Vlan、Switch、Routing、NAT
原理與實作

大綱

- VLAN 原理
- Cisco Packet Tracer 使用介紹
- VLAN LAB 模擬
  - 設定VLAN
  - 設定Trunk
  - 廣播風暴
  - 啟用STP防止接線迴圈

什麼是 VLAN

為什麼需要它

VLAN 虛擬區域網路

- 實做於區域網路交換器 (Switch) 上的網路管理技術。

- VLAN 的好處
  - 隔開廣播領域。
  - 提昇頻寬的利用率。
  - 降低延遲。
  - 增加安全性。 (適當的規劃 VLAN 時)

VLAN 的實作方式

- 實體層 (Layer 1)
  - 交換機上的網路埠。
- 資料連結層 (Layer 2)
  - MAC Address 。
- 網路層 (Layer 3)
  - IP Address 。
- 應用層 (Layer 4~7)
  - 登入的身份。

本課程用 Layer 1 VLAN 來說明 VLAN 的概念。

廣播領域 (Broadcast Domain)

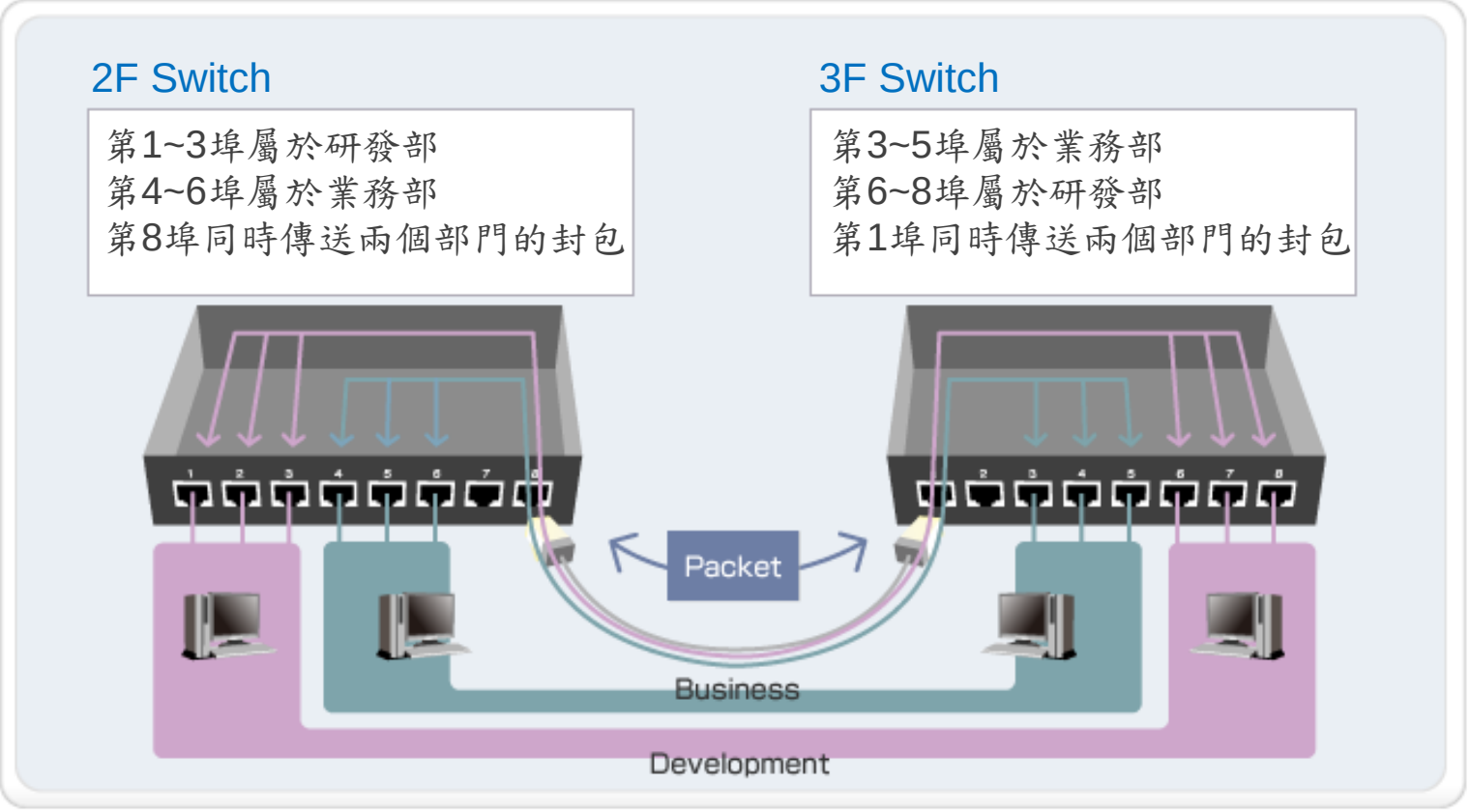
- 任意一個節點可以在 Layer 2 通過廣播的方式到達任意一個節點。
- 廣播風暴
  - 過多的廣播封包消耗了大量的網路頻寬。
  - 通常是由於網路回圈 (Loop)、網卡故障、病毒等引起的。
- Ethernet Broadcast 應用例
  - ARP
  - DHCP

VLAN 原理

Application 應用層	• 使用者所使用的應用程式或網頁
Presentation 表現層	• 資料的壓縮、解壓縮以及加解密等
Session 會談層	• 連線的建立與結束、資料的傳輸模式(全/半雙工)
Transport 傳輸層	• 流量控制、傳輸的可靠性
Network 網路層	• 定址及路由
Data Link 資料鏈結層	• 介質存取控制的方法以及定址
Physical 實體層	• 訊號傳送的介質規格、訊號編碼與轉換

虛擬區域網路（Virtual LAN, VLAN）

- 使用 VLAN 可以做到如下圖的效果，並且兩個部門彼此間不相互連通：



VLAN的特色

- 縮小廣播範圍:利用Switch適當地切割不同的VLAN，可以有效地阻擋過大的廣播網域(broadcast domain) 與廣播型病毒攻擊，並提升PC與網路效能。

