

Index

- 1. 基本指令(很基本、超基本)**
- 2. 帳號、密碼、安全性、遠端登入**
- 3. DHCP**
- 4. 開機流程、存檔機制、多重開機、TFTP 備援**
- 5. CDP / LLDP 鄰居發現協定**
- 6. 路由(Routing)協定原理**
- 7. Dynamic Routing Protocol 動態路由**
- 8. 遠送協定基礎**
- 9. RIP(Routing Information Protocol)**
- 10. EIGRP(Enhanced Interior Gateway Routing Protocol)**



- 11. OSPF(Open Shortest Path First)**
 - OSPF 常用指令**
 - Multi-Area OSPF**
 - OSPF 封包觀念**
 - OSPF Authentication 路由認證**
 - OSPF 路由表代碼**
 - OSPF Troubleshooting**
- 12. IPv6 基本觀念**

- [IPv6 Address Type](#)
- [IPv6 特殊位址](#)
- [IPv6 Configuration](#)
- [ICMPv6](#)
- [IPv6 Routing](#)
- [IPv6 Tunnel 轉換機制](#)

13. [Switch](#)

- [Switch Troubleshooting](#)
- [Switch IP 設定及 MAC 相關設定](#)
- [VLAN 觀念](#)
- [VLAN Configuration](#)
- [VLAN Trunk](#)
- [Inter-VLAN routing-ROAS\(Routing On A Stick\)](#)
- [Inter-VLAN routing-Layer3 Switch Routing](#)
- [Dynamic Trunking Protocol\(DTP\)](#)
- [Change Native VLAN](#)
- [限制 Vlan 傳送\(on trunk\)](#)

14. [Switch configuration Advanced -- VTP, Port-security, STP](#)

- [Vlan 備援與復原](#)
- [VTP\(Vlan Trunking Ptotocol\)——主幹通訊協定](#)
- [VTP 常用指令](#)
- [Switch Port Security &802.1x](#)、[常用指令](#)、[Violation mode](#)
- [STP\(Spanning Tree Protocol\)](#)、[STP 運作流程](#)、[STP 類型](#)
- [STP Advanced Configuration](#)
- [Portfast](#)、[BPDU Guard](#)

15. [Router & Switch Redundant](#)

- [Ether Channel-Switch](#)

- [FHRP\(First Hop Redundancy Protocol\)-Router](#)
- [HSRP\(Hot Standby Redundancy Protocol\)-Router](#)
- [VRRP\(Virtual Router Redundancy Protocol\)](#)
- [GLBP \(Gateway Load Balancing Protocol\)](#)

16. [ACL](#)

- [Standard ACL](#)
- [Extended ACL](#)
- [ACL on vty \(用 ACL 限制 telnet/SSH\)](#)
- [Other ACL Configuration\(查詢、註解\)、一些小技巧](#)
- [Wildcard](#)
- [IPv6 ACL](#)
- [NAT : Static、Dynamic、PAT、查詢設定、Trouble shooting](#)

17. [WAN Protocols](#)

- [Clock rate configuration](#)
- [PPP Configuration](#)
- [CHAP Configuration](#)
- [MLPPP Configuration](#)
- [PPPoE](#)

18. [Advanced WAN protocol—Frame-Relay, VPN, GRE](#)

- [VPN](#)
- [Cisco IPSec](#)
- [GRE Tunnel](#)

19. [BGP](#)

- [常用指令](#)
- [BGP Types](#)
- [BGP Neighbor](#)

20. [IP+IPv6+VLAN Troubleshooting](#)

- [用 IP SLA 進行故障檢修](#)
- [使用 SPAN 進行故障檢測](#)

■ IPv6 troubleshooting 、VLAN Troubleshooting

21. 網管工具—NTP, Syslog, Netflow, SNMP, SLA, SPAN, QoS

CCNP PART

1. Routing Concepts

- Well-known IPv4/v6 multicast address

2. Implementing RIPng

3. Advanced EIGRP

- 5 Packet Types
- EIGRP Stub Routing
- Reducing Query Scope by Using Summary Routes
- EIGRP Load Balancing
- EIGRP for IPv6

4.

基本常識



(關閉)IP 名稱查詢(節省時間)

```
Router(config)#(no) ip domain-lookup
```

在 Router(#\$%&)#各種模式下 show 指令

show 前面加個 do 就可以了

閒置多久後中斷連線

```
Router(config)exec-timeout X(分) X(秒) 可設 0 0 不中斷
```

在 consol/vty 跳過使用者模式，直接進入管理者模式

```
Router(config)#line console 0/ line vty
```

```
Router(config-line)#privilege level 15
```

在本地認證後(即帳號密碼)跳過使用者模式，直接進入管理者模式

```
Router(config)#username xxx privilege 15 password xxx
```

單一介面使用雙 ip --一個不知所云並且最好不要用的功能

```
(config-if)#ip address ip mask secondary
```

引流符號 | 用在 show 任何東西時快速查找關鍵字，比如 show ip route | include 192.168

思科自動安全設定—自動幫你關掉多餘功能、用不到的埠等等

```
#auto secure
```

使用進階式指令編輯熱鍵

<Ctrl><A> 將游標移至指令列最前

<Ctrl><E> 將游標移至指令列最後

<Ctrl><Z> 瞬移至特權模式

<Ctrl><W> 刪除一個字串

<Ctrl><U> 刪除一整列

<Ctrl><Shift><6><x> 強制中止現階段工作

<Esc><F> 移動游標後移一個字串 word.

<Esc> 移動游標前移一個字串 Word

<Tab> 自動補齊指令

--沒有前贅就是 switch/router 通用

· 在通訊界面設定模式下使用此命令可關閉通訊界面

```
Router/Switch(config-if)# shutdown
```

· 在通訊介面設定模式下使用此命令可開啟通訊介面

```
Router/Switch(config-if)# no shutdown
```

檢視輸入過的指令(history)

```
#show history
```

檢視終端機設定及歷程緩衝區大小

```
#show terminal
```

更改 history 的紀錄數量-歷程緩衝區指令

```
#terminal history size 5
```

找關鍵字

```
#show XXX | include YYY (包含)
```

(Ex: #show interface |include fastethernet)

```
#show XXX | begin YYY (開始)
```

```
#show XXX | section YYY (章節)
```

◎設定 interface IP

```
Router(config)# interface XXX(EX:g0/0)
```

```
Router(config-if)# ip address XXX.XXX.XXX.XXX(IP) XXX.XXX.XXX.XXX(mask)
```

```
Router(config-if)# no shutdown
```

☆設定 interface IP 使用 dhcp—(config-if)#ip address dhcp

◎設定 Router Loopback

```
Router(config)# interface loopback 0
```

```
Router(config)# ip address XXX.XXX.XXX.XXX(IP) XXX.XXX.XXX.XXX(mask)
```

◎看版本、組態檔名稱與來源、開機時間、configuration register(機碼)、開機映像

```
#show version
```

◎看裝置 SN

```
#show inventory
```

◎看 IOS(版本)

```
#show flash
```

◎看單獨介面

```
#show interface x x/x (status)
```

◎看所有介面狀態

```
#show interface status
```

◎看歷程紀錄

```
r#show logging
```

◎看時間

```
#show clock
```

◎設定時間

```
#clock set
```

```
#clock timezone 要打的名稱 +X(時區)
```

◎開機標語

```
Router/Switch(config)#banner motd # XXX(可換行) #
```

◎重開機

```
#reload
```

◎通訊介面說明

```
Router/Switch(config-if)#description XXXX(要打的文字) → 查詢用 sh int description
```

◎設定 show 顯示行數，x=0 一次跑完

```
#terminal length X
```

◎查看 interface 狀態(含 Loopback)

```
#show ip interface brief 提供介面的精簡概要
```

```
#show ip interface 提供有關路由器介面之第 3 層設定的資訊
```

◎檢查各介面 L1 與 L2 的狀態

```
#show protocols
```

◎連續 ping 多次(測試連線品質)

```
#ping ip repeat 次數
```

```
#ping → 只輸入 ping 再 enter 的話可使用較複雜功能，ip、repeat 次數、data size、source 等等
```

```
#ping? → 可使用多種協定
```

有時候剛設好 ip 互 ping 時會看到!!!!，而不是五個!，第一個.是逾時，是因為 ARP 需要時間將 IP 位址解析為硬體 MAC。

◎全/半雙工+速度設定

```
#duplex auto/full/half
```

```
#speed 10/100/1000
```

◎讓控制台訊息不打斷輸入中指令

```
(config-line)#logging synchronous
```

cmd 指令

◎ipconfig—不解釋

◎檢查主機路徑表

```
route print
```

◎列出 arp 表

```
arp -a
```

◎清空 arp 表

```
arp -d
```

◎清空

```
cls
```

◎查找自己的 DNS

```
nslookup
```

◎可在 CMD 下直接輸入網址找其 DNS

```
set q=a
```

◎traceroute

```
tracert IP
```

◎看 port 有開哪些

```
netstat -na| more
```

◎DHCP

```
netsh interface ip set address "區域連線" source=dhcp
```

```
netsh interface ip set dns "區域連線" source=dhcp
```

◎Static IP

```
netsh interface ip set address name="區域連線" source=static address=192.168.102.100
```

```
mask=255.255.255.0 gateway=192.168.102.254 gwmetric=1
```

```
netsh interface ip set dnsservers name="區域連線" source=static address=8.8.8.8
```

帳號、密碼、安全性、遠端登入



※遠端登入：Telnet

※認證方式：SSH、AAA(TACACS+, RADIUS)

· VTY：Virtual Type Terminal(虛擬終端機)，一個 telnet 連線用掉一個 vty，telnet 0 4 代表 vty0-vty4 五個 vty，即同時可登入五個 vty telnet。

· AAA：將帳號資訊統一儲存管理，意指驗證(Authentication)、帳務管理(Accounting)、授權(Authorization)；驗證為檢查帳密；帳務管理為該帳號使用資源計量，可做收費計算，比如該帳號使用網路頻寬的計費；授權為該帳號在系統中可用的權限。

TACACS+/RADIUS 又稱為 Dynamic ACL

· AAA Server：AAA 分為 Local 及 Server-Based。Local 的帳號資訊存在本地機器並只有 Authentication 功能；Server-Based 是將帳號資訊存在 AAA Server，支援 AAA 全功能。AAA Server 分兩種，如下表：

Feature	TACACS+	RADIUS
Transport Protocol	TCP	UDP
Port Number	49	1645,1812
Password Encryption	Y	Y
Package Encryption	Y	N
Patent	Cisco	RFC 2865

◎啟用 AAA 認證

Router(config)#aaa new-model ←啟用 AAA 功能

Router(config)#aaa authentication login xxx local ←認證來源為 xxx，使用本地帳密

Router(config)#line vty 0 4

Router(config-line)#login authentication xxx ←在 vty 套用 aaa 的 xxx 認證來源

◎查詢 AAA 連線狀態

Router#show aaa sessions

◎設定帳號密碼認證 ←在 vty、console 模式下，以 login local 指令啟用

Router(config)#username XXX password XXX

Router(config)#login local(向本機資料庫驗證) →和 login 的差別，多一個帳號

◎設定 Console 密碼(單純密碼)

Router(config)# line console 0

Router(config-line)# password cisco

Router(config-line)# login →login 的意思是「啟用密碼」

◎設定遠端登入(Virtual Terminal)密碼(單純密碼)

Router(config)# line vty 0 4 →也可各別設定不同 vty 的密碼，但沒啥卵用

Router(config-line)# password XXX

Router(config-line)# login → 和 login local 的差別，不用帳號

p.s. vty 預設值為啟動 login，可用 no login 來使 telnet 無需密碼直接登入

◎設定特權模式密碼(Enable Password)

Router(config)# enable password XXX

◎設定密碼加密(Password Encryption)

Router(config)# service password-encryption → 直接 no 就可關閉，但已加密的不會變回來

※如果要關閉加密，要先 show run 一次密碼加密才會生效

◎強制指定密碼長度

Router(config)#service password min-length x → x 代表密碼最低位數

◎設定特權模式帳號密碼

Router(config)#username XXX pri 15 password XXX

(p.s. 權限 1-14 分別有不同功用，15 為最高)

◎在 consol/vty 跳過使用者模式，直接進入管理者模式

Router(config)#line console 0/ line vty

Router(config-line)#privilege level 15

◎在本地認證後(即帳號密碼)跳過使用者模式，直接進入管理者模式

Router(config)#username xxx privilege 15 password xxx

◎遠端登入

#telnet ip

◎同時 telnet 至多個裝置(暫離但不斷線)

#ctrl+shift+6+x

◎遠端登出

Quit/logout/exit

※Config 要給別人的話，記得把 username 和 password 拿掉

◎使用 type5 加密 enable password 內容

Rounter(config)#enable secret XXX

◎將所有 password 後的文字用 type7 加密 → 沒啥卵用

Router(config)#service password-encryption

◎閒置多久後中斷連線—前置動作，要先 login 及有密碼 **--packettracer 不支援**

Router(config)exec-timeout X(分) X(秒) 可設 0 0 不中斷

◎檢視目前多少使用者在此設備

show user → * 代表自己使用中的連線

◎中斷其他連線

clear 對方的 telnet 編號 → 比如說 line vty 0

◎console 介面、ssh 登入標語

Router(config)#banner motd # XXX(可換行) #

◎遠端登入標語

Router(config)#banner login

◎看相連的設備(瞭解網路骨幹)

Router#show cdp neighbors

SSH 安全連線設定

Router(config)#ip domain-name cisco.com →設定 Domain 名稱

Router(config)#username cisco password cisco →設定本地帳密

Router(config)#crypto key gen rsa →使用 RSA 將 Domain+Hostname 產生新的金鑰

How many bits in the modulus [512]: 1024 輸入長度 512-2048 都可

p.s. SSH 的 RSA 加密方式是由 Hostname 及 Domainname 產生 key，故 hostname 必須設定

Router(config)#ip ssh version 2 →啟用 SSH 第 2 版(要有 rsa 後才能啟用)

Router(config)#line vty 0 15 →啟用 vty 介面的 SSH

Router(config-line)#login local →本機驗證

Router(config-line)#transport input all/none/ssh/telnet →全開/不開放/SSH/telnet 登入 vty

p.s. 使用 transport input ssh 後，就不能用 telnet 了

p.s. 要同時使用 telnet & ssh，把最後一行指令改成 transport input ssh telnet 就可以

◎使用 ssh 登入其它路由器

ssh -v 版本 1 或 2 admin/帳號 目的地 IP

◎檢視 SSH 版本

show ip ssh



DHCP (自動取得 IP 位址)

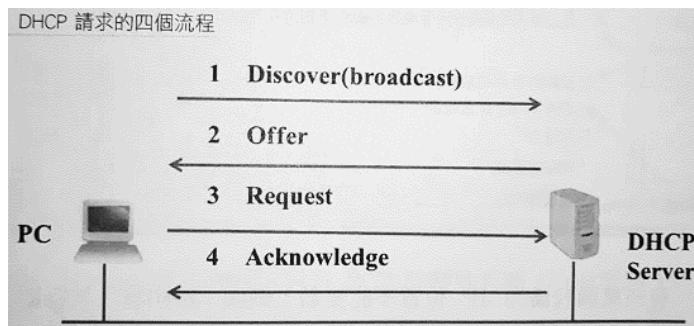
· DHCP 給 IP 的方式：

Manual：Administrator 為 Client 指定固定 IP，DHCP Server 將該 IP 傳給 Client。

Automatic：DHCP Server 從 DHCP Pool 中選擇靜態 IP，永久配置給 Client。

Dynamic：DHCP Server 從 DHCP Pool 中動態配置 IP 給 Client，有使用期限，到期重分 IP

· DHCP 分配流程與封包類型

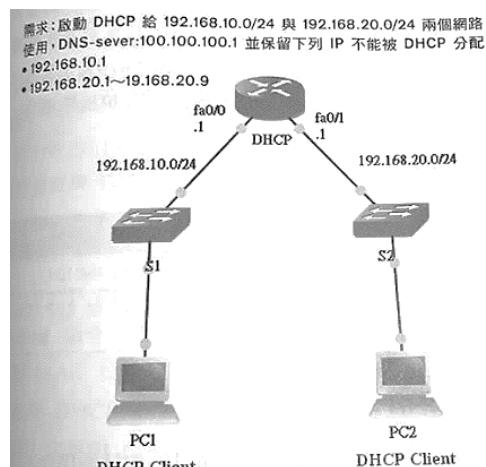


- 一、DHCP Client 廣播 **DHCPDISCOVER** 封包，尋找 DHCP Server，此時 Client 沒有 IP，所以 DHCPDISCOVER 封包的來源 IP 為 0.0.0.0，目的 MAC 為 FF-FF-FF-FF-FF-FF
- 二、DHCP Server 收到 DHCDISCOVER 封包時，使用 DHCPDISCOVER 封包中 Client MAC 查詢資料庫是否配過 IP，若有則延用，沒有就從 DHCP Pool 選一個 IP，發出 **單播 DHCPOFFER** 封包傳給 DHCP Client。
在此步驟 DHCP Server 還會使用 **ping** 及 **gratuitous ARP** 檢查 IP 衝突(Conflicts)，有衝突則該 IP 被移出 DHCP Pool，直到管理者手動處理。
- 三、DHCP Client 收到 DHCPOFFER 封包時，回傳 **DHCPREQUEST 廣播** 封包，此封包向 DHCP Server 申請該 IP，當多台 DHCP Server 存在時，Client 會收到多個 DHCPOFFER 封包，這時候會以第一個收到的為主
Client 也用 **gratuitous ARP** 檢查 DHCPOFFER 封包提供的 IP 是否衝突，若衝突則 Client 發送 **DHCP DECLINE** 封包給 Server，重新執行第一步驟。
- 四、DHCP Server 收到 DHCP REQUEST 封包後，使用 **單播 DHCPACK** 封包回復 DHCP Client。
DHCP Client 分配到的 IP 是有租期的，因此 Client 必須定期發送請求封包給 DHCP Server 更新租期。

Router/Switch as DHCP Server

· 設定 DHCP Pool

以右圖為例，有兩個網段要使用 DHCP，就必須提供兩個 DHCP Pool，並且路由器上要設定 DNS & GW



指令	說明
dhcp(config)#ip dhcp pool <u>Lan10</u>	建立 Lan10 DHCP Pool
dhcp(dhcp-config)#network <u>192.168.10.0</u> <u>255.255.255.0</u> #此處 255.255.255.0 可改成/24	設定 Lan10 Pool 可分配的 IP Range 為.10 網段
dhcp(dhcp-config)#default-router <u>192.168.10.1</u> #192.168.10.1 為 dhcp-router 的 f0/0	設定 Lan10 底下 client 的預設閘道，通常是 dhcp-server ip
dhcp(dhcp-config)#dns-server <u>100.100.100.1</u>	設定 DNS-Server IP
dhcp(config)#ip dhcp pool <u>Lan20</u> 以下同 Lan10，省略	Lan20, dhcp pool .20, gw=.20.1, DNS-Server IP=100.100.100.1
dhcp(dhcp-config)#lease <u>0 8</u> #前面是 days 後面是 hours	設定租用時間

• 設定保留 IP 範圍 (要在 dhcp 設定前做，不然一樣有可能分派到)

常識性問題，.1 給 GW，或是.254 給 Server，以本範例設定：

指令	說明
dhcp(config)#ip dhcp excluded-address <u>192.168.10.1</u>	保留單一 IP
dhcp(config)#ip dhcp excluded-address <u>192.168.20.1</u> <u>192.168.20.9</u>	保留整個 IP 範圍(9 個 IP)

• 驗證 DHCP

指令	說明
#show ip dhcp binding	列出目前提供給客戶端的所有 IP 狀態資訊
#show ip dhcp pool [poolname]	列出設定的 IP 範圍，及目前使用中位址數量，和每個 POOL 被使用的高水位等統計值
#show ip dhcp server statics	列出 DHCP Server 的很多統計值
#show ip dhcp conflict	可以看出 IP 衝突的狀況

◎查詢 DHCP 設定

PC(cmd)#ipconfig

DHCP Snooping

防止 DHCP 攻擊(spoofing attack & starvation attack)的技術。

將 port 分為 trusted & untrusted(預設)，DHCP 所有封包都可經過信任埠，不信任埠只能接收 DHCP Client 的封包。若非信任埠收到 DHCP Server 封包，該埠會直接丟棄以防止惡意 DHCP。

當電腦經過不信任埠取得 IP 組態後，交換器會將電腦 MAC 與取得 IP 位址紀錄到 **DHCP snooping bindle table**，作為合法的 MAC/IP 對應關係。

◎ Snooping 指令

Switch(config)#ip dhcp snooping	啟用 snooping 功能(在 vlan 上)
Switch(config)#ip dhcp snooping vlan __	
Switch(config-if)#ip dhcp snooping trust	設定該埠為信任埠
Switch#show ip dhcp snooping	查詢 snooping 設定
Switch#show ip dhcp snooping binding	查詢 binging table

DHCP Lab

◎ DHCP server configuration

Router(config)#ip dhcp pool XXX

◎ DHCP Lab

1. 排除 DHCP 範圍 -要先做不然會指派到無效 IP

Router (config)#ip dhcp excluded-address 起點 終點

2. 派發 POOL

Router (config)#ip dhcp pool XXXX →派發 pool 名稱

Router (dhcp-config)#network X.X.X0 /24 →pool 範圍，此處可用/輸入

3. 指定 DNS Server

Router (dhcp-config)#dns-server 8.8.8.8

4. 指定 default gateway

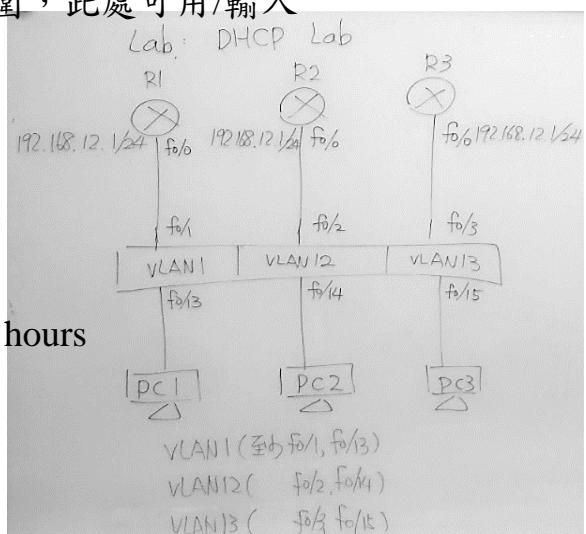
Router(dhcp-config)#default-router 192.168.12.1

5. 設定租用時間

Router(dhcp-config)#lease 0 8 →前面是 days 後面是 hours

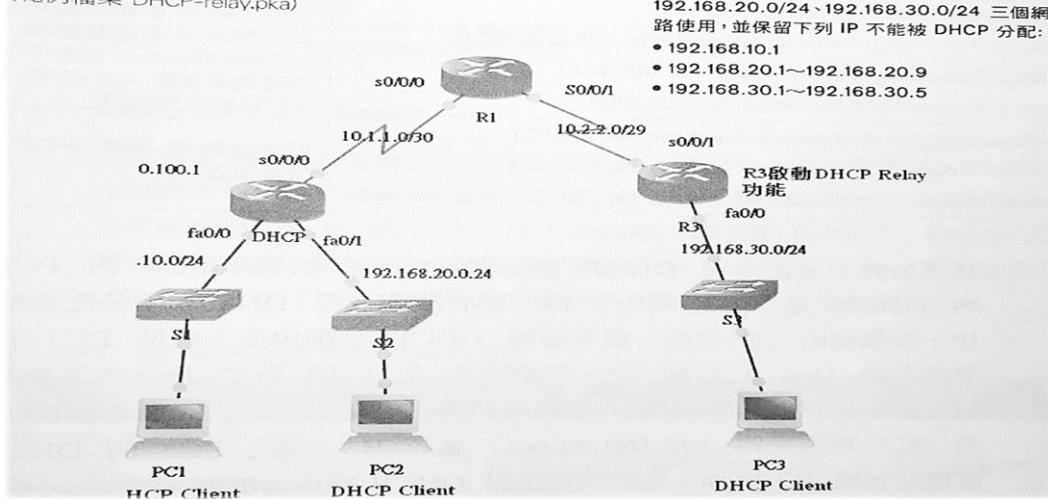
檢查 PC 端：ipconfig

檢查 Router 端：show ip dhcp binding(確認已派發的 IP)



DHCP Relay

圖表 16-79 DHCP Relay 練習架構
(範例檔案 DHCP-relay.pka)



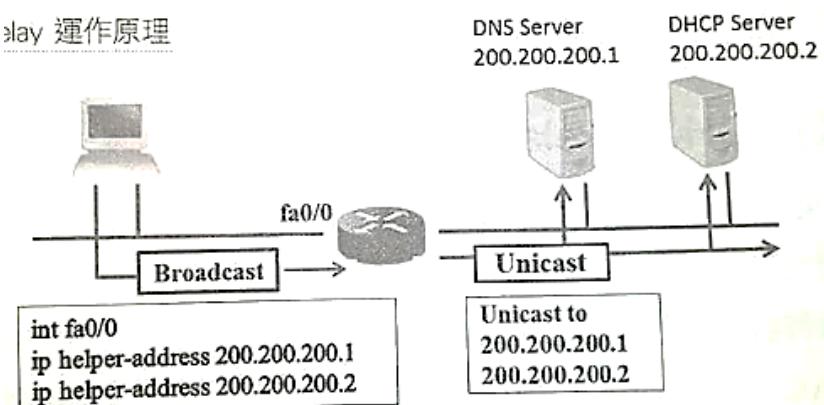
狀況一、R3 底下的.30.0 網段並沒有直連在 DHCP Router，所以 PC3 的 DHCPDISCOVER 封包無法送到 DHCP Router，故在 R3 啟用 DHCP Relay。

狀況二、另外，一個 Router 扣掉序列埠也就只有兩個 port，如果我要接更多個網段，只能使用少數交換器開多個 vlan，但這樣無法用 DHCP 的那僅有的兩個介面設定。(DHCP Relay Lab 的圖)

★DHCP Relay 原理

將 DHCP 廣播封包轉成單播封包，直接送到 DHCP 路由器，如下圖，路由器收到廣播封包的介面，可以設定多個 Relay IP(或稱為 Helper address)，路由器就會將 DHCP 廣播封包轉成單播封包，而單播封包的目的 IP 為 Relay IP，因此 Relay IP 若設定兩個，就會產生兩個單播封包，另外路由器除了會將 DHCP 的廣播封包轉成單播封包，針對某些協定的廣播封包也可以設定 Relay IP 轉成單播封包。

Relay 運作原理

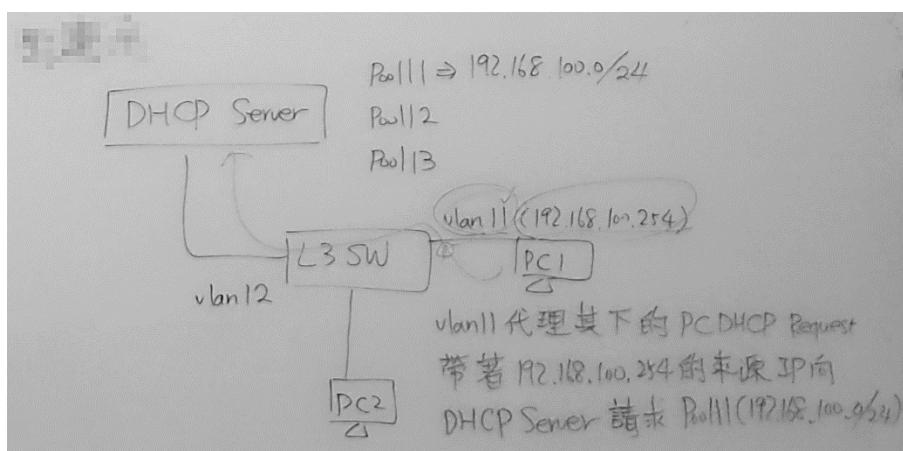


• 設定 DHCP Relay (以最上圖為例)

由於 R3 是由 fa0/0 收到 PC3 的 DHCP 廣播封包，因此要在 R3 的 fa0/0 介面執行 **ip helper-address** 指令，此指令會將 DHCP 廣播封包以單播傳送的方式送到指定的 IP，如下表指令所示，請注意 **Relay IP 可以是 DHCP 路由器上的任何一個有啟動的網路介面 IP**，另外 Relay IP 也可設定多個，如此路由器就會將廣播封包轉為多個單播封包。

指令	說明
R3#int f0/0	在 R3 的 f0/0 設定 DHCP Relay，將 DHCP 廣播封包以單播傳送的方式送到 10.1.1.1(DHCP Router 的 s0/0/0)
R3(config)#ip helper-address 10.1.1.1	

▲DHCP Relay Lab(另一種 DHCP Relay)



- 接 DHCP Lab，一個 vlan 要用一個 server，很浪費
- 所以用 DHCP Relay 讓多 vlan 只用一個 DHCP Server
- 右側為示意圖

◎DHCP Relay LAB (照片在上頁)(先完成基本設定)

指令	說明
Switch#int f0/1 Switch(conf-int)#no switchport Switch(conf-int)#ip add <u>192.168.1.254</u> <u>255.255.255.0</u>	將 L3 switch 的介面改造成 Route Port，然後就可以給它 ip 了
Switch(config)#ip routing	將 Layer3 Switch 啟動路由功能
Switch#show ip route	不解釋，承上，檢查一下 Lab 中應要有 4 筆直接路由
Switch(conf)#int vlan <u>x</u> 注意要先有 vlan x Switch(conf-int-vlan)#ip helper-address <u>192.168.1.1</u>	在 Switch 上的所有 vlan 設定 DHCP Relay IP #192.168.1.1 為 dhcp server ip
R1(config)#ip dhcp pool POOL_11 R1(config-dhcp)#network <u>192.168.11.0 /24</u> R1(config-dhcp)#default router <u>192.168.11.254</u>	在 R1 上新增三個 POOL 以回應 switch 底下 三個 vlan 的 dhcp request #192.168.11.0/24 為 POOL_11 的 IP 範圍 #192.168.11.254，POOL_11 的 gw，即為各 vlan IP #Lab 中 12.0 & 13.0 網段比照設定

Trouble—pc1、2、3 在完成 DHCP Relay 後還是無法得到 ip?

因為所有 vlan 和 192.168.1.0 不在同一網段，所以要...手動在 DHCP server 上做 static route
讓 ip→192.168.1.254→192.168.11.254
ip→192.168.1.254→192.168.12.254
ip→192.168.1.254→192.168.13.254
(指令...ip route...)

◎在 L2 底下的介面指向 DHCP 伺服器 IP

#ip helper address IP

開機流程、存檔機制、多重開機、TFTP 備援



◎Running Config 的合併與覆蓋

copy 到 run(RAM)的組態檔是用 merge(合併)方式，其它的不管是從 run copy 到 tftp 或 startup(NVRAM)或這兩個互 copy 通通都是用 Cover(覆蓋)方式進行。

※Merge—舊的 running config 和新的比較：

1. 舊檔案有，新檔案無，則保留。
2. 舊檔案有，新檔案也有，則覆蓋。
3. 舊檔案無，新檔案有，則寫入。

※Cover—新檔案完全取代舊檔案

◎Save device configuration

Router#copy running-config startup-config

Router#write 也可

◎Load device configuration

Router#copy startup-config Running-config

◎Back up a configuration to the TFTP server

Router#copy running-config tftp:

◎Delete NVRAM configuration

Router#write erase

◎Sync NVRAM and RAM

Router#write

◎Check now configuration

Router#show startup-config

Router#show configuration

Router#show running-config

◎清除現存設定，回復出場狀態

Router#write erase

Router#erase startup-config

Router#erase nvram

◎查看存在 flash 中的 IOS 狀態

Router#show flash:

System flash directory:

File Length Name/status

3 33591768 c1841-advp�servicesk9-mz.124-15.T1.bin →IOS 檔案名稱(最前面的 3 不算)

- c1841—型號
- advp�services—??映像檔，在 IOS15 版後，有 universal 映像檔
- mz—檔案格式，m=runs in RAM；z=compressed
- 124-15—版本編號，主版本 12、副版本 4.15

· T1—維護時間，M 代表擴展維護版本，Cisco 提供 44 月維護期；T 代表標準維護版本，Cisco 僅提供 12 月維護期；數字代表版本重建的號碼。

· bin—副檔名

2 28282 sigdef-category.xml

1 227537 sigdef-default.xml

[33847587 bytes used, 30168797 available, 64016384 total] →容量 64G，已用 33G

63488K bytes of processor board System flash (Read/Write)

▲Router 開機步驟

1. 執行 ROM 中 POST(Power on Self Test)程式

2. 執行 ROM 中 Bootstrap 程式(IOS 載入器--查詢 Cisco IOS 並將其載入到 RAM)

註：此時，如果有連接到路由器的主控台，你會看到螢幕上開始出現輸出內容

3. 尋找 IOS 檔案並載入 IOS 到 RAM

4. 到 NVRAM 中載入 startup-config 到 RAM 中的 running-config

5. 完成開機

※路由器開機過程中會用到的檔案及存放位置

File name	Save place	Utilities
POST	ROM	硬體的檢查程式
Bootstrap	ROM	載入 IOS 到 RAM
Mini IOS	ROM	開機失敗時，載入的簡易型 IOS
IOS 開機檔	Flash	開機程式
IOS 開機檔	TFTP Server	開機程式
Startup 組態檔	NVRAM	IOS 組態檔
組態暫存器	NVRAM	組態暫存器設定值
Startup 組態檔 IOS 檔 其他	TFTP Server	路由器備份的地方

◎Router 選擇 IOS 開機(多重開機) 預設會使用 flash 中第一個 IOS 來開機

Router(config)#boot system flash XXYY.bin →完成後先 write 再 reload

Router#show version →可以看到 Router 目前使用的開機檔

Router#show flash →檢視 flash 中存在的 IOS 及容量狀態

TFTP 備援

◎TFTP 備份 run

R1#copy running-config tftp:

Address or name of remote host []? →輸入 TFTP Server IP

Destination filename []? →給個備份檔名

◎TFTP 備份指令

Codes	Utilities
Router#copy run tftp:	備份 run config 到 TFTP Server
Router#copy startup tftp:	備份 startup config 到 TFTP Server
Router#copy flash: tftp:	備份 flash 中檔案到 TFTP Server
Router#copy run flash:	備份 run config 到 flash

◎TFTP 還原 run

Router#copy tftp: run

Address or name of remote host []? → 輸入 TFTP Server IP

Source filename []? → 先前的備份檔名

Destination filename [running-config]? → 無腦 Enter 就對了

Flash 資料備援

類似從 run 備份到 TFTP，把 run 改成 flash—copy flash: tftp:

Flash 資料還原

類似從 TFTP 還原到 run，要注意如果 flash 中有相同檔案名，會有兩次確認動作—

Warning: There is ... Do you want to over write? 以及 Erase flash:before copying?

註：此種現象不是每個 IOS 版本都會發生

密碼復原/重置

◎Cisco 1841 密碼重置復原 Password Recovery (各版本型號的 register 機碼不同)

1. Physical reload(關機再開機)

2. <Ctrl><Shift><Break>

3. 進入 ROMMON MODE

4. ROMMON#confreg 0x2142 → Bypass nvram register
ROMMON#reset

5. 進入 enable MODE

Router#copy startup-config running-config

6. Set new password then write(save)

7. Config Mode 下修改回正常機碼

Router(config)#config-register 0x2102 then write → 此處可用 do show version 檢查

8. do reload

ROMMON mode of Router IOS

- 即 ROM Monitor
- 若是 flash 上的 IOS 檔案遺失或損毀，Router 開機會進入 rommon，此時先查詢 flash 中檔案狀態

◎查詢 flash 中的檔案

rommon1> dir flash: → 若為損毀狀態，什麼都不會有

- 接下來要想辦法從 TFTP Server 將 IOS copy 到 Router，但在 ROM 模式下介面是關閉的，所以要使用 **tftpdnld** 指令—

◎在 rommon 模式下臨時開通介面，並在傳輸完檔案後關閉介面

```

rommon3>IP_ADDRESS=x.x.x.x
rommon4>IP_SUBNET_MASK=y.y.y.y
rommon5>DEFAULT_GATEWAY=z.z.z.z
rommon6>TFTP_SERVER=a.a.a.a
rommon7>TFTP_FILE=oxx.bin
最後一步
rommon8>tftpdnld
最後 reset 就復活了

```

很重要!!!!!!
一定要大寫
一定要大寫
一定要大寫
因為很重要所以說三次

p.s. 上面整個 rommon 載 flash 的過程用的是 f0/0；還有某些 Router 可能不支援 tftpdnld；另外如果 Router 有 SD/USB 介面的話，可直接複製 IOS 檔案，不用這麼麻煩

Cisco IOS File System(IFS)

指令	說明
#dir	檢視目錄中的檔案，預設值會顯示 flash:/目錄中的內容輸出
#copy	簇繁不及備載
#more	提供文字檔檢視，可用來檢視組態檔或備份的組態檔
#show file	提供指定檔案或檔案系統的內容，較少用
#delete	就是 delete，但並不會釋放空間，釋放空間指令為 squeeze
#erase/format	小心使用。使用的記憶體種類會決定是否能拒絕快閃磁碟。
#cd/pwd	改變目錄的命令，使用 pwd 命令則會列出工作中的目錄。
#mkdir/rmdir	部份思科設備用它來建立、刪除目錄，mkdir 建立、rmdir 刪除，使用 cd/pwd 命令可以變換到這些目錄中

· 利用 Cisco IFS 來升級 IOS

指令	說明
#pwd	確認預設目錄
#dir	確認預設目錄(flash:/)的內容
#show file info flash:c1841.....124-1.bin #show flash(功能同上)	檢視快閃記憶體中尚存容量 檢視快閃記憶體中某檔案大小
#delet flash:c1841.....124-1.bin #show file info flash:c1841.....124-1.bin	刪除該 ios 後並確認(請小心)，應該會是 Error opening flash...(file not found)
#copy tftp://x.x.x.x//c1841.....124-2.bin/ flash:/c1841.....124-2.bin #show flash 或#show file info flash:c1841...	用 IFS 語法更新 ios 並確認
#verify /md5 nvram:startup-config	做完之後最好做一下 md5 校驗(哈希值要一樣)

Cisco IOS Licensing(授權)

· Cisco IOS 15 後的版本都是提供通用映像檔(universal)，有四大功能如下，除 IP Base 外，其它三種都需買授權才能使用，授權種類分 Permanent 與 Evaluation(評估)，授權方式有軟體啟動功能授權、功能使用權授權、訂閱授權及數量授權。

功能	服務技術
IP Base	基礎 Cisco IOS 功能、路由協定
DATA	MPLS, ATM, and multiprotocol support
Unified Communications	主要提供語音服務，VoIP and IP telephony
Security	主要提供安全服務，Firewall、IPS、IPSEC、3DES、VPN

◎確認授權狀態

Router#show version →顯示 IOS 版本各項資訊，結尾處含有授權細項

或

Router#show license udi →可查看 PID & 路由器序號(兩者合稱 UDI)，取得授權必備

◎查詢安裝在設備上的授權

#show license 也會顯示目前運作中 IOS 映像檔的每個功能，及軟體啟用和授權相關的變項
#show license feature 為 show license 的摘要

◎安裝永久授權=將授權金鑰拷貝至路由器(快閃)

#license install url:flash:FTX.....lic

△啟動授權後要 reload 才會生效

◎安裝評估功能授權

Router(config)#license boot module c2900 technology-package securityk9 →這段自己改

△啟動授權後要 reload 才會生效

◎授權備份(如果有儲在其他地方)

#license save flash:...lic →存完後用 license install 來復原授權

◎授權解除安裝+清除+移除

#license boot module c2900 technology-package securityk9 disable →Uninstall

#license clear securityk9 →clear

#no license boot module c2900 technology-package securityk9 disable →Remove



CDP / LLDP 鄰居發現協定

- CDP : Cisco Discover Protocol , 思科專屬，可偵測直接連線的 Cisco 設備並收集資訊。
- LLDP : Link Layer Discovery Protocol , **鏈結層發現協定** , IEEE 802.1ab 定義的 Link-Layer Discover Protocol , 各廠設備都可用。

#這兩者都是 L2 協定

CDP 傳送型態長度值 (TLVs) 以提供關於每個 CDP 鄰接設備的資訊。TLVs 是內嵌於 CDP 廣播的區塊的資訊，假設遇到沒有直接連接到管理員使用的主控台路由器。要獲得此設備的 CDP 資訊，要發現設備所連接到的鄰近設備，管理員將需要先使用 Telnet 來連接鄰居，才能獲得該設備的 CDP 資訊

例如： (管理員)A → B → C → D (Router)

管理員想知道 Router D 的 CDP 資訊，則先 Telnet 連到 Router C，再使用 CDP 指令來取得 Router D 的 CDP 資訊

show cdp neighbors 指令顯示的設備 TLVs 包括下列：

- Device ID 設備 ID
- Local Interface 區域介面
- Holdtime 佔用時間
- Capability 能力
- Platform 硬體平台
- Port ID 埠 ID

下列的 TLV 只包含在 CDPv2 :

- VTP management domain name VTP 管理領域名稱
- Native VLAN 本地的 VLAN
- Full or half-duplex 全雙工或半雙工

◎查詢 CDP 整體參數

```
#show cdp → 預設值每 60 秒傳送一次，且鄰居封包保存在 CDP 表 180 秒
#cdp holdtime ?<10-255> 設定 CDP 保留期限
#cdp timer ?<5-254> 設定 CDP 計時器
```

◎看直連設備(瞭解網路骨幹) --相連介面、裝置種類

Router#show cdp neighbors → CDP 封包無法穿過 Cisco 交換器，故只能看到直連裝置，若路由器直連到交換器，就無法看到插入該交換器的任何裝置。

Router#show lldp neighbors

◎看直連設備詳細資訊 --介面、裝置種類、ip、ios 版本

```
#show cdp neighbors detail
#show cdp entry 功能同上
```

◎看特定直連設備詳細資訊

Router#show cdp entry R2 → R2 為設備名稱

Router#show cdp entry * protocol

◎不給特定介面看 cdp (cdp 預設為 on)

Router(config)#interface fx/x

Router(config-if)#no cdp enable

◎不給所有介面看 cdp

Router(config)#no cdp run

◎啟用 LLDP

Router(config)#lldp run

◎特定介面啟用 LLDP

Router(config-if)#lldp transmit → 啟用傳送 LLDP 封包

Router(config-if)#lldp receive → 啟用接收 LLDP 封包

★★用 CDP 畫出網路架構(查出網路結構)

從一台當作起點，show cdp neighbors 一路探索出去。首先從 pc 進入 gateway 開始，然後 show neighbor，沒有 ip 時用 show cdp entry 抓出 ip，再連下去。



路由(Routing)協定原理

※Routing table 的事件(event)—在路由表中，路由資訊的寫入及刪除都叫一個 event。當 event 發生時，IOS 預設是不會在終端機顯示任何事件訊息的，因此要用 debug 指令才能看到 IOS 中正在發生的事件訊息。

開啟 debug 後，把某個 interface shutdown，本來只會顯示 down，但 debug 後，還會多顯示路由表刪除 event 等等。

※Routing table 的產生：要產生路由表，先要定義兩種網路區域—直連(connected network)、遠端(remote network)，即直接 / 非直接連結路由器的網路。

