

橋接器與交換器 (Bridges and Switches)

請尊重智慧財產權

互連區域網路 (Interconnecting LANs)

- 區域網路使用集線器互有什麼不好?
 - 各自獨立的碰撞領域 (collision domain) 會變成一個大型的碰撞領域
 - 無法使用不同的乙太網路技術 (因為集線器本質上只是一個具有多埠的中繼器)
 - station 數目會有所限制
- Bridges 和 Switches

請尊重智慧財產權

橋接器 (Bridges) 簡介

- 網路第2層裝置
- 使用目的端位址來轉送和過濾 frame
- 使用 CSMA/CD去傳送 frame
- 當Bridge收到 frame，Bridge並不會將 frame copy到其它的介面。反之，Bridge會對Frame header做驗證，並且根據目的位址作選擇性的傳送
- 每一個 LAN segment 可視為一個獨立的碰接領域 (Isolated collision domain)

請尊重智慧財產權

橋接器的優點

- 獨立碰撞領域 可帶來較高的 throughput
- 不同的 Ethernet 技術可以聯繫
- 隨插即用裝置 (plug-and-play device)，可以視為 transparent bridges

請尊重智慧財產權

橋接器的主要功能

□ 過濾封包 (filter frames)

- Bridge 決定是否將封包轉送到特定的 interface，或者丟掉
- 若進入bridge的interface和出去的相同，bridge並不會轉送封包到其它的介面

□ 轉送封包 (forwarding)

- 決定將 frame 送到那一個 interface 去
- Filtering 和 forwarding 都與 bridge Table 有關
- Bridge 並不會改變 frame 的 source address

請尊重智慧財產權

Self Learning機制

- Bridge table由bridge動態學習，不需要經由網路管理者或任何資料鏈結層協定來建立
- Self learning機制
 - bridge table剛開始的時候是空的
 - bridge 收到一個frame，若frame中的目的位址不在 bridge table，則 bridge 將這個 frame 轉送到其他 interfaces
 - 當bridge每收到一個frame，bridge table將會記錄一些資訊
 - Frame的來源位址欄位中的區域網路位址
 - Frame到達bridge的interface
 - 目前的時間
 - 當bridge 收到一個frame，而且frame的目的位址可以在table中找到，則bridge會將frame轉送到適當的介面
 - 若一段時間後，沒有frame從某個位址送出，bridge可從table中刪除有關這個區域網路位址的資料

橋接器的傳送範例

- 若 A 要送 frame 到 B，因為 port 相同，bridge 便將 frame 直接丟棄
- 假設 C 要送一 frame 到 D，然後 D 再回送一個 frame 給 C
 1. C 送 frame 到 D，但 bridge table 沒有關於 D 的資訊，所以將 frame 廣播到其他的 LAN
 2. Bridge 記錄 C 在 port 1
 3. Frame 由 D 接收
 4. D 回送資料給 C
 5. Bridge 收到 frame 由 D 來
 6. Bridge 記錄 D 在 port 2
 7. 因為 bridge 知道 C 在 port 1，所以選擇性地將 frame 由 port 1 轉送出去

Spanning Tree Protocol

- 容錯型的網路 (redundant network): 具有多條傳送路徑，但容易產生下列問題
 - 迴路問題
 - 廣播風暴 (broadcast storm)
 - 多個重複的 frame
 - MAC位址不穩定
- 原始 frame 的數會不斷地增加，進而癱瘓整個網路
- 解決方法：使用生成樹協定 (spanning tree protocol)
 - 偵測可能造成迴路的多餘連線，由bridge虛擬地切斷某些介面的連線，以便從原先的網路拓撲中建立具樹狀架構的網路拓撲

請尊重智慧財產權

Spanning Tree Protocol (Cont.)