- 安全上的考量:部分單位擁有較多的機敏資料，不宜被其他部門所瀏覽，切割VLAN是區隔部門的好方法。

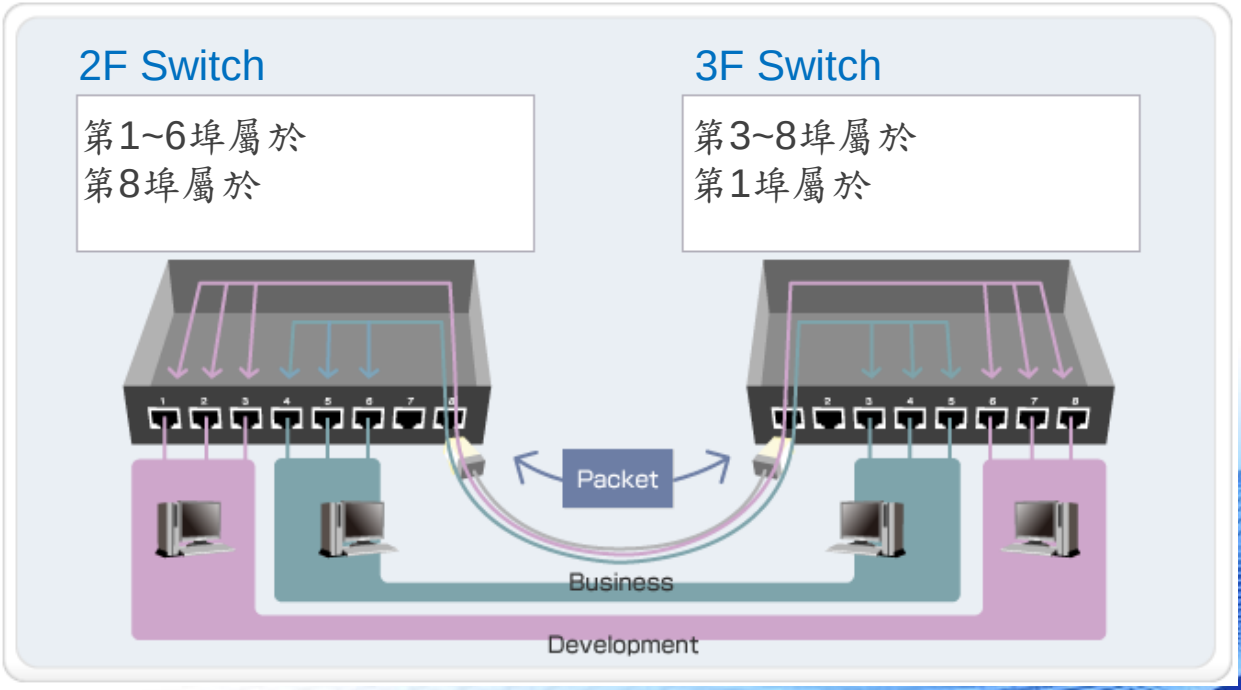
⇨除非透過路由器否則不同的 VLAN 彼此之間無法互相通訊

- 頻寬管理:部分服務需要高頻寬低延遲，例如:IP Phone，利用VLAN切割後再設定適當的QOS，可以避免被其他網路流量所干擾。

- 方便靈活:只要設定交換器連接埠至適當的 VLAN，就可以增加、移動或改變網路。VLAN 可以視為依照功能劃分的群組，與設備實際上的物理或地理位置無關。

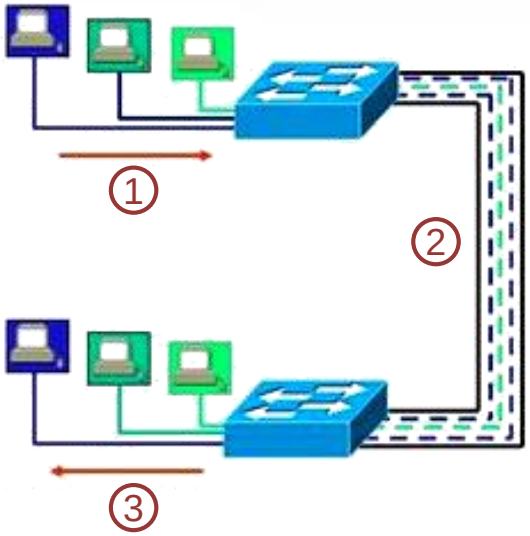
VLAN的運作方式（1/4）

- 在 VLAN 交換環境中，交換器的連接埠分為兩種類型
  - Access port：
    此類連接埠只屬於一個 VLAN，進入連接埠的訊框都會被視為屬於該VLAN
  - Trunk port：
    能夠轉發多個不同 VLAN 的訊框



VLAN的運作方式（2/4）

- 訊框在兩台交換器之間傳輸的狀況：



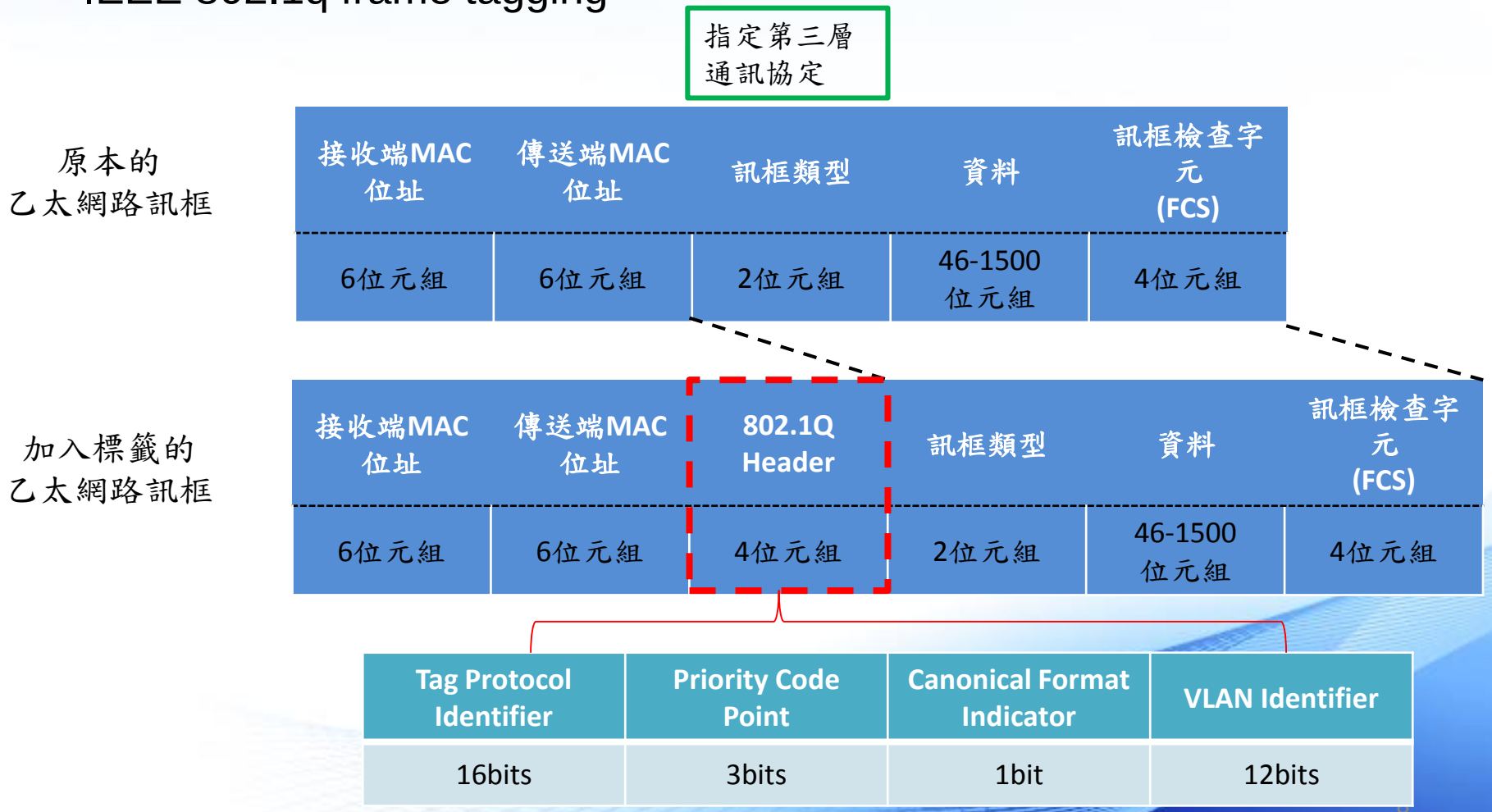
① 訊框進入 access port 之後，交換器會幫每個訊框貼上標籤（格式定義於 IEEE 802.1q ），其中包含了 VLAN 的識別資訊