Router 開機後，只會獲得 connected network 資訊，在 routing table 中為 C 的就是。

有了上述的認知，再來才會有所謂 static/ dynamic routing 的產生，即為了連結到 remote network 的指向設定。

※Cisco 的 3 種封包轉送技術：

1.行程交換(process switching)—最早期的方式，單純封包交換，即 36 步驟的遶送流程，而今已不適用，但觀念仍然有用。

2.快速交換(fast switching)—為加速交換效能提出的方案。快速交換使用快取儲存最近使用的目標，因此不再需要為每個封包進行查詢。

#快速交換又稱為以交換為基礎的 cache(快取)，或者”繞送一次，交換多次(route one switch many)”。思科路由器用快速交換程序來產生 L3 繞送資訊的快取，然後供 L2 使用，以便讓路由器快速轉送封包，因此不需要每個封包都去解析路由表。

3.Cisco 快速轉送技術(Cisco Express Forwarding, CEF)—所有新型思科路由器的預設封包轉送方法。CEF 建立許多不同的快取表來改善效能，並且由變動觸發，而非封包觸發—這意味著當網路拓樸改變時，快取也隨之改變。

◎Debug 指令—顯示正在發生的 event

Router#debug ip routing

會顯示 IP routing debugging is on

◎停用 Debug 指令

Router#no debug all

◎Console 同步(讓 debug 訊息不打斷輸入中指令)—網路出問題一直跳 syslog 時很好用

Router(config)#line console 0

Router(config-line)#logging synchronous →主要是這行

◎檢視 ip 路由表

Router#show ip route 網段

↓以下為顯示範例，顯示出來有*的為 default route，其餘協定代號均會自帶說明不解釋

O 172.16.1.0/24 [110/2] via 192.168.10.2 00:01:08 f0/1

(via=下一中繼站)

S/C/O/F/R/B	172.16.1.0/24	110	2	192.168.10.2	00:01:08	f0/1
路由協定代號 S=靜態路由 C=直連 O/F/R/B 後面 會提到的動態 路由	可到達的目地 IP 網段	AD 值	路由協定計算 出的成本	Next Hop	此筆路由存在 多久	往哪個介面丟 出封包

◎清除路由表 Routing table 內容

Router#clear ip route *

◎路徑追蹤

#traceroute XXX.XXX.XXX.XXX

#進階版 traceroute 要分段設定，範例如下

Router#traceroute

Protocol [ip]:

Target IP address:

Source address:

Numeric display [n]:

Timeout in seconds [3]:

Probe count [3]:

Minimum Time to Live [1]:

Maximum Time to Live [30]:

Static Route 靜態路由

◎Static Route configure (輸入指令告知路由器封包應該往哪去)

Router#ip route [目的網路] [遮罩] [Next Hop IP/離開介面] [管理性距離][permanent]

說明：

--Next Hop IP：負責接收、轉送封包至遠端網路的下一路由器介面 ip—這是位於直連網路的路由器介面。在新增路徑前，必須先能 ping 到該路由器介面；若輸入錯誤 Next Hop IP，或是該介面未啟動，則路由器組態中會包含該靜態路徑，但路由表中卻不會有這條路徑。

--離開介面：可用來取代 Next Hop IP，這會顯示成直連路徑。

--管理性距離:Administrative Distance, 靜態路由的預設 AD 為 1(若使用離開介面 AD 為 0)。
可在命令最後加入管理權重以改變預設值。(AD 值為 0-255，最好-最差)

--permanent：如果介面 shutdown，或路由器無法與下一中繼站路由器通訊，該路徑將會自動從路徑表中移除。反之若加上 permanent，可將該項目永遠保留在路徑表。

Ex:

Router#ip route 192.168.1.0 255.255.255.0 172.16.1.1

↑只要看到目地 IP 在 192.168.1.0~192.168.1.255 範圍的封包都往 172.16.1.1 送

Router#ip route 192.168.1.0 255.255.255.0 f0/0

↑只要看到目地 IP 在 192.168.1.0~192.168.1.255 範圍的封包都往自己的 f0/0 這個 IP 送

- Static Route configure 後可在 routing table 看到顯示 S 的那筆就是了

▲Floating static route(浮點靜態路徑)

#在 ip route 尾端加上 150，這種靜態路由擁有比任何繞送協定還要大的 AD 值，只有當動態路由協定掛掉時，該筆靜態路由才會生效。

範例：ip route 192.168.10.0 255.255.255.0 172.16.10.2 150

◎查詢路由表(複習一下)

#show ip route 網段

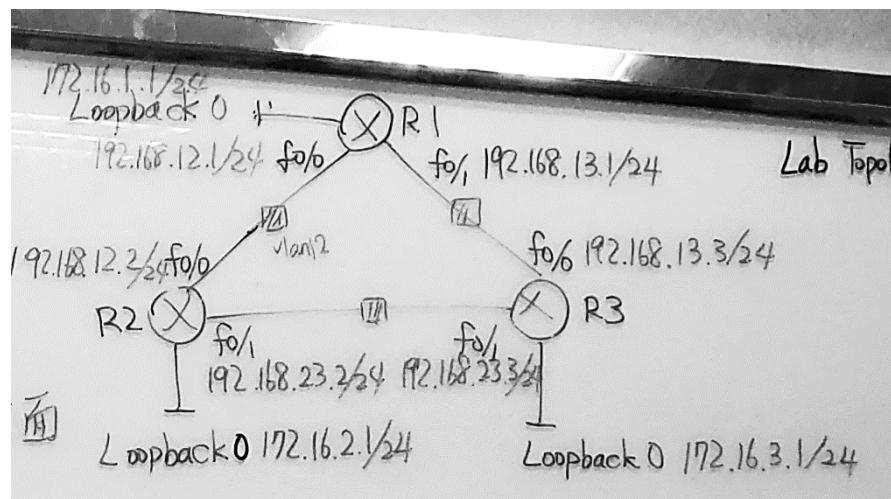
▲Default Routing 預設遶送

#Stub Router 殘根路由器。所謂殘根網路就是它只有一條路徑可抵達所有其它的網路；也即可以只使用單一預設路徑，不需建立多條靜態路由。IP 會將所有目的位址不在路徑表中的封包，使用這條預設路徑轉送；所以它又稱為閘道。以下範例：

(config)#ip route 0.0.0.0 0.0.0.0 [Next Hop IP/離開介面]

#在 show ip route 時預設路由會顯示在最後一行標記 S*，只要路由表中沒有的位址，都會往該 Next Hop IP/離開介面送出去，在加入預設路徑時要小心，有可能造成迴圈。

Static Route Lab:



R1 是 ping 不到 192.168.23. 網段 0 和另外兩個 loopback 的(不同網段)，所以要用 static route:

Router(config)#ip route 192.168.23.0 255.255.255.0 192.168.13.3

Router(config)#ip route 172.16.3.1 255.255.255.0 192.168.13.3

Router(config)#ip route 172.16.2.1 255.255.255.0 192.168.12.2

Host route(主機路由)—考試會考

- Host route 為在路由表中 /32 的那幾行，Host route 可提升路由器遶送的效能，Host route 可手動及自動設定，IOS 15 版後，直連網路的介面 IP 會自動寫到 Routing table，形成 Local Host Route(本地主機路由)，代碼為 L。
- 手動設定 Host route 的方法和 Static route 基本一樣，差別在 destination IP 改成 Remote Host IP

Hop(路由器之間的距離)

- 兩個直連路由器間的距離 hop=1，中間隔一台的路由器 hop=2，以此類推
- Recursive Lookup：遞迴查詢，使用 next hop ip 時，一筆路由會查兩次，第一次是查路由表得知 next hop ip，第二次是查 next hop ip 要使用哪個出口介面。要避免遞迴查詢，在點對點網路中盡量使用出口介面。

CCNA 會考哦

Routing Loop(路由迴圈)

- 封包從 a 出口出去到 b 出口，再從 b 出口遶送回 a 出口，直到 TTL=0，路由器丟棄封包。

Multiple access network(多重存取網路)

- 很多 Router、Switch 互相串接，從一個 Router 路由出去有多重選擇。
- 此時若 Router 使用出口介面作路由，不會直接往出口送，而是發 ARP，封包給先回應的 IP。
- 混搭 next hop ip 與出口介面：可以避免遞迴查詢，又有明確指向性—

Router(config)#ip route 目的IP 出口介面 nexthop

Default Route(預設路由)

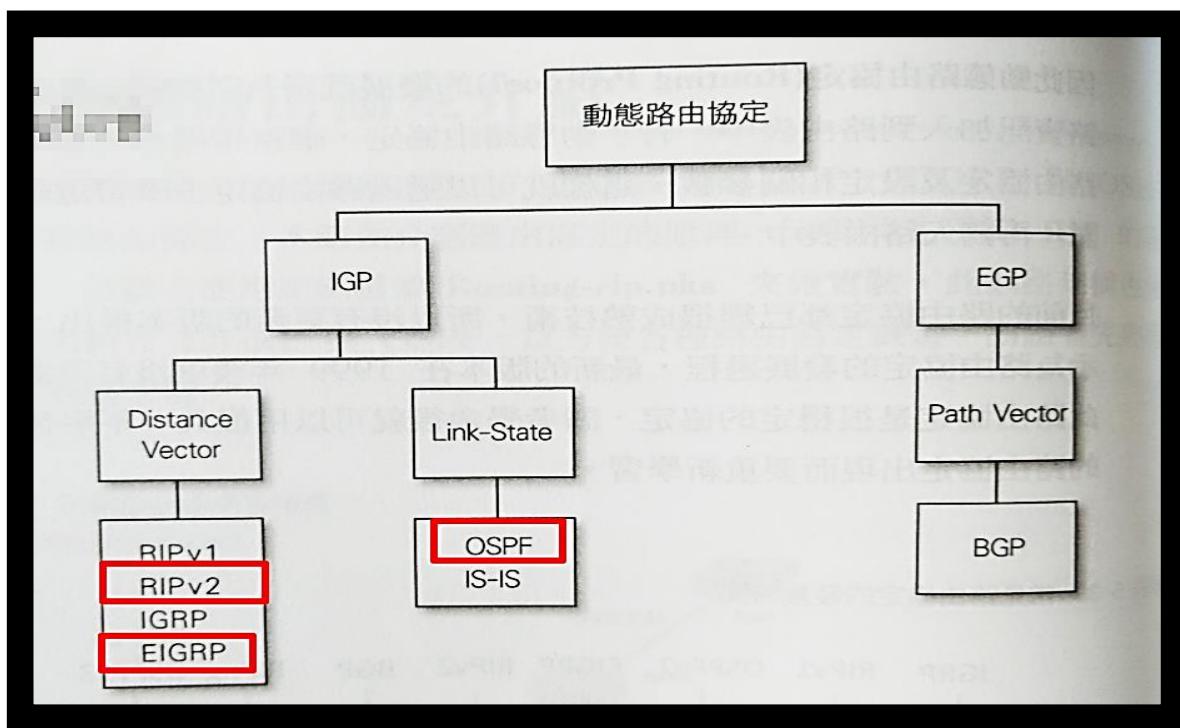
- 內外相接處的路由器稱為 Boundary Router(邊界路由器)，為內網與 ISP 的橋梁。
- 如果是一個有連到外部網路的網路環境，那麼內網的路由器就都需要設定一個 0.0.0.0/0 並往 next hop 的預設路由，如此才能連到外網。
- 所以路由表裡面找不到外網路徑時，直接往下一站送出。
- default route 在路由表中顯示為 S*，S 代表 Static route，* 代表為預設路由。
- default route 在路由表中顯示為 R*，R 代表 RIP route，* 代表為預設路由。
- 若有設定預設路由，在路由表中會顯示「Gateway of last resort is x.x.x.x to network 0.0.0.0」



Dynamic Routing Protocol 動態路由

- Router 間透過自動交換計算出遠方網路的路由。
- 區分內/外部路由(遶送)協定：
 - IGP(Interior Gateway Protocol) 在相同自治系統(Autonomous System, AS)中的路由器用來交換遶送資訊的協定，常見的有 **OSPF**、**EIGRP**，RIP 與 IS-IS 較少見，另外也有少量的 **BGP**。
 - EGP(Exterior Gateway Protocol) 在不同 AS 間的路由器溝通使用的協定，比如各不同 ISP 之間的網路。只有 **BGP**。

※AS 是指在相同行政管理網域下的一組網路，同 AS 中的所有路由器共享路由表資訊。



• 遙送協定分類：

分為 Distance Vector 距離向量、Path Vector 路徑向量、Link-State 鏈路狀態

• 距離向量協定：

根據距離找出通往遠端網路的最佳路徑。向量指示通往遠端網路的方向，代表為 RIP，它會將整個路徑表傳送給直連的鄰居。

- 缺點：定期發送完整路由表給鄰居(效率低)；收斂時間過久(可使用 hold-down timer 設定加進收斂)；潛在路由迴圈(參考 CCNP ROUTING official cert Guide 300-101)。

#Hold-down timer 抑制計時器，讓路由器在特定時間內拒絕接受路徑更新，避免路由變動頻率過高導致一直進入收斂模式。

#為避免路由迴圈，距離向量路由協定採用兩種預防方式：

- Split Horizon
- Poison Reverse：使從某介面學到的路徑以帶無限大的 priority 由該介面通告回去。(參考 CCNP ROUTING official cert Guide 300-101)

• 鏈路狀態協定：

又稱最短路徑優先協定(SPF-shortest-path-first-protocol)；每台路由器會建立 3 種表：鄰居表、拓樸表、路徑表。連接狀態路由器對網路瞭解比距離向量遼遠協定清楚。OSPF 是其中代表。連接狀態在不定期的路徑更新封包中傳送鏈路資訊。直連鄰居定期交換 hello 訊息，這種訊息可得知對方是否存活，或用來建立與維護鄰居關係。(連接狀態包括網路介面種類、IP 位址、成本、鄰居這幾個資訊)

鏈路狀態路由協定允許路由器建立網路拓樸圖，而非與鄰近路由器間彼此交換完整路由表。之後，路由器即可執行演算來計算到目的地網路的最適當路徑，就像汽車的 GPS 一樣。路由器發送鏈路狀態通告(link-state advertisement, LSA)去通知所有保持連線的網路(鄰居)，接著就可利用 LSA 來建構網路的拓樸圖。對應此拓樸圖所執行的演算法是 **Dijkstra 最短路徑優先演算法**。

鏈路狀態路由協定只在兩台路由器之間形成鄰居關係時，才會交換完整的路由資訊，有別於距離向量路由協定。建立鄰居後只根據網路變動來發送路徑更新，而非定期發送。此外，鏈路狀態路由協定的優勢勝於距離向量路由協定的是收斂時間短，但與 EIGRP 不相上下。

鏈路狀態類路由協定有 OSPF 及 IS-IS：

■開放式最短路徑優先 (OSPF) 乃指基於兩台路由器之間鏈路速度而採用成本權值的鏈路狀態路由協定，由於 OSPF 具有可擴展性、快速收斂及廠商相容性等優點，故成為普遍使用的 IGP。

■中繼系統間的通訊協定 (IS-IS) 這種鏈路狀態路由協定的操作類似於 OSPF，使用與介面相關的可設定（但無維度）權值，並執行 Dijkstra 最短路徑優先演算法。雖然將 IS-IS 當作 IGP 來使用時同樣提供可擴展性，快速收斂及廠商相容性等優點，卻不如 OSPF 那樣被廣泛地使用。

※距離向量 V.S.連接狀態：前者是看著路標開車，後者是照著地圖導航走。

• 高階距離向量：

距離向量+鏈路狀態，就是 EIGRP 啦。使用 Hello 來發現鄰居，且發生異動時只傳送部份更新資訊。距離向量的部份則是從直連鄰居學習網路其他部份資訊。

• 路徑向量：

路徑向量路由協定包含有關送到特定目的地網路的正確路徑封包之資訊，此路徑資訊一般由封包抵達目的網路時所歷經一系列自治系統(AS)所組成。在現今網路中，最可能碰到的唯一的路徑向量路由協定即邊界閘道協定 (Border Gateway Protocol, BGP)。

BGP 路徑選擇不單以 AS 轉送站為基礎，BGP 還參考了幾個其他參數(與鏈路速度毫無關係)。另外，BGP 雖然具擴展性(Scalability)，但拓樸變更不能快速收斂。BGP 的最新版是第四版 (BGP4)，且有個稱為多協定 BGP (Multiprotocol BGP, MP-BGP) 的改良版，可支援如 IPv4 與 IPv6 等多路徑協定的路由。



常用路由協定群播位址(Well-known ipv4/v6 multicast address)

Protocol	IPv4	IPv6
EIGRP	224.0.0.10	FF02::A/16
OSPF	224.0.0.5	FF02::5/16
OSPF DR	224.0.0.6	FF02::6/16
RIP	224.0.0.9	FF02::9/16
PIM	224.0.0.13	FF02::D/16

OSPF 的.5 每台路由器都會送

OSPF 的.6 只有 DR 會送

遶送協定基礎



管理性距離(AD)

評比路由器從鄰接路由器所收之路徑的可信度，0-255，0 最信任，255 則不透過該路徑傳送。

在 show ip route 時，路由資訊後有個[xx/xx]的資訊，代表 AD/Cost。

AD 值主要的目的是給每個路由協定來定義其寫入路由表的優先權(Priority)，AD 越小 Priority 越大

若路由器收到兩筆相同遠端網路的路徑更新，會先檢查 AD，將最低 AD 路徑放入路由表。

承上，若 AD 相同，則使用遶送協定的衡量指標(比如 hop 數或線路頻寬等)來找出最佳路徑。被宣傳的路徑中有最低衡量指標者會放入路由表。

若兩者有相同 AD+衡量指標，則遶送協定會有負載平衡效果(即同時使用這 2 條線路來傳遞封包)

路徑來源	預設 AD
相連的介面	0
靜態路徑	1
外部 BGP(EBGP)	20
EIGRP	90
OSPF	110
RIP	120
外部 EIGRP	170
內部 BGP(IBGP)	200
未知	255(這條路徑絕不會被使用)

· 查詢 Static Route AD：

靜態路由 AD 不會出現在路由表中，除非使用 show ip route x.x.x.x 才會看到有個 distance=1，

◎修改靜態路由 AD：

Router(config)#ip route x.x.x.x y.y.y.y int/z.z.z.z O → 在 ip route 後加上 0-255 的 priority

★Floating Static Route(浮動靜態路由)—實務上很好用

簡單來說就是用修改靜態路由 AD 的方式，將 AD 值改到比路由協定還大，讓它成為路由的備援機制，比如大家都用 RIPv2(AD120)，我就把 Static Route 改成 AD121，改完後並不會馬上出現，直到動態路由出問題時才會有效果(備而不用)，測試方法可把動態路由協定關掉或是介面關掉。

◎修改動態路由協定 AD

Router(config)#router rip/eigrp/ospf

Router(config-router)#distance x →x 就是要給定的 AD 值

p.s. 每一種路由協定都有一個 AD 值與之對應，這個值代表這個路由協定所提供的資訊的可靠程度，其值越低，代表可靠程度越高。

Administrative Distance 值簡稱 AD 值，是一個從 0-255 的整數，

因此，在一個網路內，如果同時使用多種不同的路由協定，當要傳送封包時，就會根據 AD 值來選擇比較適當的路由協定。

直接連接分數最低，代表可靠程度最高，而其次為靜態路由，因為是網路管理人員直接設定的，所以自然而然地其可靠程度高於路由器所學習而來的路由路徑。

Cost(路由協定成本)

- 同一路由協定中，對同一遠端網路，有多條路徑，則選成本最小的。
- 以 RIP 為例，成本是 hop，選 hop 最小的。

Route Redistribution(路徑重分送)

- 讓網路同時支援多個路由協定的作法。
- 搜尋本文內關鍵字…

Route Summarization(路徑彙總)

- 大多數路由協定都會自動開啟。簡言之，就是自動幫你做子網路劃分，思科技術手冊建議關閉自動彙總，因為在有備援路徑的狀況下自動彙總會發生悲劇(範例見超連結)。

RIP(Routing Imformation Protocol)

1

RIP 分為 v1、v2，v1 為 classful routing(有級別遶送)，亦即網路上的所有裝置必須使用相同的 MASK，因為 v1 在傳送路徑更新時沒有附帶 MASK，並且 v1 使用定期廣播。v2 提供前置位址遶送(prefix routing)，並且在路徑更新中包含 MASK，這被稱為 classless routing(無級別遶送)，並且 v2 使用定期群播。

RIP 預設每 30 秒廣播(255.255.255.255)/群播(224.0.0.9)，向所有作用中介面送出路由表。RIP 使用 Hop 來判斷通往遠端網路的最佳路徑，但是最大 Hop Count=15，第 16 台(Hop count 預設為無限大)就無法抵達。RIP 在小型網路中運作良好，但在設有緩慢之 WAN 鏈路的大型網路，或是安裝大量路由器的網路上則缺乏效率。如果是在具有變動頻寬鏈路的網路上，更是完全無用。

◎RIP configuration

Router(config)#router rip

Router(config-router)#version 2 → 改為 RIPv2

Router(config-router)#**no auto-summary**

※no auto-summary 關閉自動總結，通常不會讓遠送協定自動總結，要做的話最好是手動 summary，而 RIP & EIGRP 預設自動總結。

p.s. 記住在設定網路位址時，RIP、EIGRP 使用有級別位址。以子網路為 172.16.10.20/30.0 為例，它的位址是 172.16.0.0/24，所以只要輸入有級別網路位址 172.16.0.0 就可讓 RIP 找出子網路，並將它們放入路由表中。這並不表示正在執行的是有級別遶送協定，只是 RIP 和 EIGRP 的設定方式。

☆在關閉 auto summary 後，馬上 show ip route rip，因為 RIP 尚未 converge(收斂)，所以路由表不變，收斂後，R1 路由表只剩 6 筆遠端網路資訊，若要快速看到結果，可用 clear ip route * 將路由表清空，讓 RIP 重新學習。

◎清空路由表

Router#clear ip route

Routing Summary(路由資訊壓縮/摘要) :

```
Router(config)#router rip  
Router(config-router)#version 2
```

※啟用 RIPv2 後，比 RIPv1 少了幾筆遠端路由，這是因為有了 VLSM，遮罩自動壓縮取最大值，即 Routing Summary(路由摘要)。

範例—

172.30.100.0/24 , 172.30.110.0/24 , 172.30.300.16/28 , 172.30.200.32 /28 四筆會壓縮為
172.30.0.0/16 。

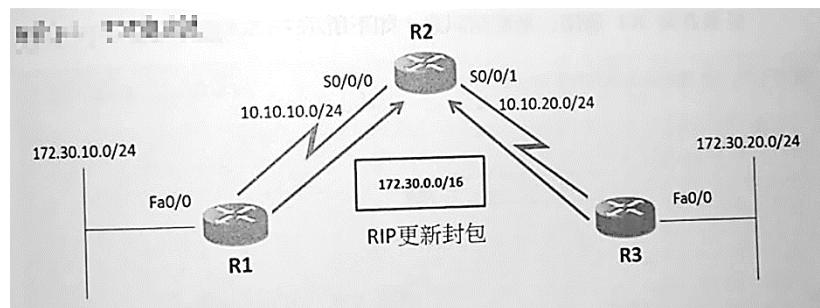
以 show ip protocols 查看，**Automatic network summarization is in effect**，表示自動壓縮功能啟用。(RIP 與 EIGRP 的自動壓縮預設啟用)

不連續網路：

下圖為一個不連續的網路，以 172.30.0.0/16 的兩個子網路分別設定在 R1 與 R3 的 fa0/0，在 R2 的兩個網路卻是 10.0.0.0/8 的子網路，因此形成 172.30.0.0/16 下的兩個子網路不連續。

若三台路由器也都啟動 RIPv2，此時因為自動壓縮的功能，R1 將 172.30.10.0/24 壓縮為 172.30.0.0/16 更新給 R2，R3 也把 172.30.20.0/24 壓縮為 172.30.0.0/16 更新給 R2，所以 R2 表會記錄 112.30.0.0/16，可能會往 R1 或 R3，如此當 R2 要送資料到 172.30.10.0/24，就不一定能送到 R1，這就是不連續網路的問題。

若將自動壓縮關閉，R1 與 R3 就會分別更新各自的子網路資訊到 R2，這樣就能解決不連續網路所造成的路由更新問題。



• 路由壓縮的優點：

- 減少更新封包大小、耗用頻寬
- 減少路由表資訊數目

• 精簡 RIP 的 network 指令

因為 RIP 只能用主網路位址的宣告方式存在組態檔中，所以如果有多筆同一 CLASS 的網段，可直接用該網段去寫，但前提還是要在同一個 MASK 下。

◎檢查 RIP

Router#show ip route → RIP 學到的路由會顯示 **R**

Router#show ip route rip → 只顯示 RIP 學到的路由資訊

△注意路由表中在路由協定學到的路由中都會有像[120/2]的玩意，前者代表 AD 值，後者在 RIP 代表 hop 數(成本)

△如果路由器收到一筆路徑更新紀錄，而更新紀錄中抵達某網路的路徑成本比既存路徑成本高，則路由器會忽視這筆更新

◎觀察 RIP 運作

Router#debug ip rip 可以看到 RIP 是預設每 30 秒更新一次路由資訊，以廣播方式傳遞

◎萬用指令—查詢所有路由協定執行資訊

Router#show ip protocols

VLSM 與 FLSM：

Variable Length Subnet Mask & Fixed Length Subnet

Mask，在 RIPv1 中，只支援 FLSM，所以不需有遮罩資訊(大家 MASK 都一樣)

應該在互連網路中使用 rip 嗎？

一個成長中的網路有數台 Cisco 路由器，但有幾台是舊的 Unix 路由器只支援 rip，但並不需要在整個網路上用 rip。

可以利用重分送(redistribution)，基本上就是將一種遶送協定轉換成另一種，表示可以使用 rip 支援舊的路由器，但在網路其它部份使用 eigrp 等。

這會阻止 rip 路徑在整個網路上傳送，並節省大量頻寬。

Passive Interface—限制路由協定封包傳送

- Passive interface：只收協定封包，不送協定封包。

◎Passive interface configuration

Router(config)#router <i>rip</i>	→可以改成 EIGRP, OSPF
Router(config-router)#passive-interface default	→通殺，全部介面 passive
Router(config-router)#passive-interface fx/x	→只對特定介面設 passive，這兩個二選一

傳遞預設路由—用動態路由協定宣傳預設路由給所有路由器。

▲RIP, OSPF 適用

Router(config)#ip route 0.0.0.0 0.0.0.0 *interface*

Router(config)#router *rip/ospf*

Router(config-router)#**default-information originate**

用 debug ip rip events 及 show ip route 檢視

- default route 若在路由表中顯示為 R*，R 代表 RIP route，*代表為預設路由。

▲RIP,EIGRP 適用--只能用在 classful

Router(config)#ip default-network x.x.x.x →宣告 x.x.x.x 為預設路由(要先有該筆靜態路由)

Router(config-router)#network 上面宣告 default-network 的 ip

路由表中有*的是預設路由，當有多筆預設路由時，會比較 AD 值、路由成本，選出來的預設路由會顯示在”Gateway of last resort”那行。

▲Redistribute—應該是所有適用

使用 **Redistribute(重分送)**宣告，這是 CCNP 的方法，將所有靜態路由/其他路由協定學到的路由，都分送給執行同協定的路由器，在 RIP 時指令如下：

Router(config)#router rip

Router(config-router)#redistribute static

◎使用 RIP 宣傳預設路徑

若某路由器(以下範例名稱為 Corp)的 f0/0 介面連到 Ethernet，以連結網際網路—例如 LAN 介面，而非序列介面連往 ISP。

此時 AS 中所有路由器都要知道如何傳送目的地為外網的封包，否則在收到遠端請求封包時，就會丟棄。

在每台路由器放入預設路徑，將資訊送到邊界路由器；邊界路器有通往 ISP 的預設路徑。假如同 AS 中路由器都執行 RIPv2，只要在邊界路由器加入通往 ISP 的預設路由，然後新增一個命令將該網路宣傳到 AS 的其他路由器(做為預設路徑)，就可讓它們知道要將目的地為外網的封包往哪送。

宣傳預設路徑指令：

```
Corp(config)#ip route 0.0.0.0 0.0.0.0 f0/0 或 next hop ip
```

→寫作 f0/0，實際上在路由表是該介面 IP，所以宣傳出去是以 IP 型式展現！

```
Corp(config)#router rip
```

```
Corp(config-router)#default-information originate
```

以上三行可以用一行 ip default-network next hop ip 取代

此時本地 show ip route 會看到

```
S*      0.0.0.0/0 is directly connected, Fastethernet 0/0
```

其他直連路由器 show ip route 會看到

```
R*      0.0.0.0/0 [120/1] via x.x.x.x, 00:00:05, serial0/0/1      →*代表預設路徑
```

最長匹配(Match)原則—實務上很好用

· 路由表中有多筆資訊可到同一網段，該如何選擇？

用 ip 的 32bits 去比對，首先比對目的網段 mask，比對完後還有多筆，就比這幾筆資訊的 mask 誰 bits 比較長，所以假如有 /20, /22, /23，最後會選擇 /23 那筆。

· 路由行為：承上，若完全比對不到，就往預設路由送，若無預設路由，則封包被丟棄。

若有預設路由，又分兩種路由行為，no ip classless(有級別)、ip classless(無級別)，只有無級別路由會使用預設路由。

p.s. 有個可以在路由器查詢路由表前，無腦指定封包方向(出口介面/下一站 ip)的方法稱作 PBR(Policy Base Route)，不過是 CCNP 的，PBR 使用 Routemap 來修改封包方向，可以不用路由表做遶送。



EIGRP(Enhanced Interior Gateway Routing Protocol)

※前身為 IGRP，IGRP 為 Classful Routing，EIGRP 則為 Classless Routing；另外 EIGRP 分為 internal / external，AD 值不同。

★以前會說 EIGRP 思科獨有，但自從 RFC7868 列入後，從 2016 開始就有越來越多廠商支持使用了。(考 CCNA 時還是要答 Cisco 專用)

※思科自己會說 EIGRP 收斂速度最快，因為使用 Topology Table

※特色：DUAL(擴散更新演算法)、Neighbor Tables(鄰居表)、Topology Tables(拓樸表)、RTP(可靠傳輸通訊協定)、最大 hop count 255。

※綜合 Bandwidth(整段路徑裡最差的那段頻寬)、Delay、Reliability、Load 進行計算。

※使用 multicast 224.0.0.10

※支援 Wildcard Mask(萬用遮罩)

※收斂速度所有動態路由協定中最快

EIGRP Neighbor Table →	EIGRP Topology →	Routing Table
建立鄰居關係表格	所有可能路徑	最佳路徑

EIGRP 是無級別(classless)高階距離向量(distance-vector)協定，使用自治系統(AS)來描述相鄰路由器；相鄰路由器執行相同遶送協定、分享路徑，並在路徑更新中包含遮罩資訊。子網路資訊的宣傳讓我們得以在設計 EIGRP 網路時使用 VLSM 與路徑總結。

EIGRP 有時又稱為混合式遶送協定(hybrid routing protocol)，因為它同時有距離向量與鏈路狀態協定的特性，例如，EIGRP 並不像 OSPF 會傳送鏈路狀態的封包，而是傳送傳統的距離向量更新，包含網路、從宣傳路由器的觀點所計算之抵達這些網路的成本等資訊。

EIGRP 有鏈路狀態的特性，啟動時先同步鄰居之間的路徑表，然後只在拓樸發生改變時傳送特定更新(限制性更新)。這使得 EIGRP 更能適合非常大型的網路。

EIGRP 的最大中繼節點計數(hop count)為 255(預設值是 100)。 HOP 的用途是計算路徑更新封包最多可經過多少由器；這會限制 AS 的範圍。

EIGRP 功能：

- IP 透過協定相依模組(protocol-dependent module, PDM)來支援 IPv6(以及一些其它無用的被遶送協定)。
- 無級別的遶送協定(與 RIPv2 及 OSPF 一樣)支援 VLSM / CIDR
- 支援路徑總結與非連續網路
- 發現鄰居
- 透過可靠傳輸協定(Reliable Transport Protocol, RTP)來通訊
- 透過擴散更新演算法(Diffusing Update Algorithm, DUAL)來選擇最佳路徑。
- 利用限制性更新(bounded update)來降低頻寬使用
- **沒有廣播。**

Cisco 將 EIGRP 視為距離向量遶送協定，或有時候稱它為進階距離向量遶送協定，甚至是混合式遶送協定。



發現鄰居

EIGRP 路由器必須先成為鄰居，才能夠互相交換路徑。建立鄰居關係必須符合 3 個條件
這 3 項條件只在直接相連的鄰居間交換：

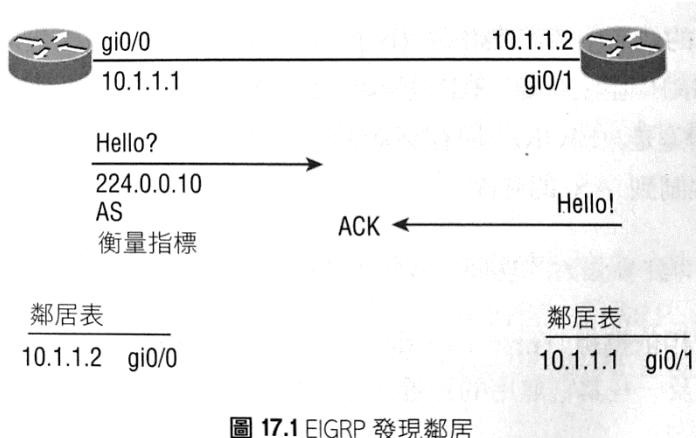


圖 17.1 EIGRP 發現鄰居

● 收到 Hello

● AS 號碼相符

● 相同的衡量指標(K 值)

鏈路狀態協定傾向於使用 Hello 訊息來建立鄰居關係，為了維護鄰居關係，EIGRP 路由器必須持續地從鄰居接收 Hello。

不同 AS 的 EIGRP 路由器不會自動地分享路徑資訊，而且不會成為鄰居。當用於大型網路時，可減少路徑資訊傳播量，但在不同 AS 之間，需要重分送(redistribution)

EIGRP 路由器間的 Hello 預設為 5 秒。與 Hello 計時相關的另一個計時器是保存計時器 (hold timer)。保存計時器會決定路由器在宣告鄰居死亡之前，等待 Hello 的時間。一旦鄰居被宣告死亡，就會從鄰居表中移除，且所有依賴它的路徑都要重新計算。保存計時器的設定並不能決定路由器在宣告鄰居死亡前要等待多久；路由器是用它來指定其他人必須等多久，才可以宣告它自己的死亡。

EIGRP 只有在發現新鄰居時會宣傳整個路徑表，並且透過 Hello 封包的交換與它形成緊鄰關係(adjacency)。此時，2 部鄰居都會宣傳它們的整個路徑表給另外一部。當每部路由器學到鄰居的路徑之後，只會宣傳路徑表的異動部份。

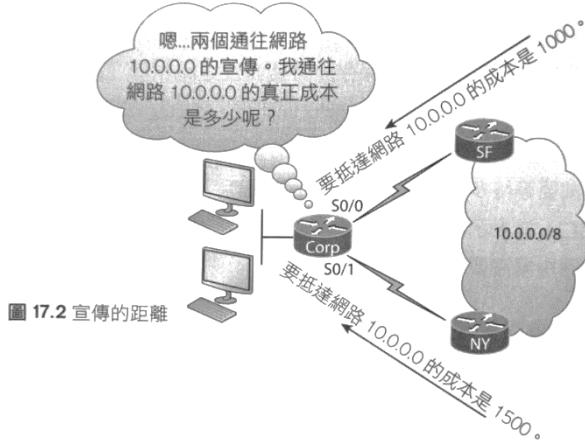
EIGRP 路由器建立鄰居表來儲存直接相連的鄰居路由器資訊。每個鄰居的路由器 IP 位址、保存時間間隔、流暢來回計時器(SRTT, smooth round-trip timer)、和佇列資訊都保存在表中。這是判斷鄰居路由器是否必須知道拓樸發生變化的重要參考。

當 EIGRP 路由器收到鄰居的更新後，將其存到本機拓樸表，其中包含從所有已知鄰居來的路徑，從中挑選最佳路徑放入路徑表。



一些術語：

- 報告的距離/宣傳的距離(**reported distance / advertised distance , RD**) 由某鄰居到遠端網路的成本，即該鄰居的路徑表成本，與拓樸表中括號裡的第二個數字一樣。第一個數字是可行距離。下圖， SF 和 NY 都會宣傳通往網路 10.0.0.0 的路徑給 Corp，但是 SF 的路徑成本比 NY 低。

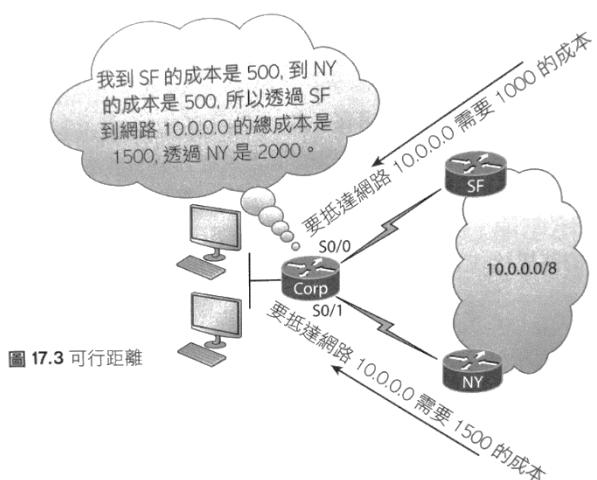


- 可行距離(**feasible distance , FD**) 這是本地到遠端網路之所有路線中的最佳成本，包括抵達當初宣傳該遠端網路之鄰居的成本。它是最佳的路徑，會出現在路徑表。要計算可行距離的成本，須使用鄰居報告的 RD 加上抵達該鄰居的 RD。在上圖中，Corp 的路徑表選擇 SF 路由器通往網路 10.0.0.0 的路徑，因為它具有最低的 FD。這是從端點到端點的最低真實成本。

觀察路徑表的 EIGRP 路徑，並且找到列出的 FD 項目：

D 10.0.0.0/8 [90/2195456] via 172.16.10.2, 00:27:0, Serial10/0

D 代表 Dual，它是 EIGRP 注入的路徑，並且是 EIGRP 用來透過鄰居 172.16.10.2 轉送交通到網路 10.0.0.0 所使用的路徑。注意這一行中的[90/2195456]，90 是管理性距離(AD) - 請不要與宣傳距離(advertised distance , RD 值)混淆，2195456 是 **FD**，即該路由器抵達 10.0.0.0 的總成本。



- 鄰居表(**neighbor table**) EIGRP 路由器學到新鄰居時，會紀錄鄰居的位址與介面，並且將資訊保存在鄰居表中；鄰居表儲存在 **RAM** 中。每個協定相依模組都會各有一個鄰居表，路由器會利用序號來比對更新封包的確認號碼，而且會記錄從鄰居所接收的最後一個序號，這樣就可以偵測到失序的封包，並且找出如何用它來做鄰居路由器間的鏈路檢測。

● 拓樸表(topology table) 拓樸表是由協定相依模組產生的，DUAL 演算法利用它來運算。拓樸表包含鄰居路由器所宣傳之所有目的地及其 IP，以及宣傳該目的地之鄰居清單，路由器會對每個鄰居記錄來自於該鄰居的路徑表所宣傳的 RD 和 FD。到遠端網路的最佳路徑會被放入路徑表中。EIGRP 放入路徑表中的路徑稱為 Successor router；具有次佳成本的路徑會被輸入拓樸表中做為備援鏈路，並且稱為 Feasible Successor。

#鄰居表與拓樸表放在 RAM 中，透過 hello 訊息與更新封包來維護。路徑表也會存放在 RAM 中，但裡頭的資訊只透過拓樸表來收集。

● 後繼者(successor) 通往遠端網路的最佳路徑(最低成本)，並放在路徑表中。

● 可行後繼者(feasible successor, FS) FS 的 RD 少於目前後繼者的 FD，即備援路徑。在 15.0 版中，EIGRP 會在拓樸表中保留最多 32 個可行後繼者，但之前的 IOS 版本最多只有 16 個。只有具備最佳衡量指標的路徑(後繼者)會拷貝至路徑表中，show ip eigrp topology 會顯示路由器知道的所有 EIGRP FS 路徑。

#FS 存在拓樸表中。Successor 存在拓樸表及路徑表中。

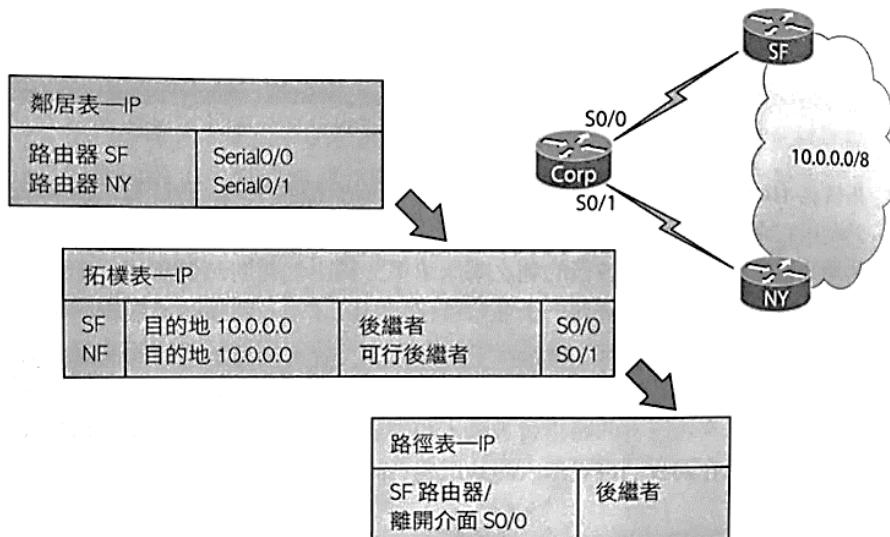


圖 17.4 EIGRP 使用的記錄表

上為範例，Corp 路由器有 2 條路徑可以用來通往網路 10.0.0.0。EIGRP 會挑選最佳路徑放入路徑表中，但是如果這 2 條鏈路具有相同的成本路徑，EIGRP 會在它們之間進行負載平衡—預設最多可達 4 條鏈路。EIGRP 利用後繼者，以及將拓樸表中的可行後繼者當作備援鏈路，可以讓網路立即收斂，而且一產生的交通只有傳送給鄰居的更新—非常乾淨俐落！

Feasible Distance(FD)：主要成本，即所有路徑中最小的路徑成本

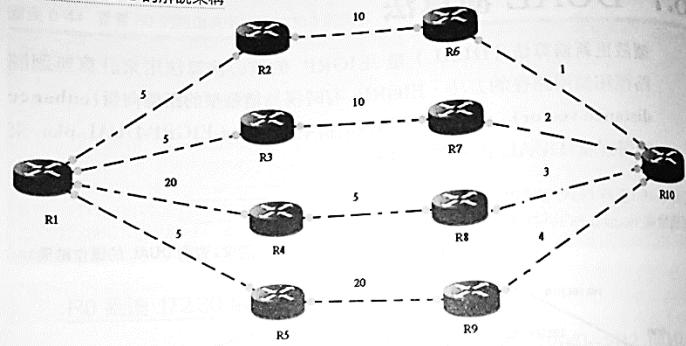
Feasible Successor(FS)：備援後繼路由器，備援路徑中的下一個路由器

