

Cisco Switch 基礎操作

宜蘭縣區域網路中心

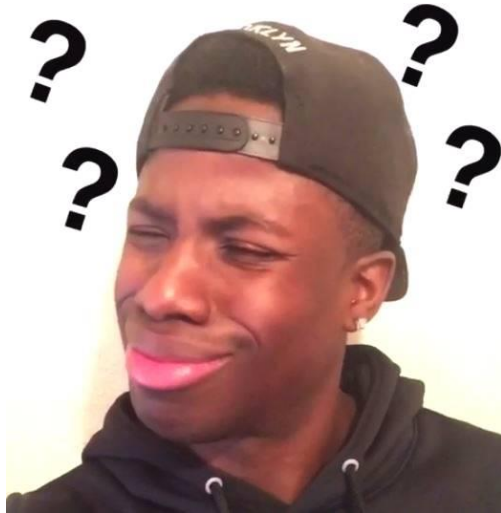
網路設備

Hub

L3
Switch

L2
Switch

Router



OSI 七層協定

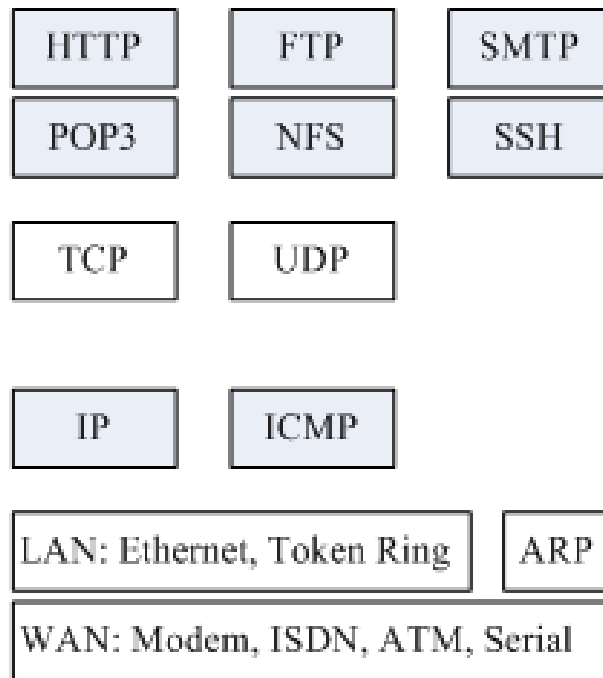
OSI 七層協定



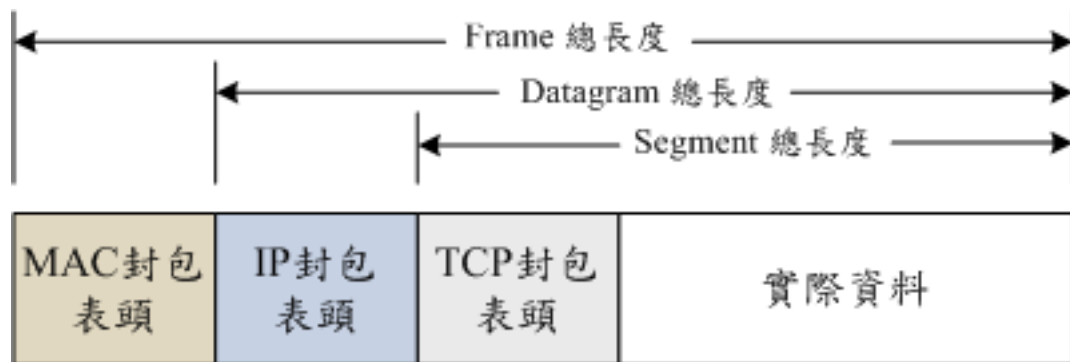
TCP/IP



相關通訊協定與標準



TCP封包組成



Wireshark的封包

The screenshot displays the Wireshark network protocol analyzer interface. At the top, the window title is '+eno1'. Below the title bar is a menu bar with options: File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. A toolbar with various icons for file operations and analysis is located below the menu bar. A display filter bar contains the text 'Apply a display filter ... <Ctrl-/>' and an 'Expression...' field.

The main display area is divided into three sections:

- Packets List:** A table with columns: No., Time, Source, Destination, Protocol, Length, and Info. Two packets are visible:

No.	Time	Source	Destination	Protocol	Length	Info
294	0.887503824	2001:c08:7f:150::f	2001:288:a001:5:9abe:133a:b3a5:ab0	QUIC	1412	Payload
295	0.887560477	2001:c08:7f:150::f	2001:288:a001:5:9abe:133a:b3a5:ab0	QUIC	1412	Payload
- Packet Details:** A tree view showing the structure of the selected packet (No. 294). The expanded view shows:
 - Frame 294: 1412 bytes on wire (11296 bits), 1412 bytes captured (11296 bits) on interface 0
 - Ethernet II, Src: Cisco_56:e2:c0 (00:1e:7a:56:e2:c0), Dst: HewlettP_1f:46:34 (6c:3b:e5:1f:46:34)
 - Internet Protocol Version 6, Src: 2001:c08:7f:150::f, Dst: 2001:288:a001:5:9abe:133a:b3a5:ab0
 - User Datagram Protocol, Src Port: 443, Dst Port: 51312
 - QUIC (Quick UDP Internet Connections)
- Packet Bytes:** A hex dump of the packet data with corresponding ASCII characters. The first few bytes are: 6c 3b e5 1f 46 34 00 1e 7a 56 e2 c0 86 dd 60 00. The ASCII column shows: l;..F4..zV... .

At the bottom of the interface, a status bar shows: Ethernet (eth), 14 bytes | Packets: 442 · Displayed: 442 (100.0%) | Profile: Default

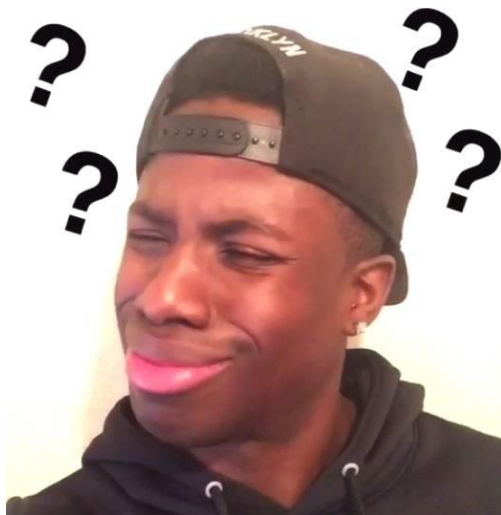
網路設備

Hub

L3
Switch

L2
Switch

Router



Hub(集線器)