- 執行Spanning tree protocol的switch會和網路內其他的switch分享訊息，而交換訊息的資料單位就是所謂的「橋接通訊協定資料單位 (Bridge Protocol Data Units ; BPDU)」
- 當Switch啟動的時候，將自動把Root ID的值設定成等於Bridge ID的值
 - **Bridge ID**是由2位元組的Priority和6位元組的MAC位址所組合而成的
 - **Priority**的值可手動更改，而其預設值是32768或0x8000（十六進位表示法, 註:以Cisco為例）。例如若MAC位址為00.50.BA.C1.7F.35，**Priority**為預設值，則Bridge ID就等於80.00.00.50.BA.C1.7F.35。
- **Priority**值最小的Switch成爲Root Bridge (Root Switch)，但若沒有手動修改**Priority**的值則每個Switch皆相同時，則MAC位址最低者爲Root Bridge
- **Root bridge**選取出來後，網路上每一個switch將會聆聽BPDU。若一個以上的**Port**聆聽到BPDU則代表這個**Switch**上有多餘的連線，這時就必須將多餘會造成迴圈的Port停止

橋接器與路由器的比較

- 皆使用 **store-and-forward** 方式交換封包
 - **Routers**：為網路層裝置，使用網路層位址來轉送封包
 - **Bridges**：為資料鏈結層裝置，使用區域網路位址來轉送封包
- **Router 的優點**
 - 提供 **firewall** 保護，避免 **broadcast storms**
 - 支援任意的 **topologies**，使用IP header的**TTL**欄位避免迴路
- **Router 的缺點**
 - 需要設定 **IP address**
 - 較長的封包處理時間

請尊重智慧財產權

交換器 (Switches)

- 與Bridge相同，使用區域網路位址 (48bit的MAC位址) 來轉送及過濾封包
- Switches 的interfaces通常較多。不需做資料鏈結層協定轉換
- 速度: 10Mbps、100Mbps以及1Gbps
- 使於主機與交換器之間的連結具有類似專線 (dedicate access) 的功能。通常為 star-topology，hosts之間不會有collision
- 支援Cut-through switching
 - 可減少 packet 的 end to end delay
 - 註: 事實上Cut through switching 與 store-and-forward switching 的差異很小 (只有在output buffer是空的時候)

交換器實驗



請尊重智慧財產權

操作方式

- Switch上的CLI指令與路由器上的大致相同
 - 網頁式視覺Switch管理員 (Web-Based Visual Switch Manager : VSM)
 - IOS的命令列介面 (Command Line Interface : CLI)

請尊重智慧財產權

Switch 的基本指令介紹

- enable
- 設定主機名稱: hostname
- 查看interface相關設定:
show interface
- show running-config
- show startup-config
- show interfaces
- show spanning-tree
- show version
- 儲存設定: copy running-config startup-config
- 清除設定: erase nvram
- 設定 ip 位址
- 設定 ip default-gateway
- 設定 interface 的多工模式
- mac-address-table static
- 查看MAC位址列表
- 設定interface MAC址位的最大數
- show vlan
- show cdp

顯示 interfaces 相關設定

要查看 interface的相關設定，可以使用 [show interfaces](#) 指令

```
S3524#show interfaces
VLAN1 is up, line protocol is up          (MAC 位址)
  Hardware is CPU Interface, address is 0030.8513.a340 (bia
0030.8513.a340)
  Internet address is 140.116.34.252/24    (IP位址)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo                (佇列管理機制)
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 30000 bits/sec, 10 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    268094697 packets input, 1764638769 bytes, 0 no buffer
    Received 267274926 broadcasts, 0 runts, 37636234 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 2221861 ignored
--More--          (錯誤報告)
```