Advertise Distance(RD)：通告成本，即鄰居路由器到目的的成本，可理解為 FD 減掉自己到鄰居路由器的 RD。

Feasible Condition(FC)：可行條件，選擇符合資格的路徑做備援路徑，並會將備援路徑紀錄到拓樸表，FC 選擇的是 $AD < FD$ 的那些路徑，可能有多條。

在 show ip eigrp topology 的時候，會看到每條路徑前有個字母，代表該路徑目前的狀態，顯示 P=Passive，表示該路徑已確定，若顯示非 P 表示 EIGRP 還在更新中

圖表 6-46 DUAL 的解說架構



- 後繼路由器(successor)：我們用上圖的解說架構，其中連線上的數字表示兩個路由器之間 EIGRP 的成本，從 R1 到 R10 會有四條路徑，其最小的路徑成本為 16 (R1-->R2-->R6-->R10)，此路徑會被 EIGRP 選為主要路徑記錄到路由表中，後繼路由器為 R1 主要路徑中的下一個路由器，即為 R2。

- 主要成本(FD)：主要成本為最小的路徑成本，以本範例為 16。
- 通告成本 (AD)：通告成本 (Advertisement Distance)又稱報告成本 (report distance)，即為 R1 的 EIGRP 鄰居路由器到目的網路的主要成本，以本範例在 R1 有四個通告成本，R2 的 11、R3 的 12、R4 的 8 及 R5 的 24。
- 可行條件(FC)：可行條件即為選擇符合資格的路徑當做備援路徑，備援路徑會被記錄到拓樸表(Topology Tables)，可行條件=主要路徑成本>通告成本，以本範例有 R3 及 R4 的通報成本有符合資格 (16>12、16>8)，R1-->R3-->R7-->R10 及 R1-->R4-->R8-->R10 兩條路徑會被 DUAL 選為備援路徑，記錄並到拓樸表。
- 備援後繼路由器 (FS)：為備援路徑中的下一個路由器，以本範例 R3 及 R4 為備援後繼路由器。

圖表 6-48 Core 中的拓樸表內容

```

Core#show ip eigrp topology
IP-EIGRP Topology Table for AS 10

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.20.0/24, 1 successors, FD is 2169856
    via Connected, Serial0/0/1
P 192.168.40.0/24, 1 successors, FD is 2169856
    via Connected, Serial0/1/1
P 192.168.30.0/24, 1 successors, FD is 2169856
    via Connected, Serial0/1/0
P 10.10.10.0/24, 1 successors, FD is 2681856
    via 192.168.40.2 (2681856/2169856), Serial0/1/1
P 172.30.30.0/24, 1 successors, FD is 2681856
    via 192.168.30.2 (2681856/2169856), Serial0/1/0
P 200.200.200.0/24, 1 successors, FD is 2300416
    via 192.168.10.2 (2300416/2297856), FastEthernet0/0
    via 192.168.20.2 (2809856/2297856), Serial0/0/1
    via 192.168.30.2 (2809856/2297856), Serial0/1/0
P 172.30.10.0/24, 1 successors, FD is 2172416
    via 192.168.10.2 (2172416/2169856), FastEthernet0/0
P 172.30.20.0/24, 1 successors, FD is 2681856
    via 192.168.20.2 (2681856/2169856), Serial0/0/1
P 172.30.40.0/24, 1 successors, FD is 2684416
    via 192.168.10.2 (2684416/2681856), FastEthernet0/0
    via 192.168.40.2 (3 FD 6/2 AD 6), Serial0/1/1
    via 192.168.20.2 (3 FD 6/2 AD 6), Serial0/0/1
    via 192.168.30.2 (3193856/2681856), Serial0/1/0
P 192.168.10.0/24, 1 successors, FD is 28160
    via Connected, FastEthernet0/0
Core#

```

可靠傳輸協定(RTP，Reliable Transport Protocol)

RTP 管理 EIGRP 路由器間的通訊，由 Cisco 設計，用多點、單點傳播來快速傳送更新。

EIGRP 用群播 IP 224.0.0.10。如果群播沒有收到某個鄰居的回應，就改用單點傳播重送相同資料—如果嘗試 16 次單點傳播之後仍然沒有取得回應，就判定該鄰居死刑；這種程序稱為可靠多點傳播(reliable multicast)。

路由器會藉由指定序號給每個封包，以記錄它所傳送的資訊，利用這種技巧，就能偵測到過時的、多餘的、或失序的資訊。您會在 EIGRP 組態設定那部份，看到鄰居表中的這項資訊。

EIGRP 使用 5 種封包：

圖表 6-47 Core 中的主要路徑成本

```
Core#show ip route
----- 省略部分資訊 -----
10.0.0.0/24 is subnetted, 1 subnets
D 10.10.10.0 [90/2681856] via 192.168.40.2, 00:24:24, Serial0/1/1
172.30.0.0/24 is subnetted, 4 subnets
D 172.30.10.0 [90/2172416] via 192.168.10.2, 00:00:06, FastEthernet0/0
D 172.30.20.0 [90/2681856] via 192.168.20.2, 00:24:21, Serial0/0/1
D 172.30.30.0 [90/2681856] via 192.168.30.2, 00:24:22, Serial0/1/0
D 172.30.40.0 [90/2684416] via 192.168.10.2, 00:00:06, FastEthernet0/0
C 192.168.10.0/24 is di FD 主要路徑成本, FastEthernet0/0
C 192.168.20.0/24 is di, Serial0/0/1
C 192.168.30.0/24 is directly connected, Serial0/1/0
C 192.168.40.0/24 is directly connected, Serial0/1/1
D 200.200.200.0/24 [90/2300416] via 192.168.10.2, 00:00:06, FastEthernet0/0
```

● **Hello** 透過不可靠的多點傳播以發現 EIGRP 鄰居：這表示它不需要確認。有兩種計時方式 Interval time / Hold time，間隔時間為 Hello 封包送出週期，保留時間用以維持鄰居關係，若保留時間歸零時未收到 Hello 封包，判定鄰居陣亡，預設保留時間為間隔時間的三倍(5/15)。
p.s. 兩台路由器 Hello time 不同，在 EIGRP 沒影響，在 OSPF 會有差

● **查詢(Query)** 針對特路徑的請求，使用多點傳播，發現遺失通往特定網路的路徑時，會傳送查詢封包並搜尋替代路徑。

● **回應(Reply)** 透過單點傳播來回應查詢。回應中包含通往被查詢目的地的特定路徑。若鄰居沒有 reply，最後會產生 SIA(Stuck in Active)。SIA 等待時間(三分鐘)到了，整個 EIGRP 鄰居關係重新建立並重新計算路由，會導致收斂時間變長。Query 的範圍可以設定，在 CCNP 會教。

● **更新(Update)** 包含路徑資訊，當送出這些封包以回應衡量指標或拓樸變動時，會使用多點傳播。當只有一台路由器需要更新時(例如發現一位新鄰居)，則會透過單點傳播傳送，請記住單點傳播方法也是需要確認的，所以不管使用的遞送機制為何，這些更新都是可靠的。

● **ACK** 使用單點傳播回應更新。ACK 不使用可靠傳送，否則它還需要另一個 ACK 來做確認。對於更新、查詢、回覆三種封包均使用 ACK 以作為可靠傳輸。當收到鄰居送來的這三種封包時，必須回一個 ACK 給鄰居以作為收到確認(Hello 封包不需要 Ack)。

擴散更新演算法(DUAL，Diffusing Update Algorithm)

用來選擇和維護最佳路徑：

- 找出備援路徑(如果存在的話)
- 支援 VLSM
- 執行動態路徑復原
- 向鄰居查詢未知的替代路徑
- 送出替代路徑的查詢

EIGRP 路由器會維護所有鄰居的路徑複本，用來計算自己通往各遠端網路的成本。所以如果最佳路徑當掉時，它通常只需要迅速掃描拓樸表，尋找可行後繼者即可。其次，如果這個快速表格查詢沒有結果，EIGRP 路由器會立刻要求鄰居協助找到最佳路徑。DUAL 利用其他路由器的資訊，故稱為「擴散」演算法。不像其他遶送協定，要將變動傳播到整個網路。

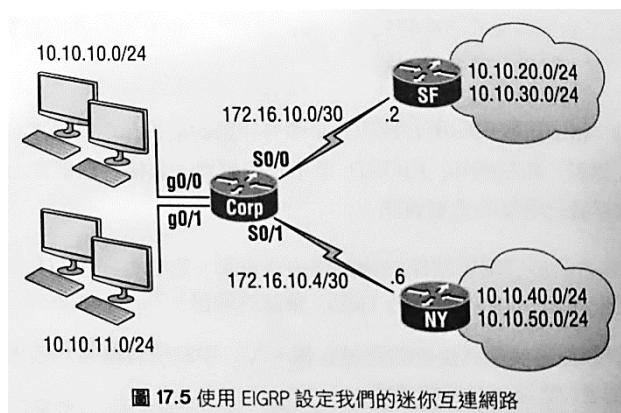
DUAL 運作的 3 項條件：

- 在有限時間內發現鄰居死亡。
- 所有傳送的訊息都有被正確地接收。
- 所有變動和訊息都依照被偵測到的順序來處理。

Hello 確保新鄰居或死亡鄰居的快速偵測，而 RTP 提供可靠的方法來傳送和維持訊息順序。根據這些基礎，DITAL 就可以選擇和維護關於最佳路徑的資訊

設定 EIGRP

EIGRP 命令有兩種模式：路由器組態模式和介面組態模式。在路由器組態模式下，可以開啟協定判斷哪個網路要執行 EIGRP，並且設定整體要素。在介面組態模式下，可以客製化總結和頻寬。



在設定 EIGRP 時，使用 Classful，也就是所有子網路和主機位元全部 off，這也是 EIGRP 的另一優點：它讓鏈路狀態協定的複雜度隱身於背後，而使用和 RIP 一樣簡單的設定程序。

EIGRP 使用 AS 來辨識要分享資訊的路由器群組。具有相同 AS 的路由器會分享路徑。

#只要所有路由器使用相同 AS 編號即可。AS=1~65535

#兩個不同群組的路由器即使有交集，EIGRP 不同便不會傳送，不過在 CCNP 會教 Redistribute，讓兩個 AS 交集處的路由器可以互相溝通。

#另外 EIGRP 最大 HOP255，但可以用上述的 Redistribute 方法來交換延伸。

★常用 EIGRP 指令



指令	說明
Router(config)#router eigrp <u>x</u>	啟動 EIGRP 協定，AS=x(可以是字串或數字)
Router(config-router)#network <u>x.x.x.x</u> <u>y.y.y.y</u>	宣告傳出的 IP, <u>可以加上 Wildcard 精準化，也可省略</u> #除非網路環境中有幾萬個子網路，不然通常不需要加 wildcard?
Router(config-router)#no auto-summary	關閉自動路由壓縮(注意要在同一 AS 才有意義)
Router(config-router)#passive-interface <u>fx/x</u>	設定 fx/x 為被動介面
Corp(config)#router eigrp <u>20</u>	指定特定群組針對特定鄰居，將原來的廣播封包改成單點傳播指向鄰居 IP(選用功能)
Corp(config-router)#neighbor <u>172.16.10.2</u>	
Router(config-router)#variance <u>1-4</u>	修改不同成本的路由負載平衡
Router#show ip protocols	查看路由器上正在執行的路由協定-萬用指令 查詢 K 值
Router#show ip eigrp interface	查看運作中的 EIGRP 介面(Passive 不顯示)
Router#show ip eigrp interface detail <u>介面</u>	承上，依照選定介面列出更多細節
Router#show ip eigrp neighbors	查看 EIGRP 鄰居表，鄰居的 IP、重送間隔、緊鄰路由器的佇列計數
Router#show ip eigrp topology section <u>網段</u>	查看 EIGRP 拓撲表(指定特定部份)
Router#show ip eigrp interfaces 10	列出路由器上有開啟 EIGRP 的介面 查看 AS=10 EIGRP 執行的介面
Router#show ip route <u>網段</u> Router#show ip route eigrp	不解釋，其中出現 D 的就是 EIGRP 路由 查詢路徑表中的 EIGRP 路徑草圖
Router#show ip eigrp traffic	列出傳送和接收到的 EIGRP 各種封包的數目/狀態
Router#show ip eigrp events	顯示每個 EIGRP 事件的 LOG
Router(config-router)#metric weights 0 1 0 1 0 0	將 metric K 值調回預設值(trouble shooting 用) #最一開始的 0 是 ToS 服務類型，固定為 0，後面的 10100 為 K 值預設值
Router#debug eigrp packets	觀察 EIGRP 低層封包狀況，沒事不要開…一開下去沒完沒了
Router(config-router)#address-family ipv4/ipv6 autonomous-system <u>123</u>	不明指令，出現的地方在 router eigrp xx 和 network 之間

△建立鄰居關係(EIGRP 下用 network 宣告)後，應該要出現類似下列提示訊息

%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 209.165.200.229 (Serial0/0/0) is up: new adjacency

VLSM 支援與總結

在互連網路中，點對點網路可以使用 30 位元的子網路遮罩。

其它細節在 RIP 已有。

#新的 15.X IOS 預設會關閉自動總結。但考 CCNA 時還是要會下這個指令。

控制 EIGRP 交通

passive-interface interface-type interface-number

interface-type 選項定義了介面類型，而 interface-number 則定義介面編號。下面的命令將序列 0/0 介面轉換為被動介面：

```
Corp(config)#router eigrp 20
```

```
Corp(config-router) # passive-interface g0/0
```

上述命令讓該介面無法傳送或讀取接收到的 Hello 封包，所以它不會形成緊鄰關係，或是傳送/接收路徑資訊，但它不會阻止 EIGRP 使用通配方式將該介面的子網路從所有其他介面宣傳出去。

#passive-interface 命令的影響取決於執行的遶送協定。例如在執行 RIP 的介面上 passive-interface 命令會阻止路徑更新的傳送，但是允許接收。具有被動介面的 RIP 路由器仍會學到其他路由器宣傳的網路。EIGRP 則不然，在 EIGRP 中使用 passive-interface 命令設定的介面將不會傳送或讀取收到的 Hello。

EIGRP 衡量指標



EIGRP 使用下列 4 項因素做為衡量指標：

- 頻寬
- 延遲
- 負載
- 穩定性

其實還有第 5 項因素：最大傳輸單位(MTU, maximum transmission unit)，不過，雖然它在某些 EIGRP 相關命令中仍是個必要參數(特別是與重分送相關的命令)，但其實並沒有使用在 EIGRP 衡量指標的計算中。MTU 的值代表的是通往目的網路路徑中的最小 MTU 值。

路徑的品質計算是透過一道數學公式，結合上述 4 項主要因素，得出單一的值，對應的衡量指標越高，表示路徑越不利，這個公式如下：

$$\text{metric} = \{K1 \times \text{Bandwidth} + [(K2 \times \text{Bandwidth}) \div (256 - \text{Load})] + K3 \times \text{Delay}\} \times [K5 \div (\text{Reliability} + K4)]$$

公式中的變項如下：

- 預設值： $K1 = 1, K2 = 0, K3 = 1, K4 = 0, K5 = 0$ (10100)
- Delay 等於路徑上所有鏈路延遲的總合。
 - $\text{Delay} = [\text{以 } 10 \text{ 微秒為單位的延遲}] * 256$
- Bandwidth 是路徑上所有鏈路中的最低頻寬。
 - $\text{Bandwidth} = [10^7 / (\text{以 Kbps 為單位的頻寬})] * 256$
- 根據預設， $\text{metric} = \text{路徑上最低頻寬} + \text{路徑上所有延遲的總和}$

視需要可以針對個別介面調整常數 K 值，衡量指標的調整會影響路徑計算的方式。

show ip protocols 可以看到 K 值：

```

Corp#sh ip protocols
***IP Routing is NSF aware***
Routing Protocol is "eigrp 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP-IPv4 Protocol for AS(1)
Metric weight K1=1, K2=0, K3=1,K4=0,K5=0

```

請注意 K1 和 K3 值預設是啟用的—例如 K1 = 1。下表是每個常數和衡量指標間的關係。

Constant	Metric
K1	頻寬(B_e)
K2	負載(路徑的利用)
K3	延遲(D_c)
K4	穩定性
K5	MTU

每個常數是用來對特定變項指定權重，表示在計算衡量指標時，演算法會提升指定指標的重要性，它表示透過指定權重，就可以指定對你最重要的因素。例如，假設頻寬對您最重要，您可以指定 K1 做加權，但是如果完全不能接受延遲，就應該為 K3 指定較大的權重。要小心的是：預設值的任何改變都可能造成不穩定和收斂問題，特別是如果延遲和穩定性一直持續改變的時候！

· 舉例

假如所有 EIGRP 介面中最小頻寬為 1000K(單位為 K)，那麼 Bandwidth 為 $10^7/1000=10000$ 而延遲時間則由經過的所有介面 DLY 時間，DLY 的預設單位為 usec，必須除 10 才是 delay time，所以如果加總為 20200usec，Delay time= $20200/10=2020$

上述總合計算 Metric= $256*(10000+2020)=3077120$

◎修改特定介面參考頻寬(serial埠會有差，兩邊不相對會連不上)

Router(config-if)#bandwidth 10/100/1000

前面那麼多都是天方夜譚，這兩行會就可以調整 EIGRP 偏向了

◎修改特定介面延遲時間(serial埠會有差，兩邊不相對會連不上)

Router(config-if)#delay-time xx → 注意單位為 usec

最大路徑和中繼站數目

EIGRP 預設提供最多 4 條相等成本鏈路的負載平衡。RIP 和 OSPF 也會這樣做。但是在 15.0 版。EIGRP 最多可以在 32 條鏈路間執行負載平衡(相等或不等都可)。指令：

```

Corp(config)#router eigrp 10
Corp(config-router)# maximum-paths?
<1-32> Number of paths

```

EIGRP 路徑更新封包預設的最大 hop 為 100，可以設到最多 255 個。

```
Corp(config)#router eigrp 10  
Corp(config-router)#metric maximum-hops ?  
<1-255> Hop count
```

路徑選擇

EIGRP 會選擇衡量指標最低者做為最佳路徑，但是這並不是 EIGRP 勝過其他協定的主要原因。EIGRP 會將鄰居的路徑資訊儲存在拓樸表中，並且只要鄰居還活著，它就不太會將該鄰居的資訊丟棄。這讓 EIGRP 能在拓樸表中標示出最佳路徑，用於本地路徑表的定位，並且在最佳路徑當掉時標示出次佳路徑做為替代方案。

分割視野/水平分割

距離向量協定在每個介面預設開啟分割視野(split horizon)，這表示如果介面從鄰居路由器收到路徑更新，它在宣傳時不會將這些網路送回給當初傳送這些網路的鄰居路由器。範例省略。

它在什麼時候會出問題呢？在點對多點鏈路，例如訊框中繼網路中，當多個遠端路由器連到單一介面的時候。我們可以使用邏輯介面(子介面)，來解決點對多點介面的分割視野問題。

EIGRP Load balance

- 負載平衡分為 相同/不同成本負載平衡(equal/unequal cost load-balance)
 - 相同成本負載平衡—RIP, EIGRP, OSPF 都支援
 - 不同成本負載平衡—EIGRP Only
- 查看路由負載平衡—show ip protocols → EIGRP maximum metric variance 1
Maximum path:4



Variance1 代表相同成本，當 variance>1 時，表示支援不同成本路由負載平衡。(即不同 FD 的路由可做負載平衡)；假設將參數設為 2，它會允許在 FD*2 的路徑間進行負載平衡。

Maximum path 表示預設的路由負載平衡最大數目 4 條，可以調到最多 16

◎調整路由負載平衡最大數量

```
Router(config-router)#maximum-paths → 還沒試過該指令，真機才能玩
```

◎調整 variance 參數

```
Router(config-router)#variance x → variance 只能設定正整數
```

範例：從 R1-R5 有三條路徑，分別為 R1-R2-R5(metric15), R1-R3-R5(metric25),

R1-R4-R5(metric35)，當 variance=1 時，自然選擇 metric15。

調整 variance=2，此時 EIGRP 會選擇 metric<最小 metric*2(此處為 30)，所以 metric25 那條也符合條件，路由表裡就會列出兩條路徑。(其餘 variance 設定以此類推)

這就是所謂的 **Unequal-cost Load-balance** 不同成本路由負載平衡。

show ip eigrp neighbors 欄位資訊說明：

IP-EIGRP neighbors for process 10								
H	Address	Interface	Hold (sec)	Uptime (ms)	SRTT (ms)	RTO	Q	Seq Cnt Num
0	209.165.200.230	Se0/0/0	12	00:22:36	40	1000	0	8
1	192.168.10.2	Fa0/1	12	00:11:57	40	1000	0	19

- H 路由器發現鄰居的先後順序
- Address 路由器鄰居的 IP
- Interface 路由器跟鄰居相接的本地介面
- Hold 以秒為單位，表示願意花多少時間等待特定鄰居的 Hello 封包，每次收到 Hello 封包時，會重置為最大值，然後倒數計時，若數到 0，則鄰居關係進入 down
- Uptime 表示鄰居關係已建立了多久
- SRTT(Smooth Round-Trip Timer) 流暢來回計時器，代表從該路由器抵達鄰居，再繞回來的完成時間。當傳送多點傳播之後，這個值會限制鄰居回覆的等待時間。如前所述，路由器會在沒有收到回覆時，嘗試透過單點傳播來建立通訊。
- RTO(Retransmission Time Out) 指定多點傳播嘗試的間隔；它是以 SRTT 值為基礎。
- Q Queue Count，指示佇列中是否有任何訊息，應該始終為零，表示路由器介面有 EIGRP 封包待發送；若始終很大，表示出了問題。
- Seq Sequence Number，EIGRP 封包最後一次更新的序號，用於維護同步，追蹤更新、查詢、回覆封包，並且避免重複訊息或失序訊息的處理。

EIGRP Troubleshooting



· 通常 **Troubleshooting** 的流程為

1. 問題回報：使用者/網管人員發現問題，回報給網管。
2. 診斷問題：大致有以下幾種方法—
 - 2.1 Top-down，用 OSI 模型由 L7 一路往下收集資訊
 - 2.2 Bottom up，上面的反過來。
 - 2.3 Divide and conquer，分而治之，從 L3 開始測試，判斷問題是往 L4 或往 L2。
 - 2.4 Trace route，根據經過的路由器逐一檢查
 - 2.5 元件更換，硬體固障
3. 提出解決方案。

★EIGRP 建議除錯步驟

Step	檢查方向	指令
1	EIGRP 路由表是否完整？	#show ip route
2	EIGRP 鄰居形成狀況？	#show ip eigrp neighbors
3	介面啟動狀況？	#show ip interface brief

4	EIGRP 介面啟動狀況?	#show ip eigrp interfaces
5	是否有 Passive interface?	#show ip protocols
6	檢查 EIGRP 的 AS no.是否相同	#show ip protocols
7	是否啟動 EIGRP 認證功能	#show run
8	Network 是否都有宣告	#show ip protocols
9	檢查自動總結(15.x 版之後不用檢查)	#show ip rotocol
10	K 值不符合	#show ip protocols
11	檢查 SERIAL 埠的頻寬、延遲時間	#show interface serial x/x/x
12	檢查是否有被 ACL 亂到	#show access-lists #show ip protocols 有一行 outgoing/incoming update filter list for ...interfaces is x

另外，如果有建立緊鄰關係(adjacency)，卻沒收到遠端網路更新，則可能有遶送問題。可能的原因有：

- EIGRP 流程沒有宣傳到正確的網路
- 存取清單阻擋了遠端網路宣傳
- 自動總結造成非連續網路的混淆

RIP / EIGRP Authentication

- 路由協定可能收到無效更新、惡意攻擊封包，因此有必要時可啟動身份認證功能，支援身份認證的路由協定有 RIPv2, EIGRP, OSPF。
- 只有認證密碼相同的路由器發送的路由資訊，才會接收，在 **RIPv2, EIGRP 中使用 key-chain** 來宣告路由認證密碼。
- Key chain—一個鑰匙箱，裡面有密碼，各組密碼有各自的 key id 用以辨識，所以路由器間要相通就必須用相同的 key id

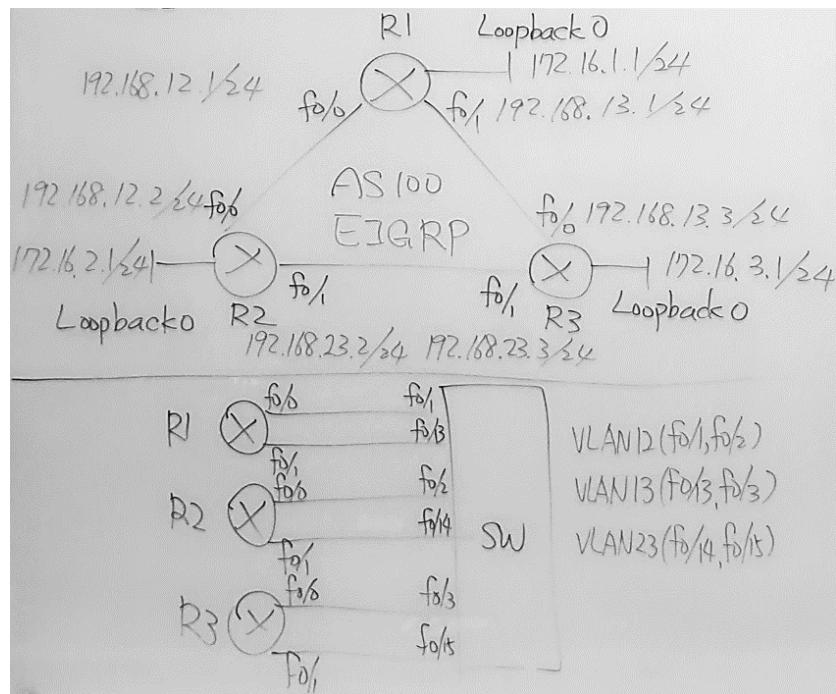
p.s. key id 可以進階設定送收的有效時間，使用 time-range 定義，屬 ccnp 範圍。

◎設定 Key-chain 並套用 key id

指令	說明
Router(config)#key chain <i>key-name</i>	命名 key chain 為 <i>key-name</i> ，
Router(config-keychain)#key <i>1</i>	並在 key 1 宣告密碼為 cisco
Router(config-keychain-key)#key-string <i>cisco</i>	
Router(config)#int fx/x	在選定的介面上啟動 EIGRP
Router(config-if)#ip authentication mode <i>eigrp x md5</i>	認證，並使用 <i>key-name</i> 所定義的密碼
Router(config-if)#ip authentication key-chain <i>eigrp x key-name</i>	

↑ key chain 要套用在兩個路由器對接的那兩個介面上才會生效

▲EIGRP Lab



設定 EIGRP AS 100，確認都學習到精準路由，以 R1 為範例(R2-R3 比照辦理)：

```
R1(config)#router eigrp 100
R1(config)#network 192.168.12.0 0.0.0.255
R1(config)#network 192.168.13.0 0.0.0.255
R1(config)#network 172.16.1.0 0.0.0.255
R1(config)#no auto-summary      →關閉自動彙整路由功能
```

#show ip eigrp neighbor (在此 Lab 裡每個 Router 應該有 2 個)

#show ip eigrp interface

#show ip protocols

R2#show ip route eigrp 會有 3 個 D

D 192.168.13.0/24 [90/30720] via 192.168.23.3, 00:03:06, FastEthernet0/1
 [90/30720] via 192.168.12.1, 00:03:06, FastEthernet0/0

172.16.0.0/24 is subnetted, 3 subnets

D 172.16.1.0 [90/156160] via 192.168.12.1, 00:03:06, FastEthernet0/0

D 172.16.3.0 [90/156160] via 192.168.23.3, 00:03:06, FastEthernet0/1
 90↑AD 值，156160 ↘ 成本

????????????不在 CCNA 範圍的東西???????????

使用 EIGRP 發佈 Default Route

R1(config)#ip route 0.0.0.0 0.0.0.0 null 0 ←null 0 指向自己，不存在 ip 的假 route

R1(config)#router eigrp 100

R1(config)#redistribute static metric 10 10 10 10 10 ←metric 的各項參數

用 show ip route 確認 R2、R3 有學習的 D*EX 0.0.0.0/0 [170/xxx]，即被 EIGRP 轉入的 Default Route

????????????????不在 CCNA 範圍的東西????????????

· 多重動態路由協定狀況

如果一個 LAN 裡同時有多種動態路由協定，比如 RIP, EIGRP，因為 EIGRP AD 較小，所以會優先使用，而 show ip route 也只會看到 EIGRP 的路由，但實際上 RIP 的 Database 還存在，並沒有停止運作，可用 debug ip rip events 看到每 30 秒一次，若要調整 RIP AD 可用 distance 指令調整，但此效果僅限本地路由器。

若多個路由協定的 AD 值一樣，那就比較各協定預設 AD 值。

◎修改 RIP 路由協定 AD 值

Router(config)#router rip

Router(config-router)#distance x →x 就是要給定的 AD 值

◎修改 EIGRP 路由協定 AD 值

Router(config)#router eigrp x

Router(config-router)#distance eigrp y z →y 為內部 eigrp AD, z 為外部 eigrp AD

◎快速啟動 EIGRP(無腦送封包)

Router(config)#router eigrp x

Router(config-router)#network 0.0.0.0

Router(config-router)#no auto-summary

◎手動路由壓縮

就是把自動壓縮功能停掉，自己手動算網段合併的方式，沒什麼好說的，指令如下 ↓

Router(config)#interface xxx

Router(config-if)#summary-address eigrp x 網段 mask

手動路由壓縮有另一種寫法，不用進 EIGRP，直接在 R3 用靜態路由 ↓

ip route x.x.x.0 mask null0 然後再進 EIGRP 中 network 宣告該筆 ip 及 wildmask

要注意手動路由壓縮後 sh ip route eigrp 中會有行

D x.x.x.0/y is a summary, 00:00:01, Null0 →Null0 代表收到往該網段的封包就會自動丟棄以
避免迴圈

另外如果用 show ip route x.x.x.0，可以看到 distance=5

EIGRP 傳送預設路由

· 不能使用 default-information 方式，該指令只用在 RIP / OSPF

· 所以必須使用製作靜態路由往外送的方法 ip route 0.0.0.0 0.0.0.0 interface/ip，又 EIGRP 預設並沒有 0.0.0.0 預設路由，所以必須使用 redistribute static 指令，把該預設路由當作靜態路由匯入到 EIGRP

◎Redistribute static

Router(config)#ip route 0.0.0.0 0.0.0.0 interface/ip

Router(config)#router eigrp x

Router(config-router)#redistribute static → 執行匯入指令

最後 show ip route 會看到一筆 D*EX(外部路由)就是了，AD 值為 170，若要讓預設路由改為內部路由，將 redistribute static 改為 network 0.0.0.0 即可。

◎Redistribute static 方法 2—只能用在 Classful

Router(config)#ip route x.x.x.x y.y.y.y interface/ip → ip and mask must be classful

Router(config)#ip default-network x.x.x.x

Router(config)#router eigrp z

Router(config-router)#network x.x.x.x

管理與控制路由 (EIGRP 延伸學習)

1. R1 到 192.168.23.0 /24 prefer R3

限制只能修改 R1 的參數，使用最適合的方法

2. R2 到 192.168.13.0 /24 prefer R1

限制只能修改 R2 的參數

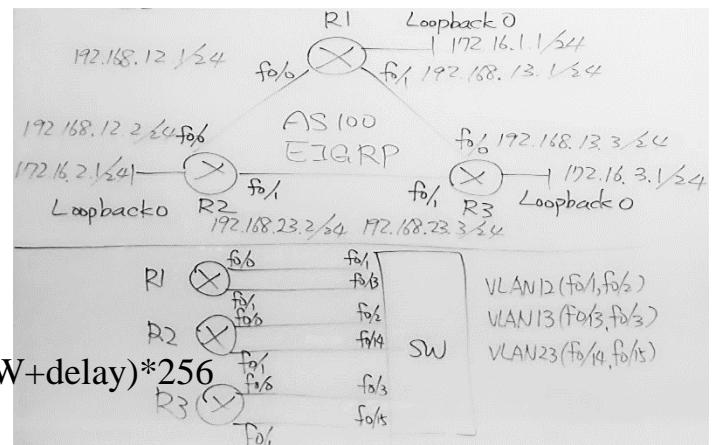
3. R3 到 192.168.12.0 /24 prefer R2

限制只能修改 R3 的參數

Ans：參考講義看 EIGRP 的計算方法—Metric=(BW+delay)*256

方法 1：修改 Bandwidth，不好

方法 2：修改 Delay time，要注意單位是 10msec





OSPF(Open Shortest Path First)

OSPF 基礎

(Open Shortest Path First)開放標準的遶送協定，各廠商都能用。它是使用 Dijkstra 演算法初始化一棵最短路徑樹，然後利用所產生的最佳路徑填入路徑表。OSPF 收斂速度很快，或許沒 EIGRP 那麼快，不過它的收斂速度的確是它受歡迎的理由之一。此外，OSPF 有 2 大優點：負載平衡，以及和 EIGRP 一樣支援 IPv6 被遶送協定。

OSPF 的優點：

- 允許建立區域與自治系統。
- 使路徑更新交通減到最少。
- 支援 VLSM / CIDR。
- 不限制中繼站數目
- 可佈建多種廠牌的設備(開放式標準)。

OSPF V.S. RIP

特性	OSPF	RIPv2	RIPv1
協定類型	鏈路狀態	距離向量	距離向量
支援無級別	是	是	否
支援 VLSM	是	是	否
自動總結	否	是	是
手動總結	是	否	否
支援非連續子網路	是	是	否
路徑的散播	異動時多點傳播	定期多點傳播	定期廣播
路徑衡量指標	頻寬	中繼站	中繼站
中繼站數限制	無	15	15
收斂	快	慢	慢
認證對等節點	是	是	否
階層式網路	是(利用區域)	否(展平的)	否(展平的)
更新	事件驅動	定期	定期
路徑計算	Dijkstra	Bellman-Ford	Bellman-Ford

OSPF 最有用的特性是階層式應用，可以將較大型的互連網路分割成幾個稱為區域(area)的較小型互連網路。

充分利用階層式設計來建置 OSPF 的 3 大理由包括：

- 降低遶送引起的額外負擔(overhead)
- 加速收斂
- 將網路的不穩定性限制在單個區域的網路內。

圖 18.1，OSPF 一定要有區域 0，而所有區域都要連結它。在 AS 內部連結其他區域到骨幹區域的路由器稱為區域邊界路由器(Area Border Router, ABR)，ABR 至少也得有一片介面屬於區域 0。

OSPF 在自治系統內部執行得很好，但也可以將多個自治系統連結在一起，將這些 AS 連結在一起的路由器稱為自治系統邊界路由器(Autonomous System Boundary Router，ASBR)。理想上，您要產生其他區域的網路，儘量讓路徑更新的量維持最小，並且避免問題擴散至整個互連網路。

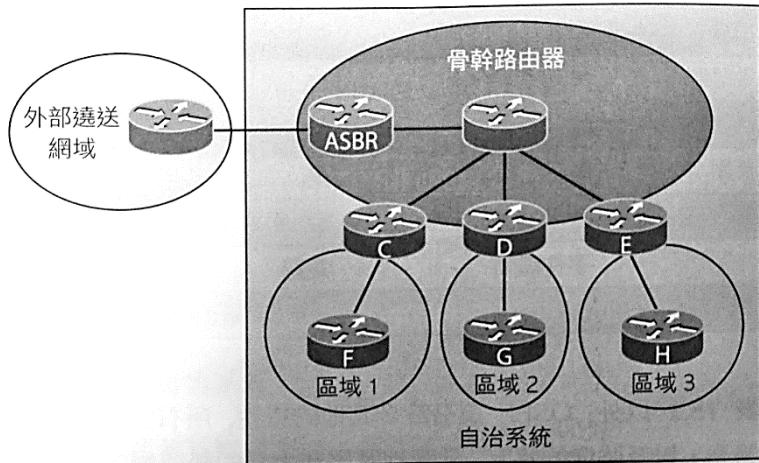


圖 18.1 OSPF 設計範例。OSPF 階層式設計會讓路徑表的項目減至最少，並且讓任何拓樸變動限制在特定區域內。

OSPF 術語

- **鏈路(link)** 一個網路或指定給某網路的路由器介面。當我們增加一片介面到 OSPF 程序時：OSPF 就會將該片介面視為一條鏈路。這條鏈路會有相關的狀態資訊(開啟或關閉)，以及一個(或)以上的 IP 位址。
- **路由器 ID** RID 是用來識別路由器的 IP。挑選 RID 的方式是使用回繞介面中 IP 最大的那個。如果沒有迴繞介面，就選擇所有運作的實體介面中 IP 最大那個。對 OSPF 而言，基本上這可以說是每部路由器的“名稱”。
- **鄰居(neighbor)** 有介面在相同網路上的路由器，例如連到點對點序列鏈路的 2 部路由器。OSPF 鄰居必須有一些共同設定，才能成功建立鄰居：
 - 區域 ID
 - 殘根區域旗標
 - 認證密碼(如果有採用)
 - Hello 與 Dead 計時器的間隔
- **緊鄰關係(adjacency)** 能直接交換路徑更新的兩部 OSPF 路由器間的關係。並非所有的鄰居都可建立緊鄰關係，OSPF 只與建立緊鄰關係的鄰居分享路徑。
在多重存取(multi-access)網路中，路由器與委任路由器、備援委任路由器形成緊鄰。
在點對點、點對多點網路，路由器與連線另一端的路由器形成緊鄰關係。
- **委任路由器(designed router, DR)** 當 OSPF 路由器連到相同廣播網路時，會選出一部 DR 以最小化緊鄰關係數量，並由 DR 將收到的遙送資訊廣播給鏈路上其餘路由器。
選舉先比優先權，具有最高優先權者為 DR。優先權相同再比較 RID。
所有路器都會與 DR、BDR 建立緊鄰，以確保所有路由器拓樸表的同步。

- 備援委任路由器(**backup designated router**，**BDR**) 是多方存取鏈路(請記住 Cisco 有時候喜歡稱它為廣播網路)上的 DR 備援，BDR 只會從 OSPF 緊鄰路由器接收遶送更新，但不會散播 LSA 更新。
- **hello 協定** 動態發現鄰居，並維護鄰居關係。hello 封包與 LSA 會建構並維護拓樸資料庫。hello 封包的位址是 **224.0.0.5**。
- **鄰居關係資料庫(neighbourship database)** 這是從一份 Hello 封包看到的所有 OSPF 路由器的清單，資料庫有所有路由器的細節，包括 RID 與狀態。
- **拓樸資料庫(topology database)** 包含路由器接收某區域所有 LSA 封包中的資訊。路由器利用拓樸資料庫中的資訊當作 Dijkstra 演算法的輸入，計算出抵達每個網路的最短路徑。
#LSA 的作用是要更新與維護拓樸資料庫
- **鏈路狀態宣傳(Link State Advertisement，LSA)** 這是一種 OSPF 資料封包，包含分享給其他 OSPF 路由器的鏈路狀態、路徑資訊。OSPF 路由器只與緊鄰路由器交換 LSA。
- **OSPF 區域(OSPF area)** 一群鄰近的網路與路由器，同區域中所有路由器共享區域 ID，又路由器可能同時屬於一個以上的區域，所以區域 ID 要關聯到路由器上的介面。於是就有可能一部路由器上的某些介面屬於區域 0，而其餘的介面屬於區域 1。同區域內的路由器有相同拓樸表。
設定 OSPF 時，一定要有區域 0，通常會設在連結骨幹網路的路由器上，區域也扮演建立階層式網路結構的角色。
- **廣播(多方存取，multi-access)** 廣播(多方存取)網路如乙太網路，可允許多裝置連結(存取)相同網路，並提供廣播的能力，將單個封包傳送給網路上的所有節點。OSPF 中，每個廣播多方存取網路必須選出一部 **DR** 與一部 **BDR**。
- **非廣播多方存取(nonbroadcast multi-access，NBMA)** 如訊框中繼(frame relay)、X.25、與 ATM 等，這些網路允許多方存取，但沒有如乙太網路的廣播能力。因此 NBMA 網路需要特殊的 OSPF 設定才能正確地運作。
- **點對點(point-to-point)** 兩部路由器間的直連，提供單一通訊線路。點對點連線可以是實體線路，如直接連結兩部路由器的序列纜線；也可以是邏輯線路，例如兩部路由器相隔千里之遠，仍然可以由訊框中繼連結。點對點不需要 **DR**、**BDR**。
- **點對多點(point-to-multipoint)** 一部路由器上的單個介面，與多路由器之間的一組連線組成，共享點對多點連線之所有路由器上的介面都屬於同一個網路，點對多點網路還可以再分為是否支援廣播。

OSPF 的運作

- 鄰居和緊鄰關係的初始化
- LSA 的洪氾(flooding)
- SPF 樹(SPF Tree)的計算

OSPF 最初的鄰居/緊鄰關係形成階段。當 OSPF 在路由器上啟始時，路由器會為它配置記憶體，並且維護鄰居表與拓樸表。一旦路由器判斷哪個介面設定為 OSPF，就會檢查該介面是否啟用，並開始傳送 Hello。



圖 18.2 Hello 協定

Hello 封包是用來發掘鄰居，建立緊鄰關係，並且維護與其他 OSPF 路由器的關係，啟用 OSPF 的介面與支援多點傳播的環境會定期送出 Hello 封包。

Hello 封包使用的位址是 **224.0.0.5**，而傳送頻率則取決與網路型態與拓樸。**廣播與點對點** 網路每 **10 秒**傳送一次，而非**廣播與點對多點**網路網路則是每 **30 秒**傳送一次。

LSA 洪泛

透過鏈路狀態更新(Link State Update, LSU)封包，包含鏈路狀態資料的 LSA 資訊會分享給區域內所有 OSPF 路由器，網路拓樸是透過 LSA 更新來建立，而洪泛法用來讓所有 OSPF 路由器有相同拓樸圖以進行 SPF 計算。

如果每台 OSPF 路由器都 **flood**，會導致大量頻寬消耗，因此需要指定 **DR(Designated Router)** 委任路由器，由 DR 收集其它路由器的 LS 封包，再由 DR 發送 LSA 給鄰居，以節省 LSA 佔用頻寬。點對多點網路 LSA 使用緊鄰路由器的單點傳播 IP。

網路型態	多點傳播位址	描述
點對點	224.0.0.5	所有 SPF 路由器發出
廣播	224.0.0.6	DR 發出
點對多點	--	--

計算 SPF 樹狀結構

在區域內的每部路由器會計算它抵達同一個區域內之每個網路的最佳/最短路徑，這種計算乃根據拓樸資料庫中所收集的資訊，以及最短路徑優先 Shortest Path First, SPF)演算法，利用區域中的每部路由器建構出一個樹狀結構—路由器是根部，而所有其他網路則沿著樹枝與樹葉排列。這是路由器用來新增路徑到路徑表所用的最短路徑樹。

很重要的是，這種樹只包含與該路由器位於相同區域內的網路，如果路由器有分屬多個區域的介面，則得為每個區域建構各自的樹，SPF 演算法在挑選路徑的程序中，有個很重要的條件是考量每條通往網路之可能路徑的衡量指標或成本。但這種 SPF 計算並不應用在從其他區域來的路徑。

DR & BDR election

多重存取網路中第一台路器啟用 OSPF 介面後，即開始選擇 DR/BDR，在多重存取網路中若僅有部份啟用 OSPF，DR 也會產生；DR 為不可插隊(non-preemptive)的，所以一旦某台路由器成為 DR 後，將保持 DR 地位，除非關閉 OSPF 介面或重啟 OSPF。因此如果要預劃 DR 路由器，要注意 OSPF 啟動順序。

