

網路基礎班

011100

01 011100

0 01 011100

111 00 0 01 011100

100 1 0 111 00 0 01 011100

111 00 0 01 011100

0 1100

1100 1 0 111 00 0 01 011100

大綱

- 常遇到的學校網路問題
 - LOOP 迴圈說明
 - Data Link 資料鏈結層
 - Arp 基本介紹 與封包傳送原理
 - VLAN 基本介紹
 - DHCP
 - DHCP Spoof Attacks
- Cisco Packet Tracer 網路封包虛擬器
 - 介面使用介紹
 - 廣播風暴
 - DHCP 封包觀察
 - DHCP Spoof Attacks

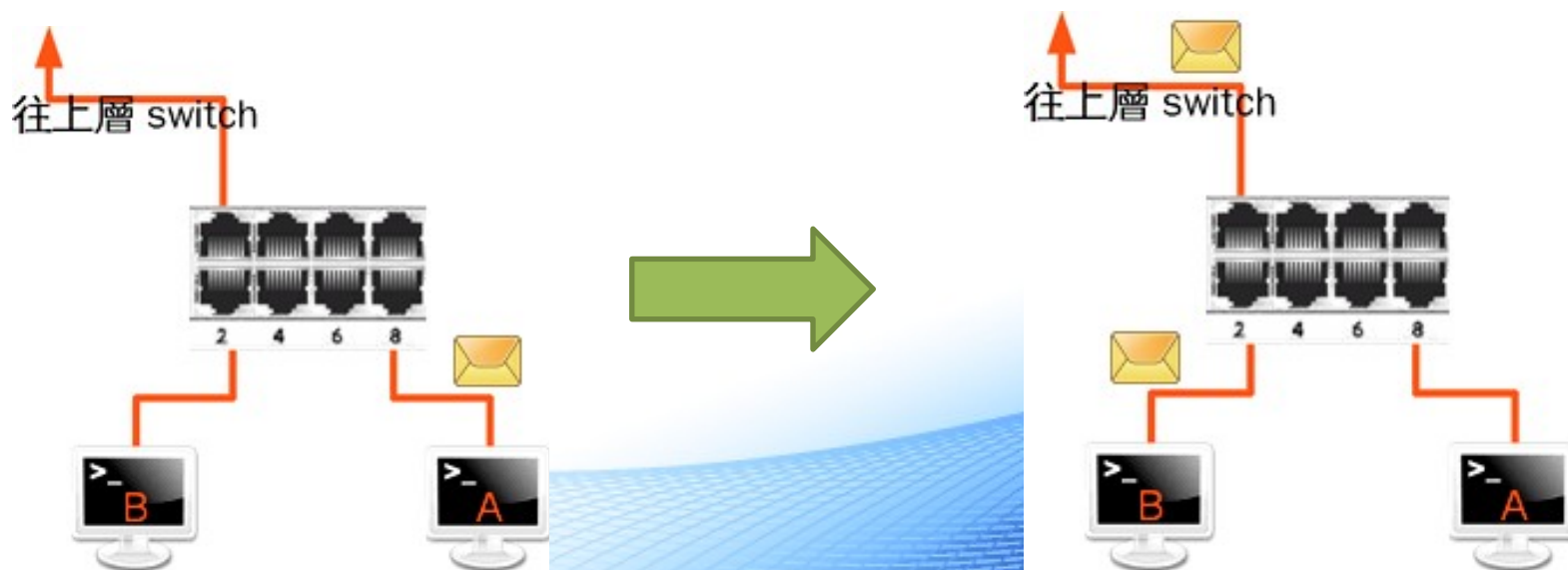


LOOP 迴圈

- LOOP 迴圈到底為什麼讓人心煩？
- 可能發生 LOOP 迴圈的三種狀況
 - 廣播風暴
 - 發送多個重複資料
 - MAC 位址資料庫不一致

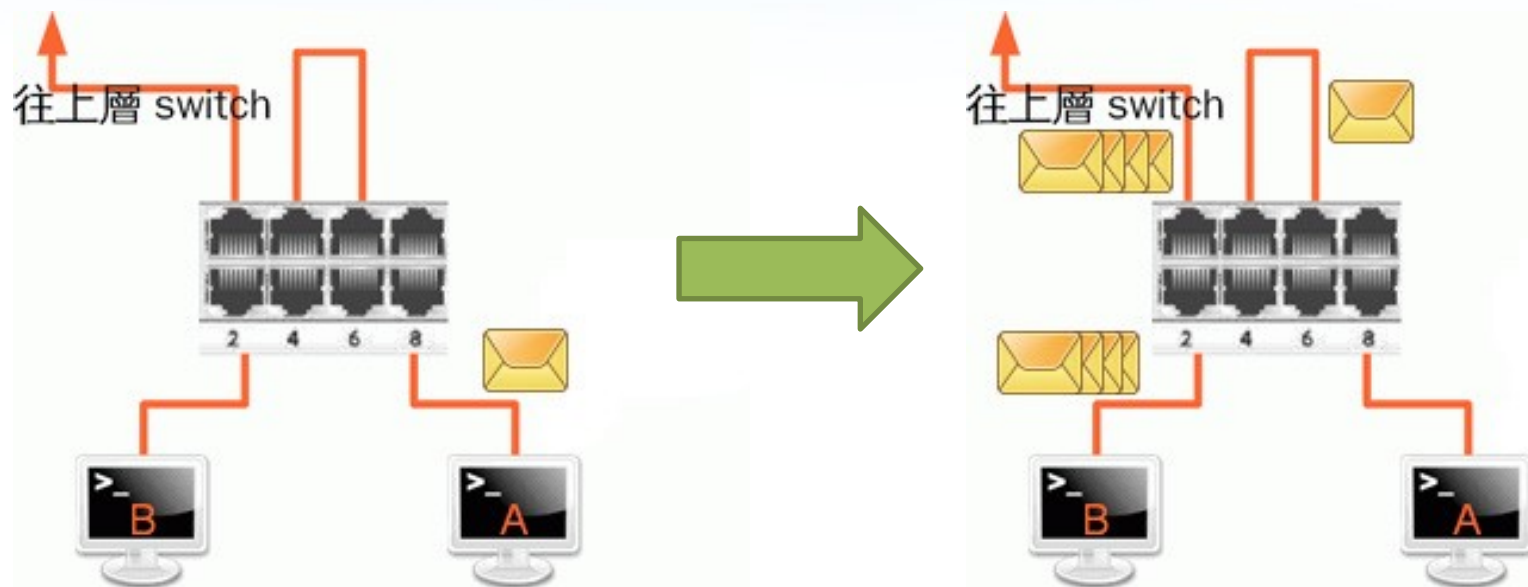
廣播風暴

- 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：



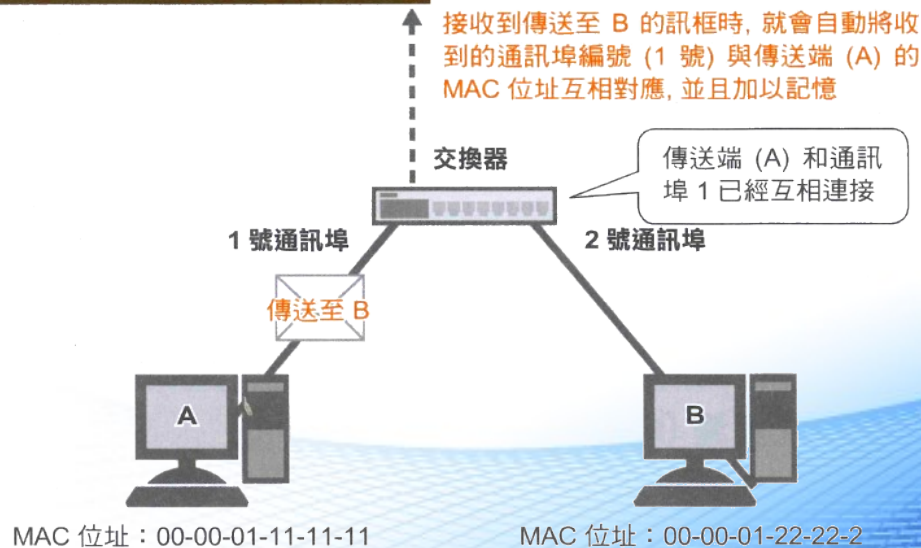
- 5 號埠發出去的封包，會經由網路線從 3 號埠回到交換器
- 交換器收到廣播封包
- 又會再送一次，只要兩者之間的網路線不拔掉，交換器會一直廣播這個廣播封包
- 那堆廣播封包會往外丟到其他的設備或交換器上，造成網路癱瘓

交換器 – Switch (1/4)

- 訊號衝突會嚴重影響傳輸效率，必須設法減少衝突的可能性
- 交換器對於訊息的傳輸會經過三個步驟，以達到切割衝突域 (Collision Domain)，減少衝突發生的目的
 - 1. 發現 (Discovery)：學習並紀錄每個通訊埠所連接網路設備的 MAC

MAC 位址表

通訊埠	MAC 位址
1號	00-00-01-11-11-11

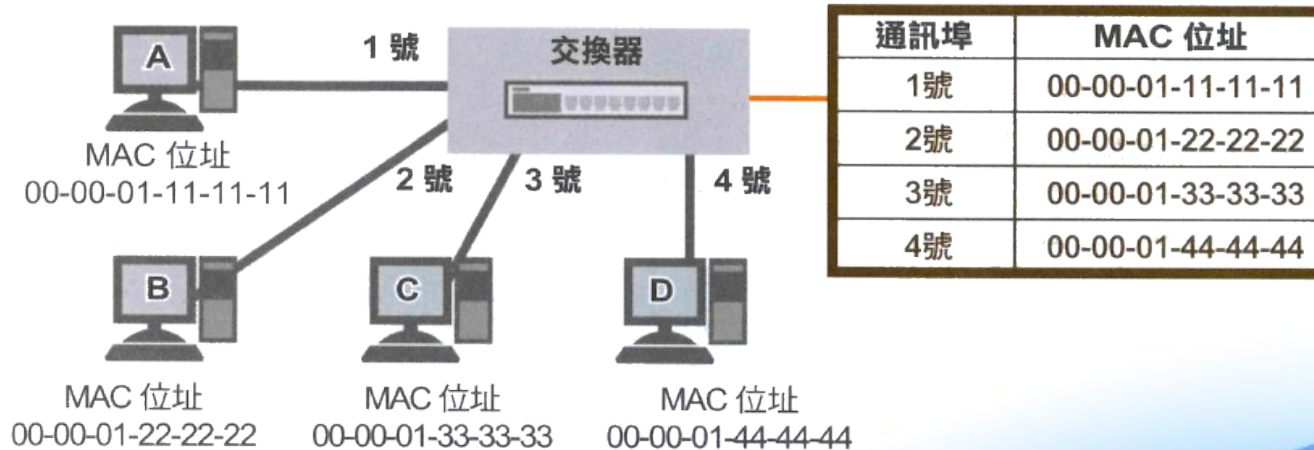


交換器 – Switch (2/4)