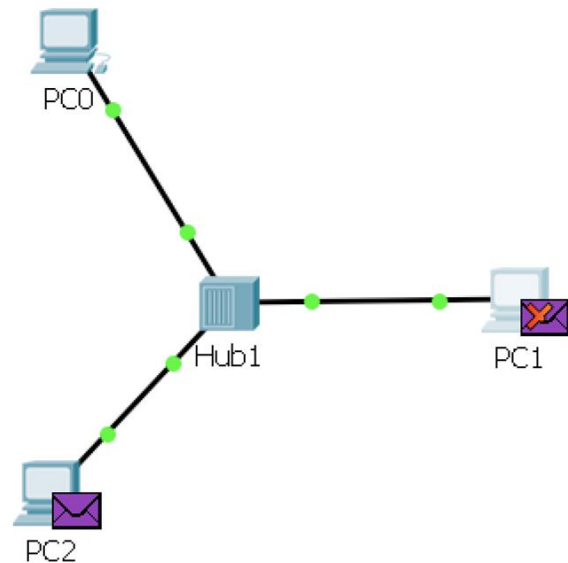
屬於OSI的第一層

★ 優點

- 便宜
- 使用方便，隨插即用

★ 缺點

- 以廣播方式傳輸資料(佔用頻寬，影響網路效能)
- 每一個在Hub上有連接的設備，都會收到封包



L2 Switch(交換器)

屬於OSI的第二層(ARP => MAC Address)

★ 優點

★ 使用方便，隨插即用

★ 封包傳送比Hub有效率

★ 將MAC位址和PORT對應
形成一張MAC表格

★ 僅將封包送往其MAC對應的埠

★ 缺點

★ 只能處理同一個網段內的資料

Vlan	Mac Address	Type	Ports
----	-----	-----	-----
1	0003.e491.dce2	DYNAMIC	Fa0/2
1	0060.474c.8852	DYNAMIC	Fa0/3
1	00e0.f943.d89a	DYNAMIC	Fa0/1

L3 Switch(交換器)

屬於OSI第三層(IP、ICMP)

網路連接情況	目的端位址	出口介面
Connected (直接連接)	10.120.2.0	E0
Learned (學習而來的)	172.16.1.0	S0

★ 優點

- ★ 可以像L2 Switch將封包送往其MAC對應的埠，也可像路由器轉發不同區域網路的封包
- ★ 用於連接不同網段，通過對預設閘道的查詢學習來建立兩個網段之間的連線
- ★ 通過專用的ASIC晶片轉發需路由的封包

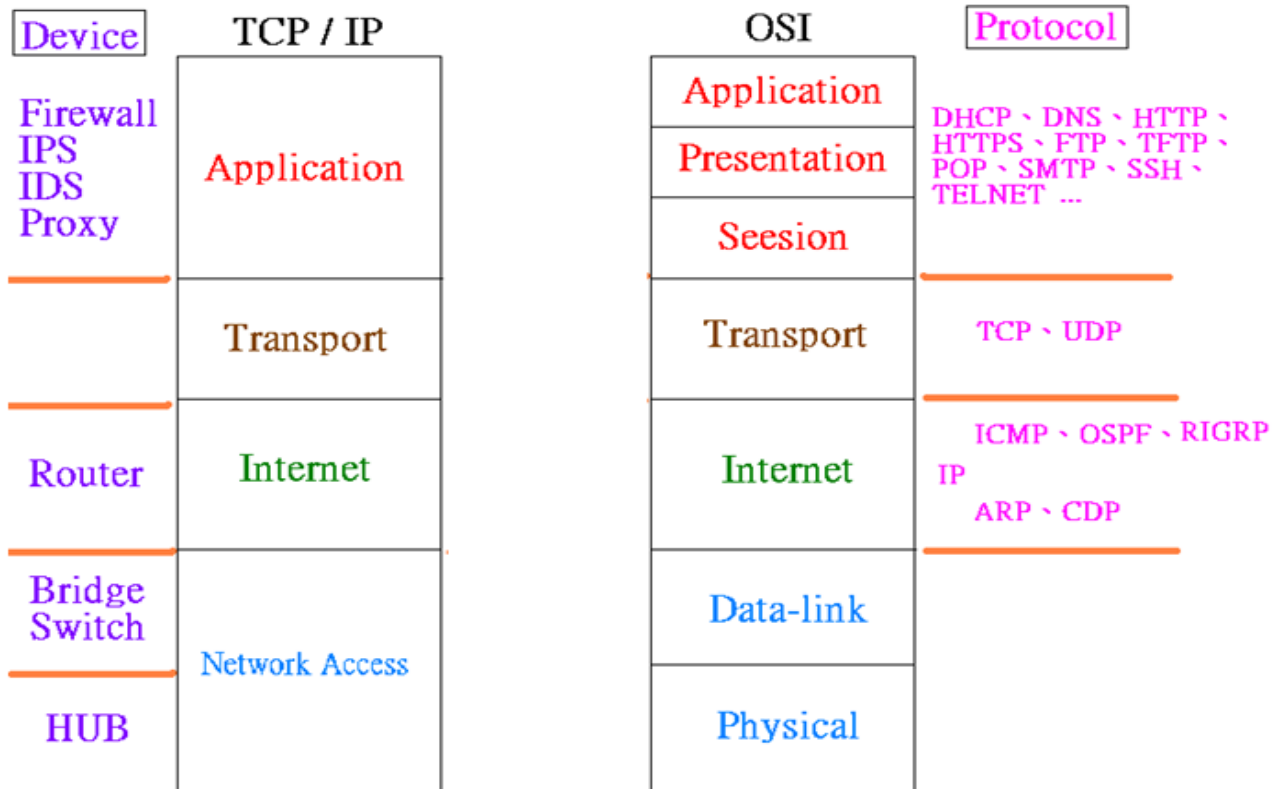
★ 缺點


- ★ 路由功能沒Router強大

Router(路由器)


- ★ 屬於OSI第三層(IP、ICMP)
 - ★ 路由器最主要的工作是決定要將網路封包送往何處
- ★ 與 L3 Switch的區別
 - ★ 三層交換器主打的功能點是二層交換技術，並附加一點路由轉發功能
 - ★ 路由器的主打功能是路由轉發，功能較強大，多用於大型網路架構
 - ★ 路由器網路介面類型較多

對照表





中華電信
小烏龜??



IP分享器
??