★一個 Area 中 DR 產生的優先順序(以 OSPF priority 和 OSPF router ID 為基準)：

● **DR** 具有最高 priority 的路由器，OSPF 介面優先權都一樣為 1，若設為 0，則該 OSPF 介面不參與 DR 選舉。(註：P2P 介面的 OSPF 優先權預設為 0)

● **BDR** 第二高 Priority 路由器，備援。

● **DR Other** 除了 DR 和 BDR 外的路由器。

△若 OSPF 介面優先權相同(通常相同)，則 RID 最大者為 DR，次大為 BDR。

△特殊情況—DR 被搶走，多台路由器 OSPF 設定不同(Hello time、認證密碼)時，無法建立鄰居，會自己當 DR，直到可以建立鄰居時再選 DR。

OSPF 封包群播 IP：

OSPF 路由器送給鄰居使用 224.0.0.5 傳送 LS 封包；但若有 DR，則一般 OSPF 路由器送 LS 封包給 DR/BDR 使用 224.0.0.6，而 DR 使用 224.0.0.5 傳送給其它 OSPF 路由器。

強迫重選 DR—把所有路由器 OSPF 介面 shutdown+no shutdown

OSPF 衡量指標

成本(cost)。SPF 樹中的每個離開介面會結合一個成本，而整條路徑的成本則是沿著該路徑所經過之離開介面的成本總和，因為成本就如 RFC 2338 所定義的那樣，是個任意值，Cisco 實作了它自己的方法來計算每個運行 OSPF 介面的成本。Cisco 使用的計算公式是 $10^8/\text{頻寬}$ ；其中頻寬是為該介面的設定頻寬。根據這個規則，100Mbps 快速乙太網路介面的預設 OSPF 成本是 1，而 1000Mbps 乙太網路介面的成本是 0.1。

這個值可利用 ip ospf cost 命令加以更改，成本的值可更改為 1 到 65535 的範圍，因為成本是要指定給每個鏈路的，所以更改成本時要注意是否有針對您所想要的介面。

★OSPF 成本計算(公式)

介面參考頻寬越大，成本越小： $10^8/\text{頻寬}$ (即 100Mbps)/介面參考頻寬(bps)

一個簡單的判別方式，Fast Ethernet interface 介面(100M)成本為 1

查詢參考頻寬—show interface x，BW 1000Kbit 那幾個字就是。

查詢 OSPF 成本—show ip ospf interface fx/x，Cost 就是

路由表 OSPF 成本

根據每個出口介面的 OSPF 成本累加，比如 R1 s0/0/0→R2 f0/0，成本就是
 $64(10^8/1544)+1(10^8/10^8)=65$ 。

Interface type	bandwidth	Cost
Fast Ethernet and faster	100 Mb/s and higher	1
Ethernet	10 Mb/s	10
E1	2 Mb/s	48
T1	1.544 Mb/s	64
128bps	128bps	781
64kbps	64kbps	1562
56kbps	56kbps	1785

★OSPF 常用指令★



指令	說明
Router(config)# router ospf ? <1-65535> Process ID	啟動 OSPF 路由協定，不同路由器間可用不同 process-id #Process-ID 只對本機有意義，用來識別 OSPF 資料庫裡的特定實例
Router(config-router)#network <u>x.x.x.x y.y.y.y</u> area <u>z</u> #這裡宣告可用 classful 也可用子網段或完整 ip	1. 2.宣告傳出的網路位址，x 為 ip，y 為 wildcard，z 為 area-id，同一個 segment 的 area-id 要相同。(要從主幹 0 開始) 3.ip 的部份也可以設介面 ip，y 為 0.0.0.0，明確指定特定介面加入 OSPF
Router(config-router)#passive-interface fx/x	設定 fx/x 為被動介面
Router(config-router)#distance 100	修改整個 OSPF 的 AD 值為 100
Router(config)#ip route 0.0.0.0 0.0.0.0 <u>interface</u> Router(config)router ospf <u>x</u> Router(config-router)#default-information originate	啟動 OSPF 傳送預設路由(發布預設路由)
Router(config-router)#router-id <u>a.a.a.a</u>	修改 OSPF 的 router-id 為 <u>a.a.a.a</u>
Router(config-router)#network 0.0.0.0 255.255.255.255 area 0	將所有網路介面加入 ospf 及其 area(懶人法)
Router(config-if)#ip ospf priority <u>b</u>	修改單一介面的 OSPF priority 為 b
Router#show ip ospf	查詢路由器上運行中的 OSPF 資訊，包括路由器 ID、區域資訊、SPF 統計、LSA 計時器資訊。
Router(config-if)#ip ospf <u>1</u> area <u>0</u>	只將單一介面加入 OSPF
Router#show ip ospf neighbor	查看 OSPF 鄰居表、緊鄰狀態、DR/BDR
Router#show ip ospf database	查看 OSPF 資料庫 包括該 AS 中的 RID、及其鄰居路由器

	ID。這個命令只會顯示 OSPF 路由器，而不像 show ip eigrp topology 會顯示 AS 中的每條鏈路。
Router#show ip ospf interface fx/x	顯示所有與介面相關的 OSPF 資訊 包括：介面 IP、區域號碼、程序 ID、路由器 ID、網路類型、成本、優先權、DR/BDR、Hello/Dead 時間、緊鄰鄰居資訊
Router#show ip route ospf	檢視 OSPF 路由
Router#show ip protocols	確認 OSPF Process ID/Router ID
Router#clear ip route	清除 Routing table
Router#clear ip ospf process	重新啟動 OSPF，在手動設定 router-id 後需要重啟
Router#debug ip ospf events (記得做這個之前先做 console 同步)	查看 OSPF 低層封包狀況
Router#ip ospf network point-to-point	改變某介面的網路型態

指令補充說明

- 一部路由器上可同時執行多個 OSPF 程序，但並不等於執行多區域 OSPF。第 2 個程序會完整地維護它自己個別的拓樸表，並獨立地管理它的通訊。可以運用它讓 OSPF 將多個 AS 連接在一起。
- 設定 OSPF 區域號碼可以從 0 到 42 億，也可以使用 IP 位址的格式來標示區域，請不要跟程序 ID 混淆了；程序 ID 是從 1 到 65535。
- 複習一下通配字元：通配遮罩中的 0 位元組代表網路中所對應的位元組必須完全符合，而 255 則表示網路號碼中所對應的位元組無關緊要。例如 1.1.1.1 0.0.0.0 的網路與通配遮罩組合，意味著只有 1.1.1.1 可以匹配其他都不行。如果您想要以非常清楚且簡單的方式在特定介面上啟用 OSPF，這真的非常有用。如果您堅持要匹配一個範圍的網路，例如 1.1.0.0 0.0.255.255 的組合表示能夠匹配的網路範圍是 1.1.0.0 到 1.1.255.255。堅持使用 0.0.0.0 的通配遮罩，並個別地指定每個 OSPF 介面是比較簡單且安全的做法，不過不管哪一種設定方式，功能都是一樣的，並沒有優劣之分。
- 區域號碼顯示該網路與通配遮罩所指的介面屬於那個區域。請記住 OSPF 路由器只有當介面設為相同 AS 時，才能成為鄰居。區域號碼的格式可以是從 0 到 4,294,967,295 的十進位值，或表示成以點號隔開的十進位符號，例如 0.0.0.0 是個合法的區域號碼。它的值其實與 0 是相同的。
- Hello/Dead 預設值為 10/40。

OSPF interface Configuration

OSPF 的介面資訊可修改，最常用到的是修改 Hello time、OSPF Cost

◎Hello time Configuration --針對特定介面

Router(config-if)#ip ospf hello-interval y

Router(config-if)#ip ospf dead-interval x →注意 x 一定要大於 y，不然會 gg

(可以省略 dead-interval，如此會預設為 4y)

◎OSPF Cost Configuration – 2 種方法

1.Router(config-if)#bandwidth x →修改介面參考頻寬(單位為 k)，使 OSPF cost 重新計算

2.Router(config-if)#ip ospf cost y →直接修改介面的 cost

p.s. 指令 bandwidth 是參考頻寬，speed 是實際頻寬，要注意

OSPF 與回繞介面

在使用 OSPF 時，設定回繞(loopback)介面是很重要的，Cisco 建議，在路由器上設定 OSPF 時最好使用它們以求穩定。

回繞介面是一種邏輯介面，它是虛擬的，純軟體式的介面，這表示它們並非實體的路由器介面。在 OSPF 設定中使用回繞介面，可確保介面會為了 OSPF 程序而一直處於作用中。

它們在診斷或設定 OSPF 上也相當方便。如果沒有在路上設定回繞介面，則在開機時，路由器上作用中的最高 IP 位址就會變成路由器的 RID！

RID 不只用來宣傳路徑，它也用來選出委任路由器(DR)與備援委任路由器(BDR)。當新的路由器啟用，並且交換 LSA 來建立拓樸資料庫時，這些委任路由器會建立緊鄰關係。

#根據預設，OSPF 啟動時會使用任何作用中介面的最高 IP 位址。然而，這可以被邏輯介面給蓋過去，任何啟用介面之最高 IP 位址總是會成為路由器的 RID。

以下為如何設定回繞介面、確認回繞位址與 RID。

設定回繞介面是 OSPF 設定中最容易的部份，首先，讓我們以 show ip ospf 命令檢視一下 Corp 路由器的 RID，然後以完全不同的 IP 位址結構來設定回繞介面。

★藉由使用/32 遮罩，我們可以用任何 IP 設在 Loopback 上，只要不衝突就可以。

★遮罩 255.255.255.255(/32)是什麼意思呢? /32 稱為主機遮罩，基本上只會用在 Loopback 上。它可以讓我們節省子網路。假如我有四個 loopback172.31.1.1-2-3-4，不使用/32，就必須為每台路由器建立獨立的子網路。

▲設定完 Loopback 並不會馬上變動 RID，有三個方法可以生效：

1.重開機。

2.刪除 OSPF 並重建路由器上的資料庫。

3.直接手動設定 RID—用(config-router)#router-id x.x.x.x

· 建立 OSPF 鄰居的訊息長這樣

00:47:30: %OSPF-5-ADJCHG: Process 20, Nbr 209.165.200.229 on Serial0/0/0
from LOADING to FULL, Loading Done

- show ip ospf neighbor 長這樣

```
R2(config-router)#
R2(config-router)#do show ip ospf neighbor

```

Neighbor ID	Pri	State	Dead Time	Address	Interface
209.165.200.229	0	FULL/ -	00:00:31	209.165.200.229	Serial0/0/0

- Neighbor ID 是鄰居路由器的 Router-id
- Pri 該介面的 OSPF 優先權，用來選舉 DR。
- State 該介面的 OSPF 狀態，有 7 種，最後一種完成式為 FULL
- Dead Time 宣告鄰居進入 down 狀態之前，等待該設備發送 Hello 封包的剩餘時間
- Address 該路由器鄰居用於與 R1 直連介面的 IP 位址，即為 next hop IP
- Interface 該路由器用於與該鄰居 OSPF 路由器建立鄰居關係的介面
- Router ID：即路由器的名字，以 IPv4 格式命名(若 Router ID 重名，int 介面會一直 up/down)

Router ID 決定順序
 1. 透過指令手動設定
 2. 較大的 LoopbackIP
 3. 較大的 Active Interface IP
 若路由器上沒有半個可用 IP，無法啟動 OSPF
 Router ID 狀態可從 show ip protocols 看到

· 各種啟動 OSPF 的方式

1. Router(config-router)#network 0.0.0.0 255.255.255.255 area 0 → 代表所有 ip 通通宣告
2. Router(config-router)#network interfaceIP 0.0.0.0 area 0 → 指定單一介面加入 OSPF

OSPF 負載平衡

在下圖範例中，Corp--Branch 間有兩條鏈路。

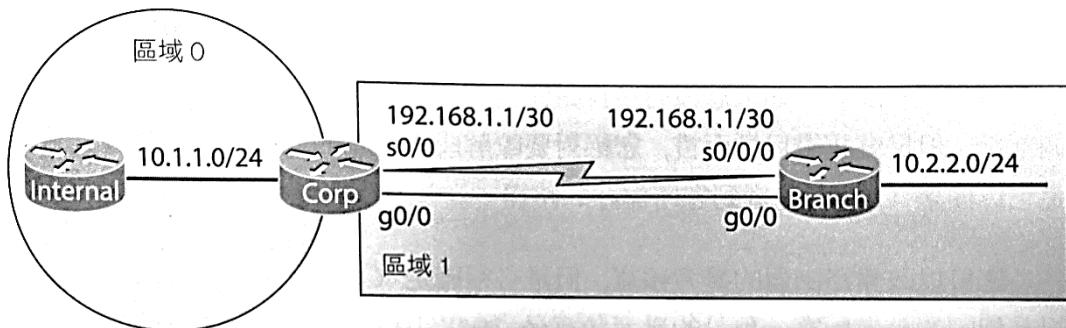


圖 19.10 具有雙重鏈路的互連網路範例

首先，在 2 台路由器間的 Gigabit 乙太網路介面，當然要好過任何序列鏈路；這表示我們希望路由器使用 LAN 鏈路。我們可以停止序列鏈路連線，並且把它當作備援鏈路。

檢查路徑表，觀察 OSPF 發現了什麼：

```
Corp# sh ip route ospf
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O 10.2.2.0 [110/2] via 192.168.1.6, 00:00:13, GigabitEthernet0/1
```

OSPF 很聰明地選擇了 Gigabit 乙太網路鏈路，因為它具有最低的成本。雖然有時可能需要插手來協助 OSPF 選擇最佳路徑，但目前最好就維持原狀。不過，這沒什麼好玩的。所以，讓我們來將這兩個介面的成本設為相同，誤導 OSPF 讓它以為這兩條鏈路是相等的：

```
Corp#config t  
Corp(config)#int g0/1  
Corp(config-if)#ip ospf cost 10  
Corp(config-if)#int s0/0/0  
Corp(config-if)#ip ospf cost 10
```

顯然，您必須在鏈路兩端都完成這項設定。現在，讓我們再來檢查路徑表

```
Corp # sh ip route ospf  
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks  
O 10.2.2.0 [110/11] via 192.168.1.2, 00:01:23, Serial0/0/0  
                                [110/11] via 192.168.1.6, 00:01:23, GigabitEthernet0/1
```

這個例子並不是說您應該將這兩種鏈路設為相同成本，但是有時候您會需要調整 OSPF 成本。如果您沒有多條鏈路通往遠端網路時，就完全不需要關心這個部份。

另外也可以改變路由器的參考頻寬，但是必須確定 OSPF AS 中的所有路由器都有相同的參考頻寬。預設的參考頻寬是 10^8 ，也就是快速乙太網路的頻寬 100 Mbps，如 **show ip ospf** 與 **show ip protocols** 命令所示：

```
Routing for Networks:  
10.2.2.1 0.0. 0.0 area 1  
192.168.1.2 0.0.0.0 area 1  
Reference bandwidth unit is 100 mbps
```

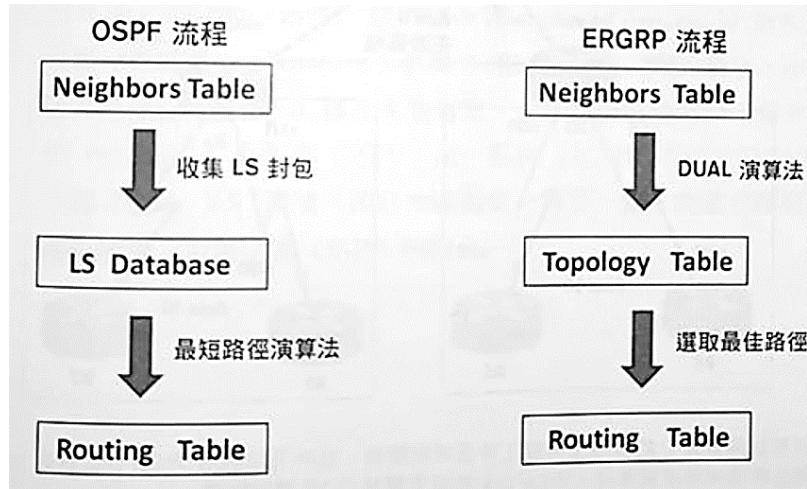
這使得任何以 100Mbps 或更高速運作的介面成本為 1。預設為 100，但如果將它改成 1000，則成本就會增加 10 倍。再提醒一下：如果要對此做改變，就必須確定 AS 中的所有路由器都完成這樣的設定！下面是它的做法：

```
Corp(route) # router ospf 1  
Corp (config-router) #auto-cost reference-bandwidth ?  
<1-4294967> The reference bandwidth in terms of Mbits per second
```

其它補充

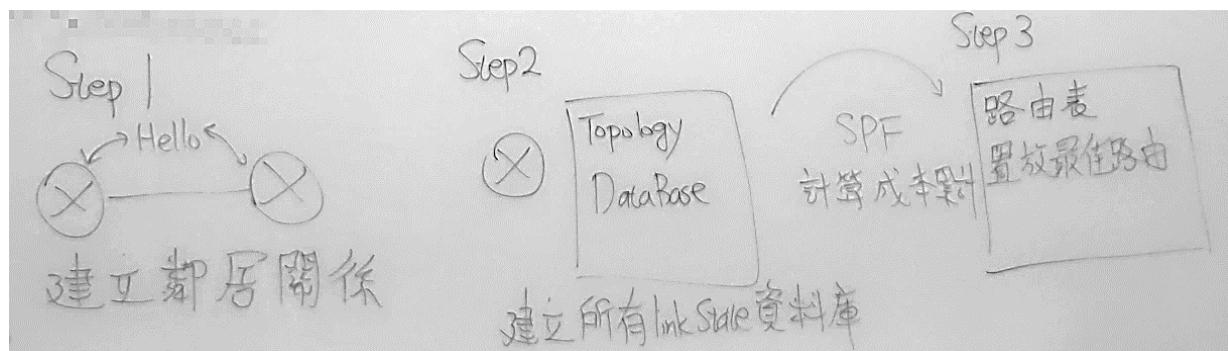
- Link-state(LS)：連接狀態，包含該路由器的所有介面資訊—IP、介面種類、成本、鄰居資訊
- Link-state DataBase(連接狀態資料庫)。由於每一條 LSA 是對一台路由器周邊網路拓撲的描述，則整個 LSDB 就是對該自治系統網路拓撲的真實反映。根據 LSDB，各路由器運行 SPF(最短路徑優先)演算法。

- OSPF v.s. EIGRP：兩者都有三階段，第一階段都是發 Hello 封包；第二階段也都是由鄰居收集相關資訊，OSPF 收集 LS 封包以建立 LSDB，EIGRP 使用 DUAL 過濾學習到的遠端網路資訊到 Topology table；第三階段 OSPF 使用最短路徑演算法挑出最佳路徑到路由表，EIGRP 則從 Topology table 挑出最佳路徑到路由表。(附圖)



p.s.若非 0 區域未和主幹相連時，可利用 Virtual Link 將它們連結，ccnp 有。

OSPF LAB



1. 先完成基本 Lab 設定
2. 指定 R1 router ID 100.100.100.100
R2 router ID 150.150.150.150
R3 router ID 200.200.200.200
3. 設定 OSPF Area 0，將所有直接介面加入 OSPF100
Codes↓

R1(config)#router ospf 100 → 100 為其資料庫代碼，即 show ip ospf interface brief 裡的 PID

```

#router id 100.100.100.100
#network 192.168.12.0 0.0.0.255 area 0
#network 192.168.13.0 0.0.0.255 area 0
#network 172.16.1.0 0.0.0.255 area 0

```

R2-R3 比照設定

☆OSPF 資料庫代碼可不同，但 Area 要同一個



AREA

OSPF 可以根據自治系統的拓撲結構劃分成不同的區域(AREA)，這樣區域邊界路由器(ABR)向其他區域發送路由資訊時，以網段為單位生成摘要 LSA(Link-State advertisement)。這樣可以減少自治系統中的 LSA 的數量。

多重區域 OSPF 的功能：

- 限制 LS 封包範圍在同一區域。
- 在不同區域的 OSPF 可以啟動路由壓縮，縮小 OSPF 路由表。

- OSPF 使用多個 Area 來局限當網路異動所影響的範圍
- 橫跨 2 個 Area 的 OSPF Router 稱為 ABR(Area Border Router)
- 橫跨 2 個不同的路由協定，稱為 ASBR(Autonomous System Boundary Router)

多區域元件類別

下面幾節將討論路由器在多區域 OSPF 網路中所扮演的不同角色，包括骨幹路由器，內部路由器，區域邊界路由器，和自治區系統邊界路由器。同時也將介紹 OSPF 網路中使用的不同宣傳類型。

鏈路狀態宣傳(LSA)用來描述該路由器以及與它相連的網路。路由器會交換 LSA，並且學習完整的網路拓撲，直到所有路由器都有相同的拓撲資料庫。在建立拓撲資料庫之後，OSPF 使用 Dijkstra 演算法來找出通往遠端網路的最佳路徑，並且只將最佳路徑放入路徑表中。

緊鄰關係的需求

一旦找出鄰居後，就必須建立緊鄰關係，以交換遼送資訊(LSA)。將相鄰的 OSPF 路由器變成 OSPF 鄰居路由器需要兩個步驟：

1. 雙向溝通(透過 Hello 協定達成)
2. 資料庫同步，包含路由器間的 3 種封包交換：
 - 資料庫描述(Database Description, DD)封包
 - 鏈路狀態請求(Link-State Request, LSR)封包
 - 鏈路狀態更新(Link-State Update, LSU)封包

一旦資料庫完成同步，兩台路由器就會被視為緊鄰，而達成緊鄰關係。

請務必記住在下列項目不符合時，鄰居間將無法形成緊鄰關係：

- 區域 ID
- 子網路
- Hello 與 dead 計時器
- 認證(如果有設定)

何時形成緊鄰關係，取決於網路類型。如果是點對點鏈路，兩個鄰居會在 Hello 封包資訊設定正確時形成緊鄰關係。在廣播式多點存取網路中，緊鄰關係只會在網路上的 OSPF 路由器，DR 和 BDR 之間形成。

OSPF 路由器角色

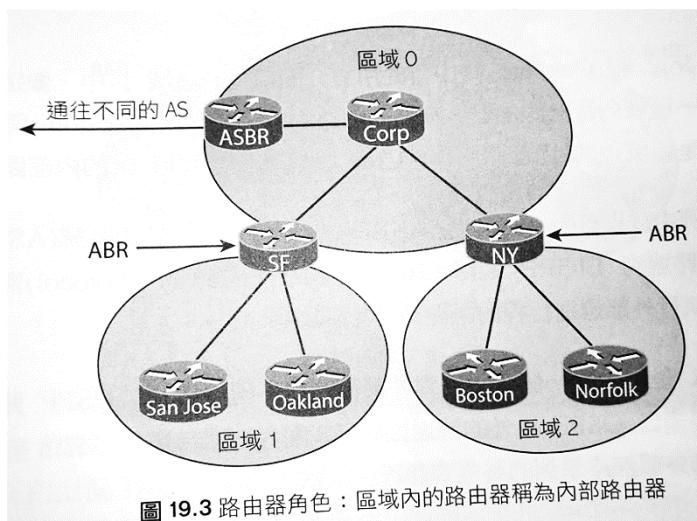


圖 19.3 路由器角色：區域內的路由器稱為內部路由器

區域 0 中有 4 台路由器：Corp、SF、NY、和自製系統邊界路由器(ASBR)。在設定多區域 OSPF 時，必須有 1 個區域稱為區域 0，也就是「骨幹區域(backbone area)」。其他所有區域都必須連到區域 0。這 4 台路由器稱為「骨幹路由器」；也就是指部分或完全存在於 OSPF 區域 0 內的任何路由器。

同時還連到其他區域的 SF 和 NY，路由器擁有不只一個區域的介面，所以也是區域邊界路由器(ABR)。除了連到區域 0 之外，SF 還有區域 1 的介面，而 NY 則有區域 2 的介面。

個區域的介面，所以。 ABR 是一個以上 OSPF 區域的路由器，它會在拓樸表中維護來自所有直接相連區域的資訊，但是並不會跟某個區域分享另一區域的拓樸細節。不過 ABR 會將某個區域的遶送資訊轉送給另一個區域。很重要的觀念是：ABR 會分隔 LSA 的洪氾區域，是總結區域位址的主要地點，通常有來源預設路徑，而且會為連結的每個區域維護鏈路狀態資料庫(LSDB)。

#請記住 1 台路由器可以扮演多個角色。在圖 19.4 中。 SR 和 NY 就同時扮演骨幹路由器和區域邊界路由器

San Jose 和 Oakland 路由器的所有介面都位於區域 1 中。像這種所有介面都在單一區域內部的路由器，稱為內部路由器。同樣地，Boston 與 Norfolk 路由器也是區域 2 的內部路由器。Corp 路由器則是區域 0 的內部路由器。

在本例中，只有唯一的一台 ASBR，連結到外部的自治系統(AS)，當一個 OSPF 網路達到 EIGRP 網路、BGP(Border Gateway Protocol)網路，或是其他任何執行外部遶送行程的網路時，就稱為是 AS。

ASBR 是至少有一個介面連結到外部網路或不同 AS 的 OSPF 路由器，當接收的路徑來自 OSPF 以外的遶送協定時，就會被認為是外部網路。ASBR 會負責將透過外部網路學到的路徑資訊注入 OSPF 中。

ASBR 並不會自動在 OSPF 遲送行程和它連結的外部遶送行程間交換送資訊。這些路徑是透過「路徑重分送」(route redistribution)的方法來交換。--CCNP



鏈路狀態宣傳

路由器的鏈路狀態資料庫是由鏈路狀態宣傳(LSA)所構成，有 5 種 LSA 類型如下：

• LS 封包定義有 11 種型態，稱為 LSA，CCNA 只教 type1-5，其餘屬 CCNP 範圍。

Danniel 版本(精簡版)

Type1(Router LSA)—Area 中的每顆都會發(一定會有)

Type2(Network LSA)—每個 Area 中的 DR 都會發(如果是一對一的狀態可能沒有)

Type3(Summary LSA)—由 ABR 發出到另一個 area 的 LSA

Type4(ASBR Summary LSA)—由 ABR 來告知誰是 ASBR

Type5(Autonomous System LSA)—由 ASBR Redistribute 比如 eigrp 轉到 ospf

複雜版

● **第 1 型 LSA** 稱為路由器鏈路宣傳(router link advertisement, RLA)，或是簡稱路由器 LSA。每台路由器會傳送第 1 型 LSA 給該區域的其他路由器。這項宣傳包含路由器在該區域內的鏈路狀態。如果路由器連到多個區域，它們針對每個區域分別傳送不同的第 1 型 LSA。第 1 型 LSA 包含路由器 ID(RID)、介面、IP 資訊和目前介面狀態。例如在圖 19.4 的網路中，路由器 SF 會透過區域 0 和區域 1 的介面，分別傳送描述其鏈路態的第 1 型 LSA 宣傳。圖 19.4 的其他路由器也是如此。

#限定在一個 OSPF 區域內傳送給所有 OSPF 路由器，不會跨過 ABR / ASBR，type1 封包所建立的 ospf 路由資訊在路由表代碼為 O。

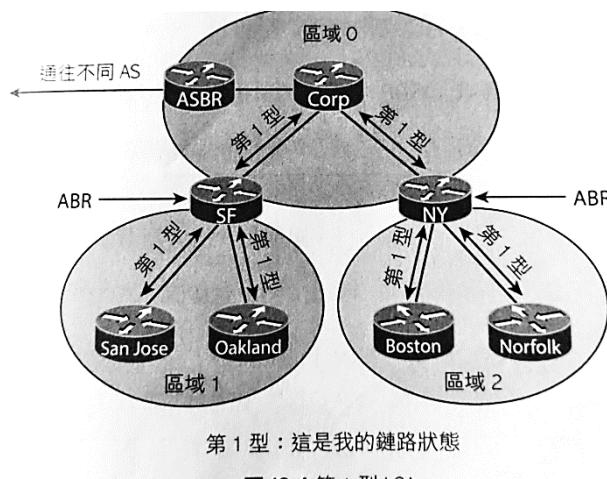


圖 19.4 第 1 型 LSA

● **第 2 型 LSA** 稱為網路鏈路宣傳(network link advertisement, NLA)，是由委任路由器(DR)所產生。委任路由器是被選出來代表網路中的其他路由器。DR 使用第 2 型 LSA 來傳送相同網路中其他路由器的狀態資訊，第 2 型 LSA 會洪氾給相同區域中的所有路由器，但是不會送到該區域之外。這些更新中包含 DR 與 DBR 的 IP 資訊。

#由 DR 送出的 LSA 定義為 type2，在路由表代碼為 O

● **第 3 型 LSA** 稱為總結鏈路宣傳(summary link advertisement, SLA)，是由區域邊界路由器所產生。這些 ABR 會將第 3 型 LSA 送往產生訊息之外的其他區域。第 3 型 LSA 會宣傳網路和通往骨幹區域(區域 0)的跨區域路徑。這些宣傳中包含 IP 資訊和宣傳該 LSA 的 ABR 之 RID。

#type3 會傳遍所有 OSPF 區域，另外 ABR 可以執行路由壓縮後再送出 type3 封包，預設不啟用壓縮，在路由表代碼為 OIA。

#總結通常是將許多小型子網路的細節隱藏在總結後的網路位址，將單一大型網路放入宣傳中。但是在 OSPF 中，總結鏈路宣傳並沒有真正包含網路總結。除非管理者手動建立總結，否則該區域中所有可用的個別網路都會完整地透過 SLA 宣傳。

● 第 4 型 LSA 由任何邊界路由器產生。ABR 會將第 4 型 LSA 向產生訊息之外的區域傳送。

這些也是像第 3 型的總結 LSA，但是包含的是其他 OSPF 區域如何抵達 ASBR 的資訊。

#TYPE4 主要用來說明 ASBR 路由器在哪邊的資訊，讓其他路由器可根據 TYPE4 LSA 及 OSPF 內部成本來計算 OSPF 外部路由成本，決定外部路由最佳路徑

● 第 5 型 LSA 稱為 AS 外部鏈路宣傳，是由 ASBR 產生，用來宣傳 OSPF 自治系統外部的路徑，並且會洪氾至所有地方，ASBR 會針對每個外部網路產生第 5 型 LSA。

#TYPE5 LSA 的內容為外部路由資訊，路由表代碼為 OE1 或 OE2

圖 19.5 是在多區域 OSPF 網路中所使用的每種 LSA。

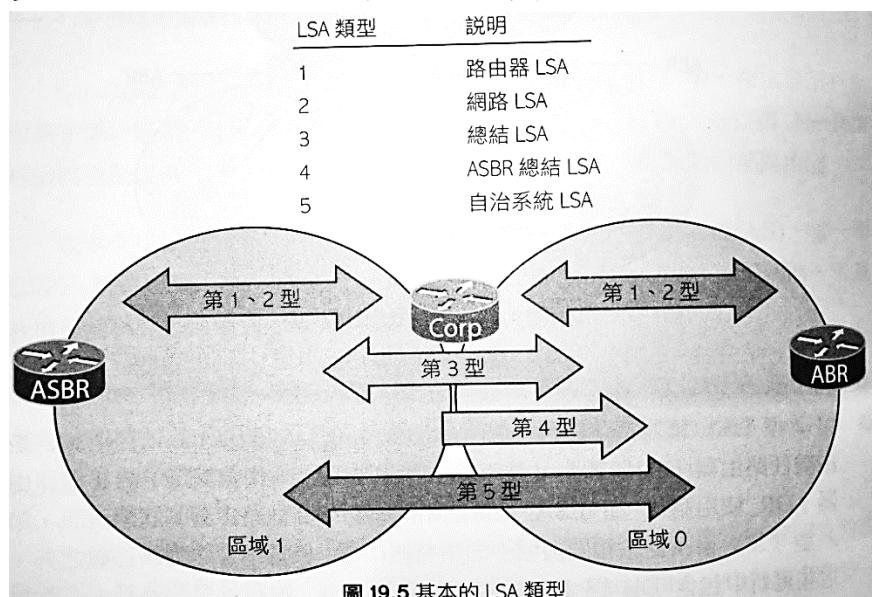


圖 19.5 基本的 LSA 類型

在圖 19.5 中，可以看到第 1-2 型 LSA 是在相同區域的路由器間進行洪氾。圖中的 Corp 路由器是 ABR，它會為每個連結區域維護 LSDB。從 Corp 路由器傳送的第 3 型 LSA 會總結從區域 1 得到的資訊，送往區域 0；反之亦然。ASBR 會將第 5 型 LSA 洪氾至區域 1，而 Corp 路由器則會將第 4 型 LSA 洪泛至區域 0，告訴所有路由器如何抵達 ASBR—相當於是代理 ASBR。

OSPF 的 Hello 協定

Hello 協定提供鄰居很多資訊。根據預設，鄰居間每隔 10 秒會溝通下列資訊：

● 路由器 ID(RID) 這是路由器上最高的作用中 IP 位址，它會優先使用最高的回繞 IP 位址。如果沒有設定回繞介面，OSPF 會從實體介面中選擇。

● Hello / Dead 間隔 Hello 封包間的時間間隔稱為 Hello 時間，預設為 10 秒，Dead 時間則是在認定鄰居失效前，用來等待 Hello 封包的時間長度—除非另外設定，否則就是 Hello 間隔的 4 倍。

- **鄰居** 這項資訊包含該路由器的所有鄰居之路由器 ID 清單；鄰居是指連到相同 IP 子網路，並且使用相同子網路遮罩的路由器。
- **區域 ID** 路由器傳送端介面所屬區域
- **路由器優先序** 這是用來協助 DR 與 BDR 選舉的 8 位元值。
- **DR IP 位址** 目前 DR 的路白器 ID。
- **BDR IP 位址** 目前 BDR 的路由器 ID。
- **認證資料** 認證類型與相關資訊(如果有設定的話)

Hello 更新訊息中的 hello / dead 計時器間隔、區域 ID、OSPF 區域類型、子網路、以及認證資料(如果有的話)，都必須完全匹配。如果任何一項不符，就不會產生緊鄰關係。

鄰居狀態

在進行 OSPF 的設定、驗證、和故障檢測之前，必須先瞭解在建立緊鄰關係時，OSPF 路由器會經過哪些狀態。

當 OSPF 路由器初始化時，它們會先使用 Hello 協定透過多點傳播位址 224.0.0.5 交換資訊。在路由器間建立鄰居關係後，路由器會透過 LSA 的穩定交換來同步它們的鏈路狀態資料庫 (LSDB)。當它們啟動時，會交換相當多資訊。

兩台路由器間的關係有 8 種可能的狀態，所有 OSPF 路由器都是從狀態 DOWN 開始，然後與鄰居進入到 2WAY 或 FULL 狀態，如圖 19.6 所示。

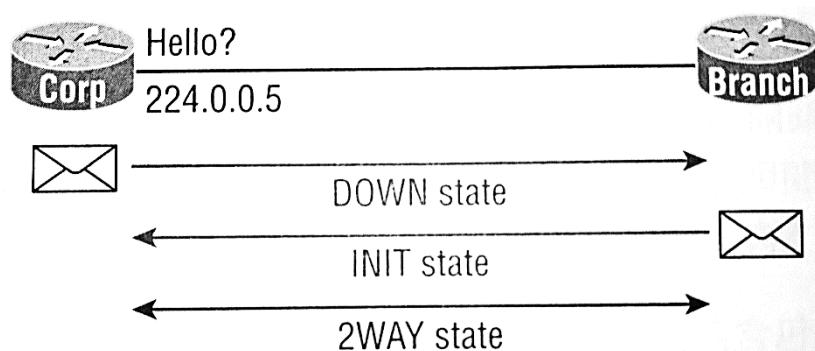


圖 19.6 OSPF 鄰居狀態--第 1 部分

這個過程從傳送 Hello 封包開始，每個在聆聽的路由器會將傳送的路由器加入鄰居資料庫中，回應的路由器會回覆它們的 Hello 資訊，讓原始傳送者加入到自己的鄰居表中，此時，雙方達到 2WAY 狀態—只有某些路由器會超越這個狀態建立緊鄰關係。

下面是 8 種可能的關係狀態：

- **DOWN** 表示介面還沒有收到 Hello 封包—不過這並不表示介面實際上是關閉的。
#還沒送出 Hello

- **ATTEMPT** 表示必須手動設定鄰居。它只適用在非廣播式多點存取(NBMA)的網路連線上。
- **INIT** 表示已經從另一台路由器收到 Hello 封包。但是在鄰居欄位中沒有接收者的路由器 ID。表示尚未建立雙向溝通。

#兩方開始交換 Hello，但尚未驗證 Hello 封包

- **2WAY** 表示已經收到鄰居欄位中包含本身路由器 ID 的 Hello 封包—雙向通訊已經建立完成。在廣播式多重存取網路中，在此狀態之後就可能發生選舉。

#兩方收到彼此的 Hello，並可用 show ip ospf neighbors 查詢鄰居表，但此時鄰居關係未完整，有時 DR 路由器的鄰居狀態還停留在 two-way

在選出 DR 和 BDR 之後，路由器會進入 EXSTART 狀態，並且準備要開始尋找互連網路上的鏈路狀態資訊，並建立它們的 LSDB，如圖 19.7

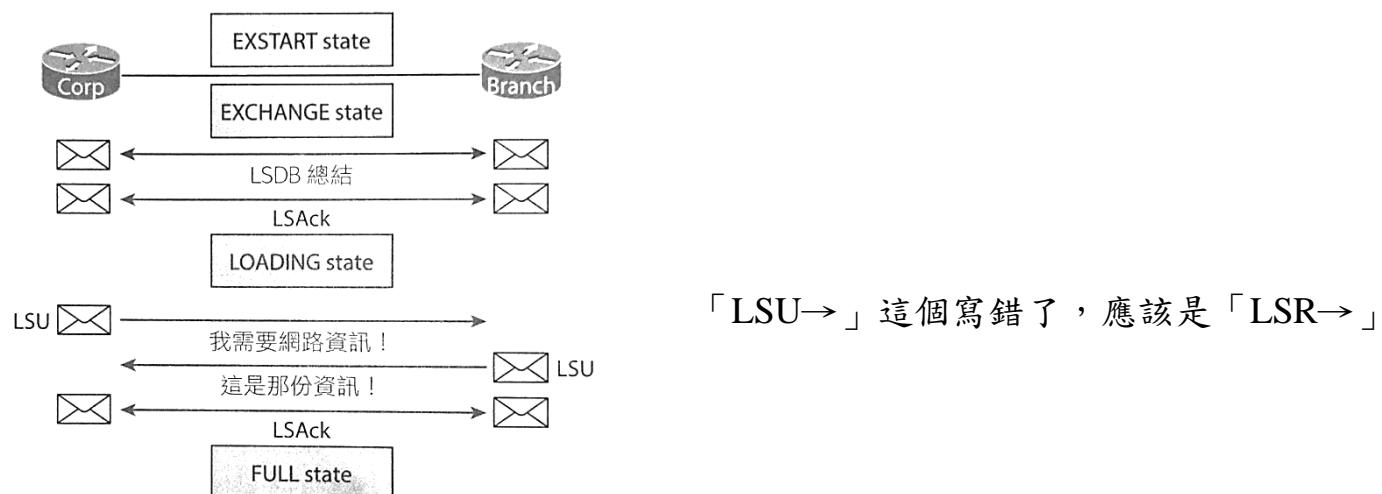


圖 19.7 OSPF 路由器鄰居狀態--第 2 部分

- **EXSTART** 表示 DR 和 BDR 已經與網路中的每台路由器建立緊鄰關係。每台路由器會與緊鄰的 DR 和 DBR 建立主從關係。具有最高 RID 的路由器會成為「主」，而主從選舉的結果會決定從哪台路由器開始進行交換。一旦路由器互相交換 DBD 封包，就會進入 EXCHANGE 狀態。

#2 部鄰居路由器無法穿越 EXSTART 狀態的一個原因是他們的 MTU 不同

#即將開始交換 DBD

- **EXCHANGE** 在這個狀態，遶送資訊會使用 DBD(或 DD，Database Description)封包和 LSR(Link-State Request) 與 LSU(Link-State Update)封包進行交換。當路由器開始傳送 LSR，就進入 LOADING 狀態。

#開始互傳 DBD

- **LOADING** LSR 封包會傳送給鄰居，用來請求在 EXCHANGE 狀態中遺漏或損壞的 LSA(Link- State Advertisement)。鄰居會回應 LSR 封包，而原路由器則使用 LSAck(Link-State Acknowledgement)封包確認。當路由器取得所有 LSR 之後，緊鄰路由器就會被視為同步，而進入 FULL 狀態。

#兩方開始處理 DBD，若收到的 DBD 與自身 LSDB 不同，則發送 LSR，等對方回覆 LSU

- **FULL** 鄰居間的所有 LSA 資訊已經同步，緊鄰關係也已經建立，路由器不應該停留在其他狀態太久。

總之，路由器最終會在 2WAY 和 FULL 狀態，而其他狀態都只是暫時的。路由器不應該長期停留在其他狀態。

▲OSPF LSDB 的組成就是靠各種 Type 的 LSA，show ip ospf database 就可以看到 LSDB 中的各種 LSA Type，利用這些 Type 可以畫出網路拓樸出來

· OSPF 無法建立鄰居的原因

- 雙方 Hello interval 或 Dead time 不一致(EIGRP 無此問題)
- 雙方 OSPF Area 不同
- IP 不在同網段
- OSPF 網路類型不一致 (OSPF 有五種網路類型，影響自動建立與 DR 選舉，CCNP 會教)
- 不正確的 OSPF network 指令
- 路由身份認證密碼不同

LSA 的五種封包

分別為 Hello, DBD, LSR, LSU, LSAck；這五種封包在 OSPF Message Type 的編號是 Hello=message type1, DBD=type2, LSR=type3, LSU=type4, LSAck=type5。

1. Hello 封包：

用於發現 OSPF 鄰居並建立鄰居關係，要使 Hello 封包有效，有三個參數 Hello interval(間隔時間)、Dead time(故障間隔時間)、Network type(網路類型)必須一致。

Interval 為 Hello 封包送出週期；dead time 用來計算建立鄰居關係後，若至歸零還未收到鄰居 Hello，則 OSPF 宣告該鄰居路由故障。

2. DBD 封包：

為 LSDB Description(LS 資料庫描述)，此封包紀錄發送端路由器的 LSDB 清單，此清單類似目錄，而接收端路由器則使用本封包與本地 LSDB 比對(僅比對清單不比對內容)，若有差異則發送 LSR 封包，要查詢 LSDB 可用 show ip ospf database 指令。

3. LSR 封包：

Link-State Request，用來請求 DBD 中任何條目的有關詳細資訊。

4. LSU 封包：

Link-State Update，用於回覆 LSR 或主動通告鄰居新資訊，一個 LSU 可能包含 11 種 LSA(Link state advertisement)。

5. LSAck 封包：

當 OSPF 路由器收到 LSU 後，會發送一個 LSAck(連接狀態確認)來做為確認接收到 LSU，類似 EIGRP 的 Ack 封包。

OSPF Authentication 路由認證



指令	說明
Router(config-if)#ip ospf authentication	在特定介面執行「明碼密碼」的 OSPF 認證，密碼為 cisco
Router(config-if)#ip ospf authentication-key <u>cisco</u>	

Router(config-if)#ip ospf authentication message-digest Router(config-if)#ip ospf message-digest-key x md5 <u>cisco</u>	在特定介面執行「md5(加密)密碼」的認證，x 為 key-id，路由器間的 key id 要一樣
R3(config)#router ospf x R3(config-router)#area 0 authentication <u>可選擇明碼或加密</u> ，以下省略	在整個 OSPF 區域執行明碼/加密密碼的認證，上面兩種的變體

