdp entry * (圖五)，用此方式可以找出連接周邊所連接之設備 IP，以及相關資訊。

```
Switch1#show cdp entry *  
  
Device ID: Switch4  
Entry address(es):  
  IP address : 192.168.0.2  
Platform: cisco 2960, Capabilities: Switch  
Interface: FastEthernet0/21, Port ID (outgoing port): FastEthernet0/22  
Holdtime: 145  
  
Version :  
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)  
Copyright (c) 1986-2005 by Cisco Systems, Inc.  
Compiled Wed 12-Oct-05 22:05 by pt_team
```

(圖五)

2. ping 255.255.255.255(圖六)，用此方式探索能看到之設備 IP(含 PC)。

```
Switch1#ping 255.255.255.255  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 255.255.255.255, timeout is 2 seconds:  
  
Reply to request 0 from 192.168.0.2, 0 ms  
Reply to request 0 from 192.168.10.1, 0 ms  
Reply to request 0 from 192.168.10.254, 0 ms  
Reply to request 0 from 192.168.10.250, 0 ms  
Reply to request 0 from 192.168.10.251, 0 ms  
Reply to request 0 from 192.168.0.101, 0 ms  
Reply to request 0 from 172.16.16.250, 0 ms  
Reply to request 0 from 192.168.10.2, 0 ms  
Reply to request 0 from 172.16.16.1, 0 ms  
Reply to request 0 from 172.16.16.251, 0 ms  
Reply to request 0 from 172.16.16.2, 0 ms
```

(圖六)

有了設備之 IP，就可以 Telnet 進入至其它之 Switch 設備，並做 VTP 之相關設定。

然而題目也有要求『希望連接使用端(PC-PT)之 Switch，無法任意增減 Vlan』，麼必須將 Switch2 & Switch3 VTP Operating mode 設置為 Client(圖七)。

```
Switch2#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch2(config)#vtp mode client  
Device mode already VTP CLIENT.  
Switch2(config)#
```

(圖七)

自我檢查：

1. Switch2#show vtp status 檢查名稱以及模式。
2. Switch2#show vtp password 檢查密碼是否設定正確。
3. 可在 Server 試著新增新 Vlan，查看其它設備是否有更新。
4. 可在 Client 試著新增新 Vlan，將會無法新增。

注意事項：

1. 用到 VTP 之設備彼此連接之線路，必須設定為 Trunk。
2. 必須設定名稱(需相同)以及密碼，才會正常傳送 VTP 更新封包。
3. 最少必須有一台 Server。

Switch1 能夠在 PVST(Pre Vlan Spanning Tree)內擔任所有 Vlan 之 Root 。
則必須更改各個 Vlan 之 BID Priority，或者是使用手動設定。(p.11-33)

先進入至 Switch 之特權模式，去查看 STP 之設定，檢查 Switch 各 Vlan 是否為此 Vlan 之 Root。如果 Root ID Address 與 Bridge ID Address 相同，代表此 Switch 之 Vlan 為 Root(圖八)。

```
Switch1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    20481
             Address     00D0.D342.703C
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    20481 (priority 20480 sys-id-ext 1)
             Address     00D0.D342.703C
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface    Role Sts Cost      Prio.Nbr Type
-----
Fa0/21       Desg FWD 19        128.21   P2p
Fa0/23       Desg FWD 19        128.23   P2p
Fa0/24       Desg FWD 19        128.24   P2p
Fa0/2        Desg FWD 19        128.2    P2p
Fa0/1        Desg FWD 19        128.1    P2p
```

(圖八)

檢查後，發現 Vlan20 並未成為此 Vlan 之 Root(圖九)。

```
VLAN0020
Spanning tree enabled protocol rstp
Root ID    Priority    24596
           Address    0001.4362.6436
           Cost        19
           Port        21(FastEthernet0/21)
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID   Priority    28692 (priority 28672 sys-id-ext 20)
           Address    00D0.D342.703C
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time  20
```

(圖九)