VLAN(802.1q)

- ★ 為什麼要用VLAN？

- ★ 效能

- ★ 若不分割vlan，broadcast的封包會傳送給所有不相關的電腦

- ★ 若分割vlan，broadcast的封包只會傳送給同一個vlan的電腦

- ★ 安全性：

- ★ 降低網路封包被竊聽的狀況，不同vlan之間，在沒有路由的狀況下不能互通

- ★ 彈性

- ★ 可在同一棟大樓或同一間辦公室區別不同網段

VLAN(802.1q)

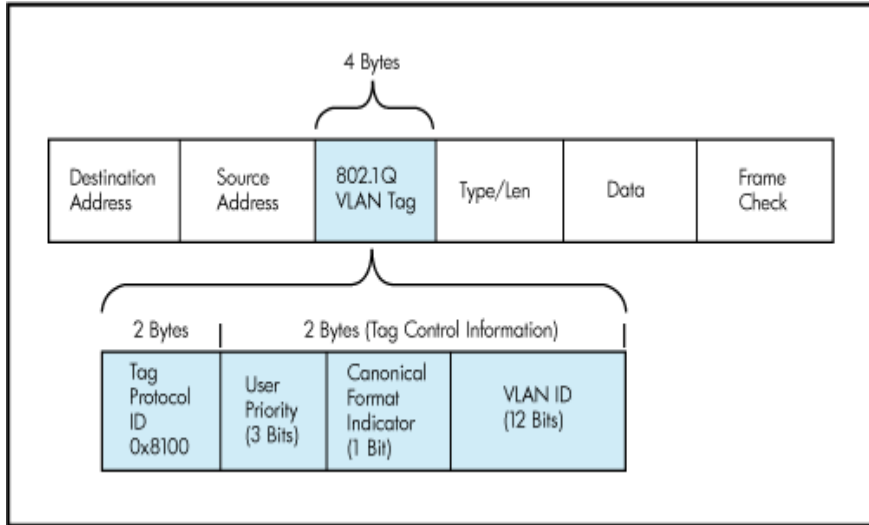
★ 什麼是VLAN(Virtual LAN)？

★ 把1個實體的LAN分割成多個虛擬的LAN



VLAN(802.1q)

★ Vlan ID(Tag)



(Untitled) - Wireshark

Filter: !stp

No.	Time	Source	Destination	Protocol	Info
269	56.661443	Cisco_82:c6:04	Cisco_82:c6:04	LOOP	Reply
270	57.841477	QuantaCo_ff:d3:5f	Broadcast	ARP	Who has 192.168.2.5? Tell 19...
278	59.307214	QuantaCo_ff:d3:5f	Broadcast	ARP	Who has 192.168.2.1? Tell 19...

Frame 278 (64 bytes on wire, 64 bytes captured)

- Ethernet II, Src: QuantaCo_ff:d3:5f (00:1e:68:ff:d3:5f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 2
- Address Resolution Protocol (request)

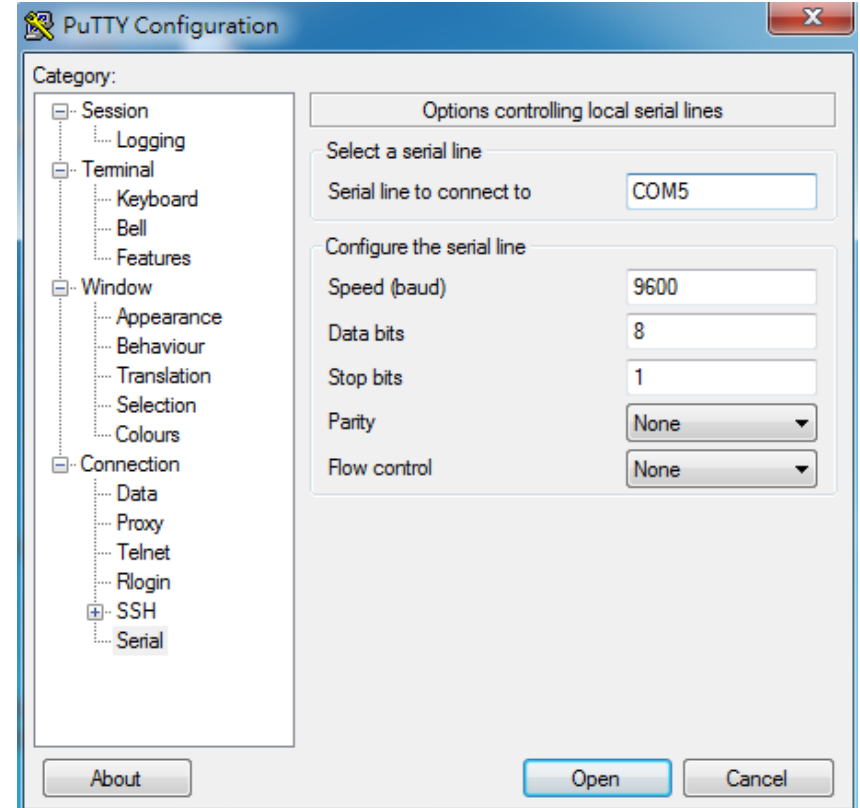
0010 08 06 00 01 08 00 06 04 00 01 00 1e 68 ff d3 5fh..

0020 c0 a8 02 02 00 00 00 00 00 00 c0 a8 02 01 00 00

0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

802.1Q Virtual LAN (vlan), 22 bytes | Packets: 332 Displayed: 80 Marked: 0 Dropped: 0 | Profile: Default

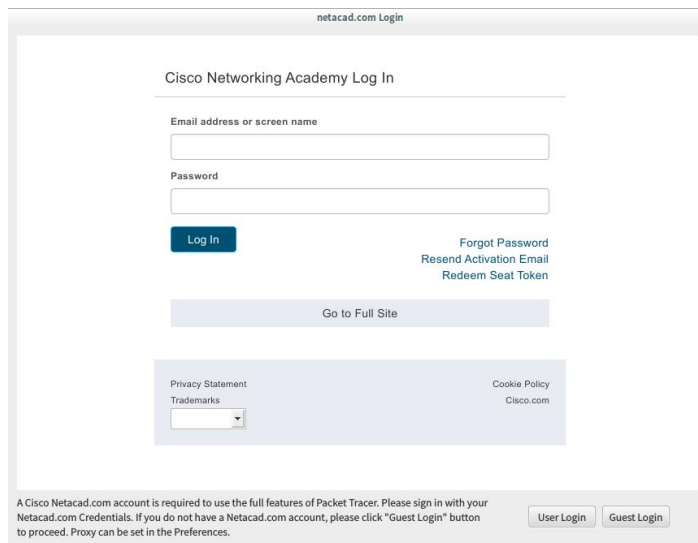
Switch初始連線方式(Console)