OSPF 不使用 key-chain 來宣告密碼，而是直接在介面/OSPF 上宣告認證密碼。

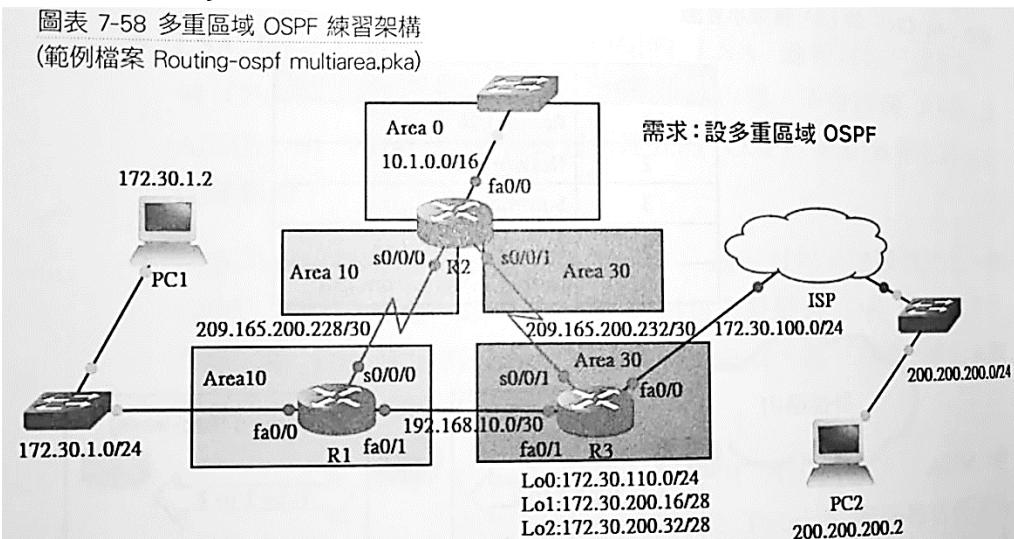
※OSPF 路由表代碼

O	同一 OSPF Area 的路由
OIA	不同 OSPF Area 的路由
OE1	Type 1 外部路由匯入到 OSPF，成本照 OSPF 規則加總
OE2	Type 2 外部路由匯入到 OSPF，成本固定



※Lab—三台路由器啟動多重區域 OSPF

圖表 7-58 多重區域 OSPF 練習架構
(範例檔案 Routing-ospf multiarea.pka)



指令	說明
R1(config)#router ospf 10 R1(config-router)#network 0.0.0.0 255.255.255.255 area 10	R1 啟動 OSPF 10 並將所有介面都啟動在 area 10
R2(config)#router ospf 20 R2(config-router)#network 10.1.0.1 0.0.0.0 area 0 R2(config-router)#network 209.165.200.230 0.0.0.0 area 10 R2(config-router)#network 209.165.200.233 0.0.0.0 area 30	R2 啟動 OSPF 20 並使用介面的方式啟動，f0/0 啟動在 area 0、s0/0/0 啟動在 area 10，s0/0/1 啟動在 area 30(R2 是 ABR)
R3(config)#router ospf 30 R3(config-router)#network 0.0.0.0 255.255.255.255 area 30	R3 啟動 OSPF 30 並將所有介面都啟動在 area 30

※Lab--外部路由匯入到 OSPF(Area30-ISP)

在 R3 設定一筆靜態路由，做為 OSPF 的外部路由，讓 R3 成為 ASBR，之後在 R3 設定將這筆靜態路由匯入(Redistribute)到 OSPF。

指令	說明
R3(config)#ip route 200.200.200.200 255.255.255.0 f0/0	R3 中設定靜態路由
R3(config-router)#redistribute static metric-type 1 p.s.匯入後會有 log “Only classful networks will be redistributed”表示只會匯入 classful 的資訊到 ospf，若要匯入到 classless 等級，要下「redistribute static metric-type 1 subnet」	將 R3 靜態路由匯入到 OSPF。 #Type 1 匯入的靜態路由會累加 OSPF 成本，若為 type 2 則不會增加 OSPF 成本(固定成本)

Show ip route 會看到有一筆路由資訊顯示為 E1，即 Type 1 的外部路由，E2 以此類推。

OSPF 路由壓縮

- 在同一 OSPF 區域中，預設路由資訊不壓縮，可能會造成路由表的路由數目越來越多，所以有需要可以手動做 OSPF 路由壓縮。(指令如下)

R2(config)#router ospf 20 R2(config-router)#area 30 range 172.30.96.0 255.255.240.0	將 area 30 的 172.30.100.0 與 172.30.110.0 兩筆路由壓縮為 172.30.96.0 並在 ABR 路由器 R2 執行壓縮指令(合併子網路的概念)
--	--

*****一些補充*****

- Adjacencies：互信(緊密)關係，一般廣播環境中，(預設)每 10 秒發一次 Hello，Time interval 40 秒(Hello time*4)
- Priority：權限等級，先比誰大再比誰活的比較久
- Passive Interface：不會傳送 Hello 訊息和宣告，只能接收，禁止該介面發言，該介面只能透過其他介面通告給他的 OSPF 鄰居。(也可以理解為 OSPF Boundary)
- Link-State Information 透過 LSA(Link-State Advertise)傳遞
- 每台 Router 透過 LSA 建立 Topology Database，而非傳送 RoutingTable
- 與 IGRP、EIGRP 不同，OSPF 使用 SPF algorithm(最短路徑優先演算法)
- Area 階層式路由協定 Area0 為 Backbone，Area1、2、3 為 Level 1(第二層)
- Designated Router(DR)在整個 multiple-access network 中，產生 LSAs 封包。
- 不同的 Area 若要互傳路由資訊的話，則必需要提供一個 Router 來做 Point-to-Point 的 BGP 連結

*****一些補充*****

OSPF Troubleshooting

※OSPF Troubleshooting 建議步驟



步驟	檢查方向	使用指令
1.	檢查 OSPF 在路由表是否完整	#show ip route
2.	檢查 OSPF 鄰居形成狀況	#show ip ospf neighbors

3.	檢查兩端網路介面啟動狀況	#show ip int brief
4.	檢查 OSPF 的介面啟動狀況	#show ip ospf interfaces
5.	檢查 OSPF 的 Area Number	#show ip ospf interfaces
6.	檢查是否有 Passive interface	#show ip ospf interfaces #show ip protocols
7.	檢查 OSPF 介面的 hello interval 是否一致	#show ip ospf interfaces
8.	檢查是否啟動 OSPF Authentication	#show ip ospf interfaces #show run
9.	檢查兩端 IP 網路位址設定	#show ip ospf interfaces
10.	若為乙太網路(多重存取)，檢查 DR 產生情況	#show ip ospf neighbors
11.	檢查 network 宣告情形	#show ip protocols
12.	檢查 OSPF 的 Process ID	#show ip protocols

OSPF Lab(參考上課時的照片)

R1 為 OSPF ABR，R1 的 f0/0 及 R2 的 f0/0、loopback 都屬於 Area1

R1 的 Loopback、f0/1 及 R3 的 loopback、f0/0 都屬於 Area0

--未完--

※R1 使用 OSPF 產生 Default Route R2/R3 自動學習到 Default Route

R1(config)#router ospf 100

#default-information original always →加 always 不管有沒有 default route 都送

※調整 Router 所有實體介面，使 OSPF Cost 都加 100(R2/R3 類推)

R1(config)#interface f0/1

#ip ospf cost 100

※設定 R2/R3，當 R1 Fail 時，R2/R3 的 loopback 一樣可互通

關鍵字：**floating static route**

R2(config)#ip route 0.0.0.0 0.0.0.0 192.168.23.3 111 →111 為 AD 值

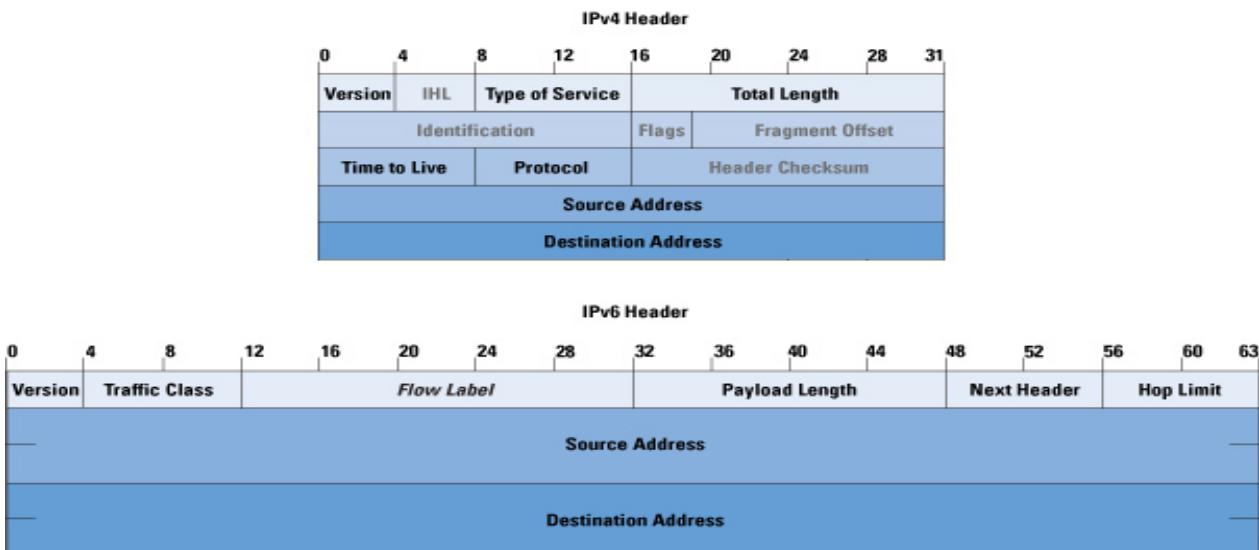
說明：使用 Static Route 方式設定一筆 Default Route，但 AD 值比原本 OSPF Default Route AD 值差的 floating static route，R3 也要設。

調整參考頻寬—用在一個環境裡有不同頻寬路由器比較用，看筆記



IPv6

IPv6 Header v.s. IPv4 Header



IPv6 Header

IPv4 的標頭長度為 20 位元組，而 IPv6 的位址是 v4 的 4 倍(128bits)，所以它的標頭長度應該是 80 位元組？不。IPv6 被設計成較少、且串流式的欄位，因此也得到較快速的被遠送協定。下圖是串流式的 IPv6 標頭中文版(同上圖)：

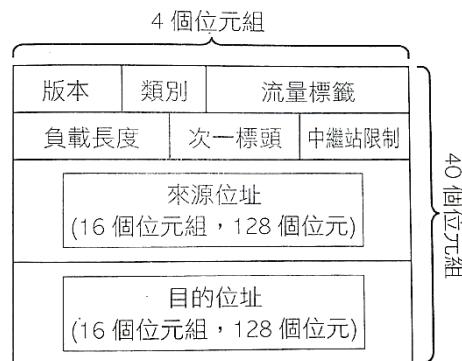


圖 14.7 IPv6 標頭

基本的 v6 標頭包含 8 個欄位，讓它只是 v4 標頭的 2 倍長(40 位元組)。

- **版本** 這個 4 位元欄位包含的是 6；v4 的則是 4。
- **交通類別** 這個 8 位元欄位等同 v4 欄位中的服務類別(ToS)，將資料流量分類，以便 QoS。
- **流量標籤 v6 才有**，這 24 位元的新欄位用來標示封包和交通流。交通流是指從單一來源流到單一目的主機、任意點位址、多點傳播位址的一系列封包。該欄位促使 v6 能有效率地進行流量分類。

- **負載長度** IPv4 是標示封包長度的全長欄位。IPv6 負載長度只包含負載本身的長度(不含表頭)。
- **次一標頭** 因為 v6 可以選擇性地延伸標頭，該欄位定義了要讀取的下一個標頭。反之，v4 要求每個封包都是靜態的標頭。沿用 IPv4 中 Protocol，表示攜帶的上一層通訊協定，另外還有可作為擴充標頭的功能；IPv6 擴充標頭無最大尺寸，因此可擴充以存放 IPv6 通訊所需的所有擴充資料。
- **中繼站限制** 指定 v6 可以穿越的最大 hop 數。

#在 CCNA 認證中，請記住中繼站限制欄位相當於 IPv4 標頭中的 TTL 欄位，而延伸標頭(在目的位址之後，圖中未顯示)則是用來取代 IPv4 的 fragmentation 欄位。

- **來源位址** 16 個位元組，封包來源。
- **目的位址** 16 個位元組，封包目的。

IPv6 v.s. IPv4 Header difference?

- 網際網路標頭長度(Internet Header Length)欄位已不再需要，故被移除。IPv6 標頭長度固定為 40 位元組，不像 v4 的標頭長度是變動的。
 - v6 的分割處理方式不同，所以不再需要 v4 基本標頭中的 flag 欄位。在 v6 中，路由器不再處理分割，改由主機負責分割工作。
 - IP 層的 Header Checksum(標頭檢查碼)欄位被移除，因為大多數 L2 技術已經執行了檢查碼和錯誤控制；這使原本是選擇性的上層檢查碼(如 UDP)成為強制性要求。
- ##CCNA 考試重點：記住 v6 標頭不像 v4 標頭，有固定長度；使用延伸標頭取代 v4 分割欄位；並移除了 v4 的檢查碼欄位。##

◎IPv6 優勢

1. IP 提供數量多
2. 效率快，simple header(沒有 checksum)
3. None broadcast
4. 內建 IPsec 安全機制
5. 取得方式多元化
6. Dual stack 雙方協定(v4 對應 v4，有 v6 才會啟用 v6)
7. Anycast(允許 IP 重覆) → DAD: Duplicate Address Detection 即 ip 衝突偵測
8. 無 Broadcast，用大量 Multicast 取代
9. 一介面可有多個 IPv6 address

補充資料

SLB(Server Load Balance)：負載平衡器，一台 SLB 底下接多台 Server 分流

CDN(Content Delivery Network)：幫別人做 SLB 的業者

IPv6 位址表示

IPv6 位址有 128bits，每 16bits 一組，每個十六進位需要 4bits，故每組有 4 個十六進位，一個 IPv6 有 32 個十六進位。格式—0000:0000....0000(八組)

◎位址簡化方式：

128bit，採用 16 進位，8 個區塊—

如 2001:0DB8:0000:0000:0001:0000:0000:abcd

--位址簡化原則：

1. 每組中的前面為零可省略，如 0DB8 可簡化 DB8
2. 0000 可簡化為 0
3. 連續的零可用兩個冒號 “::” 表示，但只能縮寫一次

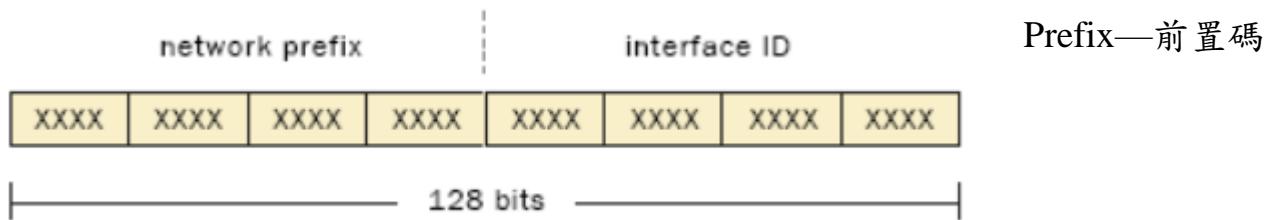
範例：

2001:0DB8:0000:0000:0001:0000:0000:ABCD

↑可縮寫為 2001:DB8:0:0:1:0:0:ABCD

↑再縮寫為 2001:DB8::1:0:0:ABCD 或 2001:DB8:0:0:1::ABCD

◎位址結構



IPv4 的 32 位元中分兩部份，Network ID & Host ID。

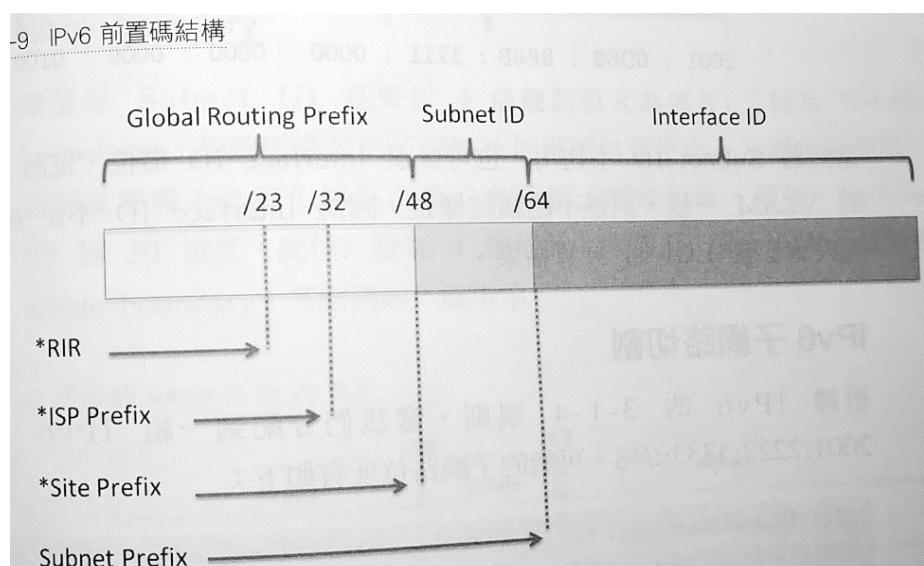
IPv6 的 128 位元也分兩部份，prefix & interface ID。

相比 IPv4 用遮罩的方式表達 IP，IPv6 用 Prefix 來表示

2001::1/96 表示網路位元 96、主機位元 32，網路部份 2001:0:0:0:0、主機部份 0:1

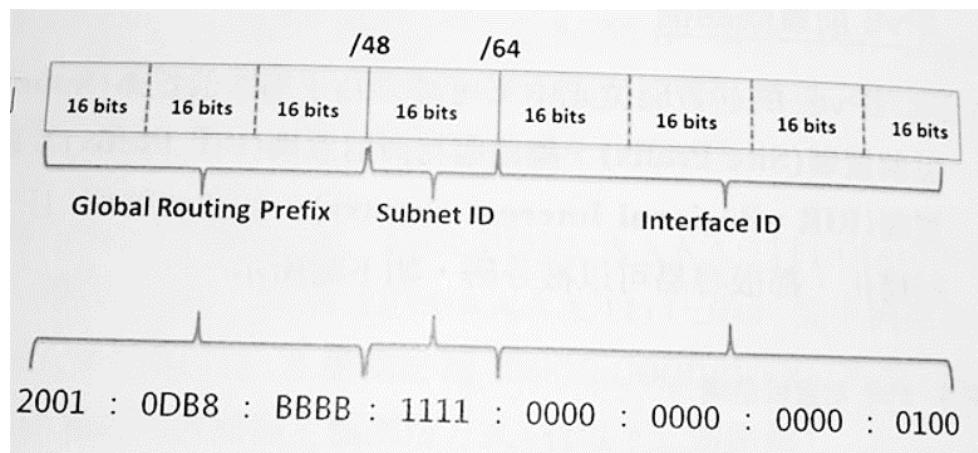
2001::1/80 表示網路位元 80、主機位元 48，網路部份 2001:0:0:0:0、主機部份 0:0:1

◎IPv6 前置碼結構



IPv6 前置碼位元中又可細分為子網路前置碼(Subnet Prefix)、站點前置碼(Site Prefix)、網路服務商前置碼(ISP Prefix)及區域網路前置碼(RIR, Regional Internet registry)。

IPv6 一樣由 IANA 管理，IANA 以/23(?)分配給其下五大 RIR，每個 RIR 中心再以/32 分配給該區域中的 ISP 使用，ISP 再以/48~/64 配給出去。



前置碼/48 稱為 Global Routing Prefix，主要是給 ISP 間主幹網路 Routing 使用，接著前置碼/48~64 部份則留給 ISP 或公司進行子網路切割(概念同 IPv4，無分級)；總結來說，IPv6 結構

規劃上有 3 組-1 組-4 組的規則，3 組為 Global Routing Prefix，1 組為 Subnet ID，4 組為 Interface ID。

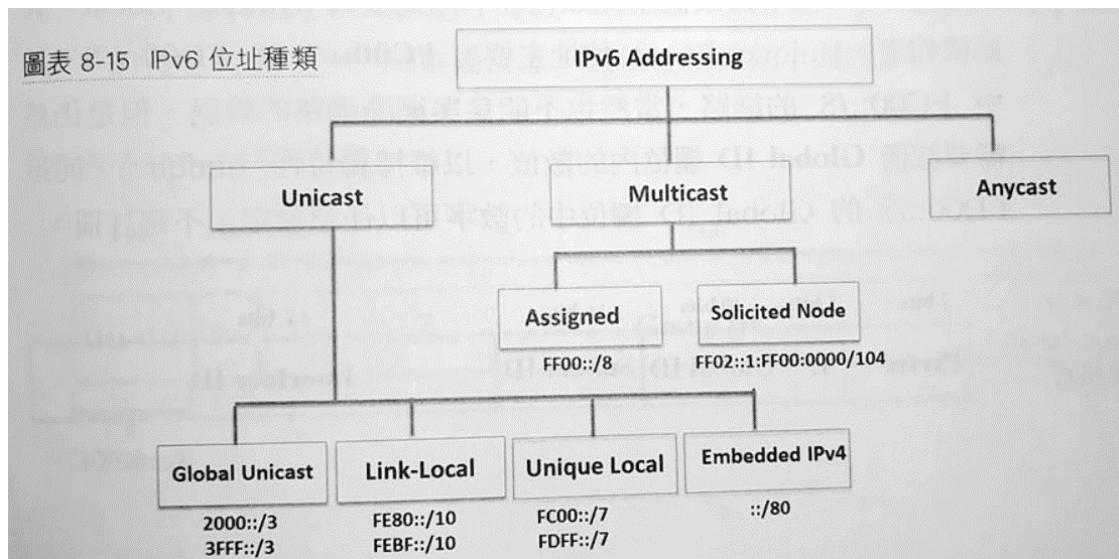
◎IPv6 子網路切割

--Nibble boundary：在 IPv6 中建議切割子網路以 4 倍數的位元為邊界(即 Nibble boundary)，如此產生的子網路位址就可以直接由十六進位來推算。好處在於可以在表示子網路時使用「2001:2222:3333:SSSS:S000::/68(假設原始為/48)」，其中 S 表示子網路。

--不是 Nibble boundary：轉成 2 進位再轉回 16 進位換算，一個 bits 有 4 個 2 進位。

IPv6 Address Type

- 主要三大類分為 Unicast, Multicast, Anycast(任播位址)，如下圖。

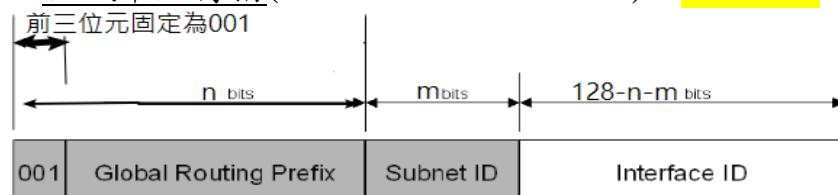


IPv4 有單播、群播、廣播；IPv6 有單播、群播、任意點傳播，並取消無效率的廣播。

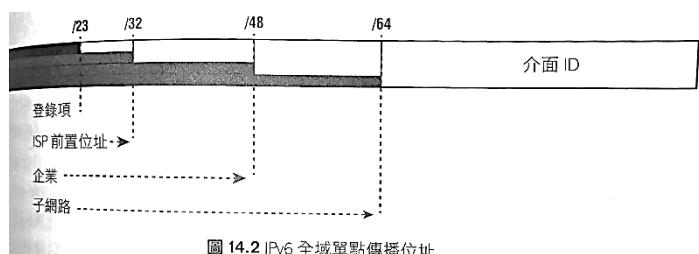
Unicast(單點傳播)

分為上圖四種。使用單點傳播位址的封包會遞送到單一介面。為了負載平衡，多個介面可使用相同位址。

全域單點傳播(Global unicast address)：2000::/3 ~ 3FFF::/3



前三位元為 001，第四位元 0/1，故 Global Unicast 位址通常以 2 或 3 開頭，並在全世界具有唯一性，可被 Internet 繞送 (Routable)，功能同 IPv4 公有 IP。



這是典型可公開遞送的位址，與 IPv4 相同。圖為單點傳播位址的分割圖。ISP 可以提供最小/48 的網路 ID；該網路 ID 又提供 16 位元來建立唯一的 64 位元路由器介面位址。最後 64 位元是唯一性主機 ID。

圖 14.2 IPv6 全域單點傳播位址

鏈路本地位址(Link-Local address/Unicast Private) : FE80::/10 ~FEBF::/10

Link Local 位址定義前 10 位元固定為「1111111010」，故換算成 16 進位，開頭的位址為 FE8~FEB，其 IP 範圍為 FE80::/10~FEBF::/10。此類 IP 僅供特定實體網段上的本地通信使用，常用在如 DHCP、相鄰設備發現和路由器發現等，故 Link-Local 不能被繞送，只能存在於一個 link 上或網路中，通常會伴隨 Global Unicast 位址設定而產生。

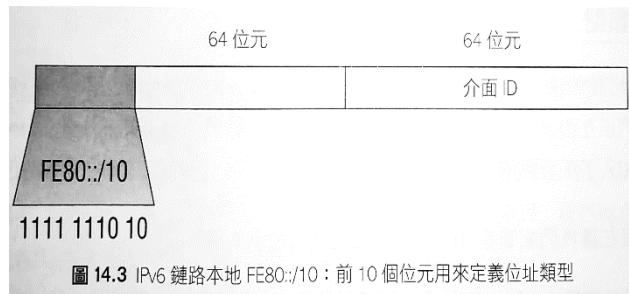


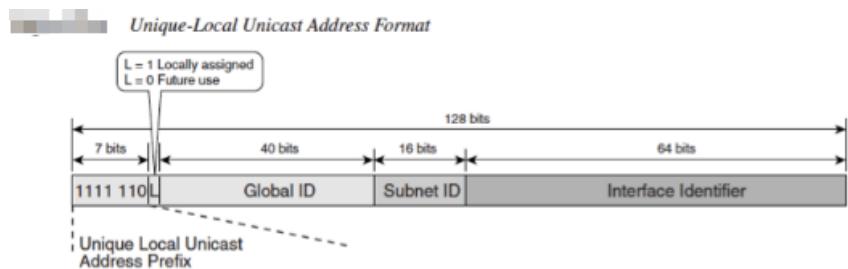
圖 14.3 IPv6 鏈路本地 FE80::/10：前 10 個位元用來定義位址類型

它就像微軟的自動私有 IP 位址(Automatic Private IP Address, APIPA)，用來自動提供不打算被遶送的 IPv4 位址。在 IPv6 中，它們以 FE80::/10 開頭，如圖。這些位址就像個方便的工具，讓您能為某場會議臨時建立 LAN，或是建立沒有要被遶送，但仍需本地共享和存取檔案及服務的小型 LAN。

唯一的本地位址(Unique Local address) : FC00::/7~FDFF::/7

這些位址也是為了非遶送目的，但它們幾乎是全域唯一的，所以您可能不會讓它們重疊。

Unique Local 的設計是要用來取代 site-local address(已廢除)，用途和 IPv4 私有 IP 相同。



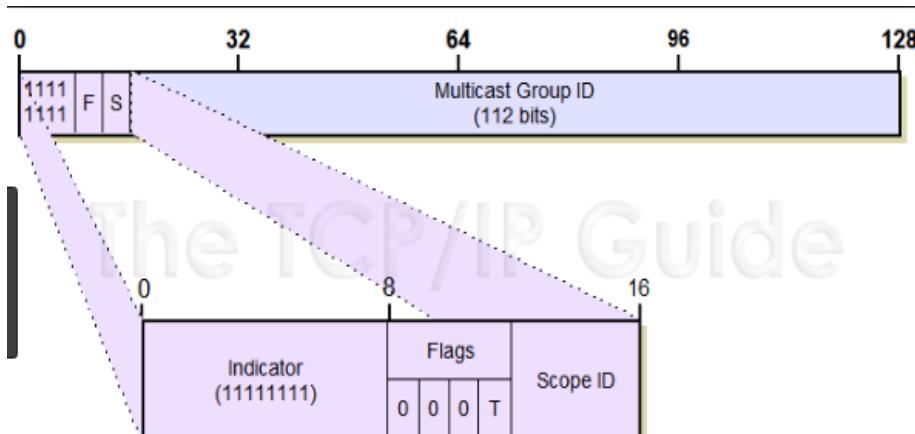
Unique Local 位址主要有 FC00::/8 與 FD00::/8，差別在 FC 需要註冊 Global ID 以維持獨特性，而 FD 的 Global ID 可任意設定，不需註冊。

由 RFC4193 定義，考試考過。

多點傳播(Multicast) : sho::/8

用多點傳播位址的封包會送到指定的所有介面。也稱為一對多位址。在 IPv6 中多點傳播位址一定是 FF 開頭。

在 IPv6 中整合了 IPv4 的群播/廣播，前 8 位元固定為 11111111(即 FF 開頭)，最後的 112 位元為群組位址，格式如下：



Flag 欄位為 0 表示該群播位址是 Well-known IP，即由 IANA 分配的。Flag 欄位為 1 表示該群播位址是動態產生的。

Scope 欄位表示該群播位址範圍。

Scope=1 Interface-Local scope

Scope=2 Link-Local scope

Scope=5 Site-Local scope

Scope=8 Organization-Local scope

另外還有一類群播位址為 Solicited Node Multicast，此類群播位址會從邀請節點的電腦 IPv6 位址計算出來，主要用於 Neighbor Discovery，取代廣播功能。

任意點傳播(Anycast)

就像多點傳播位址，任意點傳播位址也會辨識多個介面，但它只會遞送給第一個位址—更精確的說，它只送往根據遼送距離所定義的第一個位址。該位址可在多介面上應用單一位址。也稱 one to one of many。任播位址通常設在路由器上，而非在主機上，且來源位址不是任播位址。IETF 保留了每個/64 中的前 128 位址，用作任意點傳播。

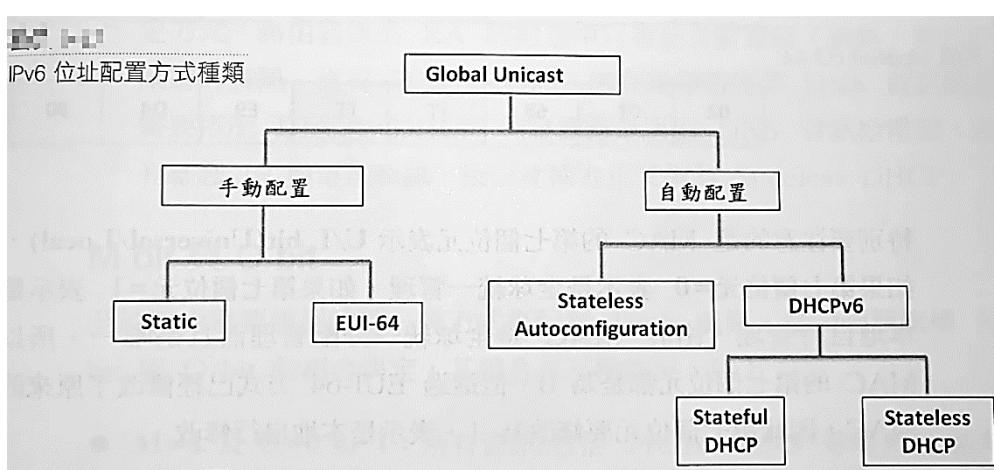
首碼長度不固定，除首碼外的位元都是 0，一個任播位址可被多個網路介面使用，但傳給此位址的封包並非真的將封包送到這些網路介面，而是送給距離最近的網路介面。

IPv6 特殊位址



位址	意義
::	相當於 0:0:0:0:0:0:0:0，等同於 IPv4 的 0.0.0.0，Unspecified。
::1	相當於 0:0:0:0:0:0:0:1，等同於 IPv4 的 127.0.0.1，Loopback。
0:0:0:0:0:192.168.100.1	這是在 IPv6/IPv4 混合的網路環境下，IPv4 位址的寫法
2000::/3	Global Unicast Address
FC00::/7	Unique Local Address
FE80::/10	Link Local Address
FF00::/8	Multicast Address
3FFF:FFFF::/32	保留供範例和文件記錄用
2001:0DB8::/32	
2002::/16	在 IPv4 過渡到 IPv6 的系統中，用來當作 6 轉 4 的通道—它的結構可以讓 IPv6 封包在 IPv4 的網路上傳送，而不需設定額外的通道。

IPv6 配置方式



手動配置

若網路介面同時支援(啟用)v4, v6 雙協定稱作 Dual Stack

Router(config)#ipv6 unicast-routing

在 Router 上啟用 IPv6-routing

#IPv6 交通轉送預設值為關閉

<p>Router(config-if)#ipv6 address <ipv6prefix>/<prefix-length></p> <p>#寫法可以是完整的 128 全域 IPv6 位址，例如： #ipv6 address 2001:db8:3c4d:1:0260:d6FF:FE73:1987/64)</p> <p>也可以使用 EUI-64(extended unique identifier)的方法。Eui-64 可以允許裝置使用 MAC，並加上填補字元來建立介面 ID，例如： #ipv6 address 2001:db8:3c4d:1::/64 eui-64</p>	設定介面的 IPv6 Address
<p>Router(config-if)#ipv6 enable</p>	讓介面可應用 Link-Local address，但只能在本地子網路 上通訊

手動配置-EUI-64—手動指定前置碼(網路)部份，介面 ID 部份會從網路介面的 MAC 位址提取，此部份稱為 EUI64 介面 ID，但 MAC 只有 48 位元，而介面 ID 有 64 位元。這中間差的 16 位元，是因為 EUI64 將 MAC 中間插入 FFFE 的 16 位元變成。

靜態配置範例：MAC 為 00:03:6B:E9:D4:80，使用 EUI64 介面 ID 為 00:03:6B:FF:FE:E9:D4:80

p.s. MAC 的第七位元為 U/L bit(Universal/Local)，如果第 7 位元=0 表示為全球統一管理，第 7 位元=1 表示為本地自行管理，又 MAC 是全球統一分配及管理，故 MAC 原始第 7 位元皆為 0，但 EUI64 修改了原來的 MAC 故 0 改 1。

◎查詢 IPv6 設定結果

```
#show ipv6 interface brief
FastEthernet0/0 [up/up]
FE80::230:F2FF:FE86:6501
2001:1:1:1::1
```

←每個網路介面會有兩個 IPv6 位址，一個是手動設定，另個是網路介面自動產生的 Link-Local 位址(FE80 開頭那個)由 EUI-64 方式產生。

◎查詢 IPv6 設定結果(說明)

```
R1#sh ipv6 int f0/0
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::230:F2FF:FE86:6501
  No Virtual link-local address(es):
    Global unicast address(es):
      2001:1:1:1::1, subnet is 2001:1:1:1::/64 ②
    Joined group address(es):
      FF02::1
      FF02::2
      FF02::1:FF00:1
      FF02::1:FF86:6501 ③
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

1. Link-Local 位址，只有一組
2. Global Unicast 位址，可設定多組，且可以在不同網段。

3. Joined group address，此部份是 R1 有加入的群播 IPv6 的位址，FF02::1 為 Well-known 的群播位址，表示 Link 上或一個網路中所有節點。另外兩筆為 Solicited Multicast(邀請群播位址)，此部份由 f0/0 的 Global Unicast 及 Link-Local 位址計算出來。

動態配置

- 無狀態式自動組態設定(Stateless/Auto config/EUI-64)：

自動組態設定非常好用，因為它讓網路上的裝置可以使用 Link-local 單點傳播位址來幫自己定址，並且隨插即用。

這個流程首先會先從路由器找到 prefix 資訊，然後把裝置自己的介面位址當作介面 ID 附加在後面。(用裝置的實體 MAC 作介面 ID)。但是因為 IPv6 的介面 ID 長度為 64bits，而 MAC 只有 48bits，所以 MAC 的中間會使用 FFFE 來補足額外的位元。

假如原 MAC 為 0060.D673.1987→
0260.D6FF.FE73.1987

- 開頭的 02?

在填補的過程中，會改變 1 個位元來指定這個位址是 Unique-Local/Global unique。被改變的是位址中的第 7 個位元。

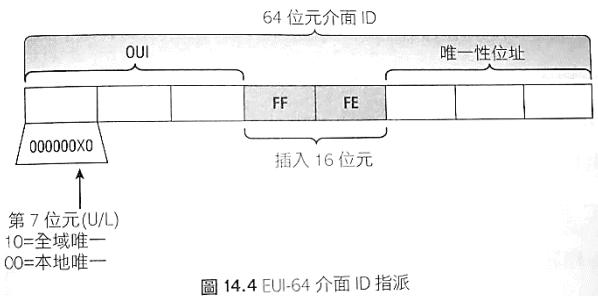


圖 14.4 EUI-64 介面 ID 指派

在介面上使用人工指派位址時，修改 U/L 位元讓使用者可以只指定 2001:DB8:1:9::1/64，而不是更長的 2001:DB8:1:9:0200::1/64。此外，如果要手動指定 Link-Local 時，也可以使用短位址 fe80::1，而不需要長的 fe80::0200:0:0:1，或是 fe80:0:0:0:0200::1。即使乍看之下，IETF 的這項設計好像讓 IPv6 標準定址更難懂，但事實上，它讓定址變得比較簡單。此外，因為大多數人通常不會去覆蓋內建的位址；U/L 位元為 0，表示大多數情況下，您會看到它被反向設定為 1。但是為了 Cisco 認證目標，您必須雙向都瞭解。

以下範例：

1.

MAC 位址：0090:2716:fd0f

IPv6 EUI-64 位址：2001:0db8:0:1:0290:27ff:fe16:fd0f

2.

MAC 位址：aa12:bcbc:1234

IPv6 EUI-64 位址：2001:0db8:0:1:a812:bcff:febcbcbc:1234

10101010 代表 MAC 位址的前 8 個位元(aa)，當第 7 位元反向時，就變成 10101000(A8)

3.

MAC 位址：0c0c:dede:1234

IPv6 EUI-64 位址：2001:0db8:0:1:0e0c:deff:fede:1234

0c 代表 MAC 位址的前 8 個位元 00001100，當第 7 位元反向時，就變成 00001110(0e)

4.

MAC 位址 : 0b34:ba12:1234

IPv6 EU1-64 位址 : 2001:0db8:0:1:0934:baff:fe12:1234

0b 代表 MAC 位址的前 8 個位元 00001011，反向時就變成 00001001(09)

· 執行自動組態設定，主機會經歷的 2 步驟流程：

1. 首先，主機需要前置位址資訊(類似 IPv4 位址的 Network ID)來設定它的介面，所以它會先傳送路由器召喚(**RS, router solicitation**)的請求。RS 的傳輸是以多點傳播的方式傳送給每台路由器的多點傳播位址。真正送出的資訊是某種 ICMP 訊息，並且這個 ICMP 訊息也有一個識別用的編號—這個 RS 訊息是 **TYPE 133** 的 ICMP。
2. 路由器會透過路由宣傳(**RA, router advertisement**)送回所請求的前置位址資訊。RA 訊息也是個多點傳播封包，會送往每個節點的多點傳播位址，並且是 **TYPE 134** 的 ICMP。RA 訊息會定期傳送出去，但是主機會送出 RS 以要求立即的回應，故而不用一直等待收到下一次的定期 RA 才能取得所需的資訊。

※另外 **EUI-64** 也稱為 **Stateless configuration**。因為它不用接觸或連線，並且可從其他裝置接收更多的資訊。在下面的 DHCPv6 中則是 **Stateful configuration**。

· 設定該介面聆聽 RA，並且透過 EUI-64 為自己指派位址

```
Router(config-if)#ipv6 address autoconfig default
```

→default 選項是用來遞送從其他路由器接收到的預設路徑，自動加入到路由器並設為預設路徑

查詢 ipv6 介面 ID

```
#show ipv6 int brief
```

，EUI-64 會看到介面 ID 中間會有 FF:FE。

· DHCPv6(Stateful)

運作方式類似 DHCPv4，差別在有支援 v6 定址架構。另外 DHCP 提供了一些自動組態無法提供的選擇。

使用 IPv4 開機時，客戶端會送出 DHCP 發現訊息來尋找伺服器，要求伺服器提供客戶端所需的資訊。但在 IPv6 中，RS 和 RA 流程會先產生。如果網路上有 DHCPv6 伺服器，則客戶端收到的 RA 會告訴它是否有 DHCP 可用，如果沒有找到路由器，客戶端會送出 DHCP 召喚訊息(DHCP solicit message)來回應—召喚訊息其實就是多點傳播訊息，並且其目的位址為 ff02::1:2，代表所有的 DHCP 代理人，包括伺服器和中繼器(relay)。

思科 IOS 對 DHCPv6 提供一些支援，但僅限於 Stateless DHCP Server，表示它並不提供 pool 的位址管理，且設定 pool 的可用選項也侷限在 DNS、網域名稱、預設閘道、以及 ISP 伺服器而已。(這意味著還需要一些其他伺服器來供應與分配其他需要的資訊，甚至於管理位址的配置)。

由 DHCP Server 配置 IPv6 位址連同 DNS 資訊給電腦使用，且 DHCP 伺服器有紀錄分出去的 IPv6 位址及電腦主機資訊，故此稱為 **Stateful DHCP**(有狀態 DHCP 的配置)。