② 如果兩台交換器都有正確設定 trunk port，被貼了標籤的訊框就會經由 trunk link 傳輸到另一台交換器

③ 交換器檢查訊框中 VLAN 的識別資訊，只在對應的 access port 送出訊框，並在訊框送出之前把標籤去掉

VLAN的運作方式（3/4）

- IEEE 802.1q frame tagging



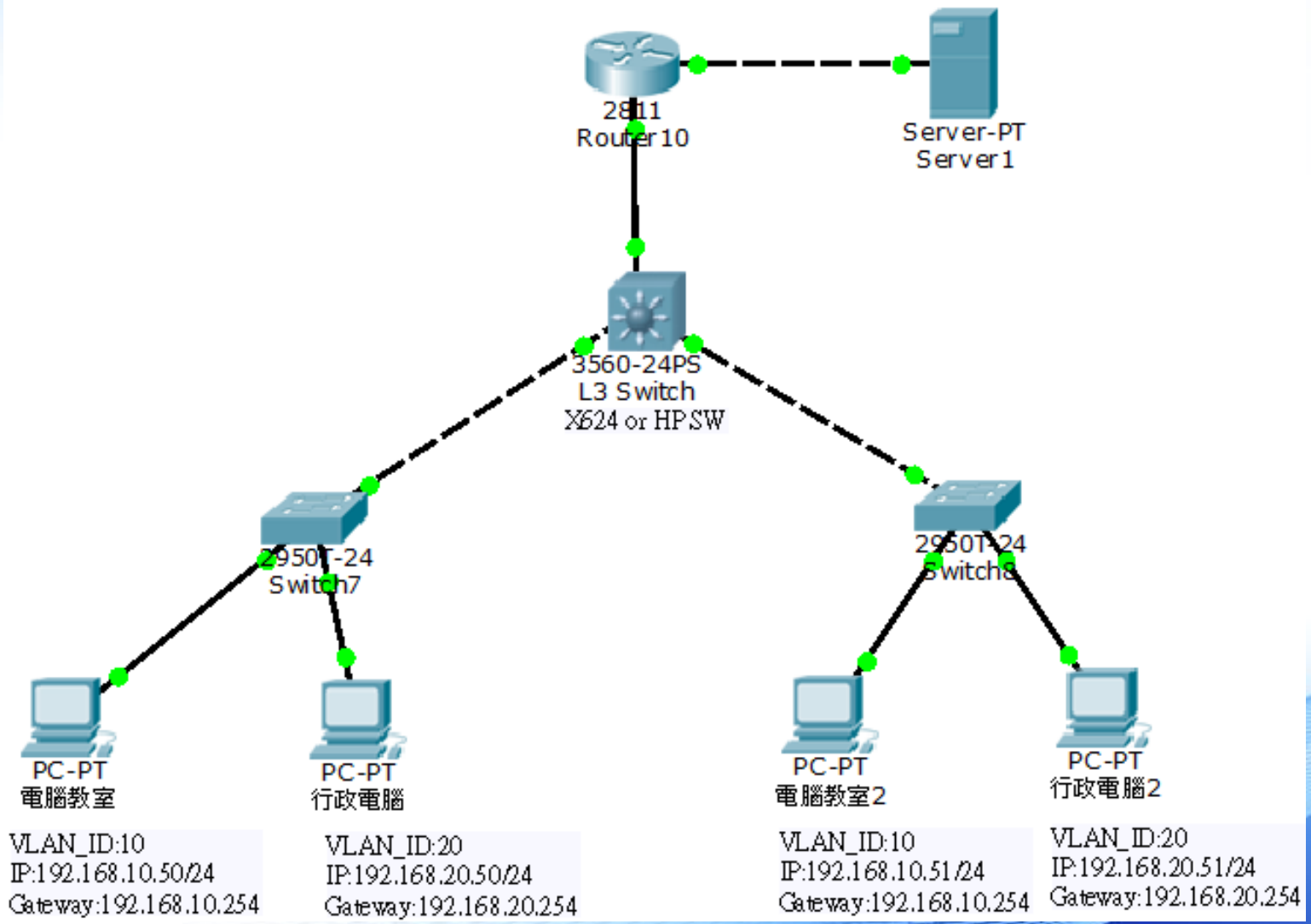
VLAN的運作方式（4/4）

- 原生 VLAN (Native VLAN)
  - VLAN ID 為 1 的 VLAN 被稱為原生 VLAN
  - 交換器的初始設定會把所有通訊埠都加入原生 VLAN
  - 原生 VLAN 可以承載未貼標籤的訊框

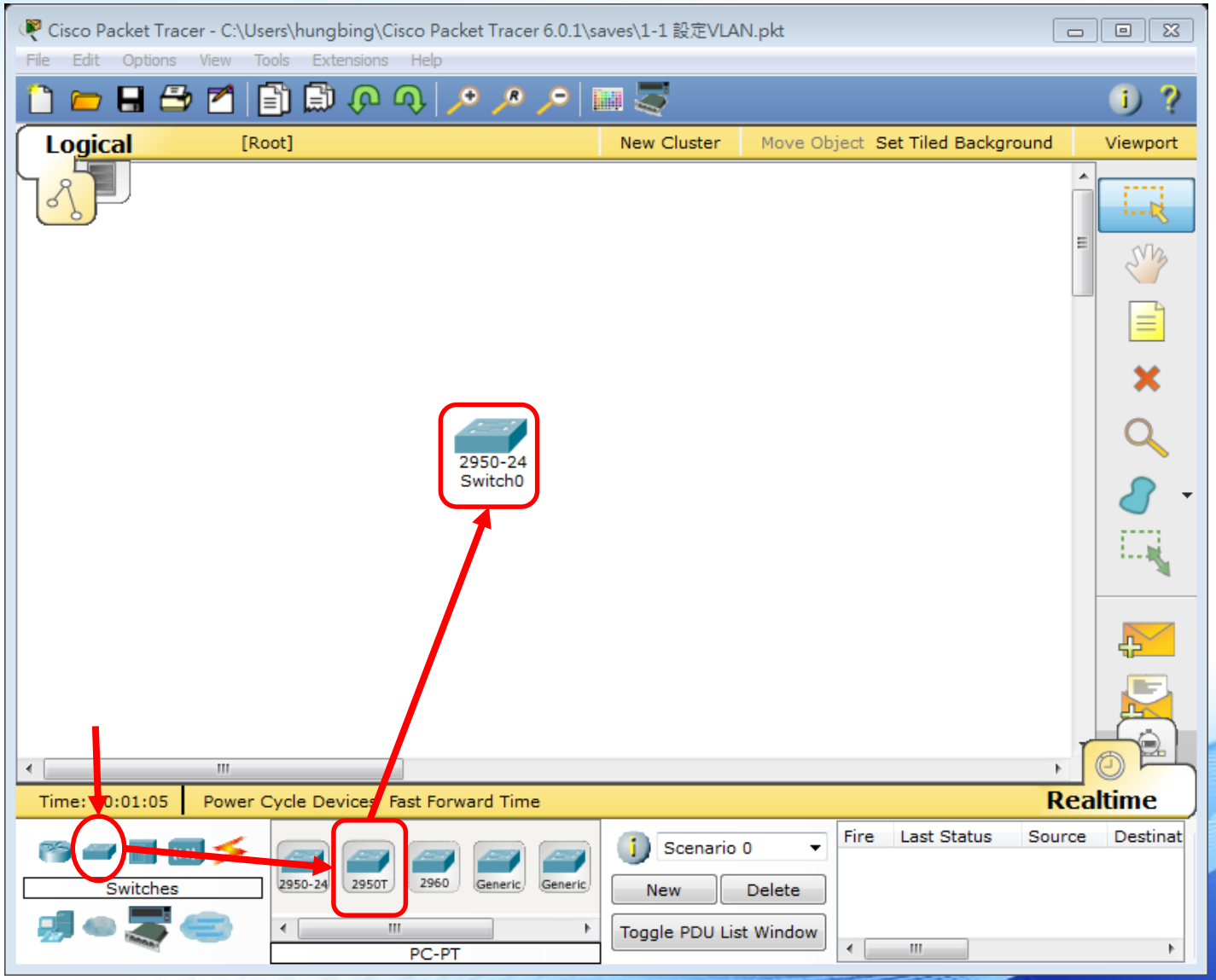
- VLAN 的管理：
  - Static VLANs：
    由網路管理員手動設定哪些埠是屬於哪個 VLAN
  - Dynamic VLANs：
    由軟體管理，可以根據 MAC位址、通訊協定甚至應用程式種類來決定該設備被劃分到哪個 VLAN