Cisco Switch 模擬器 (Packet Tracer)

註冊 Cisco Networking Academy

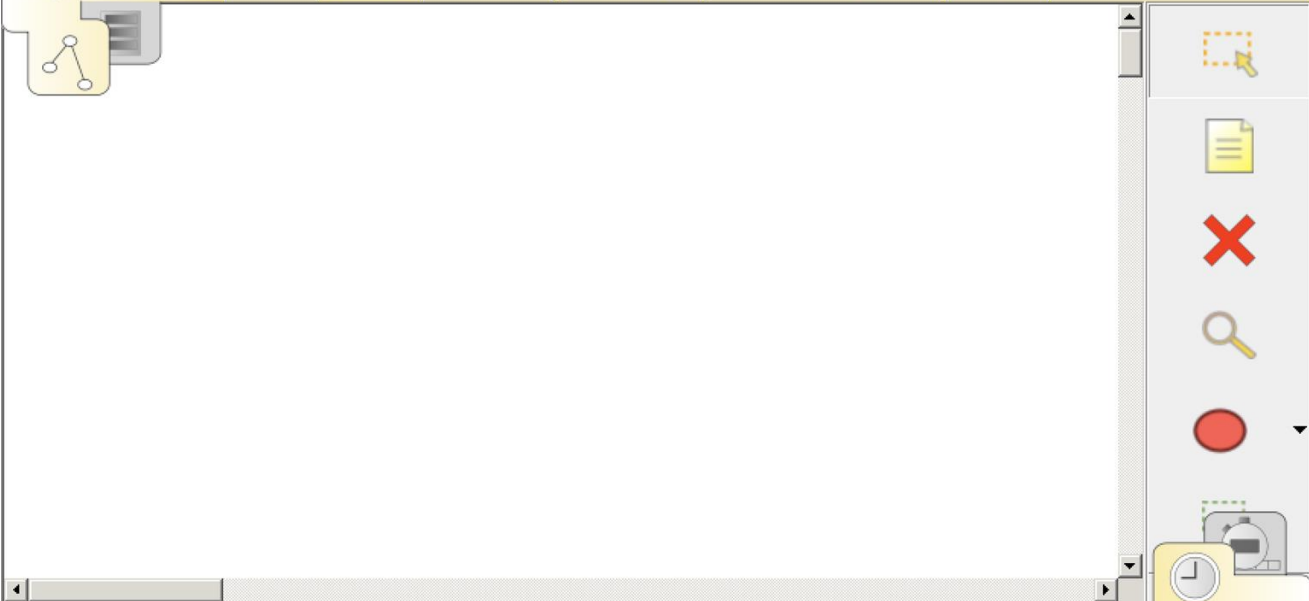
登入後下載 Packet Tracer



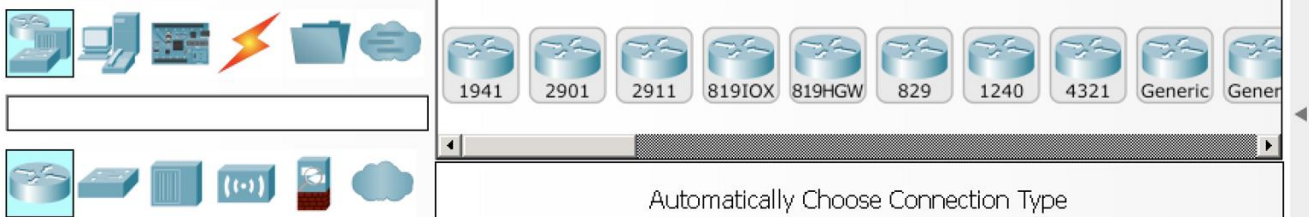
The screenshot shows the Cisco Networking Academy login page. At the top, it says "netacad.com Login". Below that, the title is "Cisco Networking Academy Log In". There are two input fields: "Email address or screen name" and "Password". A blue "Log In" button is positioned below the password field. To the right of the "Log In" button, there are links for "Forgot Password", "Resend Activation Email", and "Redeem Seat Token". Below these links is a "Go to Full Site" button. At the bottom of the main content area, there are links for "Privacy Statement", "Trademarks", "Cookie Policy", and "Cisco.com". At the very bottom of the page, there is a disclaimer: "A Cisco Netacad.com account is required to use the full features of Packet Tracer. Please sign in with your Netacad.com Credentials. If you do not have a Netacad.com account, please click 'Guest Login' button to proceed. Proxy can be set in the Preferences." and two buttons: "User Login" and "Guest Login".



Logical Back [Root] New Cluster Move Object Set Tiled Background Viewport Environment: 01:56:00



Time: 36:14:51 Power Cycle Devices Fast Forward Time **Realtime**



Switch基礎設定(使用者模式)

★ 使用者模式

- ★ 只能執行基本指令，不能設定Switch

```
Switch>?
```

```
Exec commands:
```

```
connect      Open a terminal connection
disable      Turn off privileged commands
disconnect    Disconnect an existing network connection
enable        Turn on privileged commands
exit          Exit from the EXEC
logout        Exit from the EXEC
ping          Send echo messages
resume        Resume an active network connection
show          Show running system information
telnet        Open a telnet connection
terminal      Set terminal line parameters
traceroute    Trace route to destination
```

Switch基礎設定(特權模式)

★ 特權模式

★ 可以檢視與更改Switch組態

★ 需在使用者模式下輸入 enable，才會進入特權模式

```
Switch>enable
Switch#?
Exec commands:
  clear          Reset functions
  clock          Manage the system clock
  configure      Enter configuration mode
  connect        Open a terminal connection
  copy           Copy from one file to another
  debug          Debugging functions (see also 'undebug')
  delete         Delete a file
  dir            List files on a filesystem
  disable        Turn off privileged commands
  disconnect     Disconnect an existing network connection
  enable         Turn on privileged commands
  erase          Erase a filesystem
  exit          Exit from the EXEC
```

Switch基礎設定(全域模式)

★ 全域模式

★ 更詳細設定Switch的各項功能(網路介面、Vlan、路由)