- 2. 過濾 (Filtering)：交換器發現來源端與目的端位於相同通訊埠時，就會把封包濾掉或擋掉。

3. 轉送 (Forwarding)：

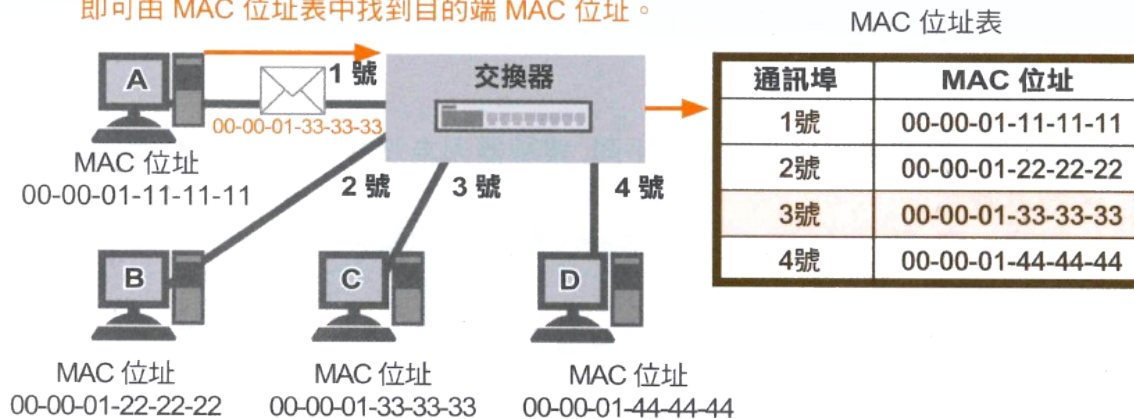
① MAC 位址表記錄著通訊埠，與該通訊埠所連接的節點的 MAC 位址間的對應關係。



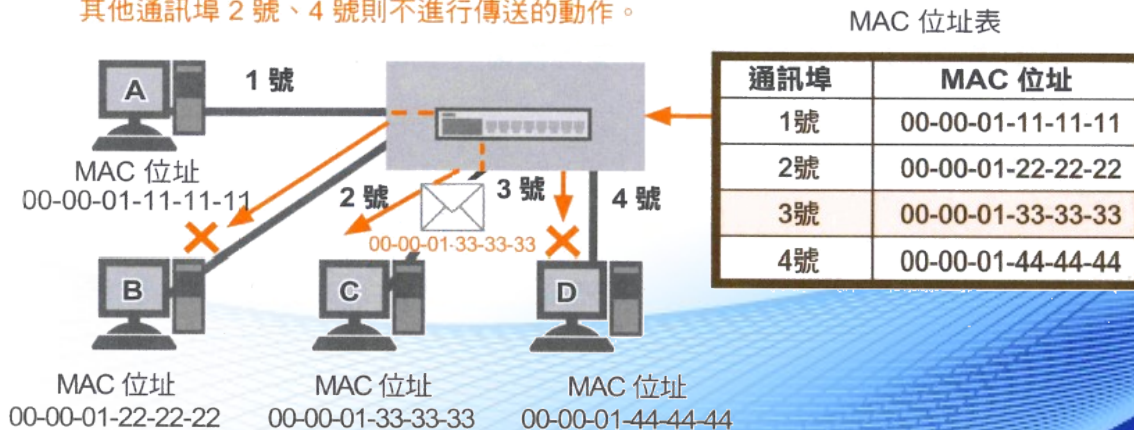
交換器 - Switch (3/4)

– 3. 轉送 (Forwarding) :

② 當訊框被送達交換器時 (此時目的地為 00-00-01-33-33-33 : C), 即可由 MAC 位址表中找到目的端 MAC 位址。



③ 使用比對結果一致的通訊埠 (此範例為 3 號通訊埠) 來傳送訊框。其他通訊埠 2 號、4 號則不進行傳送的動作。

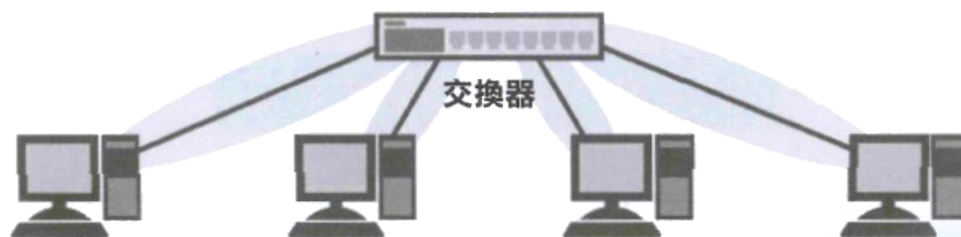


交換器 – Switch (4/4)

交換器可以避免因為衝突造成效率降低



由於集線器不會進行控制, 因此連接到通訊埠的所有主機都會被納入相同的衝突域



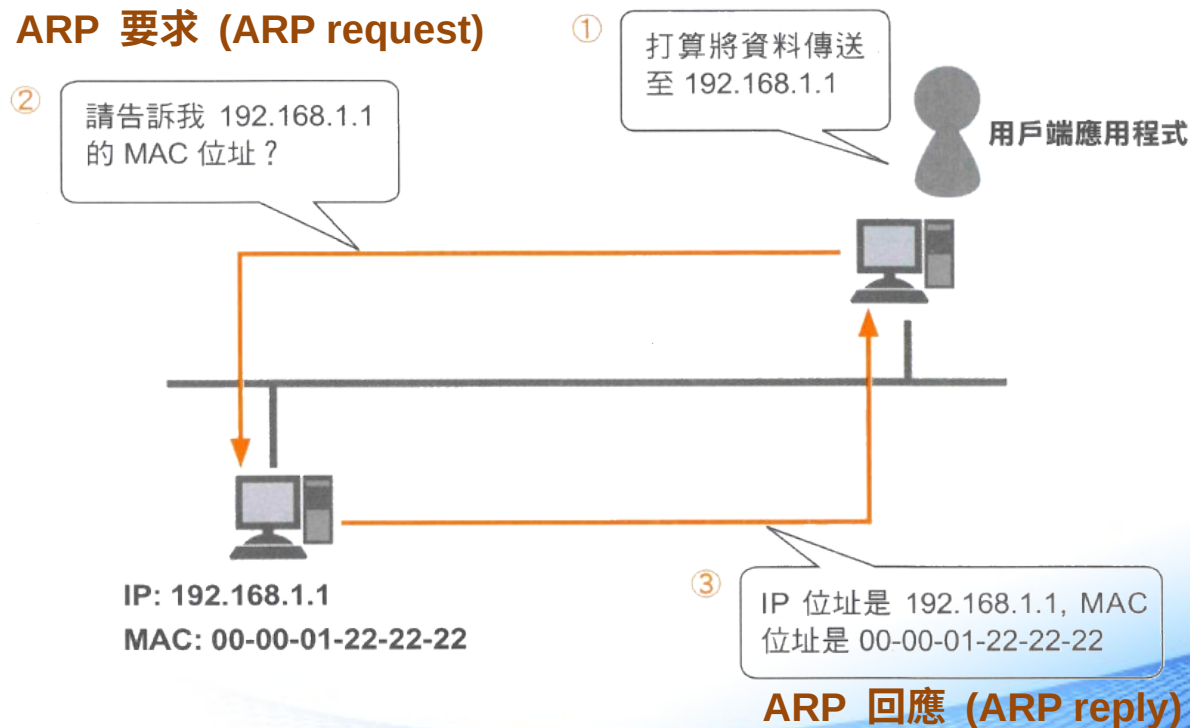
交換器在控制時是以通訊埠為單位, 來阻止衝突發生, 因此可以用通訊埠為單位來分割衝突域

位址解析通訊協定 (ARP)

- 用來取得區域網路內未知接收端 MAC 位址的方法

詢問擁有該 IP 位址的主機，「請告訴我你的 MAC 位址」

ARP 要求 (ARP request)



ARP 資料表 (1/2)