Cisco Packet Tracer 使用介紹

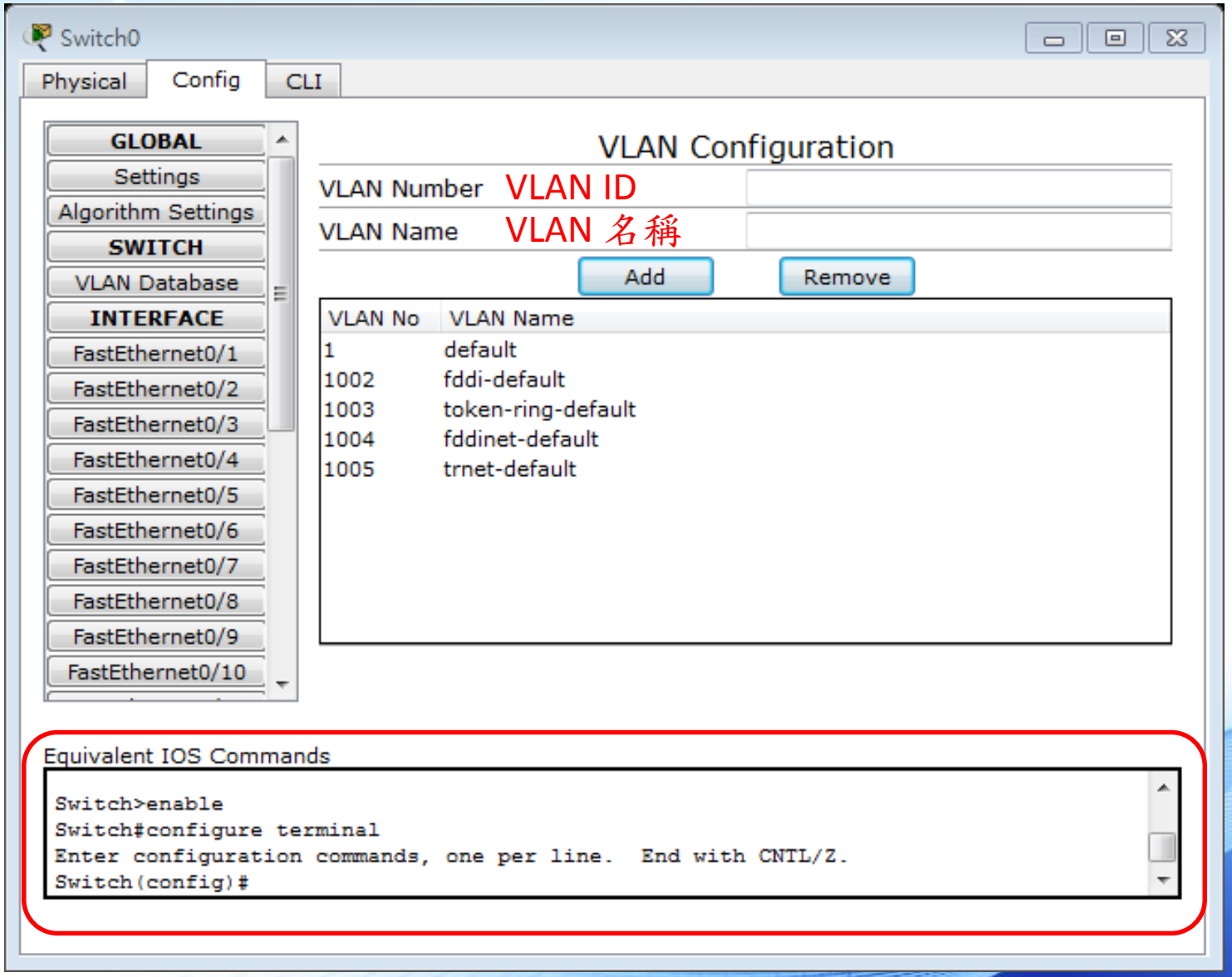
VLAN LAB 模擬－網路拓樸



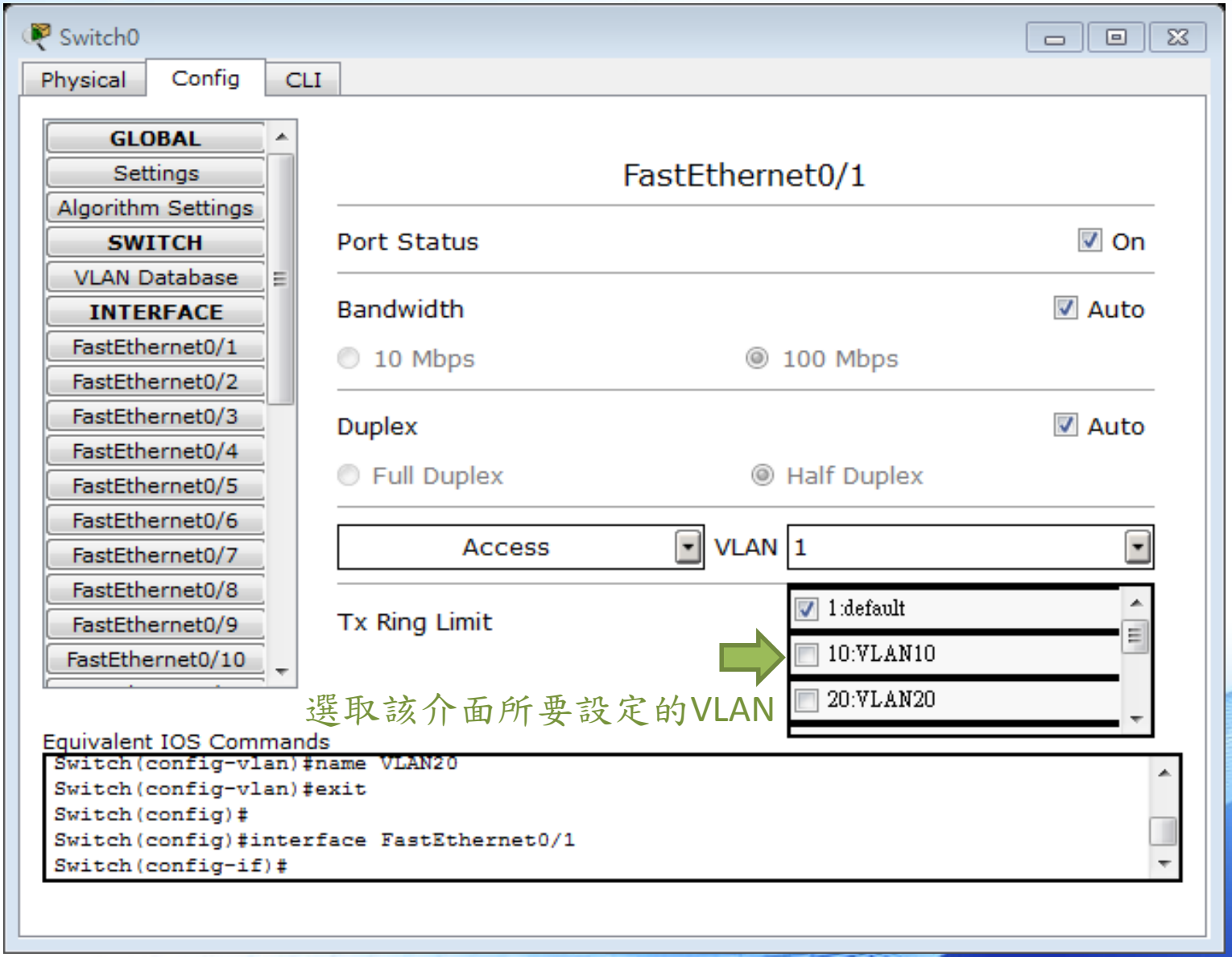
VLAN LAB 模擬--設定VLAN



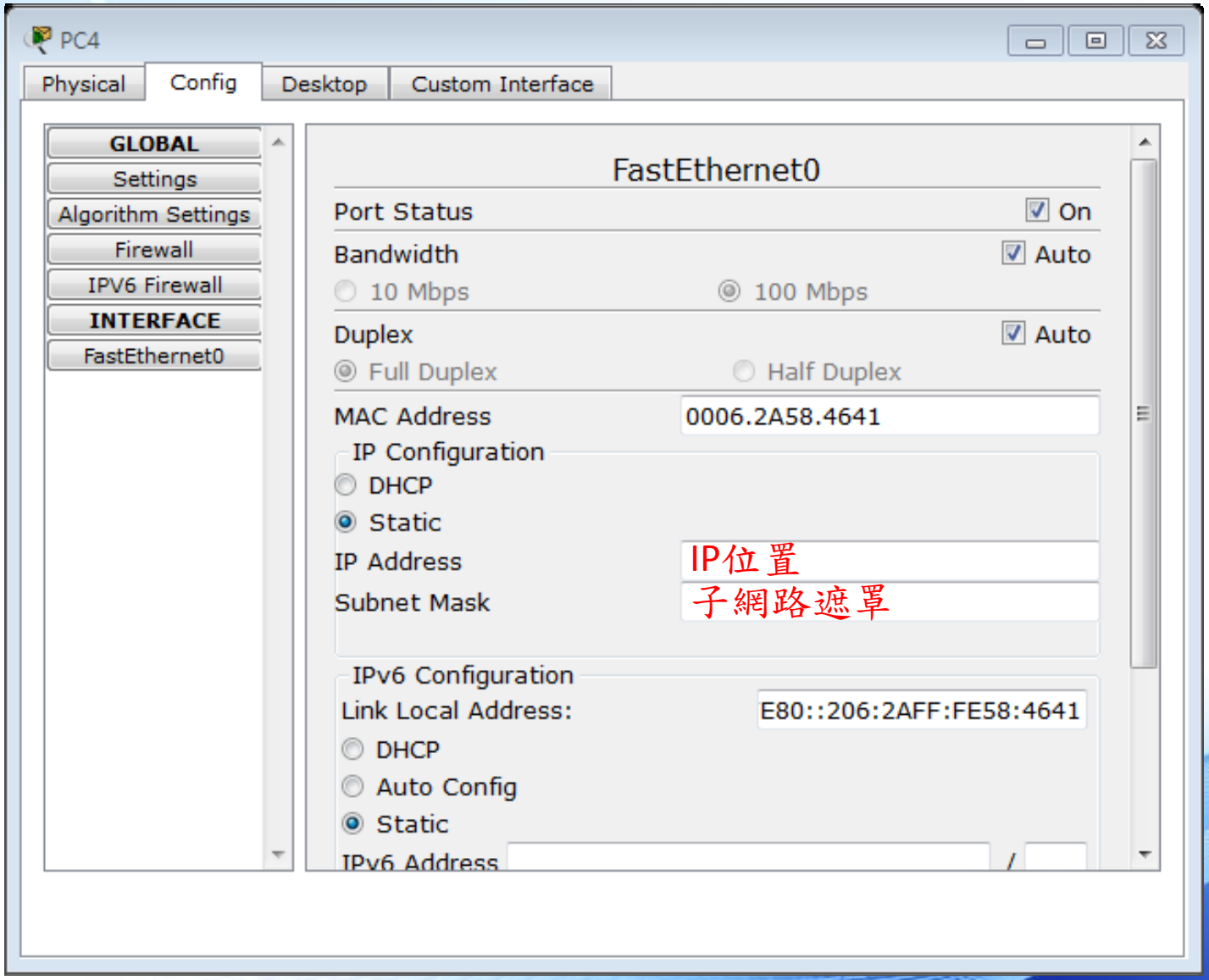
VLAN LAB 模擬--設定VLAN



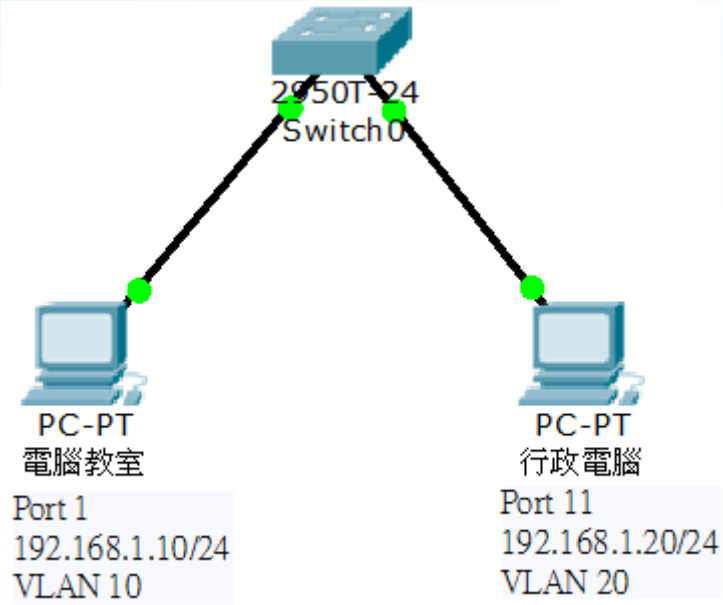
VLAN LAB 模擬—Port 指定VLAN



LAB 1 – 測試VLAN

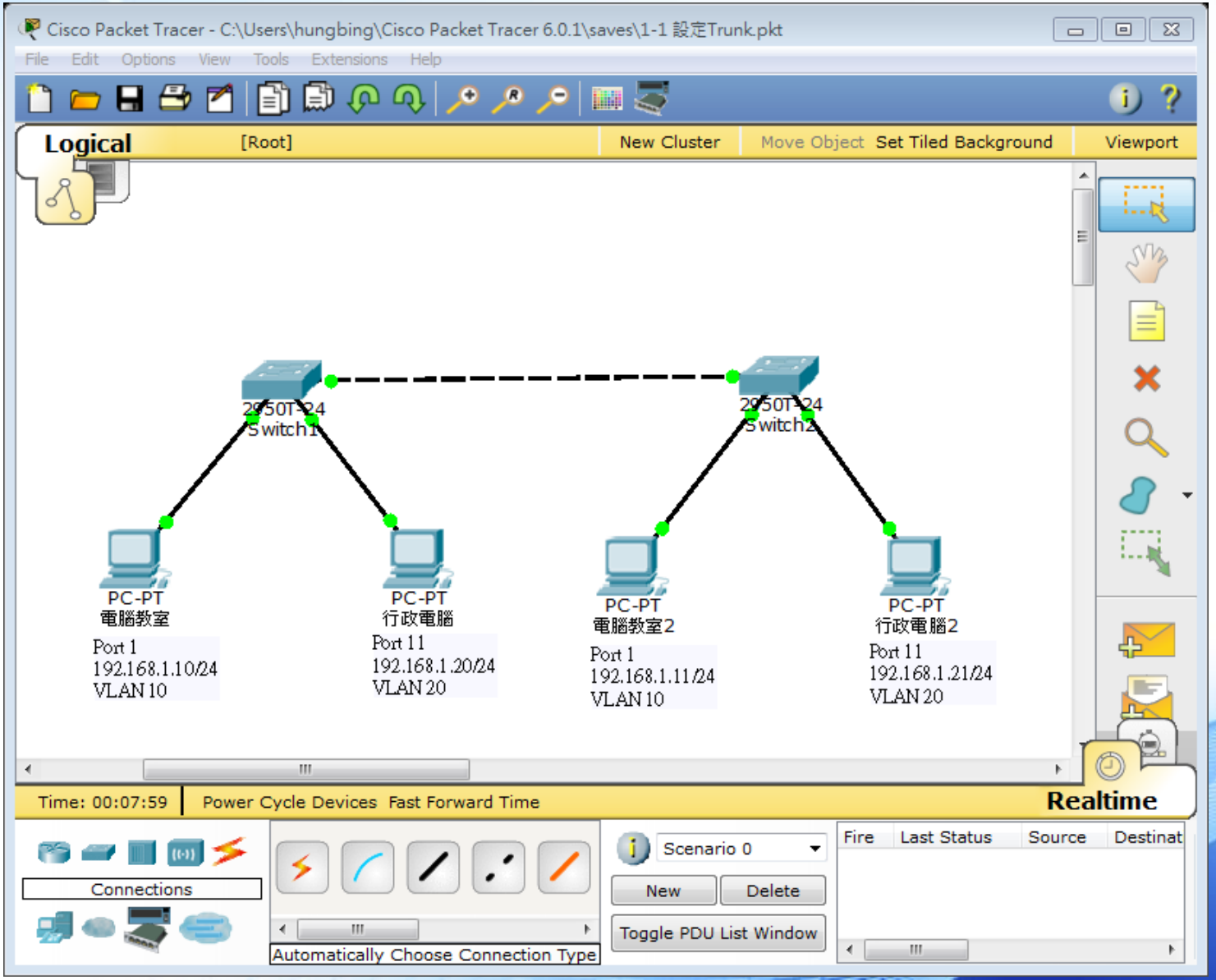