★ 需在特權模式下輸入 `configure terminal (conf t)`，才會進入全域模式

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#?
Configure commands:
  access-list      Add an access list entry
  banner           Define a login banner
  boot             Boot Commands
  cdp              Global CDP configuration subcommands
  clock            Configure time-of-day clock
  crypto           Encryption module
  do               To run exec commands in config mode
  enable           Modify enable password parameters
  end              Exit from configure mode
  exit             Exit from configure mode
  hostname         Set system's network name
  interface        Select an interface to configure
```

Switch基礎設定(基本指令)

- ★ 顯示功能
 - ?
- ★ 完成指令
 - tab鍵
- ★ 取消設定
 - no
- ★ 離開設定
 - exit

Switch基礎設定(基本指令)

- ★ 設定時間
 - Switch#**clock set 14:00:00 AUG 1 2018**
- ★ 重新啟動switch
 - Switch#**reload**
- ★ 初始設定
 - Switch#**setup**
- ★ 基本網路診斷指令
 - Switch#**ping**
 - Switch#**telnet**
 - Switch#**tracert**

Switch基礎設定(基本指令)

★ 顯示資料

○ show

- Switch#**show interface** (顯示網路介面狀態)
 - Switch#**show interface trunk** (顯示網路介面的trunk狀態)
- Switch#**show ip** (顯示IP相關狀態)
 - Switch#**show ip arp** (顯示目前IP與MAC的對應表)
 - Switch#**show ip interface brief** (顯示目前網路介面是否綁定IP)
 - Switch#**show ip route** (顯示目前路由的狀況)
- Switch#**show vlan** (顯示vlan狀態)
 - Switch#**show vlan brief** (顯示較精簡型的vlan狀態)
 - Switch#**show vlan id 1** (顯示Vlan id 1 的狀態)
- Switch#**show runnin-config** (顯示目前執行中的Switch設定檔內容)
- Switch#**show logging** (顯示Switch所記錄的相關訊息)

Switch基礎設定(interface)

★ 網路介面設定

- interface(縮寫為int)
 - Switch(config)#**int FastEthernet 0/1** (設定FastEthernet 0/1的網路介面)
 - Switch(config-if)#**description** (新增對網路介面的描述)
 - Switch(config-if)#**shutdown** (關閉網路介面)
 - Switch(config-if)#**no shutdown** (啟用網路介面)
 - Switch(config)#**int Vlan 1** (設定 Vlan 1的網路介面)
 - Switch(config-if)#**ip address 192.168.1.1 255.255.255.0**
(設定VLAN的IP位置)

Switch基礎設定(vlan)

★ Vlan設定

- Access Mode : 將網路介面加入一個VLAN(預設VLAN是1)
- 每一個埠同一個時間只能屬於某一個VLAN
- 設定方式
 - Switch#configure terminal
 - Switch(config)#interface vlan 2
 - Switch(config-if)#interface fastethernet 0/1
 - Switch(config-if)#switchport mode access
 - Switch(config-if)#switchport access vlan 2

```
Switch#sh vlan
```

VLAN	Name	Status	Ports
1	default	active	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, Gig0/1 Gig0/2
2	VLAN0002	active	Fa0/1

Switch基礎設定(vlan)

★ Vlan設定

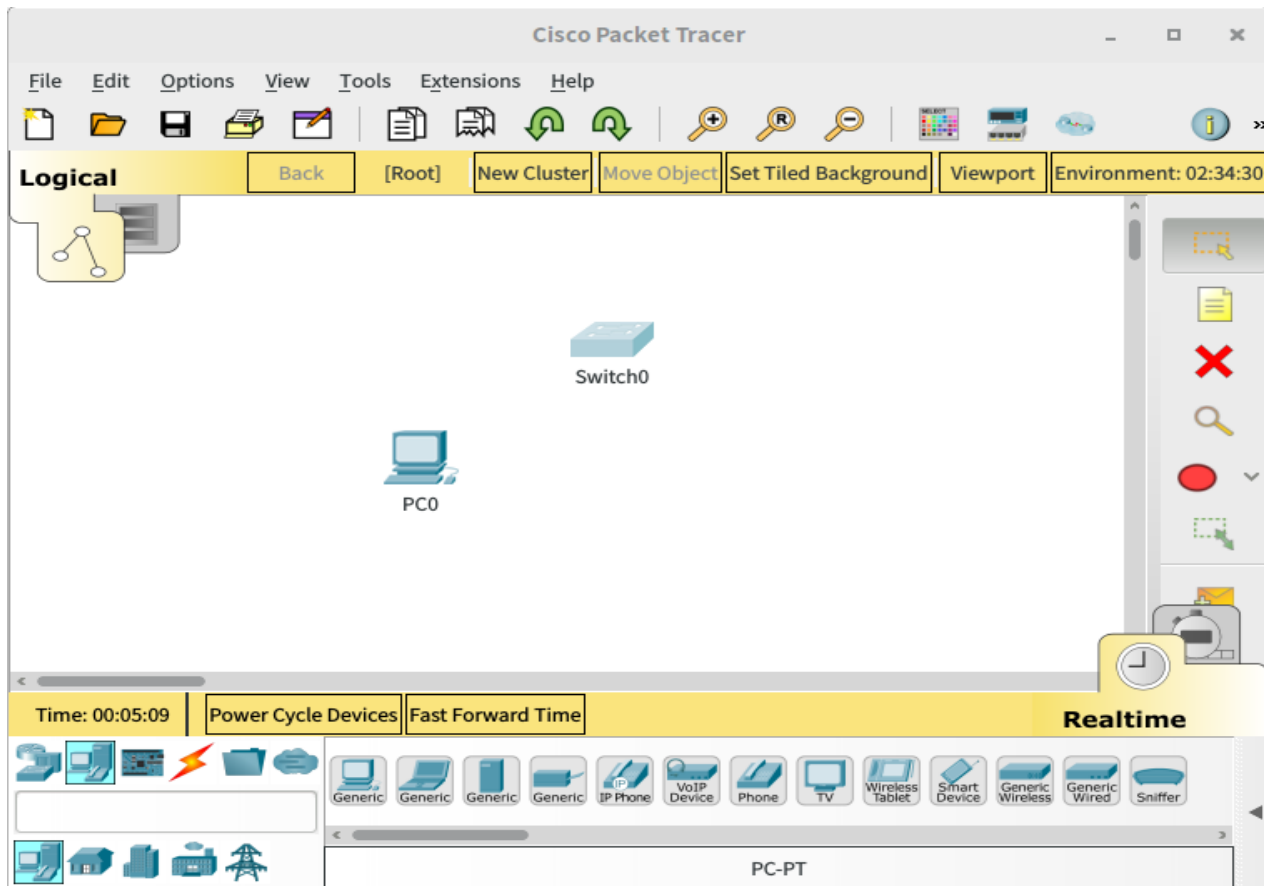
- Trunk Mode：讓多個vlan在同一個網路介面傳送資料，對接介面也需設定成Trunk mode
- 設定方式
 - Switch#**configure terminal**
 - Switch(config-if)#**interface fastethernet 0/2**
 - Switch(config-if)#**switchport mode trunk**
 - Switch(config-if)#**switchport trunk allow vlan 1,2**(只允許VLAN 1,2通過)