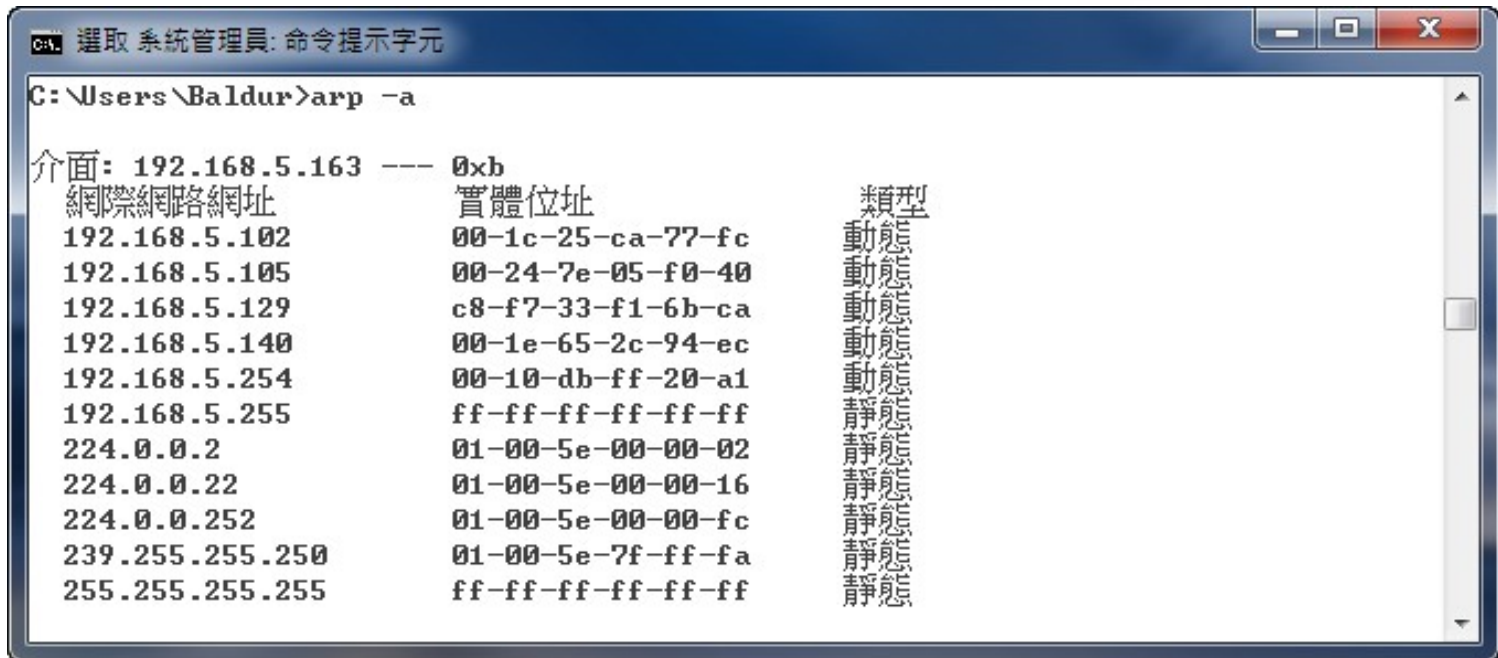
- 儲存於主機的記憶體中的 IP 與 MAC 位址對應表
- 為了加速詢問 MAC 的速度，曾經詢問過的資料會暫存於 ARP 資料表內一段時間
- 如何檢視 ARP 資料表？
 - Linux 系統：
在 Shell 下輸入 `arp -n`

```
[baldur@Lunch2013 ~]$ arp -n
```

Address	Hwtype	Hwaddress	Flags	Mask	Iface
163.16.1.40	ether	00:50:56:03:00:40	C		eth3
163.16.1.12	ether	00:50:56:a9:0b:13	C		eth3
163.16.1.254	ether	00:10:db:ff:20:a2	C		eth3

ARP 資料表 (2/2)

- Windows 系統：
在命令提示字元下輸入 `arp -a`



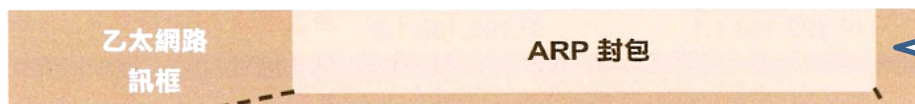
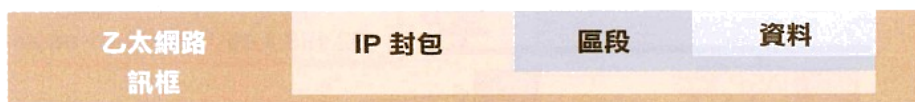
```
選取 系統管理員: 命令提示字元
C:\Users\Baldur>arp -a

介面: 192.168.5.163 --- 0xb
網際網路網址      實體位址      類型
192.168.5.102     00-1c-25-ca-77-fc 動態
192.168.5.105     00-24-7e-05-f0-40 動態
192.168.5.129     c8-f7-33-f1-6b-ca 動態
192.168.5.140     00-1e-65-2c-94-ec 動態
192.168.5.254     00-10-db-ff-20-a1 動態
192.168.5.255     ff-ff-ff-ff-ff-ff 靜態
224.0.0.2         01-00-5e-00-00-02 靜態
224.0.0.22        01-00-5e-00-00-16 靜態
224.0.0.252       01-00-5e-00-00-fc 靜態
239.255.255.250   01-00-5e-7f-ff-fa 靜態
255.255.255.255   ff-ff-ff-ff-ff-ff 靜態
```

ARP 封包

ARP 封包會將 IP、MAC 位址當作資料附加後再傳送出去

一般封包 (IP 封包)



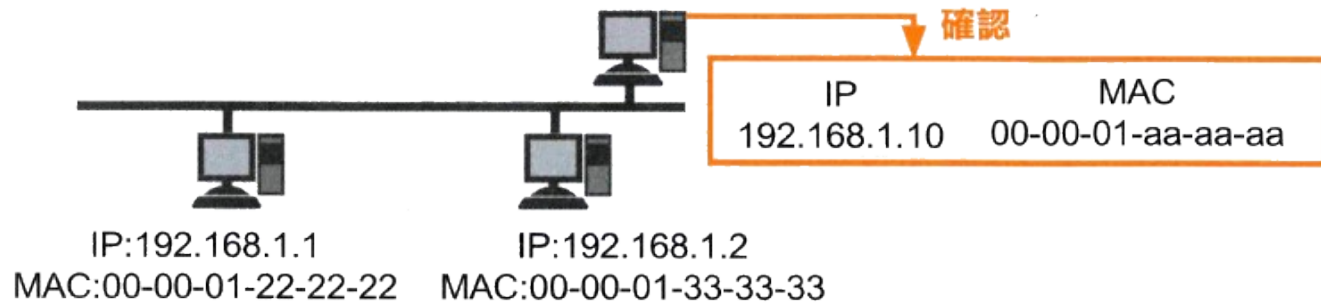
ARP 封包沒有再封裝第三層以上的封包，這代表 ARP 封包無法跨越網路層，只能運作於區域網路之中

位元	名稱	意義
4	位址類型	表示位址的方式
2	位址長度	表示位址的長度
2	操作碼	表示是否回應要求
6	傳送端MAC位址	傳送端的MAC位址
4	傳送端IP位址	傳送端的IP位址
6	接收端MAC位址	接收端的MAC位址
4	接收端IP位址	接收端的IP位址

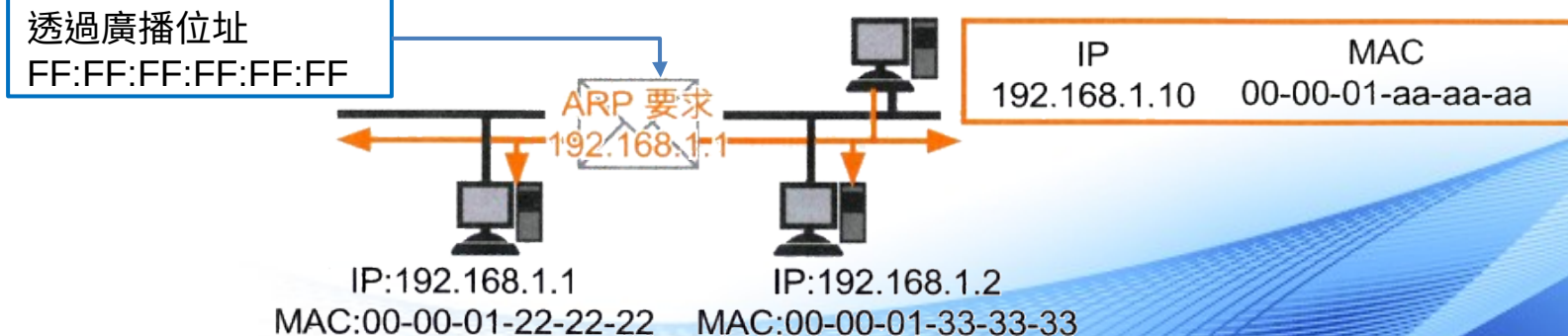
ARP 的運作方式 (1/2)

利用廣播的方式傳送至網路上的所有成員，並且只回應條件符合的主機

① 希望進行傳送的主機必須先參照本身的 ARP 資料表

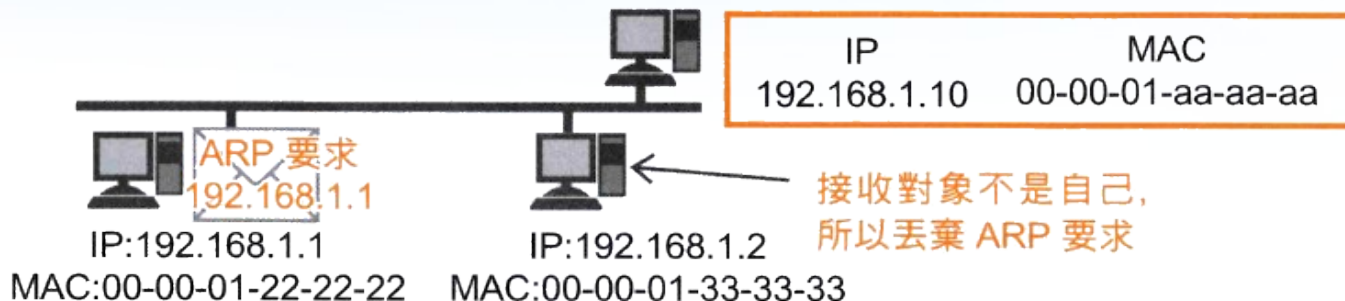


② ARP 資料表中如果沒有接收端 IP 位址時，必須廣播 ARP 要求

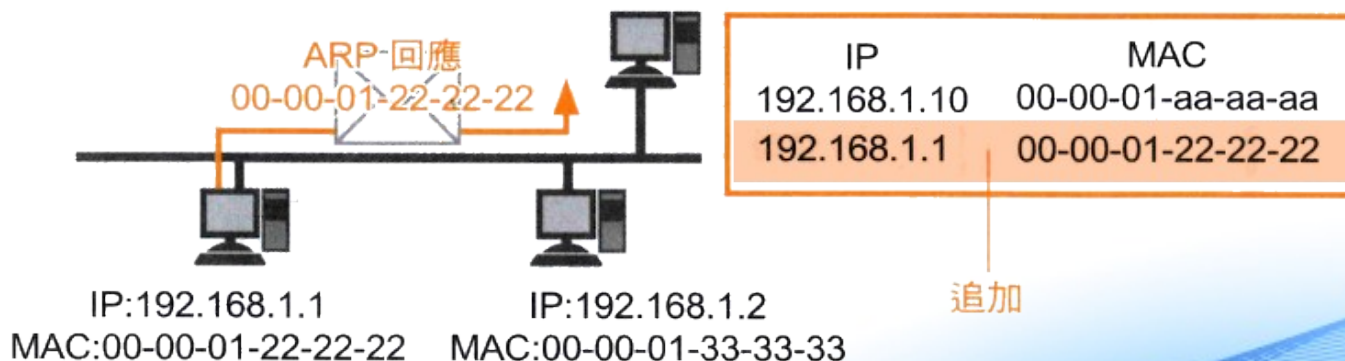


ARP 的運作方式 (2/2)