查看Spanning Tree Protocol的資訊

```
S3524#show spanning-tree
```

```
Spanning tree 1 is executing the IEEE compatible Spanning Tree protocol  
Bridge Identifier has priority 32768, address 0030.8513.a340  
Configured hello time 2, max age 20, forward delay 15  
Current root has priority 32768, address 0001.4341.0407  
Root port is 48, cost of root path is 8  
Topology change flag not set, detected flag not set, changes 6533  
Times: hold 1, topology change 35, notification 2  
hello 2, max age 20, forward delay 15  
Timers: hello 0, topology change 0, notification 0
```

```
Interface Fa0/1 (port 13) in Spanning tree 1 is FORWARDING
```

```
Port path cost 19, Port priority 128
```

```
Designated root has priority 32768, address 0001.4341.0407
```

```
Designated bridge has priority 32768, address 0030.8513.a340
```

```
Designated port is 13, path cost 8
```

```
Timers: message age 0, forward delay 0, hold 0
```

```
BPDU: sent 9785931, received 0
```

```
--More--
```


關閉 Spanning tree 功能

```
S3524(config)#no spanning-tree ?  
forward-time  Set a Spanning Tree FORWARD Interval  
hello-time    Set a Spanning Tree HELLO Interval  
max-age       Set a Spanning Tree MAX AGE Interval  
priority      Set a Spanning Tree Priority  
protocol      Spanning tree protocol type  
uplinkfast    Enable UplinkFast Feature  
vlan          VLAN Switch Spanning Trees  
<cr>
```

```
S3524(config)#no spanning-tree
```

請尊重智慧財產權

顯示系統相關訊息

S3524#[show version](#)

Cisco Internetwork Operating System Software
IOS (tm) C3500XL Software (C3500XL-C3H2S-M), Version 12.0(5.2)XU,
ROM: Bootstrap program is C3500XL boot loader

S3524 uptime is 35 weeks, 4 days, 55 minutes

System returned to ROM by power-on

[System image file is "flash:c3500XL-c3h2s-mz-120.5.2-XU.bin"](#)

cisco WS-C3524-XL (PowerPC403) processor (revision 0x01) with
[8192K/1024K bytes](#)
[of memory.](#)

24 FastEthernet/IEEE 802.3 interface(s)

....

[Configuration register is 0xF](#)

請尊重智慧財產權

清除交換器設定

- 想要清除交換器的設定時，只要使用`erase nvram`指令刪除開機設定檔（`startup-config`），重新載入或開機即可。

```
S3524#erase ?  
flash:      Filesystem to be erased  
nvram:      Filesystem to be erased  
startup-config  Erase contents of configuration memory
```

```
S3524#erase nvram  
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

接下來就會進行檔案刪除的動作了，所以執行時要特別注意！

請尊重智慧財產權

設定介面 (interface) 的IP位址

- 基本上交換器是一種plug-and-play的裝置，也就是不需任何設定即可直接使用。但如果有足夠的IP，有時爲了方便管理起見，可爲交換器設定一個IP位址

```
S3524#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3524(config)#interface VLAN1
S3524(config-if)# ip address 192.168.56.254 255.255.255.0
```

Cisco Catalyst switch預設的管理interface是在vlan1(一定會有這個vlan)，所以想設定交換器的IP位址可直接設定vlan1。

格式: ip address {ip address} {mask}

請尊重智慧財產權

設定預設閘道

- 為交換器設定IP位址後，還要設定預設閘道。這樣才能利用遠端登入進行設定。

```
S3524#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3524(config)#ip default-gateway 192.168.56.254
```

格式: ip default-gateway {ip address}

要允許遠端登入別忘了將設定 enable password 並將 telnet 功能打開喔! 部份範例如下:

```
enable password xxxx
```

```
line vty 0 4
password xxxx
login
```

請尊重智慧財產權

設定介面的多工模式

- 以高速乙太網路卡為例，interface的傳輸模式可設為半雙工 (half-duplex)、全雙工 (full-duplex)以及自動 (auto)。由於現在乙太網路卡的相容性一般來說都不錯，所以直接使用預設值 (auto) 即可，使用者也可自行設定。

```
S3524(config)#interface FastEthernet 0/1
S3524(config-if)#duplex ?
  auto  Enable AUTO duplex configuration
  full  Force full duplex operation
  half  Force half-duplex operation