```
Switch#sh int trunk
```

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

Port	Vlans allowed on trunk
Fa0/2	1-1005

新增Switch(2960)及PC



Vlan 設定

- 新增vlan並設定interface

```
Switch>en
```

```
Switch#conf t
```

```
Switch(config)#int vlan 2
```

```
Switch(config-if)#description classroom
```

```
Switch(config-if)#int fa 0/1
```

```
Switch(config-if)#switchport mode access
```

```
Switch(config-if)#switchport access vlan 2
```

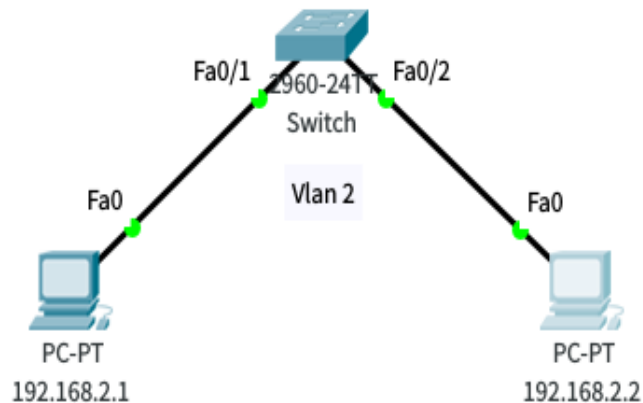
```
Switch(config-if)#int fa 0/2
```