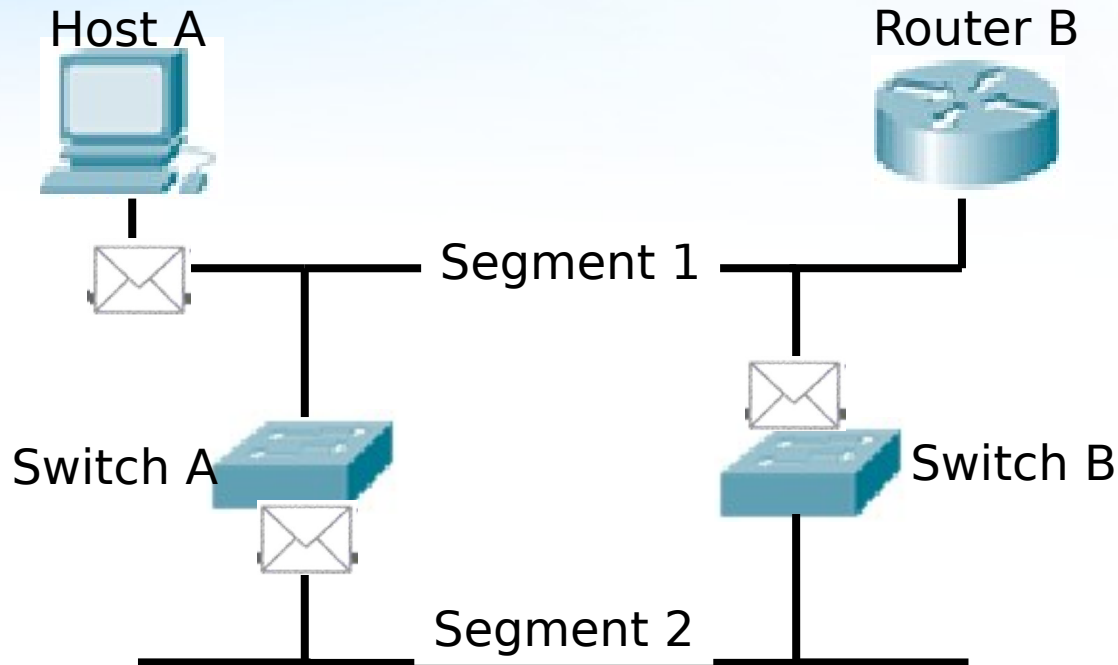
③ 確認 ARP 要求的接收對象, 如果對象是自己的話就回應, 否則就丟棄該要求



④ 收到 ARP 回應時, 必須將回應結果追加在 ARP 資料表中

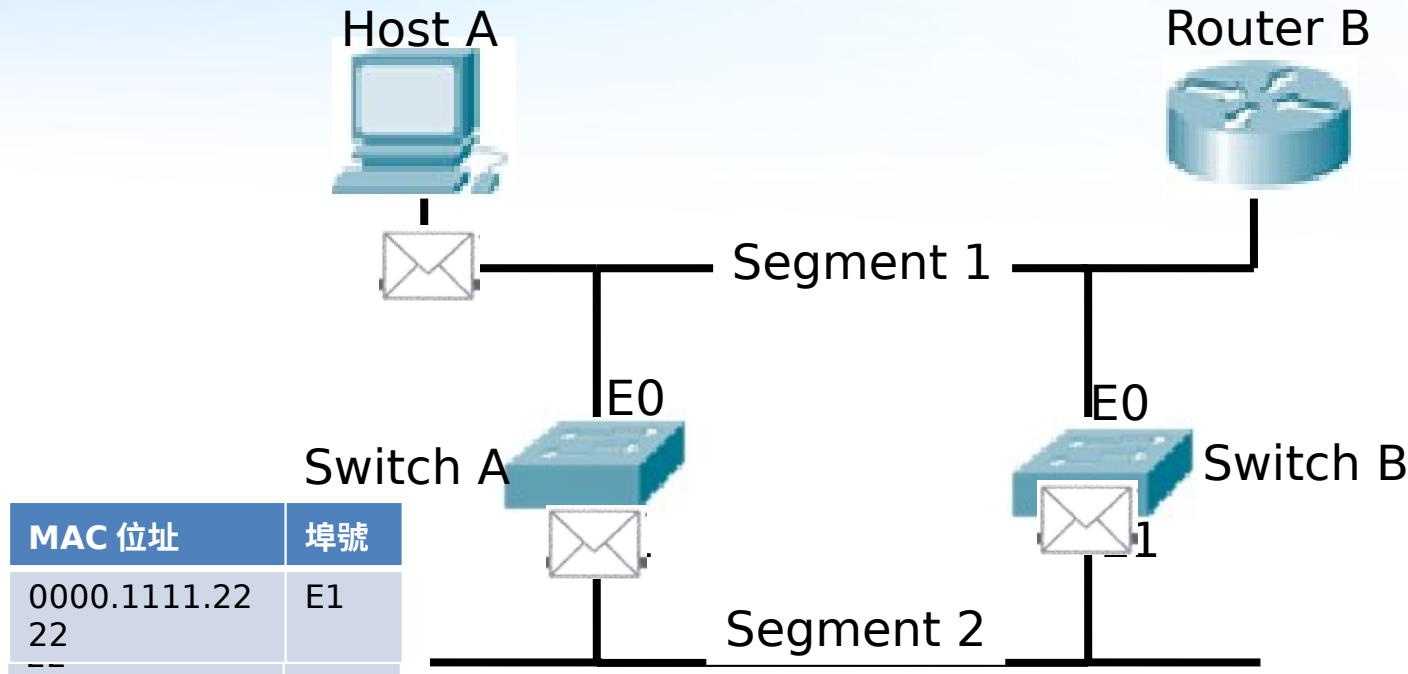


發送多個重複資料



- Host A 要發送一個封包給 Router B, 封包內的目的地 MAC 位址指定著路由器的 MAC 位址。Host A 送出這個封包之後，Router B 因為與 Host A 處於同一個網路區段，所以 Router B 會從 Segment 1 收到這個封包。
- Host A 也會把這個封包傳送給 Switch A，而 Switch A 收到之後，因為在 MAC 位址資料庫中找不到相對應的資料，所以會採用 Flooding 的做法，把這個封包傳送出去。
- 交換器 B 經由 Segment 2 網段收到由交換器 A 送過來的封包後，當然也會因為在 MAC 位址資料庫中找不到相對應的資料，又再次把這個封包 Flooding 出去。最後，路由器又會收到一次由交換器 B 送出的相同封包。

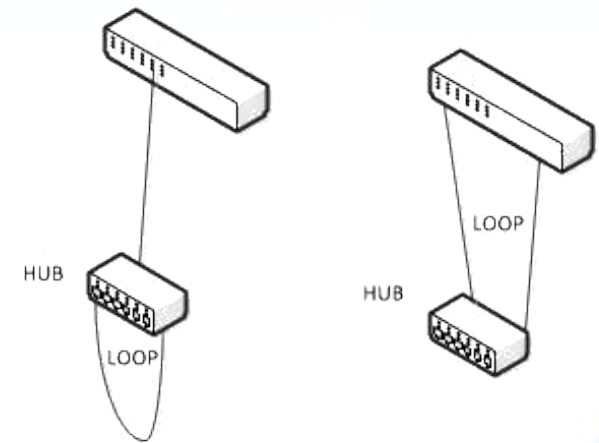
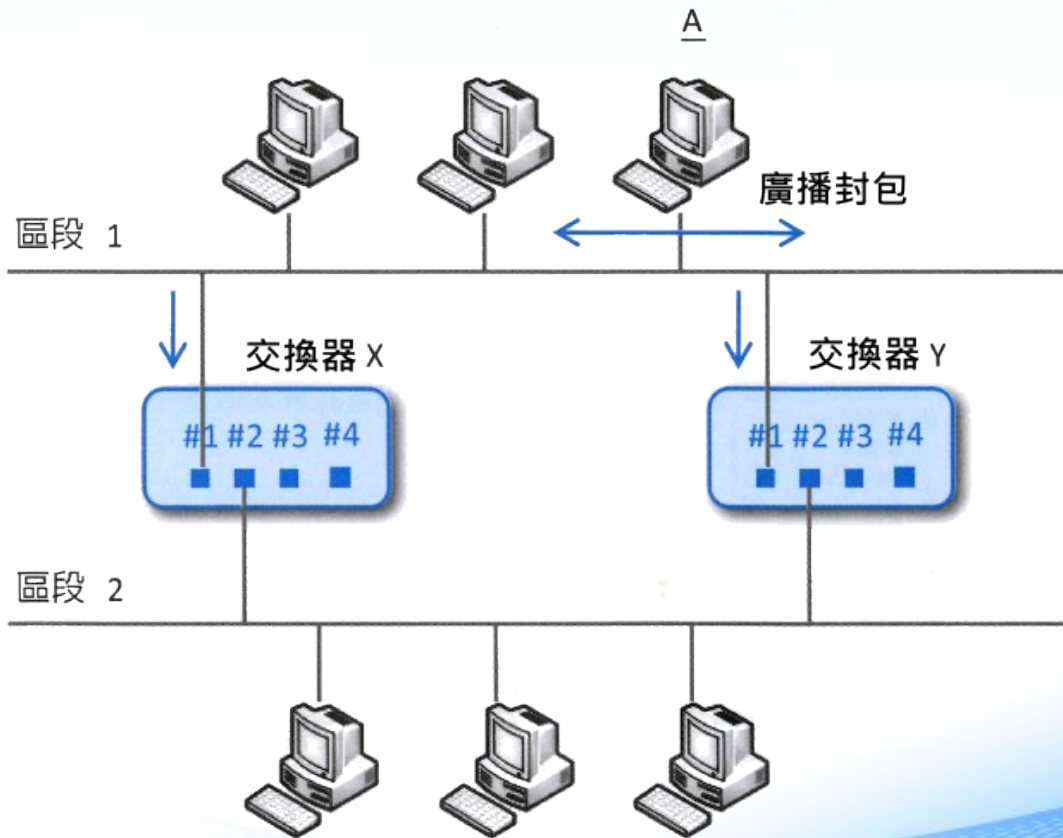
MAC 位址資料庫不一致