PC4
Physical
Config
Desktop
Custom Interface
GLOBAL
Settings
Algorithm Settings
Firewall
IPV6 Firewall
INTERFACE
FastEthernet0
FastEthernet0
Port Status
On
Bandwidth
Auto
10 Mbps
100 Mbps
Duplex
Auto
Full Duplex
Half Duplex
MAC Address
0006.2A58.4641
IP Configuration
DHCP
Static
IP Address
IP位置
Subnet Mask
子網路遮罩
IPv6 Configuration
Link Local Address:
E80::206:2AFF:FE58:4641
DHCP
Auto Config
Static
IPv6 Address

LAB 1 – 測試VLAN



- 兩台電腦互相ping 對方，是否能ping 通?
- 如果想要想互相Ping的通，有哪些做法呢?

LAB 2 – 設定Trunk



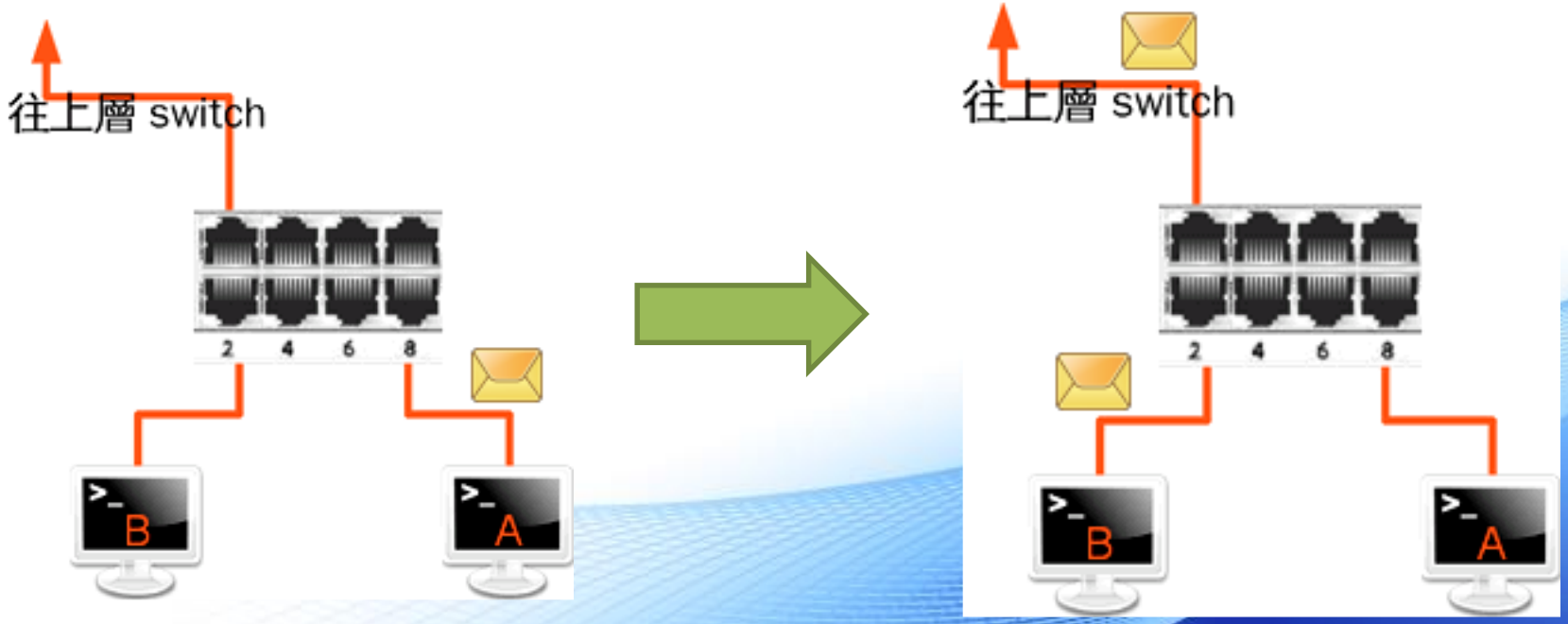
LAB 2 – 設定Trunk

- 兩邊的電腦教室電腦是否已互相Ping的到?
- 兩邊的行政電腦與電腦教室是否Ping的到?
- 有沒有方法可以不用Trunk,卻可以達到同樣的效果呢?