```
Switch(config-if)#switchport mode access
```

```
Switch(config-if)#switchport access vlan 2
```

```
Switch(config-if)#exit
```

```
Switch(config)#exit
```



Vlan 設定

- 設定Vlan trunk(Switch 0)

Switch>en

Switch#conf t

Switch(config)#int vlan 2

Switch(config-if)#int vlan 3

Switch(config-if)#int fa 0/1

Switch(config-if)#switchport mode trunk

Switch(config-if)#int fa 0/2

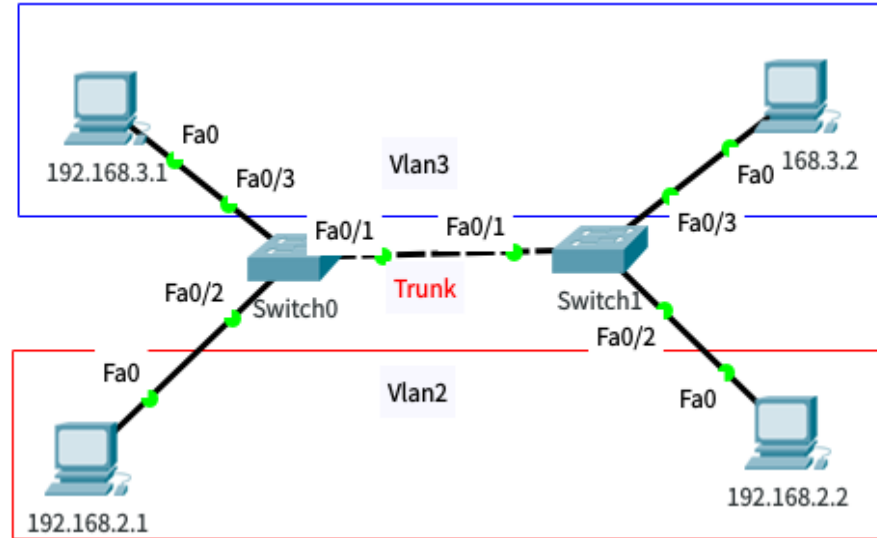
Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 2

Switch(config-if)#int fa 0/3

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 3



Vlan 設定

- 設定Vlan trunk(Switch 1)

Switch>en

Switch#conf t

Switch(config)#int vlan 2

Switch(config-if)#int vlan 3

Switch(config-if)#int fa 0/1

Switch(config-if)#switchport mode trunk

Switch(config-if)#int fa 0/2

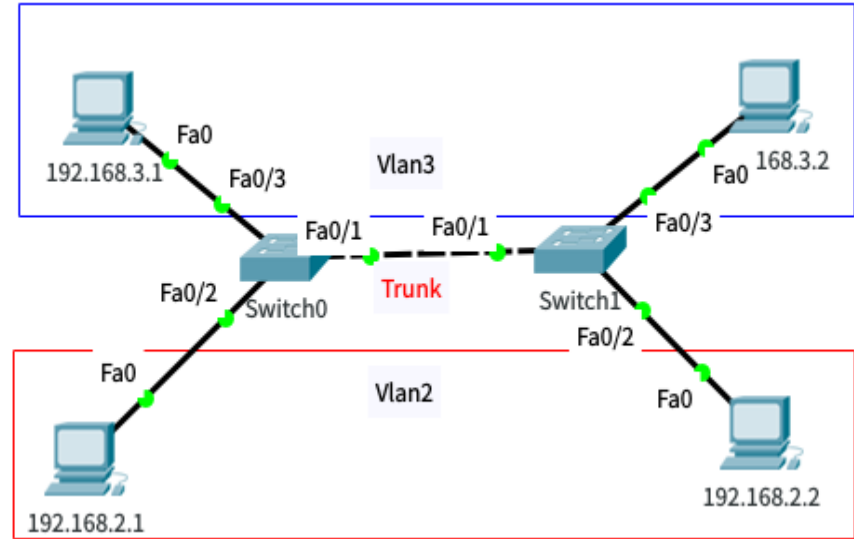
Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 2

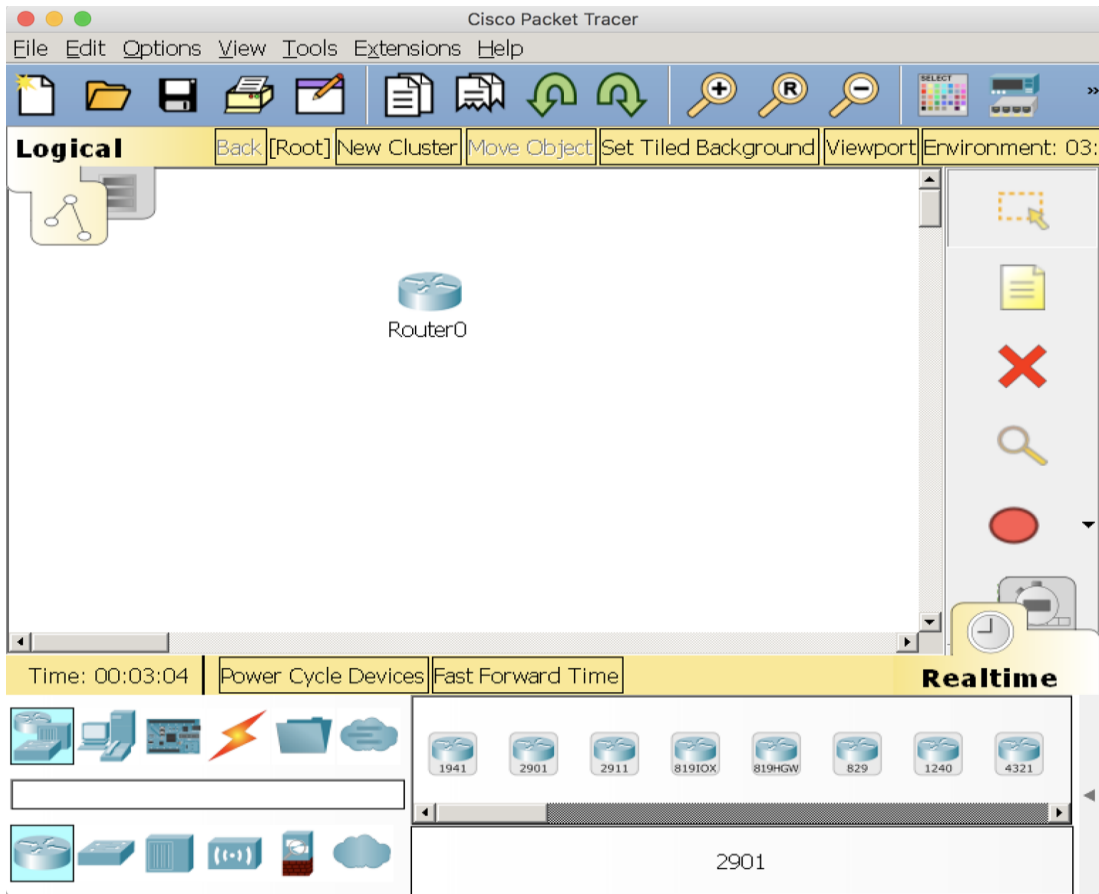
Switch(config-if)#int fa 0/3

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 3

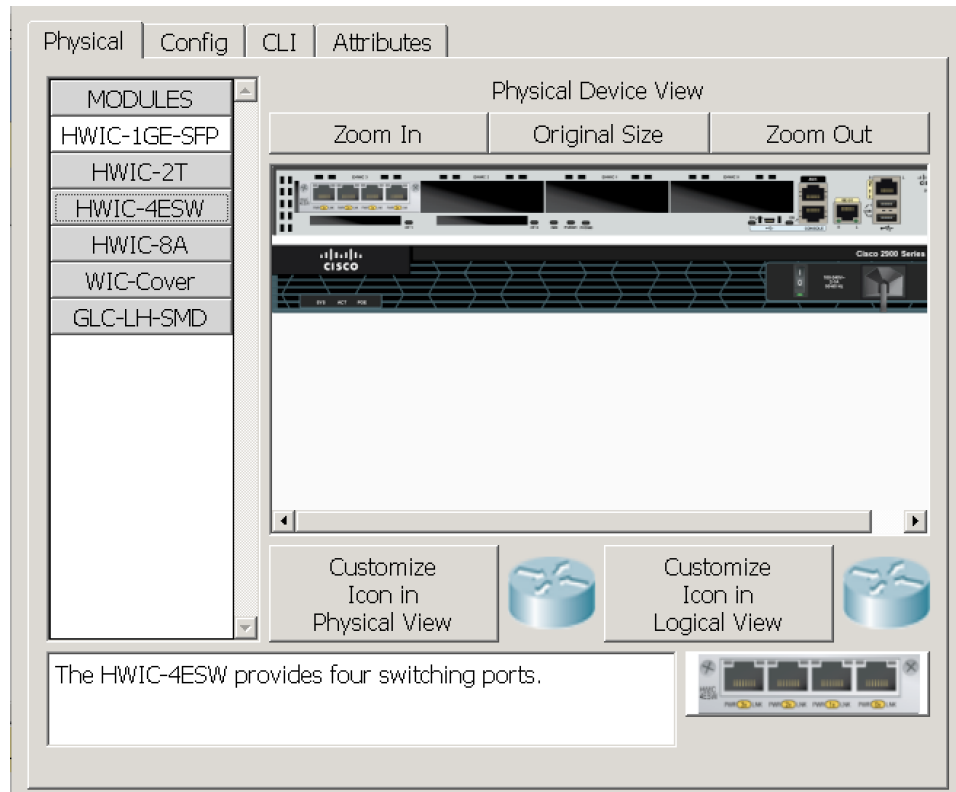


新增Router(2901)



新增Router的網路介面(HWIC-4ESW)

★需先關閉Switch電源



Vlan 設定

- 設定Vlan trunk(Router0)

```
Router>en
```

```
Router#conf t
```

```
Router(config)#int vlan 2
```

```
Router(config-if)#ip address 192.168.2.254 255.255.255.0
```

```
Router(config-if)#int vlan 3
```

```
Router(config-if)#ip address 192.168.3.254 255.255.255.0
```

```
Router(config-if)#int fa 0/3/0
```

```
Router(config-if)#switchport mode trunk
```

```
Router(config-if)#int fa 0/3/1
```

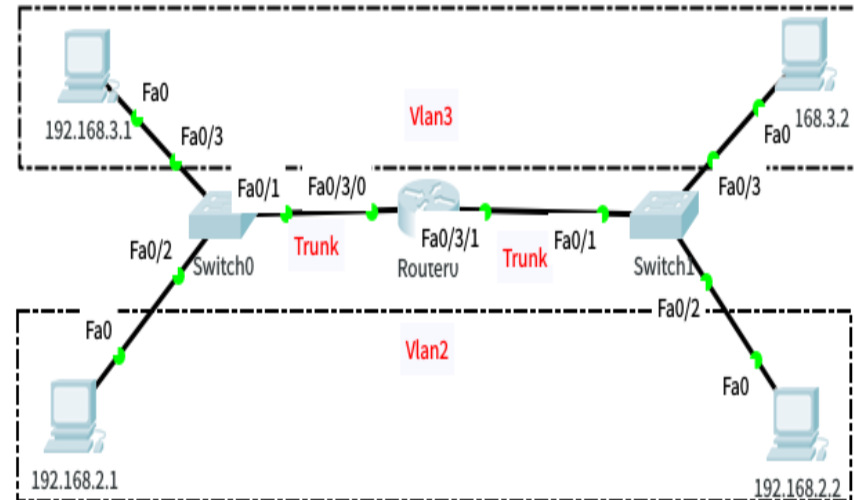
```
Router(config-if)#switchport mode trunk
```