```
#在 CCNA 考試中，無狀態和有狀態的自動組態設定都可以動態指定 IPv6 位址。
```

· 混合配置

將前兩種混合使用，首先由自動設定方式，路由器回應的 RA 封包中只包含前置碼及預設閘道資訊，無 DNS 資訊，故又搭配 DHCP 伺服器來獲得 DNS(DHCP 就只負責該功能，不維護 IP 與電腦資訊)，故稱 **Stateless DHCP**。

M bit 與 O bit

路由器使用哪種方式來配置 IPv6 組態，是由兩個 flag--M/O bit 的組合決定，有三種組合情況：

M=1, O=0 or 1：所有資訊(含 Prefix, DNS 等)都是由 DHCPv6 Server 配給電腦，並且伺服器中記錄分配出去的資訊與配置的電腦，即 Stateful DHCPv6。

M=0, O=1：使用路由器網路介面中的前置碼與預設閘道分配給電腦，但 DNS 等資訊由 DHCPv6 取得，即混合配置。

M=0, O=0：電腦將只得到路由器的前置碼及預設閘道，無法取得 DNS 等，即 Auto config。

IPv6 過渡期

在 IPv4 過渡到 IPv6 的過程中，暫時需一些過渡機制，目前主要有三種，**Dual Stack(雙重堆疊)**、**Tunnel(通道)**、**NAT-PT(通訊協定轉換)**。

◎IPv6 位址取得方式總結

- | | |
|--|----------------------------------|
| 1. Manual | 手動設定 |
| 2. Manual Prefix+EUI64 | 手動設定 Prefix+自動產生 Interface ID |
| 3. Stateless Auto Configuration(SLAAC) | 由路由器派發 Prefix+自動產生的 Interface ID |
| 4. Stateful | DHCPv6 派發所有 IPv6 參數 |
-



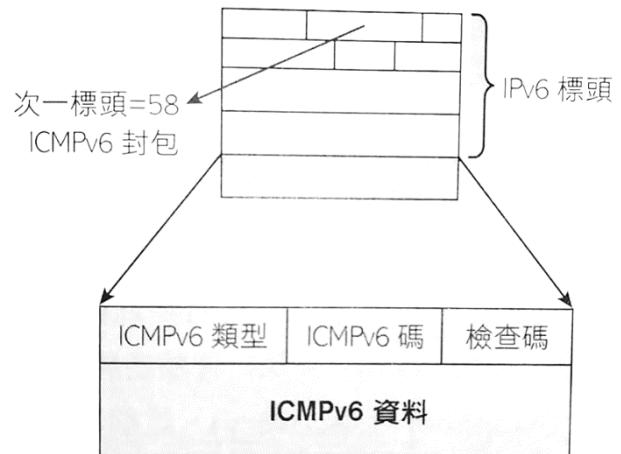
ICMPv6

IPv4 使用 ICMP 來做很多事，例如像無法抵達目的地的錯誤訊息，以及像 Ping 和 Traceroute 等故障檢測功能等。ICMPv6 還是會做這些事，但是跟 ICMPv4 不同的是。ICMPv6 並不是實作為單獨的第 4 層協定，它是 IPv6 的一部分，它是跟在基本 IPv6 標頭資訊後面的延伸標頭，ICMPv6 還新增另一項很酷的功能 - 它可以透過稱為「發現路徑 MTU」(path MTU discovery)的 ICMPv6 程序，讓 IPv6 不用分割封包(Fragmentation)- 圖是 ICMPv6 如何演化為 IPv6 封包的一部分。

ICMPv6 封包的辨識是透過次一標頭欄位值 58。類型欄位用來辨識傳送的 ICMP 訊息類別，而 ICMPv6 碼欄位則進一步指定訊息的細節。資料欄位中包含的是 ICMPv6 的負載。

下表為 ICMP 類型編號

ICMPv6 類型	說明
1	目的地無法抵達
128	回聲請求
129	回聲回應
133	路由器召喚，RS
134	路由器宣傳，RA
135	鄰居召喚，NS
136	鄰居宣傳，NA



它的運作方式如下：連線的來源節點傳送長度相當於本地鏈路 MTU 的封包。當封包穿越路徑前往目的地時，任何 MTU 小於目前封包長度的鏈路會迫使居間的路由器傳送“封包過長”的訊息給來源機器。這個訊息會告訴來源節點關於那條受限鏈路的 MTU，並且要求來源機器傳送可以通過的較小封包，這個過程會持續到終於抵達目的地為止，而來源節點則根據其結果來調整路徑的 MTU。因此，當傳送其餘的資料封包時，它們就不再需要分割。

ICMPv6 也用於路由器召喚和宣傳，鄰居召喚和宣傳(亦即找出 IPv6 鄰居的 MAC 資料位址)，以及將主機重新導向到最佳路由器(預設閘道)。

· 發現鄰居協定(NDP)

ICMPv6 現在承擔了尋找本地鏈路上其他裝置位址的任務。IPv4 使用 ARP(Address Resolution Protocol)來執行這項功能，但在 ICMPv6 中則重新命名為「發現鄰居」(Neighbor Discovery)。這個流程是使用稱為被召喚節點(solicited node)位址的多點傳播位址，而所有主機在連到網路時就會加入這個多點傳播群組。

NDP 提供下列功能：

- 找出鄰居的 MAC 位址
- 路由器召喚(Router Solicitation , RS)**FF02::2**，類型編號 133 **-eui64**
- 路由器宣傳(Router Advertisement , RA)**FF02::1**，類型編號 134 **-eui64**
- 鄰居召喚(Neighbor Solicitation , NS)，類型編號 135
- 鄰居宣傳(Neighbor Advertisement , NA)，類型編號 136
- 重覆位址偵測(Duplicate address detection, DAD)

IPv6 的最右邊 24 位元會加到多點傳播位址 FF02:0:0:0:1:FF/104 前置位址的結尾，並且稱為召喚節點位址(solicited node address)，當有裝置查詢這個位址時，對應的主機會收回它的第 2 層位址，裝置可以用類似的方式找到並記錄網路上其他的鄰居裝置，在稍早提到 RA 和 RS 訊息時，曾經說過它們使用多點傳播交通來請求和傳送位址資訊，這也是 ICMPv6 的功能之一——更具體來說，這就是發現鄰居。

在 IPv4 中，主機裝置使用 IGMP 協定告知本地路由它加入了多點傳播群組，想要接收該群組的交通。這項 IGMP 功能已經被 ICMPv6 取代，而且也被重新命名為「發現多點傳播聆聽者」(multicast listener discovery)。

IPv4 的主機只能設定 1 個預設閘道，如果該台路由器當機，解決之道只有修復路由器，改變預設閘道，或是使用其他協定來運行某種形態的虛擬閘道。在下圖中展示了 IPv6 裝置如何使用發現鄰居協定來找到預設的閘道。

#網路群組管理協定(Internet Group Management Protocol 或簡寫 **IGMP**)是用於管理網路協定多播組成員的一種通訊協定。IP 主機和相鄰的路由器利用 **IGMP** 來建立多播組的組成員。

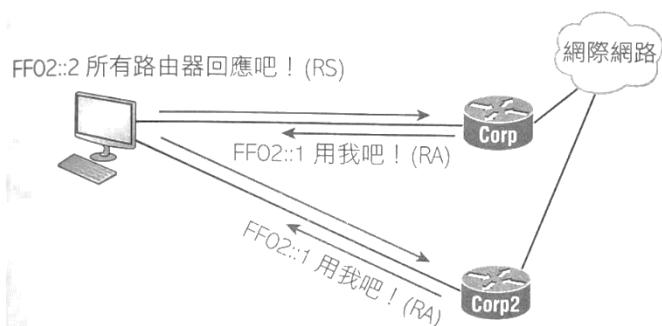
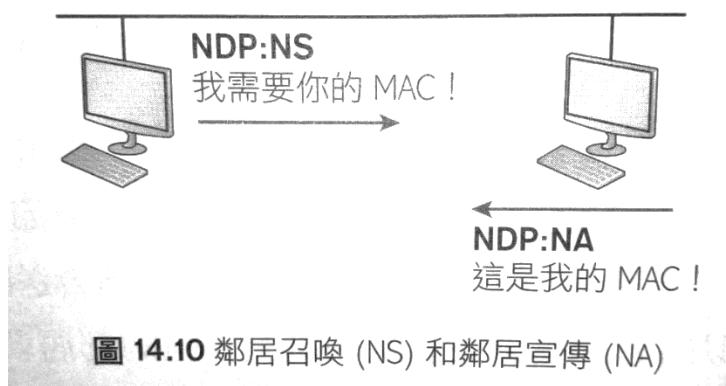


圖 14.9 路由器召喚(RS)和路由器宣傳(RA)

IPv6 主機會在鏈路上使用多點傳播位址
FF02::2 送出路由器召喚(RS)要求所有路由器回應。相同鏈路上的路由器則會使用單點傳播或 FF02::1 的路由器宣傳(RA)來回應。

此外，主機也可以使用鄰居召喚(NS)和鄰居宣傳(NA)在彼此之間傳送召喚和宣傳，如圖。



!!!!!

記住

RA 和 **RS** 是收集或提供路由器資訊

NS 和 **NA** 是收集或提供主機的資訊

「鄰居」就是相同資料鏈路或 VLAN 上的主機

!!!!!

乙太網路上的召喚節點和多點傳播的對應

如果已經知道 IPv6 位址，就能知道對應的 IPv6 召喚節點之多點傳播位址；而如果知道 IPv6 的多點傳播位址，也就能知道對應的乙太網路 MAC 位址。

例如 IPv6 位址 2001:DB8:2002:F:2C0:10FF:FF18:FC0F 就會有已知的召喚節點位址 FF02 :: 1:FF18:FC0F。

現在可以在 IPv6 多點傳播位址加上 32 位元 33:33 構成多點傳播的乙太網路位址。

例如假設 IPv6 召喚節點的多點傳播位址是 FF02::1:FF:18:FC:0F，則對應的乙太網路 MAC 位址就是 33:33:FF:18:FC:0F—這是個虛擬位址。

重複位址偵測(DAD，Duplicate Address Detection)

您可能會好奇，如果這 2 台主機隨機幫自己指定了相同的 IPv6 位址要怎麼辦？這就像是要每天中樂透彩，而且還連中一年的機率一樣。不過，為了確保它不會發生，所以有重複位址偵測(DAD)的機制：它不是真正的協定，而是 NS/NA 訊息的一個功能。下圖展示了一台主機在建立 IPv6 位址時，傳送 NDP NS 的過程：

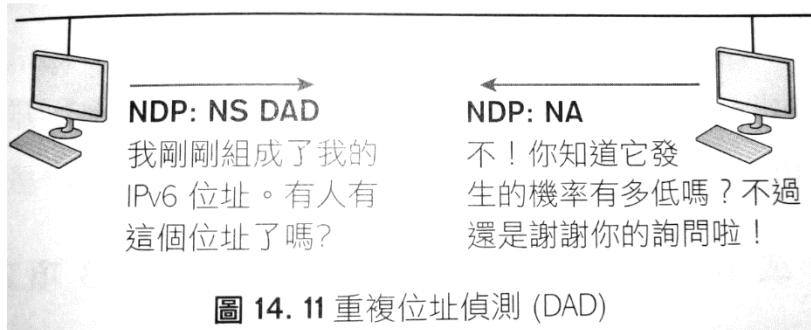


圖 14.11 重複位址偵測 (DAD)

當主機組成或接收 IPv6 位址時，它們會透過 NDP NS 傳送 3 個 DAD 出去，詢問是否有人擁有相同的位址。即使發生的機率很低，它們還是一定會進行這個詢問。



IPv6 遠送協定

在 IPv6 中仍然使用的遠送協定都有新的名稱跟改版，雖然本章的重點是 Cisco 認證目標，只涵蓋了靜態遠送和預設路徑，但筆者仍希望稍稍討論其中比較重要的一些協定。

首先是 RIPng(next generation)。已經從事 IT 產業一陣的人都知道 RIP 在較小的網路上運作得很好，這也是它仍然存在於 IPv6 的原因，另外我們也還有 EIGRPv6，因為它已經有協定相依模組，而我們要做的就是為 IPv6 協定新增一個模組，另外是 OSPFv3(IPv4 OSPF 其實是 v2)。

IPv6 的靜態遠送

靜態遠送通常是個令人不愉快的主題，因為它很笨拙、困難，而且容易出錯，但即使是 IPv6 的長位址，我們仍舊可以達成這項任務的。

要讓靜態遠送運作需要：

- 精確，而且最新的完整互連網路圖
- 每個鄰居連線的下一中繼站位址和離開介面
- 所有遠端子網路 ID

當然，動態遠送不需要這些，所以我們大多會使用動態遠送，讓遠送協定負責找出所有遠端的子網路，並且自動將它們放入路徑表中。

下圖是在 IPv6 中使用靜態遠送的絕佳範例，它並沒有那麼困難。但是就像在 IPv4 一樣，您必須要有精準的網路圖才能讓靜態遠送成功！

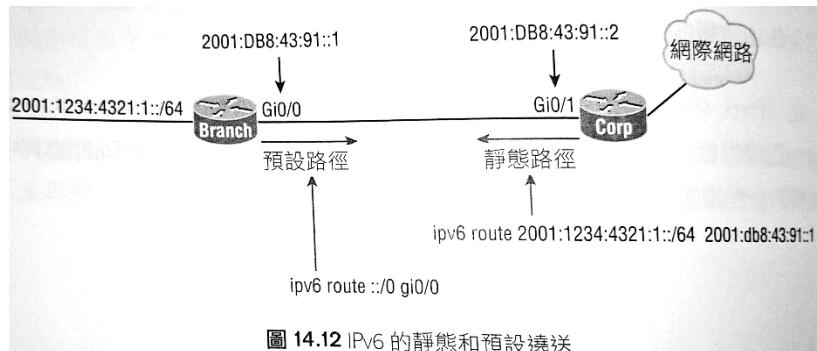


圖 14.12 IPv6 的靜態和預設遠送

首先在 Corp 路由器使用下一中繼站位址，建立通往遠端網路 2001:1234:4321:1::/64 的靜態路徑。我們也可以簡單使用 Corp 路由器的離開介面，接著使用 ::/0 設定 Branch 路由器的預設路徑，以及 Branch 的離開介面 G0/0。

IPv6 Static Route

Router(config)#ipv6 unicast-routing	在 Router 上啟用 IPv6-routing
Router(config-if)#ipv6 address 2001:db8:3c4d:11::/64 eui-64	使用 MAC+eui-64 建立 ipv6 位址
Router(config)#ipv6 route <u>x::x/xx</u> <u>nexthop/out-interface</u>	設定靜態路由
Router(config)#ipv6 route ::/0 <u>nexthop/outint</u>	設定預設路由
Router(config-if)#ipv6 address autoconfig default	設定介面上 stateless 自動組態，而 default 指令則會將本地鏈路當作預設路徑來宣傳

Router #show ipv6 route	查詢 ipv6 路由表
Router #show ipv6 route static	查詢 ipv6 靜態路由表

IPv6 Dynamic Route

支援 IPv6 的路由協定有 RIPng, OSPFv3, EIGRPv6，以下僅列指令以後有需要再詳細補充。

- **RIPng**：使用 **multicast FF02::9**

指令	說明
Router(config)#ipv6 unicast-routing	啟動 IPv6 路由協定
Router(config)#ipv6 router rip <u>p100</u>	啟動 RIPng 程序號碼 p100
Router(config)#int fx/x	在該介面啟動 RIPng 程序號碼 p100
Router(config-if)#ipv6 rip <u>p100</u> enable	

p.s. 相對應的路由器 RIPng 程序號碼不用一樣

int 下的 ipv6 rip xx enable 取代 IPv4 的 network 宣告

- **OSPFv3 & EIGRPv6**

和 IPv4 一樣要比 AD 值大小、如果本來就有 ipv4 位址可以不用設 rid

--OSPFv3

指令	說明
Router(config)#ipv6 unicast-routing	啟動 IPv6 路由協定
Router(config)#ipv6 router ospf 100	啟動 OSPFv3 程序號碼 100
Router(config-rtr)#router-id 1.1.1.1	一定要手動設定 Router-ID
Router(config)#int fx/x	使該介面在 area0 啟動 ospf 100
Router(config-if)#ipv6 ospf 100 area 0	

p.s. OSPFv3 的 router-id 因為仍使用 v4 格式故一定要手動設定

if 下的 ipv6 ospf 100 area 0 取代 v4 中的 network 宣告

OSPFv3 多點傳播位址：

- OSPF 路由器使用 FF02::5
- OSPF DR 使用 FF02::6

--EIGRPv6

指令	說明
Router(config)#ipv6 unicast-routing	啟動 IPv6 路由協定
Router(config)#ipv6 router eigrp <u>10</u>	啟動 eigrp + ASN
Router(config-rtr)#no shutdown	啟用 eigrpv6 遠送協定，IOS 15.X 版 可不用，重點是可以 shutdown(v4 不行)
Router(config-rtr)#router-id <u>1.1.1.1</u>	一定要手動設定 Router-ID

Router(config-if)#ipv6 eigrp 10	介面使用 eigrp 10 因為是在介面啟用 eigrp，所以用不到 passive-interface 指令
--	--

p.s. EIGRPv6 的 router-id 因為仍使用 v4 格式故一定要手動設定，並且 router-id 可以隨便設，，
OSPFv3 則不可以相同。

p.s. if 下的 ipv6 eigrp 10 取代 v4 中的 network 宣告

p.s2.EIGRPv6 有一種特輸語法叫 Named EIGRP，使用 AF(Address Family)可在同一啟動模式下
直接撰寫 v4,v6 指令，可同時啟動 v4,v6 的 EIGRP，不需一直切換，此為 CCNP 內容。

◎查詢路由協定狀態

#show ipv6 protocols

◎查詢/清除 NDP Cache on PC

Cmd>netsh int ipv6 show neigh

Cmd>netsh int ipv6 delete neighbors

◎查詢 NDP Cache on Router

#show ipv6 neighbors

IPv6 Auto-Config

· 在電腦端到路由器要使用 Auto-Config，Router 要注意兩件事：

1. 在介面上用 **ipv6 enable** 啟用 ipv6 功能。
2. 路由器要啟用 IPv6 遴送功能 **ipv6 unicast-routing**

◎Stateless DHCP

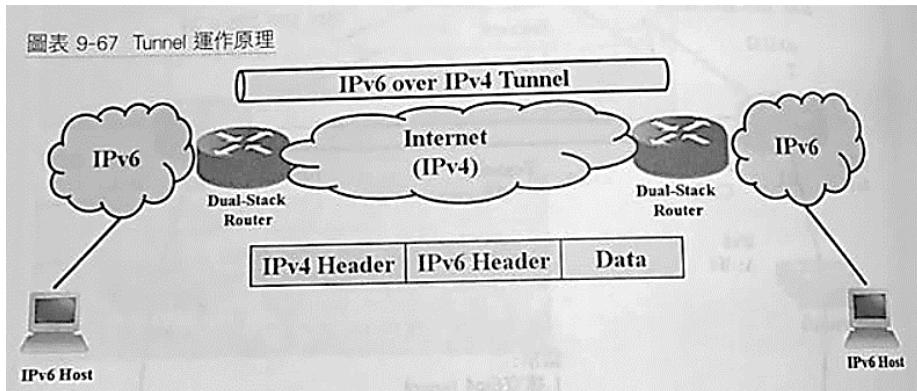
承上，上述的 Auto-Config 中，路由器 RA 封包中不包含 DNS 資訊，而在 IPv6 中路由器可利用 DHCP 伺服器來提供 DNS 位址，但 DHCP 伺服器不提供 IPv6 位址給電腦，故稱 Stateless DHCP。

指令	說明
Router(config)#ipv6 dhcp pool <i>mypool</i>	設定 IPv6 DHCP 存儲區
Router(config)#dns-server <i>x:x::x</i>	設定 DNS 位址
Router(config)#int fx/x	指定該介面使用 IPv6 DHCP 存儲區
Router(config-if)#ipv6 dhcp server <i>mypool</i>	
Router(config-if)#ipv6 nd other-config-flag	DHCP 僅會送出 DNS 資訊，O bit
Router(config-if)#ipv6 nd managed-config-flag	DHCP 負責 IPv6 位址配發，M bit



IPv6 Tunnel 轉換機制

- Tunnel 就是一條建立在 v4 環境中的專線，在專線中可傳送 v6 封包，故當 v6 電腦送出 v6 封包到 Tunnel 時，此時 v6 表頭檔不用解封裝，而是直接再封裝 v4 表頭檔，如此就可在 v4 網路中傳送。這樣送到 Tunnel 另一端後解封裝 v4 即可看到原先的 v6 封包。



指令	說明
Router(config)#int tunnel x	建立 tunnel x 介面
Router(config-if)#ipv6 address x::x/xx	設定 tunnel x 介面 IP
Router(config-if)#tunnel mode ipv6ip	設定 tunnel x 使用的模式
Router(config-if)#tunnel source int/ip	設定 tunnel x 來源
Router(config-if)#tunnel destination y.y.y.y	設定 tunnel x 目的

※注意!!兩個 host 的 tunnel 雖然建起來，但路由表互相沒有，所以兩邊都要再加入路由(可用靜態或是動態路由協定方式)。

交換器指令



· 交換服務

第 2 層交換提供 4 項重要優點：

- 硬體式的橋接(ASIC)
- 線路速度(wire speed)
- 低延遲(latency)
- 低成本

· 第 2 層的 3 項交換功能★★★ 會考已

-位址學習

第 2 層交換器(與橋接器)會記住它從介面接收之每個訊框的來源硬體位址，然後輸入這種資訊到一個稱為轉送/過濾表的 MAC 資料庫。

-轉送或過濾決策

當交換器從介面收到訊框時，會檢視其目的硬體位址，找尋它在 MAC 資料庫中所學到的離開介面，該訊框只會從特定的目的埠轉送出去。

-避免迴圈

如果為了達到冗餘目的而在交換器間建置多重連線，則有可能發生網路迴圈。擴展樹協定 (Spanning Tree Protocol, STP)，就是讓我們在提供網路冗餘性的同時、又能防止網路迴圈。

· L3 Switch v.s. Router

Feature	L3 Switch (Multilayer)	Router
Routing ability	V	V
WAN support	X	V
Advanced routing config	x	V

· 有個東西叫做 mdix，是 switch 端口上的預設值，它會自動轉換直線跳線，可 no 掉。

Trouble shooting of Switch



步驟	檢查方向	使用指令
1	檢查網路線是否有問題	
2	檢查介面是否被管理者關閉(administrative down)	
3	檢查是否出現過多的資料傳送錯誤	#show int fx/x
4	檢查 duplex 設定是否一致	
5	檢查 speed 設定是否一致	

※注意一個 Router/Switch 通用觀念，當介面 administrative down 要啟用時不能直接 no shutdown，因為會假死，要先 shutdown 一次再 no shutdown。



Switch IP

- 交換器不需 IP 就可運作，但給 Switch 一個 IP 可以方便 telnet、SSH、SNMP(這三種又稱為 in-band management，就是遠端管理啦)，通常會設在預設 vlan(Vlan1)上，不過為了安全性考量，最好更改預設 vlan 為其它。
 - 另外記住，因為交換器的所有埠預設為開啟，為了安全性，要關掉未使用的埠或是將它們指定給未使用的 vlan。
 - #Switch(config)#ip default-gateway ***ip+mask***
- 如果想從 LAN 外面管理交換器，就必須在交換器上設預設閘道，就像在主機上一樣。

◎查詢 MAC 表/清空 MAC 表

Switch#show mac address-table

Switch#clear mac address-table

◎查詢特定 MAC 位址的資訊

Switch#show mac address-table dynamic address XXXX.XXXX.XXXX(MAC)

◎查詢特定介面學到的 MAC 位址

Switch#show mac address-table dynamic vlan X 或 interface fx/x

◎指定靜態 MAC

Switch(config)#mac address-table ?/static ***aaaa.bbbb.cccc*** ***vlan 1 int f0/7***

將該 MAC 位址永久指定到介面 F0/7，並且它也只有被指定到 VLAN1

VLAN 觀念

- Switch port 是結合實體埠的第二層介面。如果該交換機埠是 access port，則只能屬於一個 VLAN；如果是 trunk port，則可以屬於所有的 VLAN。
- 理論上可建立 VLAN 為 1-4094，但實際可建立的 VLAN 為 1-1001，1、1002-1005 為保留 VLAN，不可變動。編號超過 1005 的 VLAN 稱為延伸式 VLAN；除非交換器設定為 VTP，否則它們不會被儲存在資料庫中。

#VLAN 1006-4095 只有 Cisco Core Switch 可用

- Frame tagging(訊框加標)

每部交換器收到訊框時必須先從訊框的標籤中識別出它的 VLAN ID，然後檢視過濾表中的資訊，看要如何處理該訊框。如果訊框抵達的是一部連有其他 Trunk port 的交換器，就會從 Trunk port 轉送出去。

當訊框抵達出口時，交換器就會移除 VLAN 識別子，所以目的裝置可以接收訊框，而不必瞭解他們的 VLAN 識別。另外如果使用 802.1q 的主幹通訊，它們同時支援加標與沒有加標的交通。

VLAN 的識別方法

Inter-Switch Link, ISL，跨交換器鏈路

是一種明確地為乙太網路訊框貼上 VLAN 資訊的方法，這種 tag 讓 VLAN 可以透過一種外部的封裝方法，多工於主幹鏈路上。這使得交換器能識別主幹鏈路上的訊框是屬於哪個



VLAN。這是屬於思科交換器獨有的方法，只用於快速乙太網路與 Gigabit 乙太網路的鏈路；目前思科已逐步朝向只使用 802.1q 了。

IEEE 802.1q

訊框加標的標準方法。插入一個 **4bytes** 欄位至訊框中，以識別 VLAN。若要跨廠牌交換器間建立主幹鏈路，必須使用 802.1q 才能運作。重點在於 12 位元的 VLAN ID，它的值可以到 $2^{12}-2$ (0 和 4095 為保留 VLAN)，代表 802.1q 的加標訊框可以攜帶 4094 個 VLAN 資訊。(VLAN ID 12bits)

- 為了將交換器底下的網路再切割多個廣播領域，就要使用 vlan。(一個 vlan 就是一個廣播領域)
- Native vlan 預設為 vlan 1
- 即使同一台交換器，兩個 vlan 之間資料仍是無法互通的，所以需要一台 Router/L3 Switch 來達送(Inter Vlan Routing)。



Vlan 設定

指令	說明
Switch#show vlan	查詢現有 vlan 狀態，只能顯示 access port
Switch#show vlan id <u>xx</u>	查詢特定 vlan 狀態
Switch#show interface trunk	查詢 trunk port 狀態
Switch#show int <u>fx/x</u> switchport	查詢特定介面的 vlan 設定
Switch(conf)#vlan <u>x</u> ↑設定完要 no shutdown ↑視情況給 VLAN IP & Mask(如果要 telnet switch 的話)	建立 vlan 編號 x
Switch(conf-vlan)#name happy	將 vlan x 命名為 happy
Switch#vlan database	非主流配置 vlan
Switch(config)#vlan <u>xx</u> name <u>yyy</u>	
Switch(config-if)#switchport access vlan <u>y</u>	在 fx/x 介面下，指定該 port 到 vlan y
Switch(config)#interface range f0/1-2	一次加入多個介面到 vlan
Switch(config-if)#switchport access vlan <u>XX</u>	
Switch(config)#interface range f0/3,f0/13	
Switch(config-if)#switchport access vlan <u>XX</u>	
Switch(config-if)#switchport voice vlan <u>z</u>	將該介面指定到 voice vlan z(要先建立 z)
Switch#del flash:vlan.dat	清除原有 vlan database
Switch#reload	
Switch(config-if)#ip address dhcp	VLAN 使用 DHCP
Switch#show dhcp lease	承上，查詢 DHCP 狀態

Vlan Trunk

- 利用單一線路讓所有相對應 vlan 互通(在此之前兩台 switch 的同 vlan 要相連就要一條線兩個 port，兩個 vlan 兩條線四個 port，以此類推疊加)
- Trunk 上使用的協定：
IEEE 802.1Q(dot1q)、Cisco ISL(CCNA 不討論)

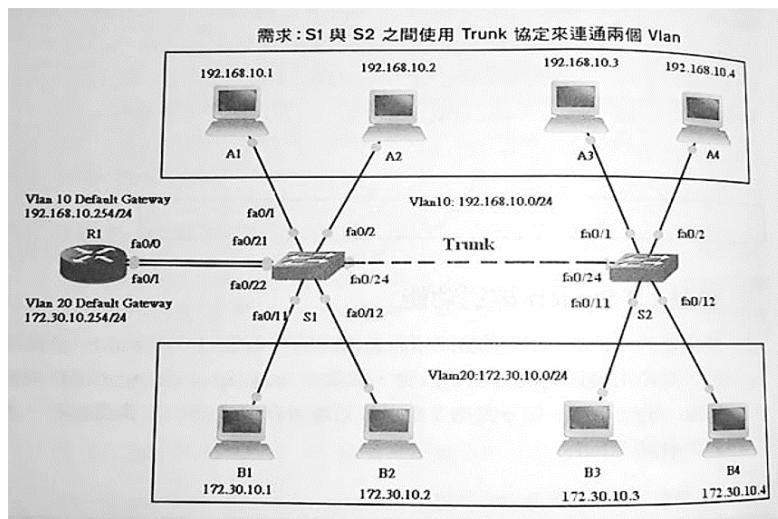


· Trunk 的原理：

交換器為 L2 設備，主要辨識 Ethernet Header(乙太網表頭)，乙太網表頭中沒有 vlan 的資訊，802.1Q 協定的主要功用就是將 Vlan ID 用 tag 方式加到乙太網表頭，用以區別資料該送到哪個 vlan；當資料經過 trunk 時，802.1Q 協定會將 tag 拿掉(untag)。

· Trunk 的各種模式(auto/desirable/trunk/access)及連接狀態(access/trunk)在後面的 DTP 有
Trunk 相關指令

指令	說明
Switch(config)#int fx/x	設定 fx/x 介面為 trunk port
Switch(config-if)#switchport trunk encapsulation dot1q	#在較新的 IOS 版本可省略 dot1Q 那行
Switch(config-if)#switchport mode trunk	
Switch(config-if)#switchport trunk <u>allowed</u> vlan y	讓特定 vlan 通過 trunk
Switch(config-if)#switchport trunk <u>allowed</u> vlan <u>remove</u> y △y 可以設定範圍比如 4-8	讓特定 vlan 不能通過 trunk
Switch(config-if)#switchport trunk <u>allowed</u> vlan all	讓所有 vlan 通過 trunk(回復預設)
Switch(config-if)#switchport trunk native vlan y #no switchport trunk native vlan → 復原	修改 trunk port 的 native vlan (要 802.1q) #trunk 的兩邊都要修改才能溝通
Switch#show int f0/24 switchport	查詢 fx/x 是否為 Trunk Port
Switch#show interface trunk Operational mode：目前的 trunk 模式	查詢 trunk 資訊 查詢有哪些是 trunk port 與哪些 vlan 可通
Switch#traceroute ip	查詢路由是否有經過 Trunk



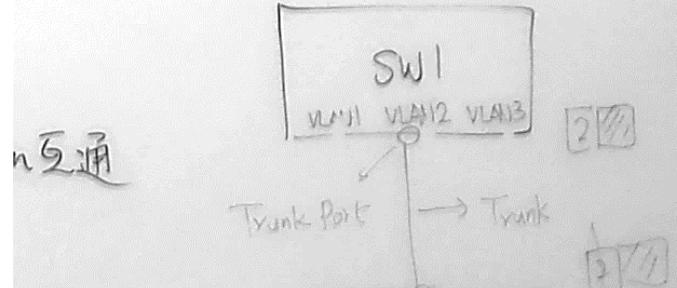
Native VLAN
不加/不設 tag 的 VLAN

Switch#show run interface fx/x

· Trunk LAB

1. 首先完成基本的 vlan 設定及分組

Switch(config)#int f0/1



```

Switch(config-if)#switchport access vlan 1
Switch(config)#int vlan 1
Switch(config-if)#ip address 192.168.1.100 255.255.255.0
Switch(config-if)#no shutdown
其餘依此類推 vlan 2 2.100    vlan3 3.100    第二台 switch100 改 200

```

2. 設定 Trunk Port

```

Switch(config)#int f0/24
Switch(config-if)#switchport trunk encapsulation dot1q(有些 ios 版本不用指定 Trunk 封裝格式)
Switch(config-if)#switchport mode trunk

```

3. 檢視

- ① 確認 f0/24 是否為 Trunk Port
show int f0/24 switchport
- ② 確認有哪些是 trunk port 與哪些 vlan 可通
show interface trunk

4. 特殊需求—要求讓特定 vlan 不能通過 trunk

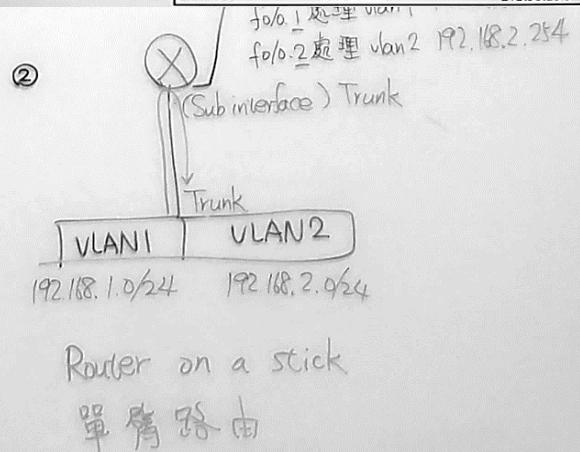
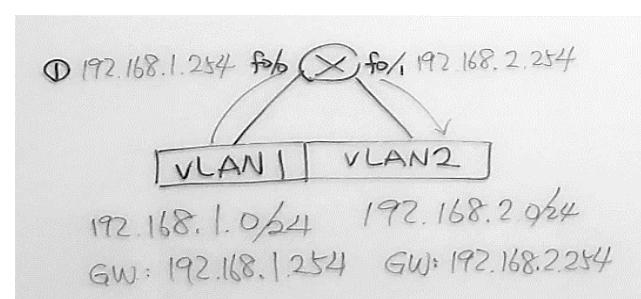
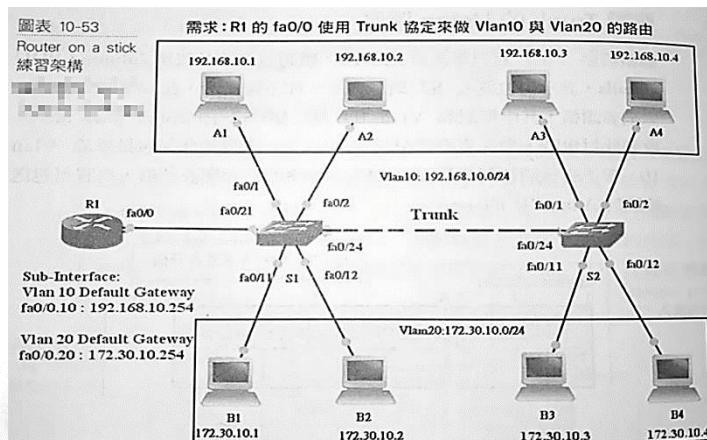
```

Switch(config)#int f0/24
Switch(config-if)#switchport trunk allowed vlan remove 2

```

跨 VLAN 遴送(IVR)—Router on a Stick(ROAS-單臂路由) ↑

- 跨 VLAN 遴送又稱為 upstream routing(上行遼送)。
- 在前面的範例中，vlan 之間要相互繞送，需要 vlan 數量的實體連線到路由器上，並不實用，所以想讓路由器與交換器間也用類似 Trunk 的方式來路由，即單臂路由(下圖)。

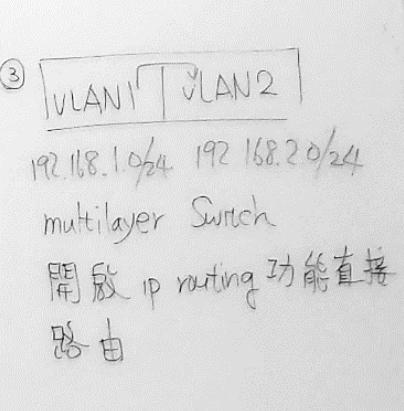


① 原始架構—由一台 Router 的兩個 port Routing，浪費 port(右上圖)

② 改良架構—由一台 Router 的單一 port Routing(左圖)

即單臂路由

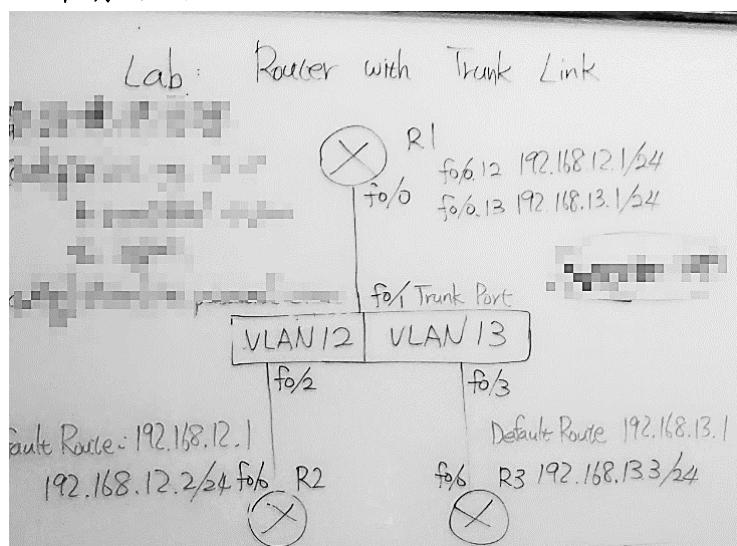
使用路由器的單一 port 做 Trunk，此種做法需在該 port 底下建立 Sub-interface(子介面)



• 單臂路由指令

指令	說明
Router(config)#int <u>fx/x</u>	在 fx/x 介面下產生.y 的子介面並賦予 IP
Router(config-if)#int <u>fx/x.y</u>	p.s.子介面跟隨實體介面，故只要實體 no shut 子介面就是 up
Router(config-subif)#ip add	
Router(config-subif)#encapsulation <u>dot1Q z</u>	將 fx/x.y 子介面設為 trunk，使用 802.1Q 協定，z 代表要處理的 vlan tag
Switch(config)#ip default-gateway <u>IP</u>	指定交換器通往路由器的 GW

• 單臂路由 Lab



◎Router with Trunk Link

1.首先完成基本配置(注意 R2、R3 的 default route)

R2(config)#ip route xx xx 192.168.12.1

R3(config)#ip route xx xx 192.168.13.1

(完成可用 show ip route 確認是否有*s 0.0.0.0/0 的預設路由)

2.設定 Switch 的 Vlan 且 f0/1 設為 trunk port

Switch(config)#int f0/1

Switch(config-if)#switchport trunk encapsulation dot1q

(有些 ios 版本可省略這行)

Switch(config-if)#switchport mode trunk

3. 在 R1 的 f0/0 上建立 subinterface 以處理不同 vlan

#int f0/0.12

#encapsulation dot1q 12 → 處理 vlan12 tag

#ip add x.x.x.x x.x.x.x

#int f0/0.13 → 作法比照 0.12，12 改 13，ip 改一下

p.s. R1 開啟遠端管理(telnet line vty)

會比較方便

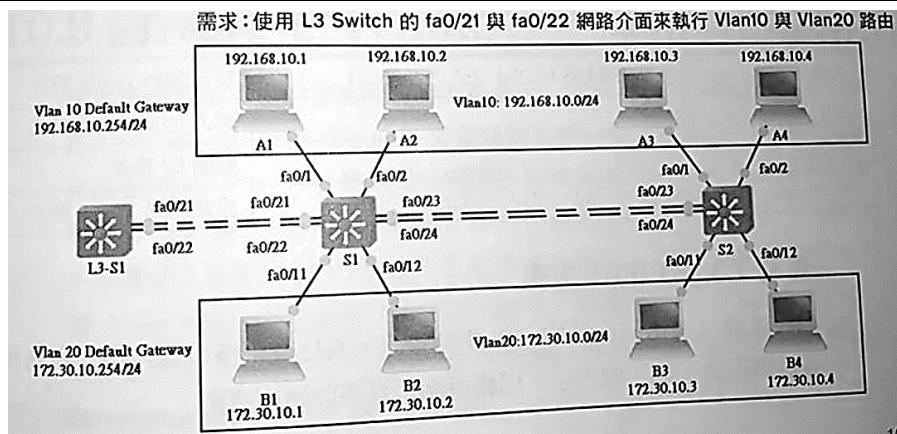
p.s. 檢查可用 traceroute 檢查

跨 VLAN 遶送—Layer3 Switch Routing



- 在一顆正常的交換器上，所有 port 都是預設為 L2 的，因此不能設定 IP，所以需要在介面下 no switchport 指令關閉 L2 功能。
- 在一顆正常的交換器上，不會有繞送功能，故要用 ip routing 指令啟動繞送。

指令	說明
L3Switch(config)#int fx/x	關閉 fx/x 介面的 L2 功能
L3Switch(config-if)#no switchport	
L3Switch(config)#ip routing	啟動 L3 Switch Routing 功能



- 在第 3 層交換器的基板(backplane)上設定邏輯介面；這就是所謂的「跨 VLAN 遶送」(inter-VLAN routing, IVR)，並且是使用交換式的虛擬介面(switted virtual interface, SVI)來設定。
- 配置同單臂路由，將路由器換成 L3 交換器。
- L3 交換器沒有 subinterface 功能，要使用另一個功能：SVI(Switch virtual interfaces)，SVI 類似 loopback 也是一個虛擬介面，只是 SVI 對應到 Vlan，正常的交換器會有一個預設 Vlan=Vlan 1 以及一個 SVI=int Vlan 1；在 L3 Switch 中則是每個 vlan 的 SVI 可以當作該 vlan 的 GW，所以可以直接使用 L3 Switch 的 SVI 來做 VLAN 縱送。

• SVI Configuration 注意!!!要先有 **vlan XX** 再做 **int vlan IP** 才會生效!!!

指令	說明
L3SW(config)#ip routing	建立 SVI x，賦予 IP 並啟動 L3 縱送功能
L3SW(config)#int vlan x	#不需路由表，只要在兩個 svvi 上給 ip 及啟動
L3SW(config-if)#ip add ...略	縱送就可以直連路了



Dynamic Trunking Protocol(DTP)動態偵測 Trunk

- 交換器的 port 上只會有兩種連接模式，Access mode / Trunk mode，用 show int fx/x switchport 可查到：

```
S1#sh int f0/2 switchport
Name: Fa0/2
Switchport: Enabled 1
Administrative Mode: dynamic auto
Operational Mode: static access 2
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On 3
Access Mode VLAN: 1 (default) 4
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

- 1**目前 f0/2 port 的模式，Administrative Mode 欄位為管理者設定 mode 的方法，有 dynamic 或是手動(access/trunk)；Operational Mode 欄位為現在的狀態，static access 為 access mode。
2表示 trunk 的封裝協定
3表示 f0/2 目前所屬的 vlan
4表示為 native vlan

思科 DTP 自動協商(思科自己建議不要用的東西)

預設啟用在兩部裝置間協商主幹通訊，以及協商封裝類型要用 .1q 或 ISL。當想要有專用的 TRUNK 時，可以使用 nonnegotiate 指令。

圖表 10-64 DTP 參數對應表

	Auto	Desirable	Trunk	Access
Auto	access	trunk	trunk	access
Desirable	trunk	trunk	trunk	access
Trunk	trunk	trunk	trunk	N/A
Access	access	access	N/A	access

正常的思科交換器上連接埠預設為 DTP auto，而 DTP 提供 auto/desirable 兩個參數

指令	說明
Switch(config-if)#switchport mode <u>access</u> 不管鄰接介面是否為主幹，這個埠將成為專用的第 2 層埠	將介面(存取埠)放入永久的非主幹模式，並協商要將鏈路轉換成非主幹鏈路。
Switch(config-if)#switchport mode dynamic <u>auto</u>	讓介面自動轉換為 trunk，如果鄰接介面設定為 trunk/desirable，該介面就會成為 trunk。許多 Cisco 交換器預設是 dynamic auto，但較新的機型則改為 dynamic desirable
Switch(config-if)#switchport mode dynamic <u>desirable</u>	讓介面主動地試圖將鏈路轉換成主幹鏈路。如果鄰接為 trunk/desirable/auto，它就會變成 trunk。
Switch(config-if)#switchport mode <u>trunk</u>	將介面放入永久的主幹模式，並協商要將其鄰接鏈路轉換成主幹鏈路。該介面會變成主幹介面，不管其鄰接介面是否為 trunk
Switch(config-if)#switchport <u>nonnegotiate</u>	停止該介面產生 DTP 協商(訊框)。只有當介面的交換埠模式是存取或主幹時，才使用該命令。必須手動將其鄰接介面設為主幹介面，才能建立起主幹鏈路。(可用來建立專屬 trunk)

Switch#show int trunk #欄位下 Encapsulation 會顯示 n-802.1Q，其中 n 表示 negotiate(協商)	查詢 DTP 協商結果 查詢有 trunk port 有哪些
Switch#show int fx/x switchport	查詢該介面的 DTP 狀態

--使用 switchport negotiate 停止協商後，即使設定為 trunk port 也不會 on



修改原生 Native Vlan

- Trunk port 的 native vlan 為 1，在 802.1Q 主幹協定中，當資料目的是 Native Vlan 時，該資料經過 trunk port 不用 tag，即沒有 tag 的資料都往 native vlan 丟。
- 有一種網路攻擊針對 native vlan 稱為 vlan hopping，所以從資安角度來說會想辦法關閉 native vlan 的功能，使用指令 Switch(config)#vlan dot1q tag native。

◎修改 Native vlan 為其它 vlan

Switch(config)#int f/x →trunk port

Switch(config-if)#switchport trunk native vlan x →要注意另一台 switch 相對應的 trunk port 也要改 native vlan，否則無法建立 trunk

◎修改 native vlan 後的單臂路由

Router(config-subif)#encapsulation dot1q x native



限制 Vlan 傳送(on trunk)

指令	說明
Switch(config-if)switchport trunk allowed vlan <u>x</u>	限制只有 vlan x 可使用 trunk
Switch(config-if)switchport trunk allowed vlan <u>x, y, z</u>	上面指令的複數版
Switch(config-if)#switchport trunk allowed vlan ? ?=remove/all	加入/移除/其它設定 vlan 到 trunk，功能自己查



ACL (Access Control List)

- ACL 語法

#permit host *ip* → 允許 ip 通過
#deny host *ip* → 拒絕 ip 通過

- ACL 執行

設定完 permit/deny，只是讓條件存在 run config，還需要在網路介面上啟動 ACL 的指令。

ACL 執行的方向性

在網路介面啟動 ACL 時要注意方向性，分別 **inbound(進入) & outbound(離開)**。

ACL 種類

分為兩種，Standard(標準型) & Extended(延伸型)，差別在檢查的條件，標準型只能檢查封包 source，延伸型可以檢查的包含來源、目的、協定、服務。

名稱式 ACL—技術上來說只有兩種，只是標準/延伸型可以改成有名稱，實際功能相同。

ACL 敘述的設定方式

分兩種，一種是使用 Number，一種用 Name，詳述如下表

IPv4 ACL 種類	數字範圍或名稱
Number Standard	1-99, 1300-1999
Number Extended	100-199, 2000-2699
Named(Standard & Extended)	Name

ACL 執行順序

有點像是寫程式的迴圈，if 第一個條件成立(**Match**)就執行(**Deny or Permit**)，第二個條件之後的就不執行，if 第一個條件不成立就檢驗第二個條件，以此類推。

另外 ACL 有隱藏條件為 Deny any。

- ACL 的設計重點

— 每個介面的每個協定的每個方向只能指定一個 ACL。這表示在產生 IP 存取清單時，每個介面只能有一個進入的 ACL 和一個離開的 ACL。

— 無法從 ACL 中移除單一列，所以最好用文字編輯器先編好存取清單。若是試圖移除單一列，通常會移除整個清單。所以要編輯 ACL 前，先備份好原先的 ACL。唯一的例外是使用名稱式 ACL。

— 每個清單至少有一個 permit 描述，不然就和該介面單方向 shutdown 沒有兩樣。

— ACL 用來過濾經由路由器的交通，但不會過濾由路由器發起的交通。

— 盡可能將標準式 ACL 配置在靠近目的的地方，因為標準式只能過濾來源 IP，放在靠近出發點會導致沒有封包能通過。

— 盡可能將延伸式 ACL 配置在靠近來源的地方。因為延伸式 ACL 可以過濾特定的 IP 目的與協定，放在靠近來源可以減少流經整個網路的封包數，提高有效頻寬。

— 常用的 ACL 內容(內網跨外網)

1. 拒絕來源為內部網路的 IP。
2. 拒絕 127.0.0.0/8
3. 拒絕 RFC1918 表列的私有 IP。
4. 拒絕 224.0.0.0/4(群播位址、動態路由協定)

Standard ACL



◎Standard 標準型 - 只能檢查來源 IP

數字 ACL

access-list	Number	Permit/deny	sourceIP+wildcard
-------------	--------	-------------	-------------------

名稱 ACL

ip access-list standard	Name	Permit/deny	sourceIP+wildcard
-------------------------	------	-------------	-------------------

· 常用指令

指令	說明
Router(config)#access-list <u>n</u> <u>permit/deny</u> host <u>ip</u> <u>wildcard</u>	新增一筆編號 n 的 ACL 敘述 Host & wildcard 二選一
Router(config)#int fx/x Router(config-if)#ip access-group <u>n</u> <u>in/out</u>	在 fx/x 啟動編號 n 的 ACL，並檢查 進入/離開的封包
Router#show access-list	查詢 ACL 設定

#注意標準數字型編號為 1-99、1300-1999。

#要確認 ACL 是否生效可以用 Ping 製造封包讓它經過路由器，之後再 show access-lists 就會看見有括號(matches)。

· access-list xx permit/deny 後的三個選項：

1. 使用 any 來允許或拒絕任何主機或網路。
2. 使用單一 IP 來設定單機或一個範圍的主機。
3. 使用 host 來設定一部特定主機。

◎重設 ACL 執行計數器 讓 matches 的數目歸零

Router#clear access-list counters

ACL on vty 用 ACL 限制 telnet/SSH

- 限制 IP 存取 VTY，不用在每個介面的 IN 使用 ACL，只要限制 VTY 本身就可。
- ACL 本身有一個 deny any 的隱性限制，所以除了清單 permit 之外都不可 telnet。

Router(config)#access-list 10 permit host 10.10.10.123 →也可以用整段子網路取代 IP

Router(config)#lin vty 0 4

Router(config-line)#access-class 10 in →只允許該 ACL 允許的 ip 使用 telnet



Extended ACL

- 用來限制單純幾種服務或是限制目的 IP

· (config)#access-list 110 deny ?