- Host A 要發送一個封包給路由器，而此時 Router B 的 MAC 位址還沒有被下面這兩台交換器設備學習到，當 Host A 送出要給 Router B 的封包之後，這兩台交換器設備都是從 E0 介面收到這個封包，但由於在 MAC 位址資料庫中找不到相對應的資料，所以都會從 E1 的介面 Flooding 出去。
- 當 Host A 送出要給 Router B 的封包之後，這兩台交換器設備都是從 E0 介面收到這個封包，但由於在 MAC 位址資料庫中找不到相對應的資料，所以都會從 E1 的介面 Flooding 出去。

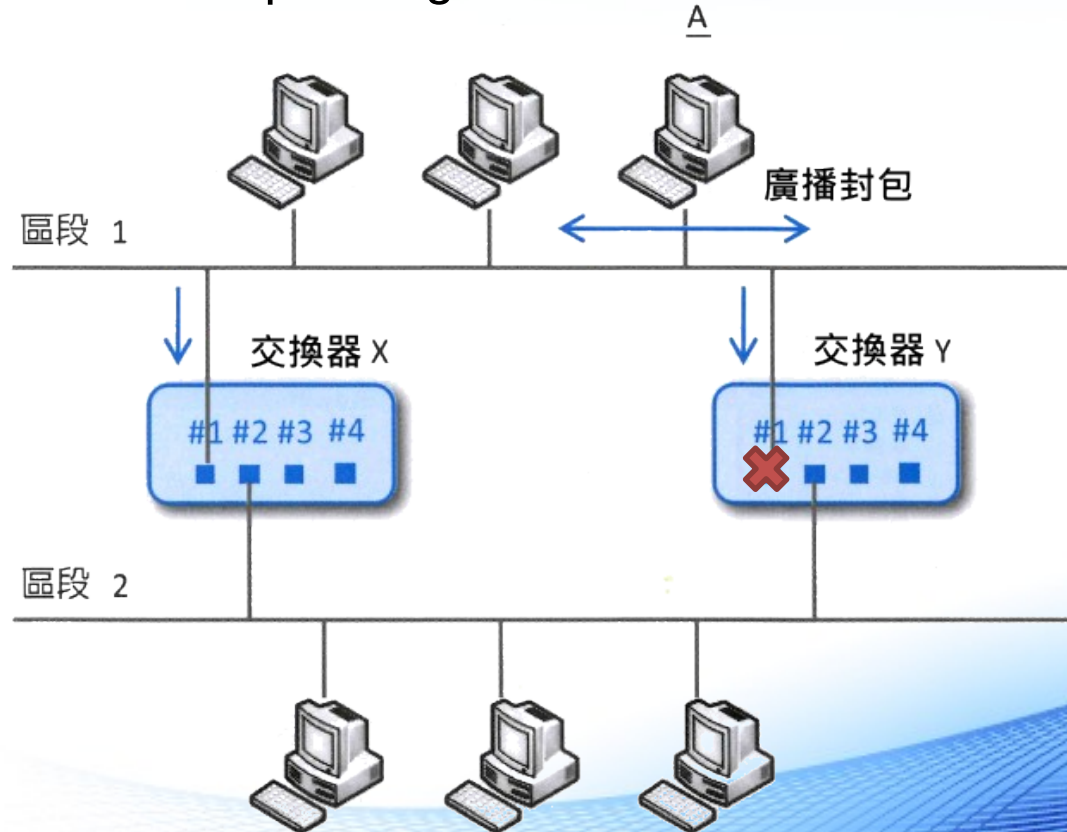
防止接線迴圈 (1/2)