```
Router(config-if)#int fa 0/3/2
```

```
Router(config-if)#switchport mode access
```

```
Router(config-if)#switchport access vlan 2
```

```
Router(config-if)#switchport access vlan 3
```



完成項目

1、設定4個vlan

- . Vlan1: 讓switch連線用
- . Vlan2: 192.168.2.0/24網段用
- . Vlan3: 192.168.3.0/24網段用
- . Vlan4: 192.168.4.0/24網段用

2、設定Vlan IP

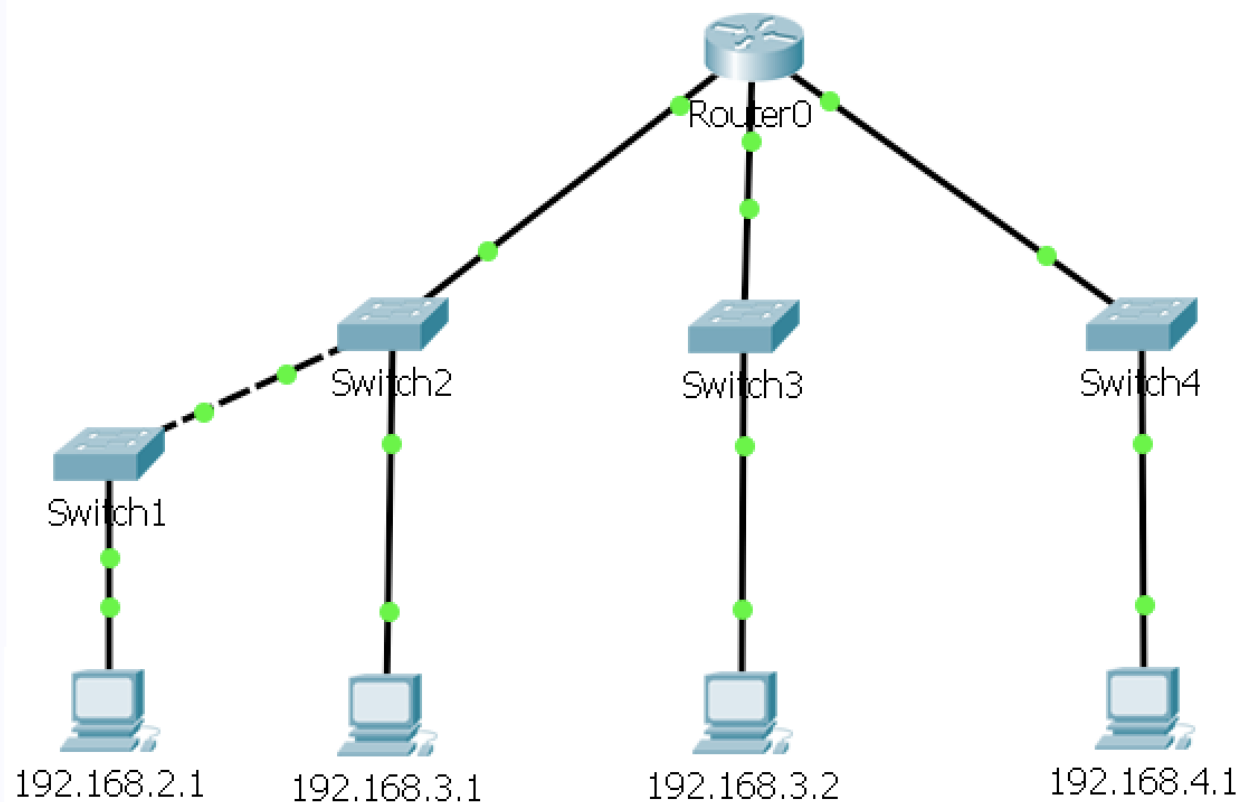
- . Vlan1: 192.168.1.254/24
- . Vlan2: 192.168.2.254/24
- . Vlan3: 192.168.3.254/24
- . Vlan4: 192.168.4.254/24

3、每個PC之間可以互相連線

- . 192.168.4.1可以ping到192.168.3.1
- . 192.168.3.2可以ping到192.168.2.1

4、設定Switch的管理IP

- . Switch1: 192.168.1.1/24
- . Switch2: 192.168.1.2/24
- . Switch3: 192.168.1.3/24
- . Switch4: 192.168.1.4/24



基本安全性設定

★ 設定console連線

- Switch(config)#**line console 0**
Switch(config-line)#**password 123**
Switch(config-line)#**login**

★ 設定telnet連線

- Switch(config)#**line vty 0 4**
Switch(config-line)#**password 123**
Switch(config-line)#**login**

★ 設定特權模式密碼

- Switch(config)#**enable password 123** (未加密)
Switch(config)#**enable secret 123** (有加密)

★ 將密碼有關的文字都加密

- Switch(config)#**service password-encryption**

查詢電腦在那個網路介面

★ 查詢 IP 所屬 MAC及VLAN

○ Router#sh ip arp

```
Router#sh ip arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.1.1 31 0001.42CE.7C80 ARPA Vlan1
Internet 192.168.1.2 29 0001.64E8.49C1 ARPA Vlan1
Internet 192.168.1.3 28 0001.C9E4.42E8 ARPA Vlan1
Internet 192.168.1.254 - 0060.2F7E.45E4 ARPA Vlan1
Internet 192.168.2.1 4 00E0.A33E.7C61 ARPA Vlan2
```

★ 查詢 MAC 所屬 Port

○ Router#sh mac-address

```
Router#sh mac-address-table
Mac Address Table
```

```
-----
Vlan Mac Address Type Ports
----
```

1	0001.42ce.7c80	DYNAMIC	Fa0/3/1
1	0001.63dd.c701	DYNAMIC	Fa0/3/2
1	0060.5c9b.7401	DYNAMIC	Fa0/3/1

儲存設定

★ 將更動後的設定儲存在Switch

- Switch# **copy running-config startup-config**

★ running-config

- Switch設定檔，儲存在RAM中，重新開機後，設定的資料被清除
- 執行階段，資料都保存在RAM

★ startup-config

- Switch設定檔，儲存在NVRAM中，重新開機後，設定的資料會保留
- 開機時，switch會先讀取 startup-config中的資料，之後再將資料寫入RAM