#如果想要過濾應用層協定，必須在 permit/deny 的敘述之後選擇適當的第 4 層協定，例如，若要過濾 Telnet 或 FTP，必須選擇 TCP，因為 Telnet 與 FTP 在傳輸層都使用 TCP。若選擇 IP，稍後就不能設定特定的應用層協定。

· (config)#access-list 110 deny tcp ?

#設定主機或網路的 source IP(也可用 any 允許所有來源)

· (config)#access-list 110 deny tcp any ?

#設定目的 IP

· (config)#access-list 110 deny tcp any host 172.16.30.2 ?

#拒絕目的 IP 為 172.16.30.2 的封包

· (config)#access-list 110 deny tcp any host 172.16.30.2 eq ?

#用 equal 命令來設定要拒絕的服務類型。可以選擇埠號或使用應用的名稱。

· (config)#access-list 110 deny tcp any host 172.16.30.2 eq 23 log

#範例為只阻擋 Telnet(23 埠)至 172.16.30.2 主機。Log 命令可用來紀錄每次比對成功時的訊息，用於監視不當的存取很好用。但在大型網路中，這會產生很多的 log。

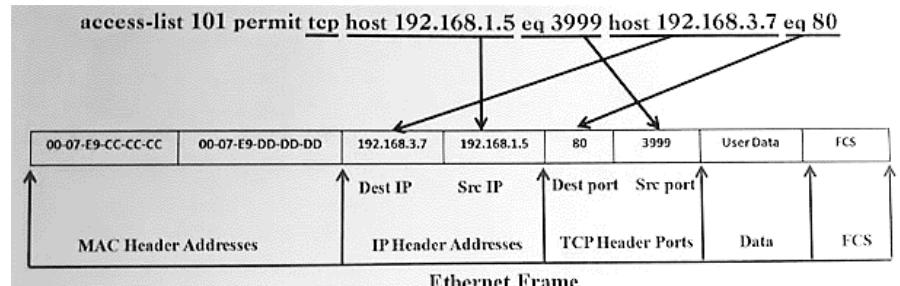
再補上一行 access-list 110 permit ip any any

#因為預設隱含 deny any，所以以限制少數功能為主的 ACL 不加上 permit any 的話就等於 shutdown 介面。其中的 ip 很重要，因為它會允許 IP 堆疊。Any 相當於 0.0.0.0 255.255.255.255。最後(config-if)#ip access-group in/out → 最後套用到介面上

範例說明：

#access-list 101 permit tcp host 192.168.1.5 eq 3999 host 192.168.3.7 eq 80

檢查來源為 192.168.1.5 與目的為 192.168.3.7，且封包要使用 tcp 協定與 http 服務(eq 80)，另外 eq3999 表示要檢查封包的 source port number=3999，如此才符合該 ACL 條件。如下圖所示為延伸 ACL 四個條件的語法，其中服務是檢查 Destination port number，寫在目的電腦 IP 後面，但是來源電腦也可以檢查 source port number，只是 source port number 為視窗編號，檢查沒有意義，通常不會寫出來。



◎檢查 Port Number 的運算子

Eq 等於(equal)

Gt 大於(greate)

Lt 小於(little)

Neq 不等於(not equal)

Range 在給定的 port number 範圍

◎Extended 延伸型 - 可檢查封包來源、目的、協定、服務四項

數字 ACL

access-list extended	Number	Permit/ deny	Protocol	sourceIP +wildcard	eq/lt/gt	Source Port	destinationIP +wildcard	eq/lt/gt	Destination port
-------------------------	--------	-----------------	----------	-----------------------	----------	----------------	----------------------------	----------	---------------------

紅字打完要先 Enter 一次，分段式設定

名稱 ACL

ip access-list extended	Name	Permit/ deny	Protocol	sourceIP +wildcard	eq/lt/gt	Source Port	destinationIP +wildcard	eq/lt/gt	Destination port
----------------------------	------	-----------------	----------	-----------------------	----------	----------------	----------------------------	----------	---------------------

紅字打完要先 Enter 一次，分段式設定

TCP/IP 封包範例

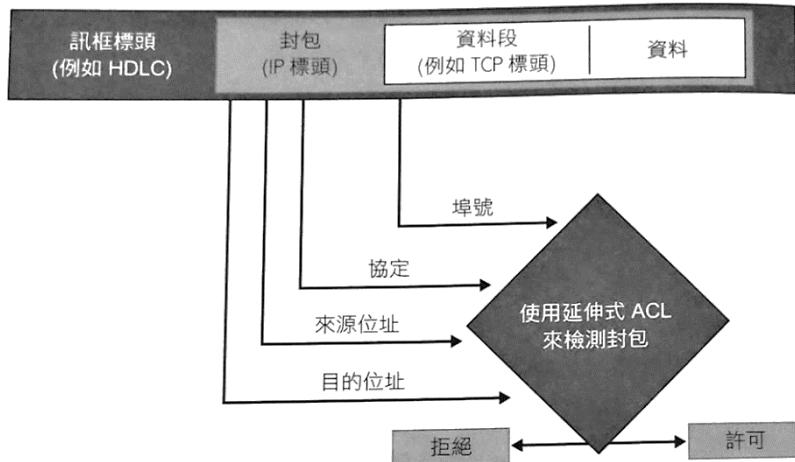


圖 20.3 延伸式 ACL

· 延伸 ACL 範例

1. permit ip host 192.168.10.1 any

檢查條件為來源 192.168.10.1，目的是任何網路，協定使用 IP，三個條件都符合就 permit。

2. permit ip host 192.168.10.2 host 207.16.10.1

檢查條件來源 192.168.10.2，目的是 207.16.10.1，協定使用 IP，三個條件都符合就 permit。

· ACL 使用設計原則(僅供參考)

-根據需要過濾的封包，決定使用標準型或延伸型。

-決定在 inbound or outbound 啟動 ACL。

-每個網路介面的每個方向只能啟用一組 ACL

-每個 ACL 都有一個隱含條件為 deny any，此為路由器主動執行，可用 permit any 來取消

-ACL 條件嚴謹度，越前面的越嚴謹，越後面的越寬鬆。

P.S. 交換器也有 ACL，稱為 VACL(vlan)及 PAACL(port)，而路由器的稱為 RACL，VACL/PACL

為 CCNP

· 複習一下常用 PORT 號

FTP 20/21	SSH 22	Telnet 23	SMTP 25	DNS 53	HTTP 80	HTTPS 443
(TCP)	(TCP)	(TCP)	(TCP)	(TCP/UDP)	(TCP)	(TCP)

Ping 沒有 port 號，但服務是用 ICMP

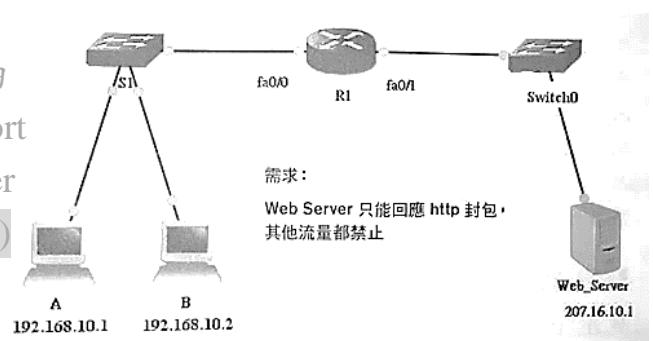
檢查 Source Port 的 ACL (上課沒教過的哦)

· 檢查 source port 的 ACL 用法在 stateful firewall(有狀態防火牆)語法中會用到。

· 範例如右，要求 Web server 只能回應 HTTP 封包

其他流量都禁止，以 R1 的 inbound 方向設計，由於 Web server 回應 http 封包是由自己的 source port 80 送出，所以要檢查來源 ip 的 source port number

#permit tcp host 207.16.10.1 eq 80 any (套用在 f0/1 in)



此種應用在於讓 Server 只回應 http 流量，避免其它種類流量向 Server 請求回應，如此也可以保護 Server 不回應不正常流量。

一般 ACL 不用特別檢查 Source port number，因為一般電腦送出的 tcp 封包，source port number 只代表視窗編號。

Access-list xx permit any any

通常加在 ACL 的最後一行，因為 ACL 的功用只是要阻擋特定功能，而不是要全擋。

Remark

·就是 ACL 的註解，可以加在 permit/deny 的前面或後面都可，但盡量選同一個位置以免搞混。
範例 1：

```
Router(config)#access-list 110 remark HAPPY DAY EVERY DAY
```

```
Router(config)#access-list 110 permit/deny...
```

範例 2：

```
Router(config-ext-nacl)#remark ARE YOU SERIOUS
```

```
Router(config-ext-nacl)#permit/deny...
```

查詢 ACL 設置狀態及內容

指令	說明
#show access-list	顯示路由器上所設定之所有 ACL，以及其參數。這個命令不會顯示 ACL 套用在哪些介面上。(使用中+非使用中)
#show access-list 110	只顯示 110ACL 的參數。這個命令也不會顯示 ACL 套用在哪些介面上。
#show ip access-lists	只顯示路由器上所設定之 IP 存取清單(使用中)
#show ip interfaces	顯示哪些介面套用了 ACL

ACL 微調—新增、修改、刪除

指令	說明
R(config)#ip access-list extended <u>NAME</u>	只有名稱型 ACL 可以刪除和插入新的 ACL 條件，另外 ACL 條件編號預設為 10 的倍數。
R(config-ext-nacl)#no <u>10</u>	
R(config-ext-nacl)# <u>數字</u> deny/permit...	

IPv6 ACL

首先，要瞭解您只能建立延伸的名稱式 IPv6 ACL，所以不用在名稱式清單中指定是標準式或延伸式。而且，雖然看不到序列編號，但某種程度來說，您還是可以編輯名稱式的 IPv6 ACL；也就是說，您可以刪除單一命令列，但是只能在 ACL 的最後面做新增。

此外，每個 IPv4 存取清單的最末端都有一個內隱的 **deny ip any any** 敘述；但是 IPv6 存取清單最末端其實有 3 個內隱的敘述：

- permit icmp any any nd-na
- permit icmp any any nd-ns
- deny ipv6 any any

上面兩個許可敘述是用於鄰居發現協定(neighbor discovery protocol)，這是 IPv6 的一項重要協定，用來取代 ARP。

· IPv6 ACL 常用指令(範例)

指令	說明
R1(config)#ipv6 host <u>Server1</u> 2001:db8:...略:be3d R1#show host	建立一個本機 DNS 在後續使用上會比較愉快
Router(config)#ipv6 access-list <u>name</u> Router(config-ipv6-acl)#deny/permit <u>protocol</u> <u>2001:AAAA::/64</u> host <u>2001:CCCC::2</u> <u>eq protocol</u>	使用命名方式，名為 name，後續使用方式同 ipv4 ACL，wildcard 改成 prefix
Router(config-ipv6-acl)#permit ipv6 any any	無條件允許 ip 封包通過，加在最後一行
Router(config)#int fx/x Router(config-if)#ipv6 traffic-filter <u>name in/out</u> Router(config-if)#no ipv6 traffic-filter <u>name in/out</u>	在 fx/x 介面 in/out 方向啟用該 ACL 在 fx/x 介面 in/out 方向停用該 ACL
Router#show access-lists	不解釋
R1#show ipv6 int br	快速檢視各介面上 ipv6 位址
R1#show run	這不是一句廢話，在 IPv4 中可以用 show ip int 來檢查是否有設定 ACL，而在 IPv6 中只能用 show run 來檢查

補充說明

- 不使用 wildcard，改用 prefix，但在細節上較無彈性，比如無法區分奇偶數子網路。
- ACL 種類與語法，IPv6 只有一種分類與一種語法，在分類上 IPv6 使用類似 Extended 語法，而 Extended 語法也有辦法做到 Standard 語法的效果，另外寫法上都使用命名式。
- 比較表

Features	IPv4	IPv6
執行指令	#ip access group	#ipv6 traffic-filter
檢查方式	Wildcard Masks	Prefix length
命名方式	支援	支援
數字方式	支援	不支援

ACL LAB

◎一些細節

- (eq/lt/gt+來源 port) → 省略不打時，代表所有 port
- (目的 IP+Wildcard) → 用 any 取代時，代表 0.0.0.0 255.255.255.255
- any 有時候可以代表所有 IP，所以有時候會有 any any 出現

5.Wildcard 如果是 0.0.0.0 可用 host 代替 →ip+0.0.0.0 = host+ip

◎ACL 使用流程

1. 創建一張 ACL
2. 設定 ACL 裡的 statement，一般來說最後一條要加上 permit ip any any
3. 進入特定介面(int、vty 等等)，套用 ACL，指定方向 in/out
4. 沒用到的 port 最好關閉，比如 http 的 80 port
5. 設完後用 show ip access-lists 確認一下

※ACL statement 預設序號為 10、20...其中的數字可以用來做事後插入其他條件

※ACL statement 預設一條隱藏條件 implicit deny all，所以設完條件後要加 permit 條件

※都打完之後要再插入 ACL statement，進入該張 ACL 內，用數字插入

Ex: 11 deny tcp host 192.168.12.2 host 192.168.12.1 eq 23

※都打完之後要再刪除 ACL statement，進入該張 ACL 內，用數字刪除(僅限名稱型)

Ex: no 11 對不要懷疑就這樣

範例:

- ① ip access-list extended DENY_TELNET ←創建一張 ACL 名叫 DENY_TELNET
- ② deny tcp host 192.168.13.1 host 192.168.13.3 eq 23 ←拒絕從 13.1 到 13.3 的 TCP telnet
- ③ **permit ip any any** ←因為預設為 implicit deny，所以設完以上的 statement 後，要再允許其它功能
- ④ int f0/0 ←進入 f0/0 介面才能套用 ACL
- ⑤ **ip access-group DENY_TELNET in** ←最後一個 in 代表方向為 in，out 代表對外
- ⑥ 複習一下，怎麼看介面上套用的 ACL? show ip int (fx/x 可不加)

◎Cisco SDM 功能

R3(config)#ip http server ←啟用 Cisco SDM 功能(類似瀏覽器功能 80port)

R3#telnet 192.168.13.3 80 ←最後一個是 80port 的意思

get ←可以看到用哪個版本的套件，Server 哪家的

◎拒絕 http (80)port

(沒使用的 port 最好關閉)

ip access-list extended DENY_TELNET

21 deny tcp host 192.168.13.1 host 192.168.13.3 eq 80

◎刪除 ACL 表

R3(config)#no ip access-list extended/standard XXX

◎用 Wildcard 把奇數和偶數 IP 分開成 2 羣

答:關鍵在最後一個 Wildcard bit , 用 11111110 來比較分類就好

Wildcard

- 可以使 ACL 一次過濾一整個網段，類似 mask 的功能。
- 不加 wildcard 的話，就只能針對固定的 ip。
- 快速算法：255.255.255.255-mask
- 快速算法 2：一個網段裡的 ip 數量-1=mask，比如有 4 個 ip(255.255.255.252)，wildcard=4-1=3
- bit=0 則比對，bit=1 不比對，和 mask 剛好相反。
- 特殊 wildcard：
 - 0.0.0.0=全符合，即指定該 ip；255.255.255.255=全部忽略。
 - #permit 192.168.10.1 0.0.0.0 可以寫成 permit host 192.168.10.1
 - #permit 任何 ip 255.255.255.255 可以寫成 permit any



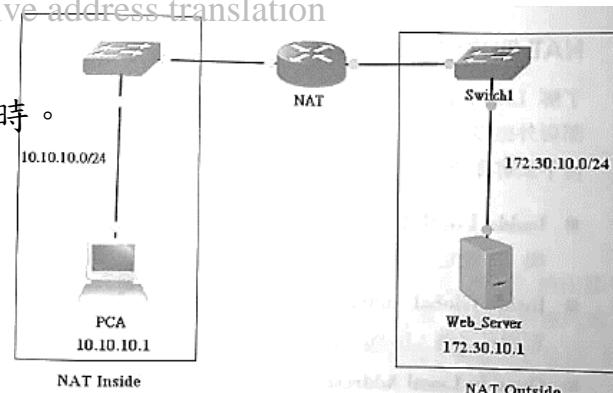
NAT 轉換

- NAT，Network Address Translation，將 RFC1918 私有 IP 轉成公有 IP。

#NAT 別稱 network masquerading、ip masquerading、native address translation

- 適合使用 NAT 的時機：

- 必須連上網際網路，但是主機又沒有全域唯一的 IP 時。
- 更換到新的 ISP 而必須重新為網路編號時。
- 必須合併兩個具有重複私有 IP 的企業內網路時。
- 通常使用在邊界路由器上



- NAT 運作過程

需要有個 NAT Table，此轉換表記錄 IP 位址轉換的對應關係。NAT Table 中共有四種位址的專有名詞，後面詳述。

p.s. NAT 也可以私有轉私有，比較少見

需求:Inside Local 對應 Inside Global :
10.10.10.0 to 200.200.200.1
Outside Local 對應 Outside Global :
150.150.150.1 to 172.30.10.1

- NAT Inside & Outside

以圖為例，左邊為內部，右邊為外部，故左邊 ip nat inside，右邊下 ip nat outside。

※CCNP 有教一種 NAT Virtual Interface 技術，可以不用管內部或外部，只要啟用 NVI 功能

Local 與 Global 位址

除了定義 Inside & Outside，還要定義 Local 與 Global，以 NAT 內部角度來看：

- Local：表示 NAT 轉址前的原始 IP
- Global：表示 NAT 轉址後的新 IP

• NAT 的名稱(四種位址)

用來描述NAT的名稱非常簡單。經過NAT轉換後的位址稱為Global Address，通常是公有IP。不過如果不連上網際網路也可以用私有IP。

Inside Local Address：NAT內部轉換前IP，也就是嘗試連上網際網路之傳送主機真正使用的私有IP，即**內部主機IP**。

Outside Local Address：NAT外部轉換前IP，由管理者定義IP，作為轉址到外部主機IP用。

通常是連到ISP的路由器介面的位址，也通常是封包開始其旅程所用的公有IP。

Inside Global Address：NAT內部轉換後IP，此IP為管理者定義，作為內部主機IP轉址用。

Outside Global Address：即**目的主機IP**。

名稱 意義

Inside local	轉換前的內部來源位址名稱—通常是RFC1918私有IP
Outside local	網際網路認識的來源主機位址。這通常是連到ISP的路由器介面的位址—實際的網際網路位址(對外部目的主機而言)
Inside global	轉換後要送往網際網路的內部來源主機位址；這也是真正的網際網路位址
Outside global	轉換後的外部目的主機位址；也是真正的網際網路位址

◎查詢NAT Table

```
#show ip nat translations
```

• NAT 位址轉換方式 -3 種

NAT Static(一對一)

在Local位址要轉換前，事先由管理者定義IP對應在NAT Table中，此筆對應不會移出NAT Table，除非使用移除NAT Static指令。另NAT Static從NAT in/outside都可，而下面的動態只能從內部連線。靜態NAT需要網路上的每部主機都各自有一個實際公有IP對應。

NAT Dynamic(多對多)

Local IP要進行轉址時才在NAT Table產生臨時IP來對應，當內部電腦不連線時，此臨時IP會移出NAT Table。動態NAT需要定義可用的Global IP範圍與定義哪些Local IP可使用Dynamic NAT功能。必須有足夠的公有IP，供每個想要與網際網路收送封包的機器使用。

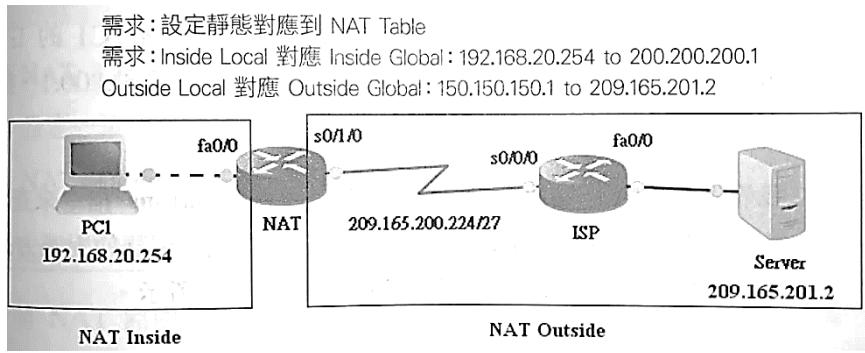
PAT(一對多)

Port Address Translation,也是一種Dynamic，在轉址過程中只會用到port number，如此可讓多個Local IP轉址到一個Global IP。最普遍的NAT組態，又稱overloading(超載)。藉由使用不同埠號，將多個私有IP對應到單一公有IP。藉由PAT(或NAT overloading)，只需要一個公有IP，就可以讓很多個使用者與網際網路連線。

=====



NAT Static



◎設定靜態 NAT

```
NATRouter(config)#ip nat inside source static 192.168.20.254 200.200.200.1
                    (inside local ip) (inside global ip)
```

◎移除 NAT 內部靜態對應 -no 掉就可以了

設定好上述指令還不能執行 NAT，因為尚未定義 Inside & Outside，照上述規劃 f0/0 為 in, s0/1/0 為 out，故以下指令：

內部	外部
NAT(config)#int f0/0	NAT(config)#int s0/1/0
NAT(config-if)#ip nat inside	NAT(config-if)#ip nat outside

◎設定 NAT 外部靜態對應

```
NAT(config)#ip nat outside source static 209.165.201.2 150.150.150.1
                    (outside global) (outside local)
```

◎清除 nat translations(只能清除動態項目)

```
#clear ip nat translations *
```

◎全部做完別忘了 show ip nat translations

NAT Dynamic



- 將 NAT 內部 Local IP 與 Global IP 臨時性對應，而這些 Global IP 位址會先定義在 **NAT Pool** (**儲存區**)。 #如果 Local IP 數量超過 Global IP 數量，會有部份 Local IP 沒有家
- 設定 NAT 動態轉址對應 -4 steps
 - ① 定義可用的 NAT 內部 Global IP 到儲存區中
 - ② ~~用 ACL 限制內部網路可使用 NAT 儲存區~~
 - ③ 定義內部網路使用指定 NAT 儲存區
 - ④ 定義 NAT 內部與外部

#其中的 ACL 重點不在 permit/deny 交通或是過濾交通之類的安全設定，而是要用來選擇或指定 interesting traffic(關注的交通)。當關注的交通與 ACL 批配時，就會被拉到 NAT 程序中進行轉換。這是存取清單的一般性用法，它們並非永遠都扮演在介面阻擋交通的角色。

#記得確定 POOL 裡有足夠的位址提供所有內部主機做轉換，否則會無法運作，另外 POOL 名稱的大小寫要一樣不然也無法運作。

• 設定 NAT 動態轉址 (黃底)

指令	說明
NAT(config)#ip nat pool <u>xxx</u> 200.200.200.1 200.200.200.2 netmask 255.255.255.0 考試時叫你 nat 的 ip 是多少，起點最就從多少開始 Netmask 的另一寫法是 prefix-length?	要設定動態 NAT 要先建立 pool(指定 ip 範圍)，指令範例名稱為 xxx，紅字為 ip 起點，綠字為 ip 終點，netmask 後寫遮罩
NAT(config)#access-list <u>n</u> permit IP/網段 wildcard	用 ACL 限制可使用 NAT 的 IP 來源
NAT(config)#ip nat inside/outside source list <u>n</u> pool <u>xxx</u>	設定 n 這張 ACL 套用到 pool xxx
NAT(config)#int ... NAT(config-if)#ip nat inside	NAT(config)#int ... NAT(config-if)#ip nat outside
NAT#show ip nat statistics	查詢 NAT 動態轉址統計內容 查詢 NAT 分配資訊

PAT(Port Address Translations) Configuration



使用 Port 位址解決多對一問題

L4 中有 Port 位址欄位，當電腦開一個視窗，作業系統就會給它一個 Port 號，L4 傳輸層就拿來源 Port 號作為來源位址，而目的 port 位址則為應用程式服務的號碼，比如 http 80、telnet 23，因此 PAT 就是將來源 Port 加入到轉址的 ip 位址中，兩個位址間用冒號隔開，以下表為例：

電腦	私有 IP 位址	公有 IP 位址
PC1	192.168.10.10:1011	200.200.200.1:1011
PC2	192.168.10.11:2011	200.200.200.1:2011
PC3	192.168.10.12:2011	200.200.200.1:2012

• PAT 指令：和 NAT 大致相同，差在第三步後面多一個 overload，表示轉址會帶上 port，或是理解為可以讓 ip 超載。

指令	說明
NAT(config)#ip nat pool <u>xxx ip 起點 ip 終點</u> netmask <u>遮罩</u>	設定 Global IP(大多數環境中只會有一個 IP 即起點=終點，少數會有多個 IP)到 pool xxx 中
NAT(config)#access-list <u>n</u> permit IP/網段 wildcard	用 ACL 限制只有某網段可使用 NAT
NAT(config)#ip nat inside source list <u>n</u> pool <u>xxx overload</u>	將 ACL 套用在 IN 端，並使用 pool xxx，及使用 port 位址

#int ...	#int ...	設定 inside/outside
#ip nat outside	#ip nat inside	

#show ip nat translations 會看到一行 Total translations：其中 extended 就是 PAT

#show ip nat translations 底下有一行 access-list n pool x refCount 數字，表示用 NAT pool 轉址成功的數目

※PAT 多對一簡易寫法

由於大多數PAT的定義就是要一對多，所以可以不用特別做一個只有一筆Global IP的pool，可將NAT Outside的位址作為Global即可，會變成只要寫三段，範例如下：

1. NAT(config)#access-list n permit ip wildcard
2. NAT(config)#ip nat inside source list n interface s0/0/0 overload ←s0/0/0=outside 介面
3. 指定 inside/outside

NAT 簡易驗證



◎檢視基本IP位址轉換資訊

#show ip nat translations

◎另外可以使用 debug ip nat 來驗證 NAT 組態。它的輸出會在每一列 debug 訊息中顯示傳送端位址、轉換、及目的位址。

◎檢視 NAT 組態摘要，並計算作用中(active)的轉換類型數目。並且還會計算現有的 HIT 數 /MISS 數

#show ip nat statics

◎清除 NAT 表格

#clear ip nat translation →要全清的話結尾用*

◎PAT LAB (0519) --多個 inside local 共用一個 inside global IP 但不同 port

R3(config)#int f0/0

R3(config-if)#ip nat outside

R3(config)#int loopback 0

R3(config-if)#ip nat inside

R3(config)#access-list 1 permit 172.16.3.0 0.0.0.255 (不要用 any，有 bug)

R3(config)#ip nat inside source list 1 int f0/0 **overload**

做完 lab 後用 loopback0 ping 看看：

Ping 對方 IP 「source」 + 「loopback IP」 →packettracer 不能用哦抱歉

#還有 show ip nat statistics



NAT Troubleshooting

步驟	檢查方向	使用指令
1	檢查是否有進行 IP 位址轉換	ping、show ip nat translations
2	檢查是否有啟動 NAT	#show ip nat statistics
3	檢查介面是否有宣告 NAT 內部/外部	#show ip nat translations
4	如果是動態 NAT 則檢查 ACL 宣告	#show access-list
5	如果轉址成功卻無法連線則檢查路由	#show ip route
6	如果有些電腦可轉有些不行則檢查 NAT Pool 是否有足夠 IP	#show ip nat statistics

· 每個 NAT 對應會用掉約 160bits 的記憶體，很偶爾的時候會需要限制 NAT 數量，可使用 **#ip nat translation max-entries** 來設定。

· translation timeout：

每當產生一個新的 NAT 項目到 NAT 表時，該項目的計時器就開始計時，計時器的持續時間即 translation timeout。當每次有該項目封包經路由器轉換時，計時器就會重新計時。若計時器逾時，該項目就會從 NAT 表中移除，而相對應的 IP 也會釋放出來。思科預設的轉換逾時為 86400 秒(24 小時)，但可以用 **ip nat translation timeout** 命令來變更。

Switch configuration Advanced -- VTP, Port-security, STP



Vlan 備援與復原

- vlan 資訊不是存在 running config，是存在 flash 中一個叫 **Vlan.dat** 的檔案，show flash: 會看到
- port-vlan 資訊存在 running config。

指令	說明
#copy flash ____	備援/復原 vlan
#copy ____ flash	____=要存的地方，諸多選項參考備援那篇 #更新 vlan 設定後要存檔重開 switch 才會寫入，除非使用下面的 vtp

VTP(Vlan Trunking Protocol)—vlan 主幹通訊協定



- 在一台交換器要建 vlan20 要下一次指令，在一百台交換器要建 vlan20 怎麼辦？
- 使用 vtp 讓 vlan 資訊自動更新(類似動態路由協定放出路由的概念)，只要設一台，其它台會自動同步。

這也是 Cisco 建立的。VTP 的基本目標是要管理交換式互連網路上的所有 VLAN，並且維持他們在網路上的一致性。VTP 可以新增，移除，和重新命名 VLAN—這些資訊會再傳播到 VTP 網域中的其他所有交換器。

下面是 VTP 的一些特性：

- 讓網路上的所有交換器有一致的 VLAN 組態設定
- 在混和式網路上建立 VLAN 主幹，例如乙太網路對 ATM LANE，甚至於 FDDI
- 精確的 VLAN 追蹤和監視
- 動態回報新增的 VLAN 紿 VTP 網域中的所有交換器
- 以隨插即用的方式新增 VLAN

在讓 VTP 管理網路上的 VLAN 之前，必須先建立 VTP 伺服器(可能不需要做這件工作，因所有交換器預設都是 VTP 伺服器模式，但還是要確定有這個伺服器)所有要共享 VLAN 資訊的伺服器都必須使用相同的網域名稱，而且交換器一次只能位於一個網域。因此，基本上一台交換器只能和其他設定在相同 VTP 網域的交換器共享 VTP 網域資訊。如果有多台交換器連結在相同網路上，則可以使用 VTP 網域，但是如果所有的交換器都只屬於同一個 VLAN，那您根本也不需要使用 VTP。記住 VTP 資訊只會透過主幹埠在交換器間傳送。

交換器會宣傳 VTP 管理網域資訊，組態版本編號(revision number)，和所有已知的 VLAN 及特定的參數，此外，還有所謂的 VTP 透明模式(transparent mode)，可以設定交換器透過主幹埠轉送 VTP 資訊，但是不要接收更新或是更新它們的 VLAN 資料庫。

如果怕有使用者偷偷將交換器加入 VTP 網域，可以加上密碼，但是別忘了—每台交換器都必須設定相同的密碼，您可以想像，這會造成多大的管理爭議。

交換器會在 VTP 宣傳中偵測新增的 VLAN，然後準備在主幹埠中一併傳送資訊給這個新定義的 VLAN。更新會以包含總結宣傳的版本編號送出。交換器只要看到較高的版本編號，就知道這是較新的資訊；它就會使用最新的資訊來覆蓋現有的 VLAN 資料庫。

VTP 要在交換器間溝通 VLAN 資訊(VTP 預設啟動)，必須滿足下面 4 個要求：

- VTP 版本必須相同
- 交換器的 VIP 管理網域名稱必須相同
- 其中一台交換器必須設定為 VTP 伺服器
- 視需要設定 VTP 密碼
- 交換器間必須為 Trunk

它並不需要路由器，接下來，我們要更深入了解 VTP 模式和 VTP 的修正。

p.s.VTP 有三種版本 v1, v2, v3，1&2 可相容，差別在 v2 支援 token ring；1&2 只支援一範 vlan id 範圍的傳遞，v3 才支援 vlan id 範圍延伸—ccnp。

• VTP 運作模式

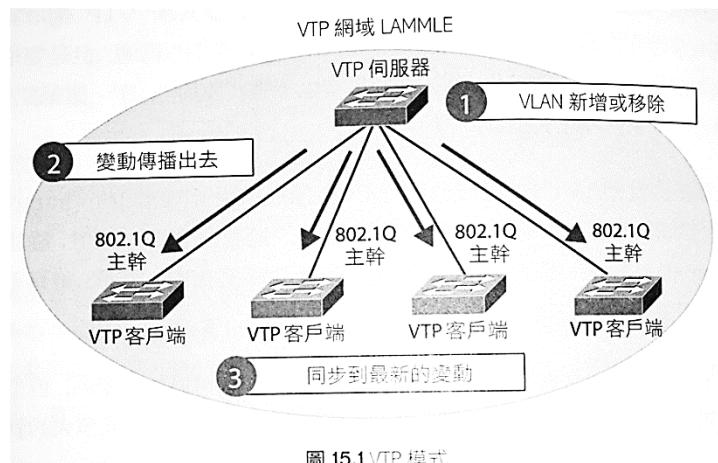


圖 15.1 VTP 模式

● **伺服器** 這是所有 Catalyst 交換器的預設模式。在 VTP 網域中至少要有一台伺服器，以便在傳播 VLAN 資訊。此外這台交換器必須處於伺服器模式，以便在 VTP 網域中建立、新增、和移除 VLAN。VLAN 資訊必須要在伺服器模式下變動，而且在伺服器模式的交換器上所做的任何 VLAN 變動都會傳播到整個 VTP 網域。在 VTP 伺服器模式中，VLAN 組態是存放在交換器的 NVRAM 中。

● **客戶端** 在客戶端模式下的交換器會接收來自 VTP 伺服器的資訊；此外，它們也會接收和轉送更新—此時，它們相當於是 VTP 伺服器的角色。最大差異在於它們不能建立、變動移除 VLAN。此外，在 VTP 伺服器通知客戶端交換器有新的 VLAN，且該 VLAN 已經存在客戶端的 VLAN 資料庫之前，客戶端交換器的埠都無法加入新的 VLAN。從 VTP 伺服器傳送的 VLAN 資訊不是存放在 NVRAM—這很重要，因為它意味著當交換器重新開機或重新載入時，VLAN 的資訊會被刪除。提示：如果您希望某台交換器成為伺服器，首先將它加入客戶端，以便接收所有正確的 VLAN 資訊，然後再將它改成伺服器-這會容易得多。

基本上，VTP 客戶端模式的交換器會轉送 VTP 總結宣傳進行處理。這台交換器會學習 VTP 組態，但不會存放在運行組態中，也不會存放在 NVRAM 中。在 VTP 客戶端模式的交換器只會學習和傳送 VTP 資訊。

● **透通式** 透通模式的交換器不會參與 VTP 網域或是分享它的 VLAN 資料庫，但是它們還是會透過設定的主幹鏈路轉送 VTP 宣傳。它們可以建立、修改、和移除 VLAN，因為它們會保管自己的資料庫—不會與其它的交換器共享，雖然透通模式的 VLAN 資料庫會保存在

NVRAM 中。但其實它只對本機有意義，透通模式的完整目標是要讓遠端交換器能透過不參與相 VLAN 指派的交換器，然後從 VTP 伺服器端接收到 VLAN 資料庫。

· VTP 修剪

VTP 提供方法來設定要保留的頻寬，以減少廣播、多點傳播、和單點傳播的封包量—稱為修剪(pruning)。開啟 VTP 修剪的交換器只會將廣播送到確實需要這項資訊的主幹鏈路上。

它的做法如下：如果 Switch A 並沒有任何埠設定為 VLAN 5，並且有一項廣播是送往 VLAN 5，則該廣播將不會穿越主幹到 Switch A。根據預設，交換器上的 VTP 修剪是關閉的。筆者認為這樣的預設是合理的。當您開啟 VTP 伺服器上的修剪功能時，就相當於對整個網域開啟，根據預設，VLAN 2 到 1001 是可以修剪的，但 VLAN1 因為是管理性 VLAN，所以永遠不可被修剪掉。VTP 第 1 版和第 2 版都有支援 VTP 修剪。(2 版最主要差別在可以自動同步其它交換器為版本 2，除了少數交換器不支援)

使用 **show interface trunk** 命令可以看到，根據預設所有 VLAN 都可以穿越主幹鏈路。

vlan in spanning tree forwarding state and not pruned.