- 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：



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

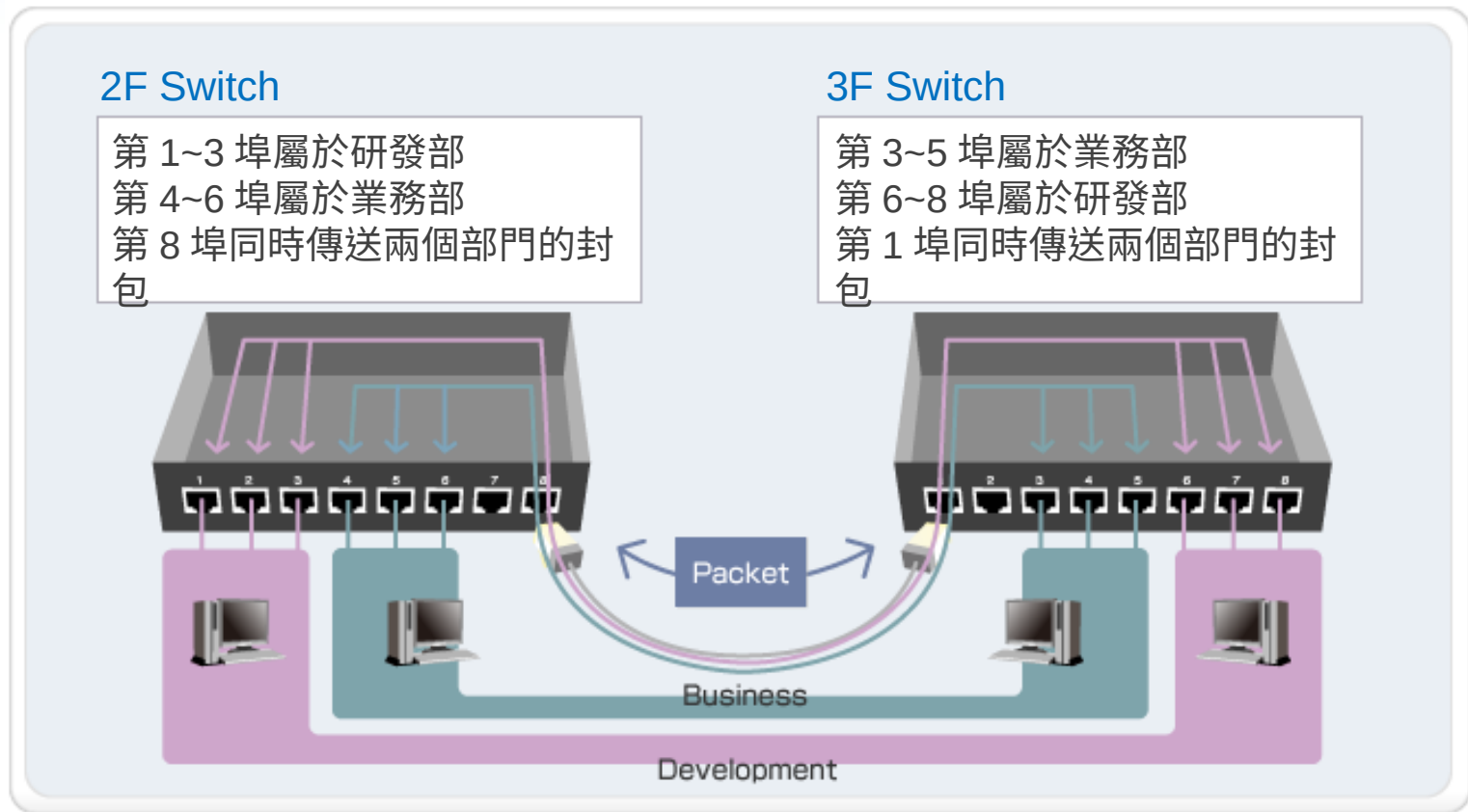
介質存取控制的方法以及定址

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

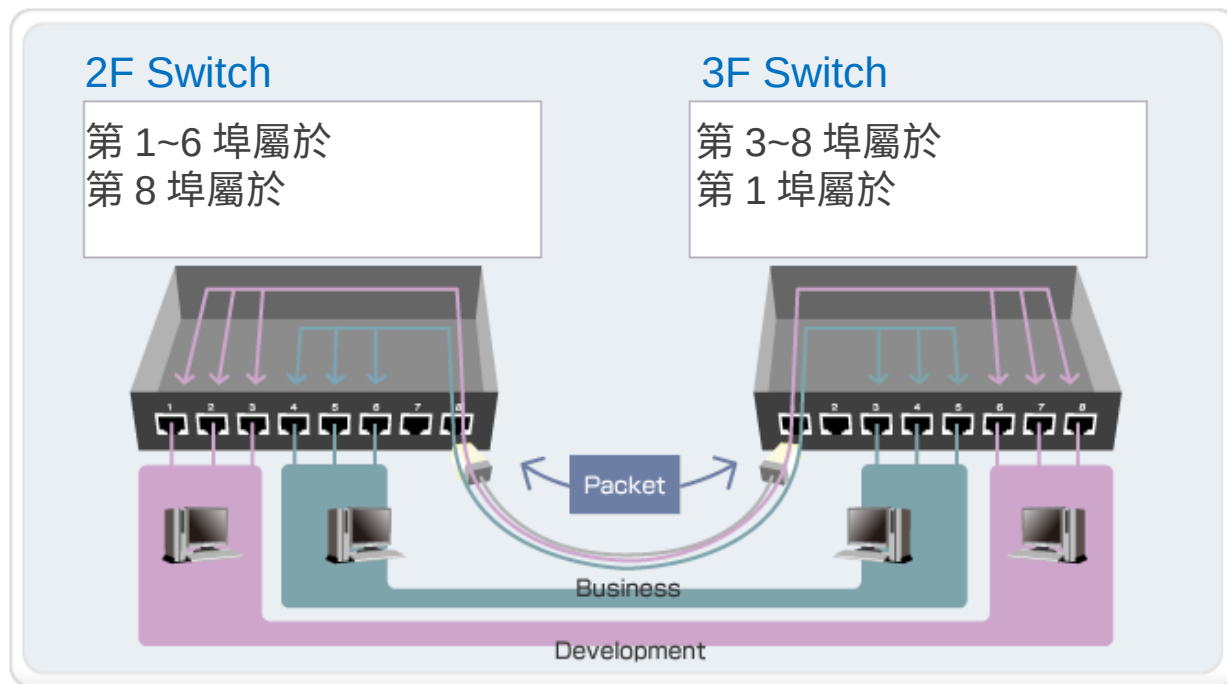


VLAN 的特色

- 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。

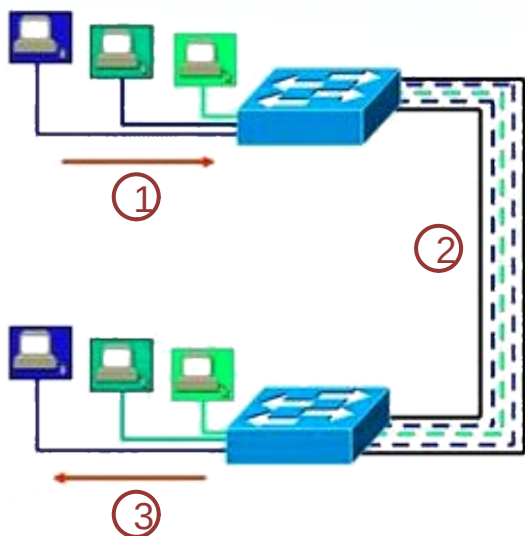
VLAN 的運作方式 (1/4)

- 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

指定第三層
通訊協定

原本的
乙太網路訊框

接收端 MAC 位址	傳送端 MAC 位址	訊框類型	資料	訊框檢查字 元 (FCS)
6 位元組	6 位元組	2 位元組	46-1500 位元組	4 位元組

加入標籤的
乙太網路訊框

接收端 MAC 位址	傳送端 MAC 位址	802.1Q Header	訊框類型	資料	訊框檢查字 元 (FCS)
6 位元組	6 位元組	4 位元組	2 位元組	46-1500 位元組	4 位元組

Tag Protocol
Identifier

16bits

Priority Code
Point

3bits

Canonical
Format
Indicator

1bit

VLAN
Identifier

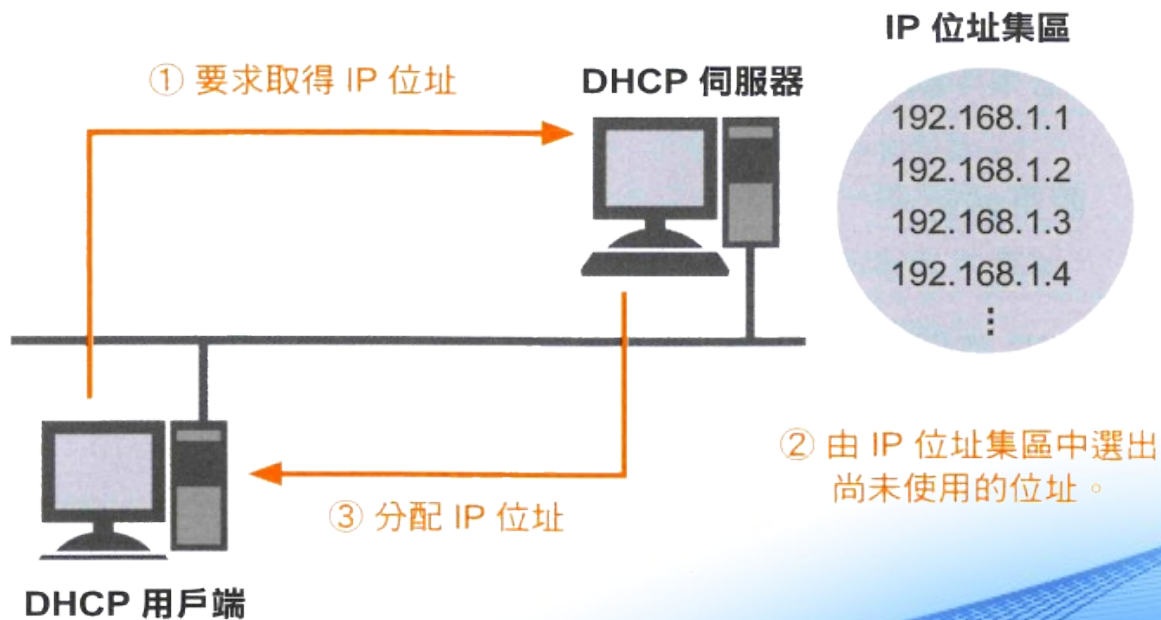
12bits

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

動態主機組態協定 (DHCP)

DHCP 係由 2 部分所組成的, 一個是負責管理所要分配的 IP 位址, 並且實際執行分配作業的伺服器, 另一個則是被分配的用戶端



DHCP 的封包格式

- DHCP 除了分配 IP 位址之外，還可以把子網路遮罩、預設閘道、DNS Server、租用期限等資訊一併傳送給用戶端

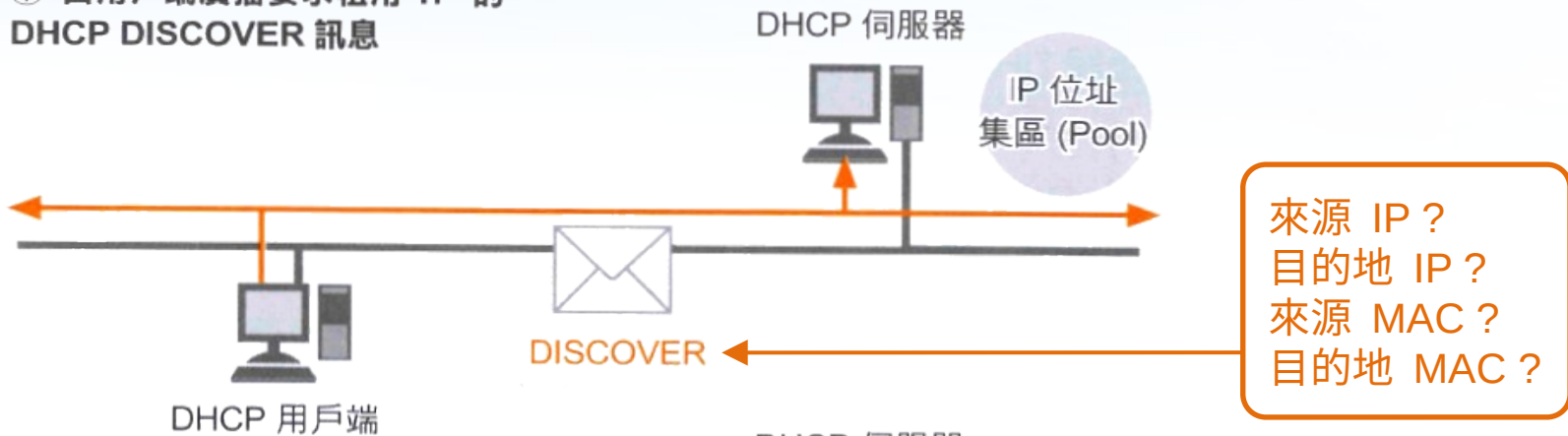
將 IP 位址以外的資訊附加在
選項後再傳送出去



名稱	說明
操作碼 (Operation code)	用戶端→伺服器---1 伺服器→用戶端---2
分配的 IP 位址	伺服器所分配的 IP 位址
伺服器 IP 位址	伺服器的位址
用戶端硬體位址	用戶端的 MAC 位址
伺服器名稱	伺服器的主機名稱
選項 (Option)	用戶端其他的設定資訊

DHCP 的運作 (1/2)

① 由用戶端廣播要求租用 IP 的 DHCP DISCOVER 訊息



② 收到 DISCOVER 訊息的伺服器會由 IP 位址集區中選出所要分配的 IP 位址, 然後再利用廣播的方式, 通知用戶端該 IP 位址 (DHCP OFFER)



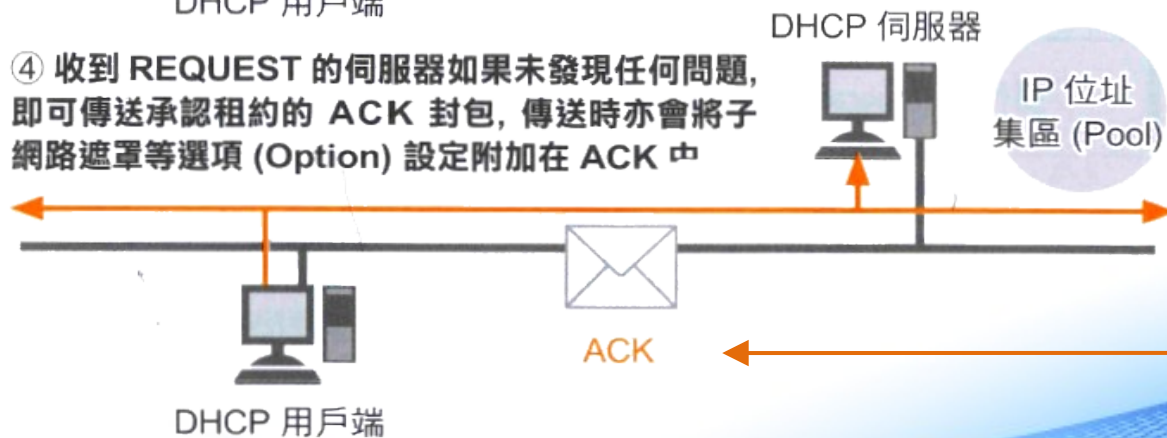
DHCP 的運作 (2/2)

③ 如果用戶端所收到 OFFER 訊息中的 IP 位址並確認無誤，即可向伺服器送出接受租約的 DHCP REQUEST 廣播



來源 IP ?
目的地 IP ?
來源 MAC ?
目的地 MAC ?