廣播風暴

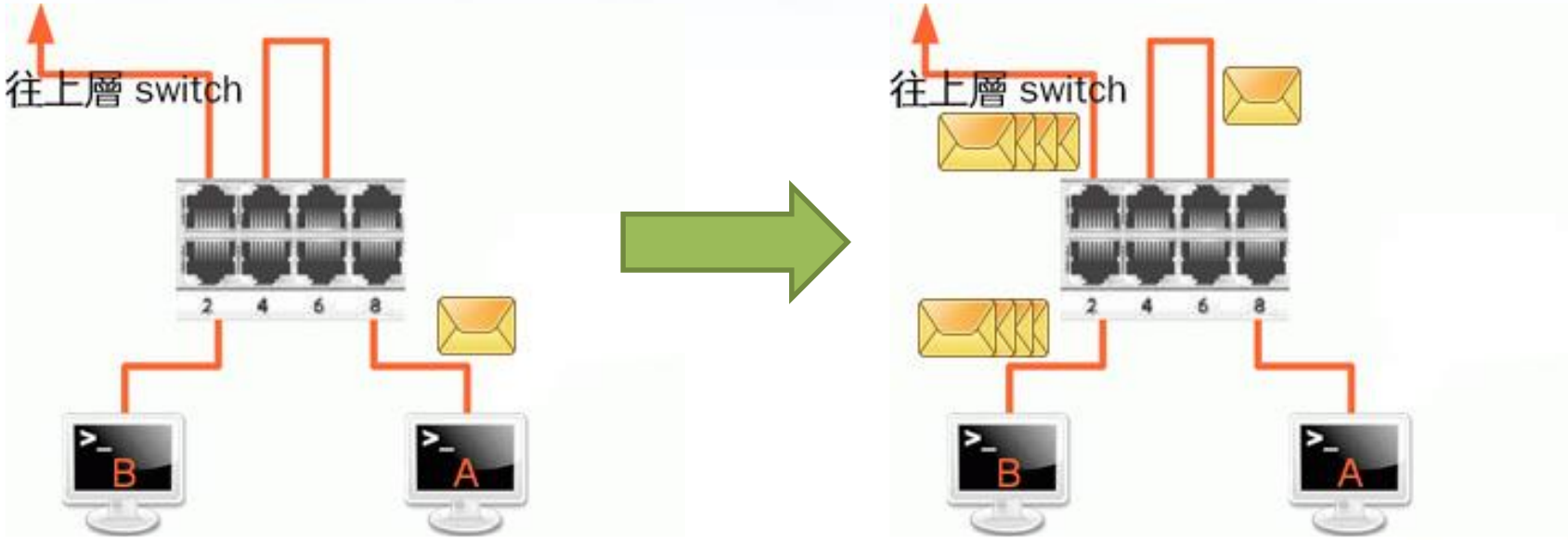
- 動態主機組態協定(DHCP)以及位址解析協定(ARP)會使用目的地MAC位址為FF:FF:FF:FF:FF:FF的廣播封包，而交換器會在所有連接埠上發送這種廣播封包

- 假設A設備和B設備接在一個交換器上，這個交換器再往上接到上一層的交換器，正常狀況下，當A設備對外發送廣播封包時：



廣播風暴

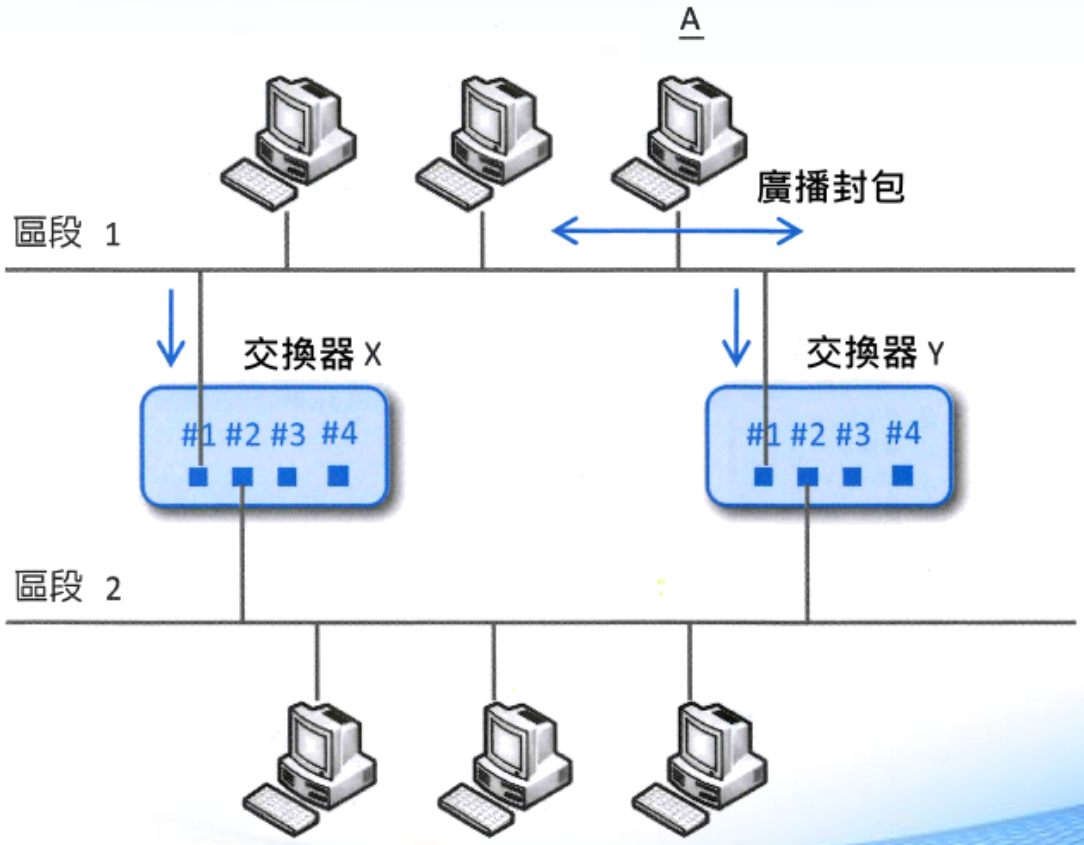
- 接線迴圈(loop)下，當A設備對外發送廣播封包時：

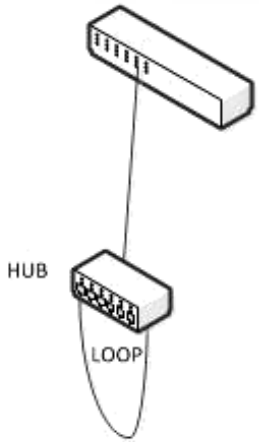


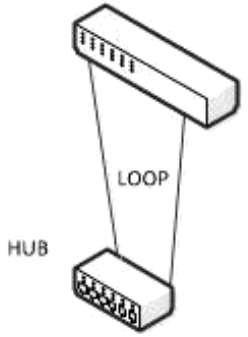
  - 5號埠發出去的封包，會經由網路線從3號埠回到交換器
  - 交換器收到廣
  - 播封包又會再送一次，只要兩者之間的網路線不拔掉，交換器會一直廣播這個廣播封包
  - 那堆廣播封包會往外丟到其他的設備或交換器上，造成網路癱瘓