改變 STP Root 方式：

1. Spanning-tree vlan 20 priority <0-61440>(圖十)，用此方法設定 Vlan 之 priority。要將 Vlan20 變成 Root，priority 就必須比現在之 Root 之 priority 還小。

```
Switch1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)#spanning-tree vlan 20 priority 1
% Bridge Priority must be in increments of 4096.
% Allowed values are:
   0      4096  8192  12288  16384  20480  24576  28672
 32768  36864  40960  45056  49152  53248  57344  61440
Switch1(config)#spanning-tree vlan 20 priority
```

(圖十)

2. Spanning-tree vlan 20 root primary(圖十一)，用此方法直接指定為 STP 此 Vlan 之 Root。

```
Switch1(config)#spanning-tree vlan 20 root primary
```

(圖十一)

設定完後，再檢查一次是否成功變成 Root(圖十二)。

```
VLAN0020
Spanning tree enabled protocol rstp
Root ID    Priority    20500
           Address    00D0.D342.703C
           This bridge is the root
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID   Priority    20500 (priority 20480 sys-id-ext 20)
           Address    00D0.D342.703C
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time  20
```

(圖十二)

自我檢查：

1. Switch#show spanning-tree 檢查 STP 各 Vlan 之 Root。

不允許有新 Switch 加入參與此架構之 PVST，則是讓架構圖內之 Switch 阻擋 BPDU，所以必須將沒用到之介面，設定 BPDU Guard。(p.11-55)

再設定 BPDU Guard 之前，必須先確認哪幾個介面卡是連接目前的 Switch(圖十三)，以免誤設定，造成介面卡 Error disable。而連接至本地端的介面為 Interface。

```
Switch1#show cdp entry *  
  
Device ID: Switch4  
Entry address(es):  
  IP address : 192.168.0.2  
Platform: cisco 2960, Capabilities: Switch  
Interface: FastEthernet0/21, Port ID (outgoing port): FastEthernet0/22  
Holdtime: 129
```

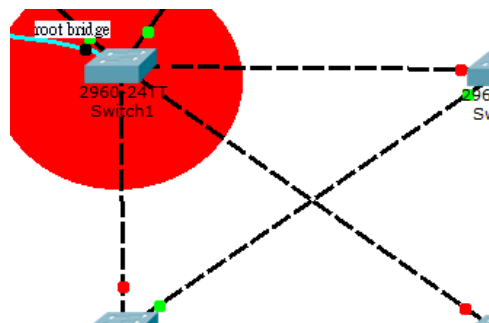
(圖十三)

確認後，就將沒用到之介面卡設定 BPDU Guard。而這裡示範的是，先將所有的介面都設定 BPDU Guard(圖十四)。

```
Switch1#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch1(config)#interface range fastEthernet 0/1-24  
Switch1(config-if-range)#spanning-tree bpduguard enable
```

(圖十四)

這時候有連接 Switch 之介面卡，會變成 Error disable(圖十五)。



(圖十五)

檢視介面卡資訊也會寫說 Error disable(圖十六)

```
Switch1#show interfaces fastEthernet 0/21
FastEthernet0/21 is down, line protocol is down (err-disabled)
```

(圖十六)

如果變成 Error disable，那麼必須進入到介面卡內，將 BPDU Guard 停用，然後再將介面關閉重啟(圖十七)，這樣就能夠正常使用。

```
Switch1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#interface fastEthernet 0/21
Switch1(config-if)#spanning-tree bpduguard disable
Switch1(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively d
own
Switch1(config-if)#no shutdown

Switch1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state
to up
```

(圖十七)

注意事項：

1. 因 BPDU Guard 停用的介面，必須關閉再開啟，才能正常使用。
2. BPDU Guard 是針對 Switch 所使用，其它設備不會影響。

最後必須**確定整個網路架構圖，是否完整能夠彼此相互連通。**

自我檢查：

1. 單臂路由設置是否完整。
2. 設備 Default gateway 是否設定。
3. Switch 介面模式設定是否正確。