④ 收到 REQUEST 的伺服器如果未發現任何問題，即可傳送承認租約的 ACK 封包，傳送時亦會將子網路遮罩等選項 (Option) 設定附加在 ACK 中



來源 IP ?
目的地 IP ?
來源 MAC ?
目的地 MAC ?

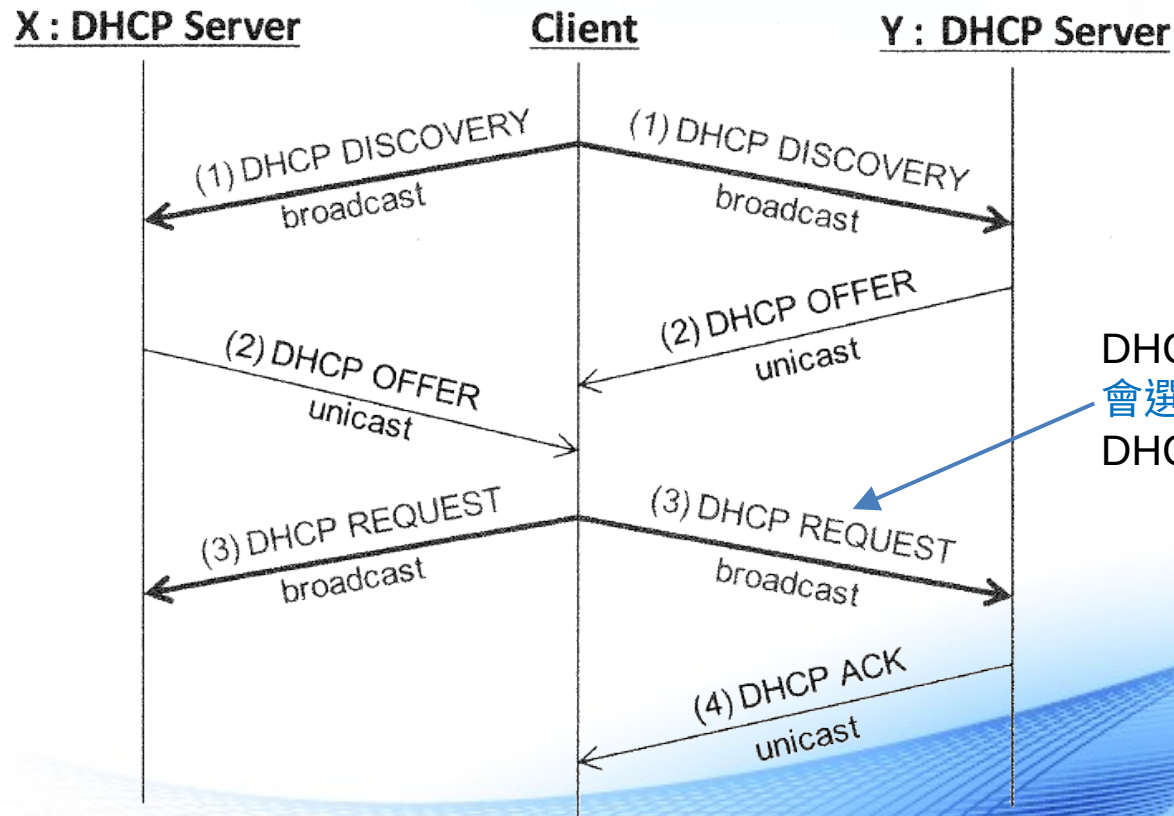
DHCP 用戶端資訊

- 在 windows 的命令提示字元下輸入：`ipconfig /all`

```
乙太網路卡 區域連線:
    連線特定 DNS 尾碼 . . . . . : kh.edu.tw
    描述 . . . . . : Realtek RTL8169/8110 Family PCI Gigabit Ethernet NIC (NDIS 6.20)
    實體位址 . . . . . : 00-E0-4C-01-06-6C
    DHCP 已啟用 . . . . . : 是
    自動設定啟用 . . . . . : 是
    IPv6 位址 . . . . . : 2001:288:8201:5:f414:38e3:1666:f72f<偏好選項>
    臨時 IPv6 位址 . . . . . : 2001:288:8201:5:4c1c:ef76:fec8:6090<偏好選項>
    連結-本機 IPv6 位址 . . . . . : fe80::f414:38e3:1666:f72f%11<偏好選項>
    IPv4 位址 . . . . . : 192.168.5.103<偏好選項>
    子網路遮罩 . . . . . : 255.255.255.0
    租用取得 . . . . . : 2014年9月1日 上午 08:41:12
    租用到期 . . . . . : 2014年9月2日 上午 11:11:17
    預設閘道 . . . . . : fe80::10:dbff:feff:20a1%11
    . . . . . : 192.168.5.254
    DHCP 伺服器 . . . . . : 192.168.5.254
    DNS 伺服器 . . . . . : 163.28.136.10
    . . . . . : 163.28.136.2
    . . . . . : 163.16.1.23
    NetBIOS over Tcpip . . . . . : 啟用
```

存在複數 DHCP 伺服器的影響

- 如果在同一個區域網路存在兩台 DHCP 伺服器 X 與 Y，當 DHCP 用戶端發出租用 IP 的請求 (DHCP DISCOVER) 時：



DHCP 用戶端只會選擇先回應的 DHCP 伺服器

DHCP 用戶端手動租約更新 (1/2)

- 用戶端取消 DHCP 租約
在 windows 的命令提示字元下輸入：`ipconfig /release`

```
乙太網路卡 區域連線:
    連線特定 DNS 尾碼 . . . . . :
    描述 . . . . . : Realtek RTL8169/8110 Family PCI Gigabit Ethernet NIC (NDIS 6.20)
    實體位址 . . . . . : 00-E0-4C-01-06-6C
    DHCP 已啟用 . . . . . : 是
    自動設定啟用 . . . . . : 是
    IPv6 位址. . . . . : 2001:288:8201:5:f414:38e3:1666:f72f<偏好選項>
    臨時 IPv6 位址. . . . . : 2001:288:8201:5:4c1c:ef76:fec8:6090<偏好選項>
    連結-本機 IPv6 位址 . . . . . : fe80::f414:38e3:1666:f72f%11<偏好選項>
    自動設定 IPv4 位址 . . . . . : 169.254.247.47<偏好選項>
    子網路遮罩 . . . . . : 255.255.0.0
    預設閘道 . . . . . : fe80::10:dbff:feff:20a1%11
    DNS 伺服器 . . . . . : fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1
    NetBIOS over Tcpip . . . . . : 啟用
```

DHCP 用戶端手動租約更新 (2/2)

- 重新取得 DHCP 租約
在 windows 的命令提示字元下輸入：`ipconfig /renew`

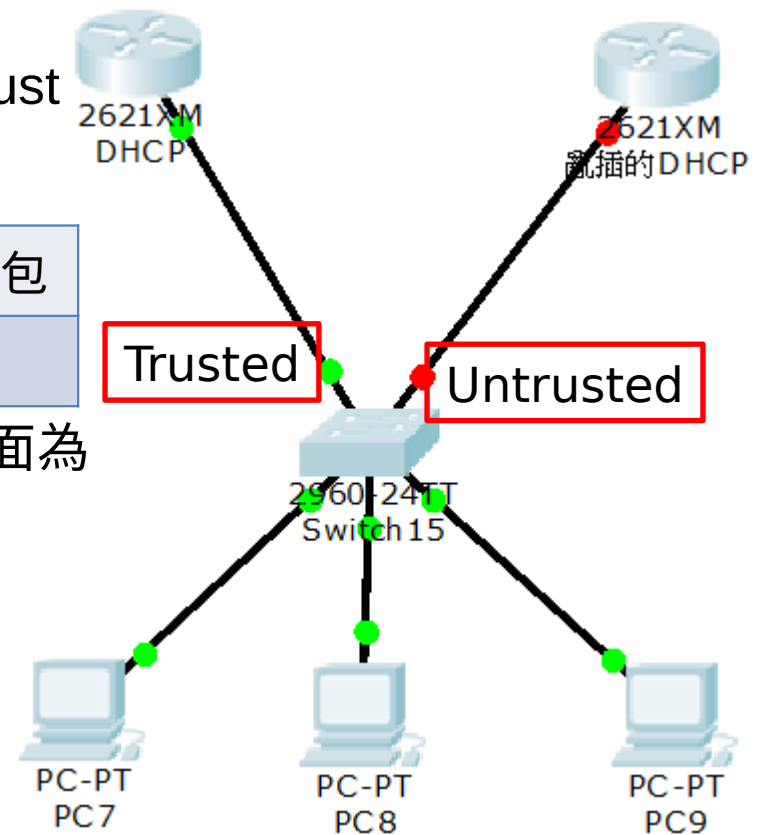
```
乙太網路卡 區域連線:
    連線特定 DNS 尾碼 . . . . . : kh.edu.tw
    描述 . . . . . : Realtek RTL8169/8110 Family PCI Gigabit Ethernet NIC (NDIS 6.20)
    實體位址 . . . . . : 00-E0-4C-01-06-6C
    DHCP 已啟用 . . . . . : 是
    自動設定啟用 . . . . . : 是
    IPv6 位址 . . . . . : 2001:288:8201:5:f414:38e3:1666:f72f<偏好選項>
    臨時 IPv6 位址 . . . . . : 2001:288:8201:5:4c1c:ef76:fec8:6090<偏好選項>
    連結-本機 IPv6 位址 . . . . . : fe80::f414:38e3:1666:f72f%11<偏好選項>
    IPv4 位址 . . . . . : 192.168.5.103<偏好選項>
    子網路掩罩 . . . . . : 255.255.255.0
    租用取得 . . . . . : 2014年9月2日 上午 11:43:20
    租用到期 . . . . . : 2014年9月2日 下午 12:43:20
    預設閘道 . . . . . : fe80::10:dbff:feff:20a1%11
    . . . . . : 192.168.5.254
    DHCP 伺服器 . . . . . : 192.168.5.254
    DNS 伺服器 . . . . . : 163.28.136.10
    . . . . . : 163.28.136.2
    . . . . . : 163.16.1.23
    NetBIOS over Tcpip . . . . . : 啟用
```