S3524(config-if)#duplex auto
```

請尊重智慧財產權

查看MAC位址列表

```
S3524#show mac-address-table
```

```
Dynamic Address Count:      118
```

```
Secure Address Count:      0
```

```
Static Address (User-defined) Count: 0
```

```
System Self Address Count: 49
```

```
Total MAC addresses:      167
```

```
Maximum MAC addresses:     8192
```

```
Non-static Address Table:
```

```
Destination Address  Address Type  VLAN  Destination Port
```

```
-----
```

Destination Address	Address Type	VLAN	Destination Port
0000.e289.8f14	Dynamic	1	GigabitEthernet0/2
0001.293e.86a9	Dynamic	1	GigabitEthernet0/2
0001.4341.0407	Dynamic	1	GigabitEthernet0/2
0001.e6b2.66e5	Dynamic	1	GigabitEthernet0/2

請尊重智慧財產權

設定靜態MAC位址表

[mac-address-table](#) 指令可以讓我們設定靜態的MAC位址對映表，確保只有特定的設備才能連上指定的 port

```
S3524#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3524(config)#mac-address-table static 000a.4804.6298 ?
  FastEthernet    FastEthernet IEEE 802.3
  GigabitEthernet GigabitEthernet IEEE 802.3z
S3524(config)#mac-address-table static 000a.4804.6298 FastEthernet0/5
```

執行後可以使用 [show mac-address-table static](#) 指令觀察設定結果

```
S3524#show mac-address-table static

Static Address Table:
Destination Address  VLAN  Input Port  Output Ports
-----
000a.4804.6298      1 Fa0/1
                    1 Fa0/2
```


Configuring Port Security

```
Switch(config)#interface e0/4  
Switch(config-if)#port secure  
Switch(config-if)#port secure max-mac-count 1
```

指令: port secure [max-mac-count *count*]

請尊重智慧財產權

查看Switch的MAC位址表

```
Switch#show mac-address-table
```

```
Number of permanent addresses : 0
```

```
Number of restricted static addresses : 0
```

```
Number of dynamic addresses : 3
```

Address	Dest Interface	Type	Source Interface	List
0010.7B3A.8DB5	Ethernet 0/2	Dynamic	All	
00E0.1E60.9BC5	Ethernet 0/1	Dynamic	All	
0050.F036.C300	FastEthernet 1	Dynamic	All	

```
Switch#
```

- ❑ Configures an interface to be a secured port
- ❑ Define a maximum number of mac addresses allowed in the address table for this port
- ❑ Count can be from 1 to 132
- ❑ Default is 132

請尊重智慧財產權

顯示虛擬區域網路 (VLAN) 設定

```
S3524#show vlan id 1
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, 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

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1
1 enet	100001	1500	-	-	-	-	1002	1003

執行 [show vlan id 1](#) 的結果和 [show vlan name default](#) 基本上是相同的

查看CDP的相關訊息

- CDP是Cisco所研發的一種探測鄰居設備的通訊協定，可以用來查看有無其它Cisco網路設備 (僅有Cisco的網路硬體設備產品可以使用)
- Disabling CDP: 可使用 `no cdp run` 指令關閉

```
S3524#show cdp
```

```
Global CDP information:
```

```
    Sending CDP packets every 60 seconds           (每60秒廣播一次)
```

```
    Sending a holdtime value of 180 seconds
```

```
    Sending CDPv2 advertisements is enabled
```

```
S3524#show cdp neig
```

!查看其它相連的設備

```
S3524#show cdp neighbors
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
```

```
                  S - Switch, H - Host, I - IGMP, r - Repeater
```

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
S3548	Gig 0/2	162	T S	WS-C3548-X	Gig 0/2

附近有一台Cisco 3548交換器

查看指令執行的歷史紀錄

```
Switch#show history
ena
conf term
show spantree
show cdp
show cdp neighbors
show cdp interface
show vlan
show interface
show history
```

請尊重智慧財產權

Loop的實驗

- 將Spanning tree關掉，觀察網路的狀況

請尊重智慧財產權