防止接線迴圈 (1/2)

- 有時候要查出接線迴圈並不容易：

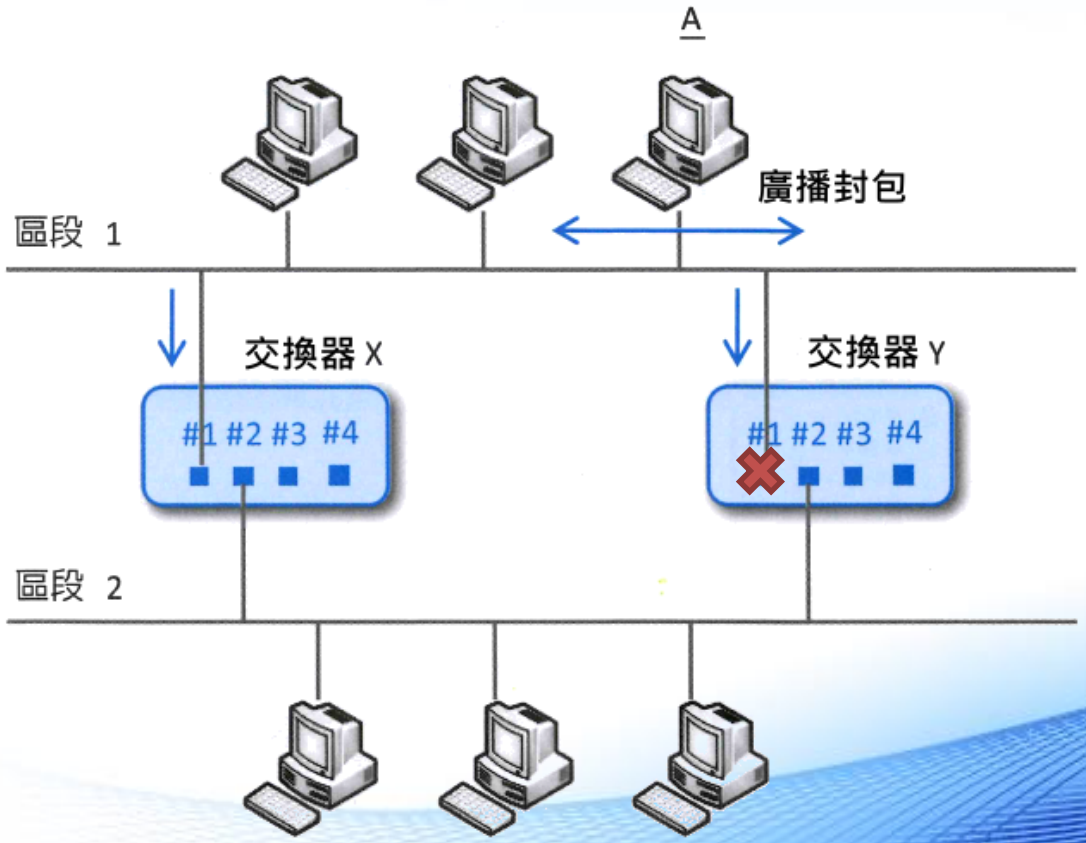






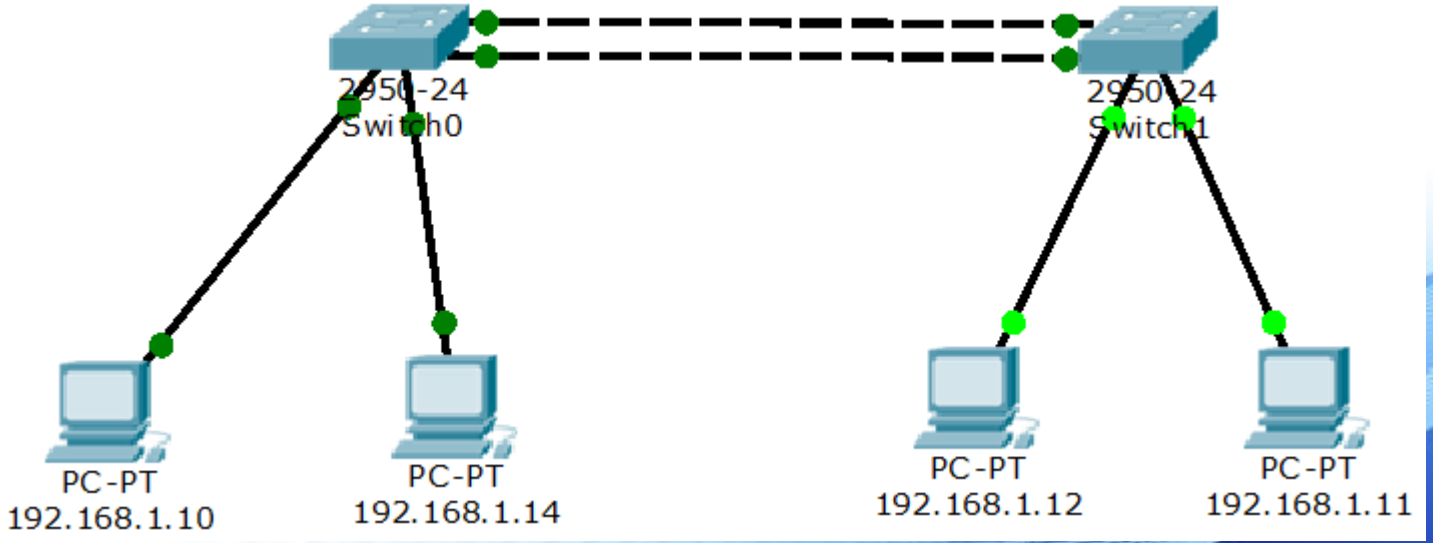
防止接線迴圈 (2/2)

- 使用支援 Spanning Tree Protocol (STP, IEEE 802.1d) 的交換器，這類交換器使用 Spanning Tree 演算法來避免產生接線迴圈：



LAB 3 –廣播風暴

- 因Switch預設會開啟SPT(Spanning Tree Protocol)，故該實驗先將該功能關閉。
  - enable(進入特權模式)
  - conf t(進入config 模式)
  - no spanning-tree vlan 1(關閉STP)
- 利用模擬工作區，查看封包傳遞狀況，以及利用ping看看是否如上述理論。



LAB 4 –開啟STP

- 因Switch預設會開啟STP(Spanning Tree Protocol)，故該實驗先將該功能關閉。
  - enable(進入特權模式)
  - conf t(進入config 模式)
  - spanning-tree vlan 1(開啟STP)
- 利用Ping，查看ICMP傳遞狀況。