防止接線迴圈的防護 DHCP Spoof Attacks

- (1) Cisco 在配發 IP 前會先用 ICMP-ping 去檢查有無使用此 IP
- (2) DHCP Snooping 使用 Untrust 及 Trust 介面去區分要不要收到 DHCP 的封包

Untrusted	不允許收到 DHCP Offer 封包
Trusted	允許收到 DHCP Offer

- (3) 啟用 DHCP Snooping 預設全部介面為 Untrust
- (4) DHCP Snooping 啟用在 L2 的 Access port



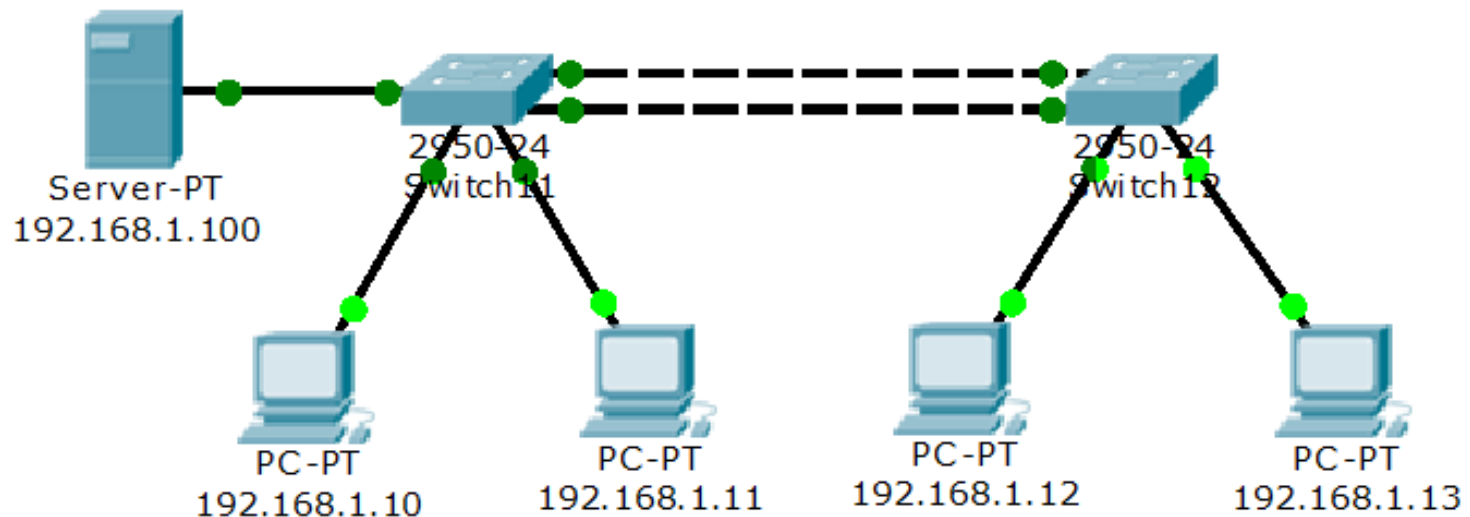
Cisco Packet Tracer 使用介紹



網路元件區

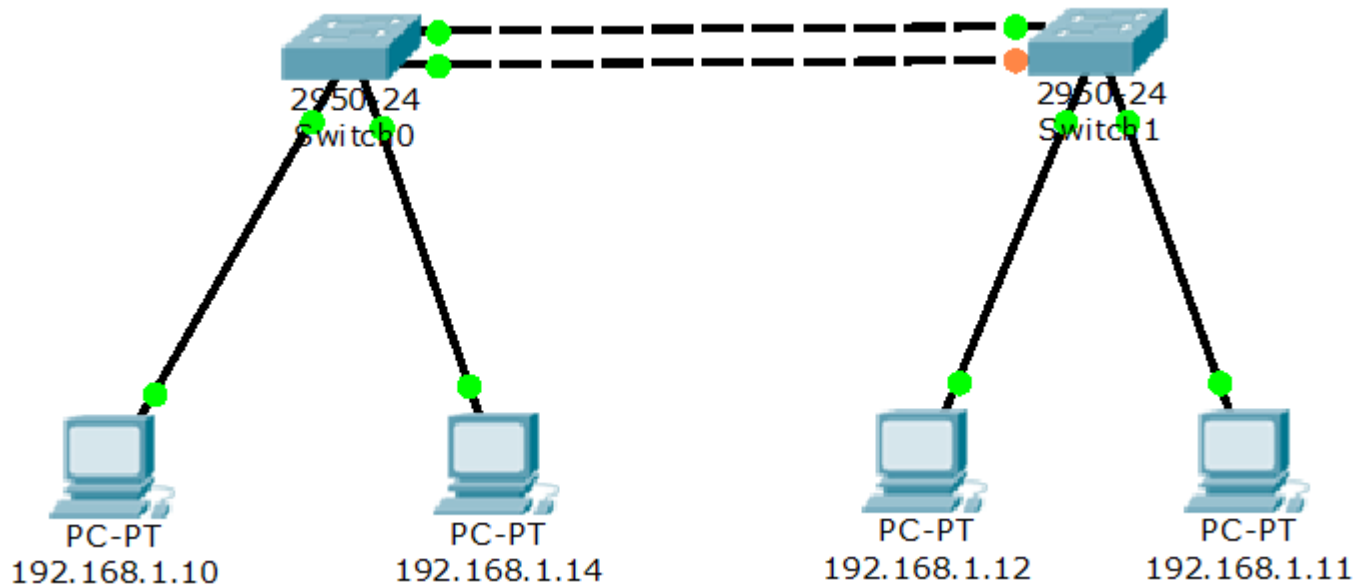
LAB 1 - 廣播風暴

- 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)
 - 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。



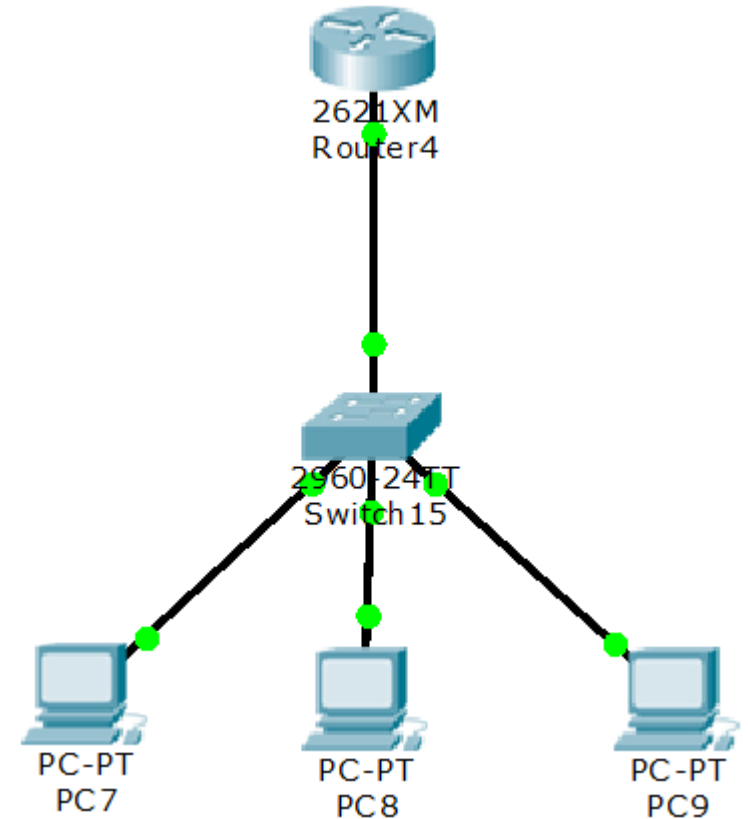
LAB 2 - 開啟 STP

- 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。



LAB 3 - DHCP 觀察

- 利用 Packet Tracer 查看 DHCP 封包相關資訊
 - Router>enable
 - Router# conf t
 - Router(config)#hostname R1
 - R1(config)#int fa0/0
 - R1(config-if)#ip address
192.168.10.1 255.255.255.0
 - R1(config-if)#no shut
 - R1(config-if)#exit
 - R1(config)#ip dhcp pool IP10
 - R1(dhcp-config)#net
192.168.10.0 255.255.255.0
 - R1(dhcp-config)#default 192.168.10.1
 - R1(dhcp-config)#exit



LAB 3 - DHCP 觀察

- 點選 PC0 至 Desktop 的頁籤，再選擇”Command Prompt” 後打下重新或去 DHCP 的指令。指令 :ipconfig /renew
- 查看 DHCP 封包內容與 DHCP 封包確認流程。

LAB 4 – DHCP Spoof

- 點選 PC0 至 Desktop 的頁籤，再選擇”Command Prompt” 後打下重新或去 DHCP 的指令。指令 :ipconfig /renew
- 查看 DHCP 封包流向是否已依照我們所設下的 DHCP Spoof 的規則呢？