VTP 修剪預設關閉。要對列出來的 VLAN 在整個交換網路上開啟 VTP 修剪功能，只需要一個命令 **switchport trunk pruning vlan x-y**

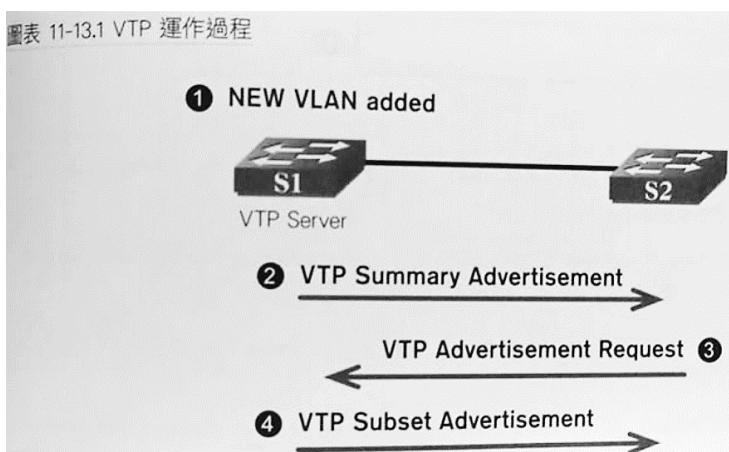
可有效修剪的 VLAN 是 2-1001。延伸範圍的 VLAN(106-4094)則無法被修剪，而無法修剪的 VLAN 可能會收到大量交通。

· 設定 VTP 常用指令、進階 trunk 設定



指令	說明
Switch(config)#vtp mode <u>server</u>	設定 vtp 為 server/client/transparent 模式
Switch(config)#vtp domain <u>oxxx</u>	設定 vtp domain 名稱為 oxxx
Switch(config)#vtp password <u>ccna</u>	設定 vtp 密碼為 ccna
Switch#show vtp password	檢查 vtp password
Switch#show vtp status	查詢 VTP 狀態
VTP 版本、組態版本、本地支援最大 VLAN 數、現有 VLAN 數、VTP 運作模式、VTP 網域、MD5 的 VTP 密碼	
Switch(config-if)#switchport trunk native vlan <u>x</u>	修改 native vlan 為 x
Switch(config-if)#switchport trunk allowed vlan <u>x</u>	只有 vlan x 可通過 trunk
Switch#show int fx/x switchport	查詢 fx/x port 狀態
Switch#show int trunk	查詢 trunk port

#所有思科交換器預設都是 VTP 伺服器；要設定 VTP，要先有網域名稱(或是一台 SERVER 一



台不設)。另外要改變並分送交換器上的任何 VLAN 資訊，就必須處於 VTP Server mode。

- VTP 封包

種類	說明
Summary advertisements(摘要通報)	VTP Server 資料庫異動時由 server 發出 summary 約定給鄰居 client/server 比對，類似 OSPF DBD，每 300 秒或 VLAN 異動時由 VTP Server 送出。
Advertisement request(請求通報)	根據 summary 比對本地 vlan 資料庫，再發送請求通報，類似 OSPF LSR，由 VTP Client/Server 送出
Subset advertisements(更新通報)	根據 request，vtp server 送出更新通報，類似 OSPF LSU。

1. S1 資料庫異動，可能是新增、刪除、修改 VLAN
2. 由 S1 送出 Summary 約定給 S2(server or client)比對 S2 比對 Summary 中的 Domain & Version，Domain 名稱不同則丟棄，Version 若小於本地紀錄表示 S1 的資料比 S2 舊，S2 會直接送出更新通報 Subset 約定給 S1。
3. S2 根據 Summary 比對本地 VLAN 資料庫，然後發送 Advertisement request。
4. S1 根據 S2 的 Advertisement，送出 Subset 約定給 S2，S2 據以更新本地 VLAN 資料庫。

- VTP Domain Name

前面有提到要運作 vtp，彼此的 domain name 要一樣，但在交換器裡預設 domain name 為 null(空值)，可在 show vtp status 看到。

使用 vtp domain xx 指令完成設定。

▲vtp domain name 實在只要設在一台 server 上就好，其它非 transparent 交換器預設 domain name=null 的會被 vtp 更新封包強制更新。

· 驗證 vtp 更新狀態用 show vtp status 時有個 Configuration Revision，代表本地 vlan 更新次數，在同一個 vtp domain 裡的交換器，Revision 版本較大的 Server 會發出更新封包將其它交換器的 Revision 覆蓋。

p.s. 在沒有準備好的情況下把交換器 trunk 在一起可能會破壞原先的 vlan 設定，請小心。

- Revision(VLAN 版本)歸零

為了防止新來的交換器有 Revision 覆蓋的狀況，可以把 Revision 歸零，方法很簡單，直接改變 domain name 就可。(改一次就會歸零，但要和原始網路架接，所以要先改成其它的再改一次回來)

- VTP 密碼設定：沒啥好說的，資安控管用，指令在上面。

- VTP Trouble Shooting Steps—使用指令 show vtp status

1. 檢查交換器是否彼此 trunk
2. Trunk 兩端至少要有一台 server
3. Vtp domain name 要一樣
4. Vtp password 是否設定或設為不同



Switch Port Security & 802.1x --必考

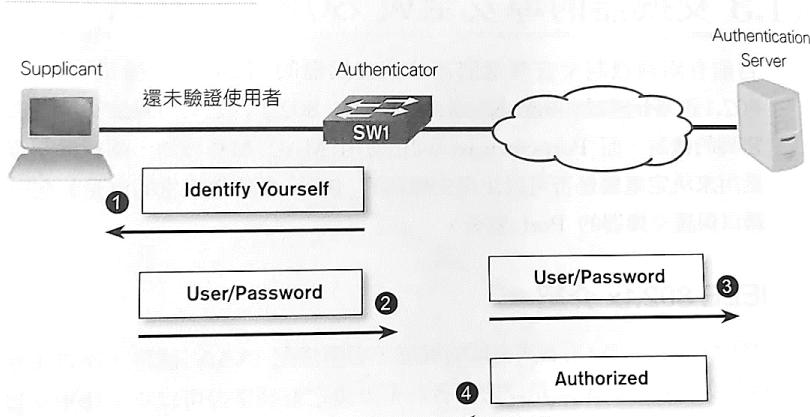
- 目前有兩種機制管理電腦連線到交換器的 port，一種是 IEEE 802.1X，一種是 Port-Security。802.1x 使用帳號密碼，Port-Security 使用 MAC 檢查。

• IEEE 802.1x

驗證帳密，搭配 AAA 認證，不檢查 MAC。交換器啟動 802.1X 後會變成驗證者，只接收 802.1X 的封包。啟動 802.1x 的交換器 port 一定是 access 而非 trunk。

802.1x 的運作流程中，Client 端稱為 supplicant，交換器端稱為 Authenticator，另外還要有一台驗證伺服器(必須使用 AAA Server)，帳密都放在 AAA Server，Client to Authenticator 使用 EAP(Extensible Authentication Protocol)來交換帳密，因此電腦的作業系統必須支援 EAP。

圖表 11-21.3 802.1x 運作流程



★Port Security

要如何阻止別人將一台主機插入交換器的一個埠中—或者更糟的是將一台集線器、交換器、或 AP 插入辦公室的乙太網路插孔呢？根據預設，MAC 會動態的出現在 MAC 轉送/過濾表中。可以使用 Port Security 來阻止攻擊。

Port security 的主要功能是檢查特定 port 下連接的 MAC，設定檢查的 MAC 稱為 Secure MAC。

- 用來限制與認證合法的 MAC
- 可限制單一介面有限的 MAC 數量
- 認證方式—指定特定 MAC(static)、黏貼式(sticky)、混合式
- Port security 只能設定在對 End 端的介面，不要設在對其它 Switch、Router 的介面(會打架)

• 設定 Secure MAC 的三種方式(細節)：

1. Static Secure MAC :

手動輸入安全的 MAC，設定好後資料存在 **Secure MAC Table** 及 **MAC Table** 中，並會寫到 running config。此外 Secure MAC 會永遠存在，除非用指令清或設定 Age-Out 時間。

2. Sticky Secure MAC :

也是動態學習，但需要輸入指令設定，Secure MAC Table 不會寫到 startup config，沒有 wr 的話 reload 就沒了。(有 wr 的話才會留著)

3. Dynamic Secure MAC :

只要啟用 port-security 就會有的預設值，無保護作用，頂多能加個 maximum 限制最多幾個 MAC 通過。

4. Hybrid : 1+2



· Port Security 常用指令

指令	說明
Switch(config-if)#switchport mode access #大多數 Cisco 的交換器在出貨時都是將交換埠開啟在 desirable mode—這表示這些埠在感測到另一部剛連上的交換器時，會主動與它進行主幹通訊 trunk，所以首先要將這些埠從 desirable 改成 access，否則無法設定 port security	☆很重要 設定連接埠為存取模式
Switch(config-if)#switchport port-security Switch(config-if)#switchport port-security mac-address <u>MAC</u> ----- <u>sticky</u>	啟動 port-security 設定 Static-secure(對應 MAC) 設定 Sticky-secure
Switch(config-if)#switchport port-security maximum <u>x</u>	設定 secure-MAC 的最大數量 #沒設定的話預設值為 1
Switch(config-if)#switchport port-security violation <u>shutdown</u> Switch(config)#errdisable recovery cause psecure -violation	遇到違規 MAC 的動作，有三種 當 Port security 出現 errordisable 則自動復原(至少要等 30 秒)
Switch(config)#errdisable recovery interval 30	如果 30 秒內無發生違反行為則自動復原
Switch#show mac-address-table <u>count</u>	查詢交換器 MAC Table
Switch#clear mac-address-table	清除交換器 MAC Table
Switch#show port-security	查詢 port-security 設定
Switch#show port-security address	查詢 Secure MAC Table
Switch#clear port-security all	清除 Secure MAC Table
Switch#show port-security int fx/x	查詢該 port 的 port-security 設定
Switch#show processes cpu	看 cpu 使用狀況
Switch#show interface status	看 interface 的狀態(比如顯示 err-disabled 等)

· Port Security Violation



圖表 11-28 違反安全 MAC 處理的三種模式				
違規模式	轉送流量	產生 Syslog	違規計數器	關閉 port
保護(Protect)	No	No	No	No
限制(Restrict)	No	Yes	Yes	No
關閉(Shutdown)	No	Yes	Yes	Yes

- Protect：將未經認證(未知)或超過允許數量的封包丟棄，直到移除足夠的 Security MAC，降到低於最大值為止。
- Restrict：也會丟棄封包，並且會發送安全違規通知，即交換器發出 SNMP trap、syslog 訊息記入日誌以及違規計數器次數增加(Secure Violation Count)。
- Shutdown：預設模式，此模式下，介面會變為 error-disabled 狀態，並關閉連接埠 LED 燈

號，也會傳送 SNMP trap，遞增違規計數器並發送安全違規通知。

#當介面處在 error-disabled 狀態下直接 no shutdown 是沒用的，因為介面會假死，要先 shutdown 再 no shutdown 才會復活。

#所謂的假死，準確來說，第一次 shutdown 其實是關閉 error-disable 功能，這樣講比較正確。

※在 Secure MAC Table 全滿的狀態下如果要調降 maximum 是不行的，必須先 clear 掉再調降。

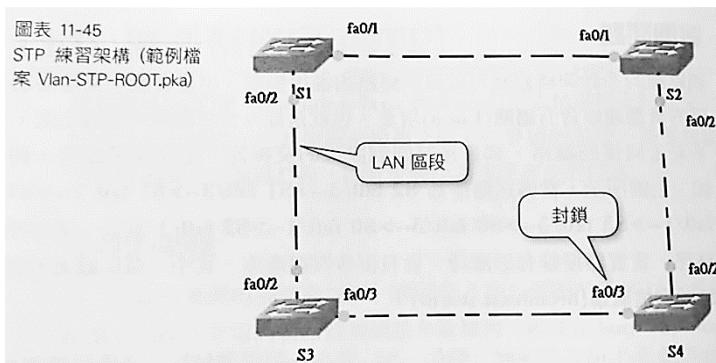
測試 port security 步驟

1. 當介面完成 Port Security 設定後，先到 Switch show run 確定 mac address 設定已被寫入。
2. 修改 Router mac address，進 Router 的對應 interface 修改 mac
3. 確認 Router 介面 mac—show interface fx/x
4. 確認 Switch 介面—show interface fx/x(應該要出現 error-diable 並且實際介面無燈號)



Spanning Tree Protocol(STP)

- 主要用在 Layer2，邏輯上(Logically)防止交換器間實體連線迴圈(Loop)，即交換器間允許迴圈存在，但利用擴展樹協定擋掉迴圈。使用擴展樹演算法(Spanning-Tree Algorithm, STA)建立拓樸資料庫，然後搜尋並關閉冗餘鏈路。
- Redundant Topology(多餘架構)**
在實務網路環境中，網路都會做備援，常用的備援機制就是多餘架構，可以多買一台設備或多架一條線路。
- Loop(迴圈)**
多餘架構在提供備援機制的同時也會產生迴圈，即收到自己發出的封包。迴圈問題最嚴重的狀況是 Broadcast Storm 廣播風暴，其它的問題還有多重訊框複本、MAC 表劇烈變動等。



常用 STP 指令

指令	說明
Switch(config)#spanning-tree vlan <u>x</u> priority <u>12345</u>	設定該交換器在 vlan x 的 BID Priority 為 12345
Switch(config)#spanning-tree vlan <u>x</u> root primary	設定該交換器在 vlan x 為 root Switch
Switch(config)#spanning-tree portfast default	設定該交換器所有介面啟用 Portfast
Switch(config)#int fx/x	特定介面啟用 Portfast
Switch(config-if)#spanning-tree portfast	
Switch#show spanning-tree	查詢 STP 執行狀況
Switch#show spanning-tree vlan x	只查詢 vlan x 的 STP 狀況 在 Root Bridge 上會直接顯示“This bridge is the root”

STP 術語

- 根橋接器(root bridge)** 即是有最低橋接器 ID 的那台。STP 網路中的交換器會選舉出根橋接器，網路中所有決定—例如哪個埠要凍結，哪個埠要設在轉送模式—都是從根橋接器的觀點來進行的。一旦選舉出根橋接器後，所有其他橋接器都必須建立通往它的最佳路徑，而有最佳路徑的通訊埠就稱為根埠。
- 非根橋接器** 根橋接器以外的所有橋接器。非根橋接器會與所有其他橋接器交換 BPDU，並且更新所有交換器上的 STP 拓樸資料庫，這樣可以防範迴圈，並且有助於因應鏈路的故障。

- **BPDU** (Bridge Protocol Data Unit) 每台交換器會比較它們透過 BPDU 傳送給鄰居、以及從鄰居收到的參數。BPDU 裡面放的是橋接器 ID。
- **橋接器 ID** STP 用橋接器 ID 來追蹤網路中的所有交換器。它是由橋接器的優先序(所有 Cisco 交換器上的預設是 32768)與 MAC 共同決定的。可以藉由將特定交換器的優先序設定為低於預設值，強制該台裝置成為根橋接器。
- **埠成本** 當兩部交換器之間有多條鏈路時，以埠成本來決定最佳路徑。成本由頻寬所決定。
- **路徑成本** 交換器可能有多條路徑通往根橋接器。將個別路徑上遇到的埠成本相加可得到該路徑的成本。

橋接器埠的角色

- **根埠(root port)** 若有多條鏈路到 RB，則可以藉由檢查每條鏈路的頻寬來找出埠成本。最低成本埠就是根埠，如果有多條鏈路達到相同裝置，則使用連到上游交換器中最小埠號者，RB 自己沒有 RP，但其他所有交換器都必須且只能有 1 個根埠。
- **委任埠(designated port)** 具有通往特定網段之最低成本的埠。DP 會被標示成轉送埠，且每個網段只能有一個轉送埠。
- **非委任埠** 成本比 DP 高的埠，決定完 RP、DP 後剩下來的埠。NDP 會被放入凍結模式 (blocking mode)或丟棄模式—NDP 不會是轉送埠。
- **轉送埠(forwarding port)** 可轉送訊框，可以是 RP 或 DP。
- **凍結埠(blocked port)** 不會轉送訊框，用來預防迴圈；但仍會聆聽 BPDU 訊框，並且丟棄所有訊框。
- **替代埠(alternate port)** 對應到 802.1d 的凍結狀態，也是 802.1w(Cisco 快速擴展樹協定)所使用的名詞，當 LAN 網段上連接不只一台交換器，且其中一台交換器持有 DP 時，另一台交換器連接該網段的埠即是替代埠。(備援埠在別人身上)
- **備援埠(backup port)** 對應到 802.1d 的凍結狀態，也是 802.1w 所使用的名詞。當交換器有一個連到 LAN 網段上的埠是 DP 時，若有另一個連到同網段的埠就是備援埠。(備援埠在自己身上)

擴展樹的狀態

將主機插入交換器埠後：

- 1.燈號變橙，此時主機還沒有從伺服器取得 DHCP 位址。
- 2.一分鐘後再變綠，這是 STA 透過不同埠的狀態轉換，來確認新加入的裝置沒有造成迴圈。
#STP 為了不讓網路產生迴圈，故而需讓主機逾時。

執行 IEEE 802.1d STP 之交換器，其埠會經歷 5 種狀態：

- **關閉(disabled)** 處於管理性關閉狀態的埠，不會參與訊框轉送或 STP。簡言之就是沒有運作。
- **凍結(blocking)** 不轉送訊框，只聆聽 BPDU。目的是要防止使用會造成迴圈的路徑。交換器開機時所有埠都是預設凍結。

- **聆聽(listening)** 聆聽 BPDU，以便在傳送訊框前確定網路中沒有迴圈，聆聽狀態只是準備傳送訊框，尚未建立 MAC 表。
- **學習(learning)** 聆聽 BPDU，並學習交換式網路中所有路徑。已建立 MAC 表，未轉送訊框。
轉送延遲—從聆聽到學習，或是從學習到轉送的時間：預設 15 秒，可用 show spanning-tree 查詢。
- **轉送(forwarding)** 接收和傳送該埠上的所有訊框。若該埠在學習結束後是 RP、DP，就會進入轉送。

#交換器只會在學習和轉送模式下產生 MAC 表。

#交換埠最後通常是凍結或轉送狀態。

收斂(convergence)

交換器上所有埠都是轉送或凍結模式時，就稱為收斂(convergence)。收斂完成才會開始轉送資料。收斂過後所有裝置都會有相符的資料庫。

原始的 STP(802.1d)預設需要 50 秒才能完成收斂，大型網路中可以調整這些計時器，不過用其它 STP 版本會更好。

鏈路成本

埠成本是根據鏈路頻寬算出，即單一鏈路的成本。路徑成本則是通到根橋接器的各埠成本總合。

速度	成本	STP 中用埠成本來算出 RP。必背
10Mb/s	100	
100Mb/s	19	
1Gb/s	4	
10Gb/s	2	

· STP 運作步驟

精簡版—

- ① 先選舉出 RB
- ② 在每台 Non RB 上選出 RP
- ③ 在每個 Segment 選出 DP
- ④ 其它介面 blocking

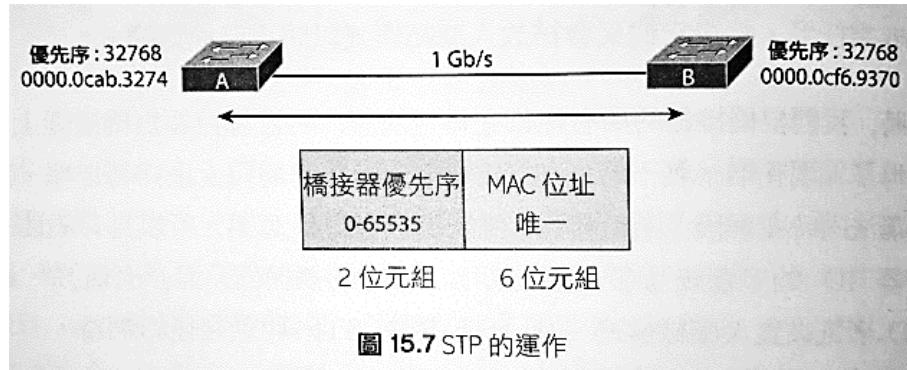


· STP 運作步驟

詳細版—

選擇 Root Bridge

前略，橋接器 ID 長度為 8 個位元組，包括裝置的優先序與 MAC 位址，如圖所示。IEEE 802.1d 之預設優先序為 32768。



如果兩部交換器優先序一樣，則比較 MAC 誰最低。上圖中的兩台交換器優先序同為預設值，所以用 MAC 來判斷。交換器 A 成為根橋接器。

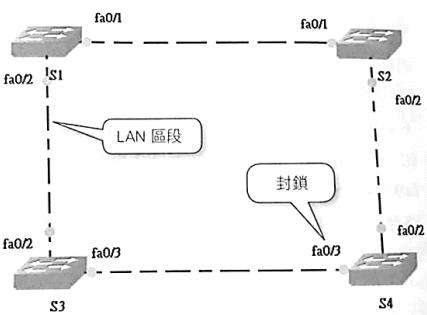
在選出根橋接器之前，橋接器每 2 秒就會從所有作用中的埠送出 BPDU，為根橋接器的選舉依據。

選擇 RP(範例)—先比 path cost 再比 BID 最後比 PORT-PRIORITY

先看 S3 中 f0/3 到 Root Bridge 的路徑 $S3 \rightarrow S4 \rightarrow S2 \rightarrow S1$ ，每前每個路徑的速度為 100M(Fast Ethernet)，所以 f0/3 的 Path Cost=19+19+19=57，Port Cost=19；同樣的算法，S3 的 f0/2 Path Cost=19，Port Cost=19，故 f0/2 選為 RP。

p.s.若將 F0/2 改為 speed 10 則其 Port Cost=100，Path Cost=100

圖表 11-45
STP 練習架構 (範例檔案 Vlan-STP-ROOT.pka)



路徑成本相同

當一台交換器到達 Root Bridge 的多個埠 Path Cost 相同時，要比較該埠 Upstream 的交換器的 BID & Port ID。以 S4 為例，f0/2 及 f0/3 的路徑成本相同，再來比較往上接的交換器 BID， $f0/2 \rightarrow S2$, $f0/3 \rightarrow S3$ ，比較 S2 & S3 的 BID，假如 S2 的 BID/MAC 較小，則 f0/2 選為 RP。

比較 Port-priority

當一台交換器同時兩埠直連到另一台交換器時，Path Cost 相同、Upstream BID 也相同時，就只能比往上接的 Port-priority，Port-priority 以 Port ID 值比較，故對面是 f0/1 及 f0/2 的狀況下，會以對 f0/1 的當 RP。

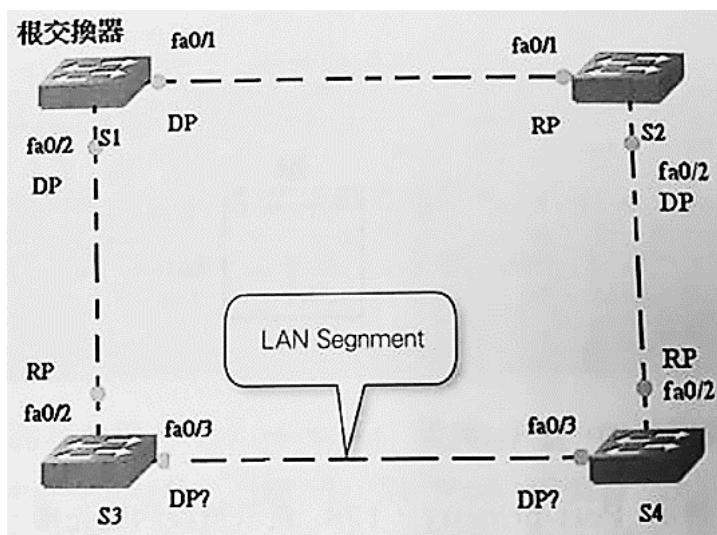
※Port-priority 預設值為 128，可調整。用 show spanning-tree 會看到，格式為 128.x，x 為 Port-ID

選擇 DP

原則為每個 segment 中只有一個 DP，同 LAN 區段內交換器間到達根交換器的最小路徑成本，較小者為 DP，若路徑成本相同則為 DP 為 BID 較小者。

範例：

先把除了 RP 之外的連接埠全部設為 DP，又一個 segment 只有一個 DP，所以 RP 的對面一定是 DP。最後剩下 LAN 兩邊都是 DP 再來做比較。



如圖中的 S3 f0/3&S4 f0/3

首先兩個埠比較 Path Cost，S3 有 19 & 57，S4 有兩個 38。19 比 38 小，故 S3 f0/3 為 DP，S4 f0/3 為 NDP。

※NDP 有很多，但每台 Non-Root 交換器只有一個 RP，以及每個 Segment 只有一個 DP。

※可將 DP 視為送出 BPDU 的埠，而 RP 則是接收 BPDU 的埠。



STP 的類型

- IEEE 802.1d 橋接和 STP 的最初標準，非常緩慢，只需要很少的橋接器資源。也稱為一般性擴展樹(Common Spanning Tree，CST/STP)。
- PVST+ Cisco 對 STP 的專屬改良，對每個 VLAN 提供獨立的 802.1 d。和 CST 協定一樣慢，但是可以有多個根橋接器。效率較高，耗用資源比 CST/STP 多
- IEEE 802.1w 也稱為快速擴展樹協定(Rapid Spanning Tree Protocol,RSTP)。改良了 BPDU 交換，但是每個網路仍舊只有一台根橋接器。使用的資源比 CST 多，比 PVST+少。
- Rapid PVST+ Cisco 的 RSTP，同樣使用 PVST+，並在每個 VLAN 提供個別的 802.1w。收斂最快、最佳化的交通流量，以及使用最多的 CPU 和記憶體。

STP

在有冗餘鏈路的交換式網路中執行 STP，會選出根橋接器—即所有 VLAN 的根，且所有交換器都會建立對它的單一路徑。(下圖範例)

SW-A 是所有 VLAN 的根橋接器，所有交換器都必須建立對它的單一路徑—對部份 VLAN 並非最佳路徑。

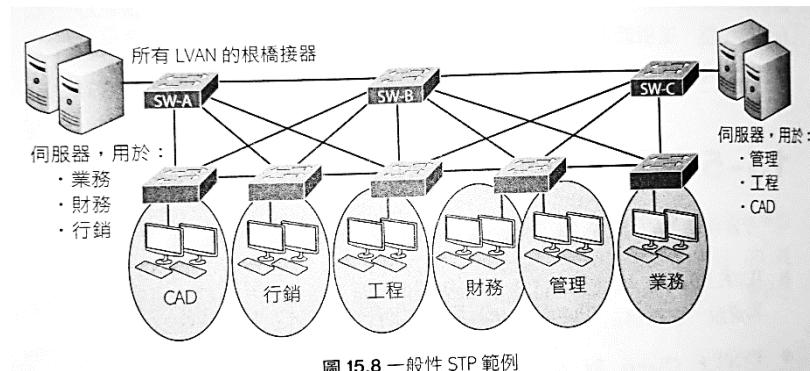


圖 15.8 一般性 STP 範例

PVST+

Cisco 對 CST 的改良，對每個 VLAN 提供獨立 STP，收斂時間預設為 50 秒。Cisco 交換器預設執行 PVST+。藉由將根橋接器設定在每個 VLAN 的中心，STP 可以對每個 VLAN 的交通做最佳化。(下圖範例)

PVST+收斂跟 802.1d 的 CST 類似，差別在 PVST+的收斂是以 VLAN 為單位。

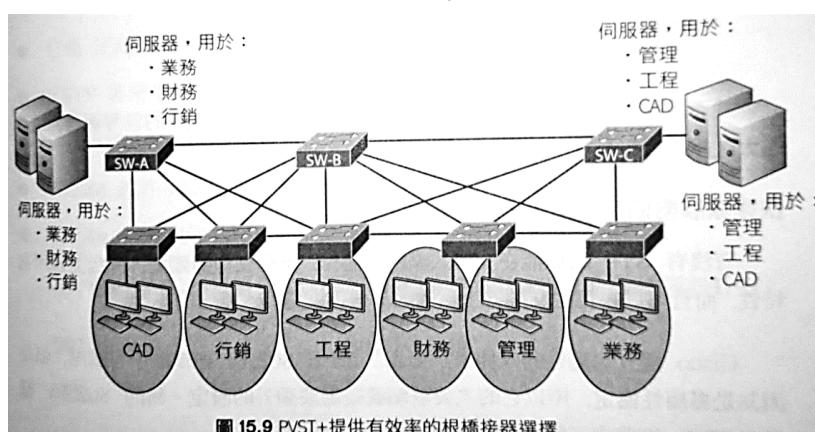


圖 15.9 PVST+ 提供有效率的根橋接器選擇

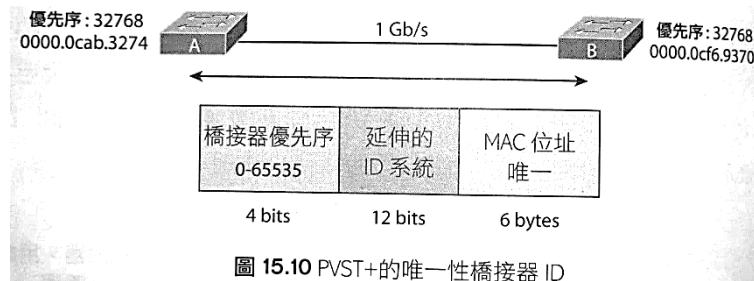


圖 15.10 PVST+的唯一性橋接器 ID

要讓 PVST+運作，須在 BPDU 中加入一個欄位以存放延伸的系統 ID，讓 PVST+可以針對每個 STP 設定根橋接器。橋接器 ID 會變小—只有 4 個位元—所以橋接器的優先序是以 4096 為單位遞增。延伸的系統 ID(VLAN ID)有 12 位元，可以透過 **show spanning-tree** 命令檢視。

RSTP

CST 的進化版，有更快的收斂速度。但仍然只允許單一的 STP。當建立 802.1w 時，維持了向後相容性(能和 802.1d 兼容)。

△RSTP 不需要 CST 的延遲計時器。

△RSTP 能夠以埠為基礎回復為 CST，以便與傳統交換器互通。

△RSTP 定義了 5 种端口角色 (STP 只有 3 种)：禁用端口 (Disabled Port)、RP、DP、为支持 RSTP 的快速特性规定的替代端口 (Alternate Port) 和备份端口 (Backup Port)

RPVST+

Cisco 對 RSTP 的改良，提供每個 VLAN 獨立的 RSTP。需要最高的 CPU 和記憶體。

#Cisco 文件可能會使用 STP 802.1d 和 RSTP 802.1w，但是其實是指 PVST+/RPVST+

802.1d V.S. 802.1w :

STP 狀態 RSTP 狀態

關閉	丟棄
凍結	丟棄
聆聽	丟棄
學習	學習
轉送	轉送

各種 STP 協定	版本	耗費資源	收斂速度	STP 的數目
STP	IEEE 802.1D	低	慢	一個
PVST	Cisco	高	慢	每個 Vlan 一個
RSTP	IEEE 802.1w	中	快	一個
Rapid PVST	Cisco	很高	快	每個 Vlan 一個

#RSTP 只會經歷丟棄、學習、和轉送。

MSTP

MSTP(多重擴展樹協定)也就是 IEEE 802.1s，提供跟 RSTP 一樣快速的收斂，但是藉由將多個有相同交通流需要的 VLAN 對映到相同的 STP，它可以減少所需的 STP 數量。它可以建立 VLAN 集合，也就是在 **STP 上執行的 STP**。--CCNA 會考



修改、確認橋接器 ID / 手動調整 STP

Root Bridge 要求性能較高，但實際上不一定會將性能高的交換器作為 Root Bridge，此時就需要手動設定。

· 常用指令

指令	說明
Switch(config)#spanning-tree vlan <u>x</u> priority <u>y</u> #優先序的值可從 0-61440，以 4096 為單位遞增。將優先序設為 0 代表和其它橋接器 id 設為 0 的交換器相比，只要該交換器 MAC 較低，它就一定會成為 root。	將該交換器在 vlan x 的 priority 設為 y，y 必須為 4096 倍數
Switch(config)#spanning-tree vlan <u>x</u> root primary/secondary #上面那個指令的自動化寫法，該指令不會改變 priority	將該交換器在 vlan x 設為 Root Bridge(primary)，或是第二順位(備援) Root Bridge(secondary)
Switch#show spanning-tree <u>vlan x</u> —只顯示特定 vlan 的 Switch#show spanning-tree summary (這個是總表)	查詢 STP 的所有資訊—Priority, Root ID, BID, Port role, Status, Cost, Type
#show spanning-tree summary	查詢每個 STP 的連接埠狀態、執行的 STP 種類。
Switch(config)#spanning-tree mode stp/pvst/rapid-stp/rapid-pvst	更改 STP 類型

p.s.#show spanning tree 底下的 BID Priority 會是 Priority+Vlan ID，比如預設為 32768，vlan 1，所以 Priority=32769

#注意 show spanning-tree 底下的 **sys-id-ext x**(給 vlan x)，這是在 BPDU 的 12 位元 PVST+欄位，用來運送多重 VLAN 的資訊。優先序與 sys-id-ext 相加，以得到 vlan 的真正優先序。(管他是什麼鬼，反正會考就對了)

※802.1D 的 STP 中有三種計時器，預設 Hello Time=2sec、Max age=20sec、Forward delay=15sec，使用 show spanning-tree 會顯示三種計時器，在接收與學習狀態都需要 forward delay 15 秒，故運作一次 STP 約需 30 秒時間，三種計時器為 CCNP 內容。

#show spanning-tree + show cdp neighbors，可以根據 RP 找到根橋接器。

STP Lab

1. 完成下圖設定後 show spanning tree，看看哪個會變成 Root Bridge

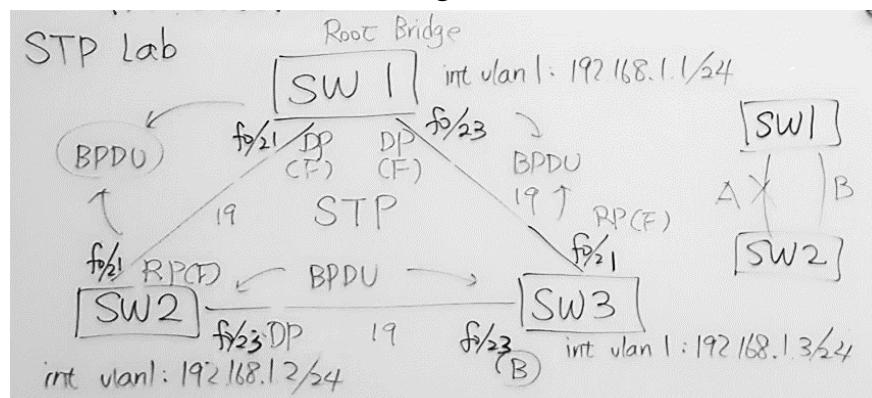
Root Bridge 特徵：接口全為 DP

2. 手動指定 Root Bridge：

SW1(config)#spanning-tree vlan 1
root primary

3. 把其中一條 segment 切斷試試看它的備援狀況

4.#show spanning-tree

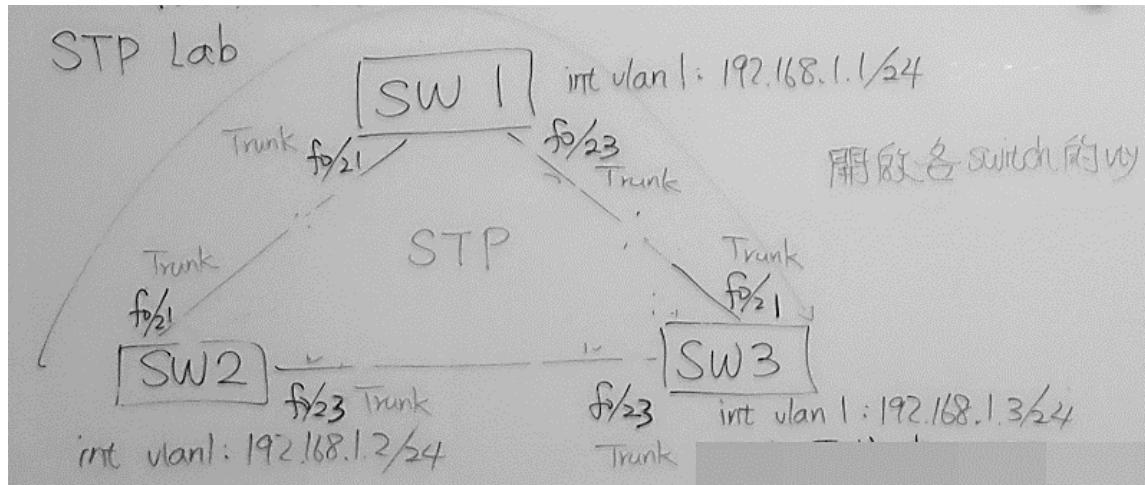


交換器負載平衡

以資料流量觀察，三個 Vlan 流量會集中在 Root Bridge 上，要修正這種狀況就要讓每個 vlan 的 Root Bridge 都不同。

設定方式如同前述的手動調整各 switch 對應各 vlan，將不同 Vlan 的 Root Bridge 設為 root primary 就可以了，要做備援的話再在另一台設 root secondary。

PVST Lab



① Switch 設定同 STP Lab

② 要求：手動設定各 Switch 的 Root Bridge 等級(Primary、Secondary 以及 Priority 值)

SW1 為 vlan1 的 Root Bridge

SW2 為 vlan2 的 Root Bridge (vlan2 192.168.2.0 /24)

SW3 為 vlan3 的 Root Bridge (vlan3 192.168.3.0 /24)

SW2 為 vlan1 的備用 Root

SW3 為 vlan2 的備用 Root

SW1 為 vlan3 的備用 Root

③ 提示：不要忘記一個 Switch 多 vlan 時要用 trunk



PortFast

如果可以確定連到交換埠上的其他裝置無 STP 也不會迴圈，就可以使用 Cisco 802.1d PortFast。使用 portfast 會立即從凍結進入轉送，節省收斂時間(STP 檢查一次至少 30 秒)。

範例：圖 15.19 的網路有 3 台交換器，每台都有條主幹連到其他兩台。S1 交換器還連結 1 台主機和 1 台伺服器。

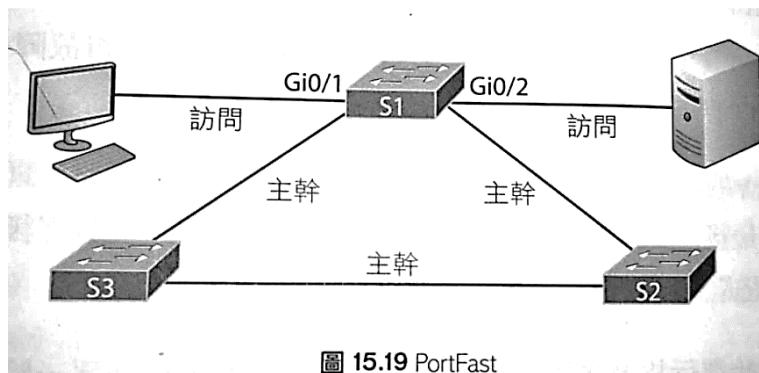


圖 15.19 PortFast

• PortFast 指令

指令	說明
Switch(config)#spanning-tree portfast default	該交換器上的所有埠都啟動 PortFast
Switch(config)#int range fx/x-y Switch(config-if)#spanning-tree portfast	將 fx/x 啟動 PortFast
Switch#show spanning-tree interface fx/x portfast	檢視 Portfast 及 BPDUguard 設定



BPDU Guard

如果在交換器埠開啟 portfast，最好也開啟 bpdu guard。

為了防止 portfast 介面接上交換器的意外，用 BPDU Guard 來避免產生迴圈。(Portfast 的埠一樣會送出 BPDU)

※停用 STP 功能在 conf 下或是 int 下 **no spanning-tree vlan x**

當開啟 PortFast 的交換器埠收到 BPDU 時，它會將該埠置入 error-disable 狀態，有效地防止任何人意外地將一台交換器或集線器連到設定了 PortFast 的交換器埠。這是為了防止網路嚴重阻滯，或甚至完全當掉。

p.s. Error-disable 狀態要重新啟動要先 sh 再 no sh

指令	說明
Switch(config)#spanning-tree portfast bpduguard default	啟動 portfast 埠的 BPDU Guard 功能(整體設定)
Switch(config-if)#spanning-tree bpduguard enable	在 fx/x 啟動 BPDU Guard(特定介面)
Switch(config-if)#spanning-tree bpduguard disable	在 fx/x 停用 BPDU Guard #注意這裡不是用 no
Switch#show spanning-tree interface fx/x portfast	檢視 Portfast 及 BPDUguard 設定

補充資料

- 備援機制：FT > HA > Redundant
 - BPDU Filter：BPDU guard 的進化版，有兩種模式—
 - #SW(config): 在 Config 底下設定，只要任一 port 收到 BPDU，將禁用其 Portfast 及 BPDU filter，並自動將 port 改回 STP 狀態，開始 listen & learn。
 - #SW(config-if): 對單一 portfast 的 port 啟用，此 port 將不發送 BPDU 及忽略所有收到的 BPDU。
- ※BPDU filter 和 BPDU guard 同時存在，優先使用 filter。
- BPDU Filter 指令：將 bpduguard 九個字換成 bpdufilter，用法同 bpduguard。



Ether Channel & FHRP—交換器&路由器備援

在交換器間包含冗餘鏈路的設計中，STP 會將或多個埠置於凍結模式。此外，動態路由協定會將冗餘鏈路視為個別鏈路，增加遶送上的負擔。

Ether Channel(Cisco)可將兩交換器間多條實體線路綑綁(bundle)為一條虛擬線路，增加頻寬並備援。如下圖，兩條 fast ethernet 實體連線綑綁後，等於一條 200Mbps 的頻寬。

EtherChannel 開啟並運作之後，L2 STP 與 L3 遲送協定會將綁在一起的鏈路視為一條—STP 不會進行凍結，遶送協定則只看到一條鏈路，只會形成單一的緊鄰關係。

Ether Channel 可以做到負載平衡的功能。

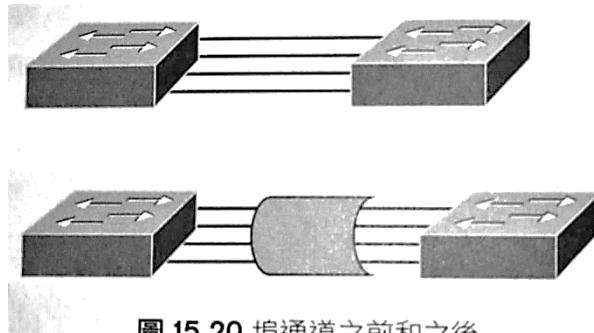


圖 15.20 埠通道之前和之後

Ether channel 的 Cisco 的版本稱為 PAgP(埠聚合協定，Port Aggregation Protocol)，IEEE 802.3ad 標準則稱為 LACP(鏈路聚合控制協定，Link Aggregation Control Protocol)。

Ether Channel 可將交換器間最多 8 個埠綁一起。但埠必須具有相同的速度、雙工、VLAN。
#同一組 Ether Channel 中不能混和不同的介面類型和組態。

一些術語：

- **埠通道技術(Port channeling)** 將 2 台交換器間最多 8 個埠組合成單一邏輯鏈路，以取得更多頻寬和彈性。
- **EtherChannel** Cisco 對埠通道技術的專用名詞。
- **PAgP** Cisco 專屬協定，用來自動建立 EtherChannel 鏈路。群組中的鏈路都必須符合相同的參數(速度、多工、VLAN 資訊)。 EtherChannel 會被當作單一埠加入 STP，PAgP 則每 30 秒傳送封包來管理鏈路的一致性、新增、和故障。
- **LACP(802.3ad)** 與 PAgP 目的相同，但可以在各牌交換器中運作。
- **channel-group** 用來將指定介面加到 EtherChannel 中的指令。
- **Interface port-channel** 建立群組介面的指令。

p.s. 一個 EtherChannel 中的一個 Port-channel 只能連接兩個不同的交換器，不能一個 port-channel 對多台交換器

EtherChannel Configuration

設定類似 DTP，分為手動及動態協商，手動就是直接將 port 指定運作 EtherChannel，但無法知道對應 port 狀態；動態協商有 **PAgP**(Port Aggregation Protocol)及 **LACP**(Link Aggregation Control Protocol)兩種，兩者都是要協商 port 為 EtherChannel。

- **目的：**增加頻寬、負載平衡(Load Balance)、穩定性及安全性、備援(Reudndant)

• 要捆綁為同一 EtherChannel 的 Port 要注意的事項：

Speed、Duplex、Port Access/Trunk、Native Vlan 要一樣

PAgP

PAgP 有三個參數，和 DTP 一樣，因為 DTP 也是思科開發的協定。

1. On :

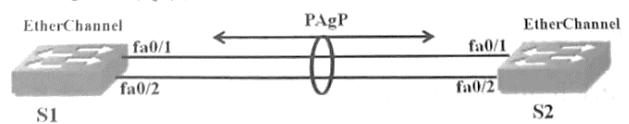
手動設定 EtherChannel，對應埠也要手動設定才能建立成功。

2. Auto :

被動協商，兩邊都被動的話就不會建立。

3. Desirable :

主動協商，不管另一邊設什麼都可以建立成功



Channel 能否建立	On	Desirable	Auto
On	YES	NO	NO
Desirable	NO	YES	YES
Auto	NO	YES	NO

LACP

只要網路設備有支援就可以使用，三個協商參數。

p.s. 兩邊交換器必須使用相同協商協定，不可 LACP 對 PAgP

1. On :

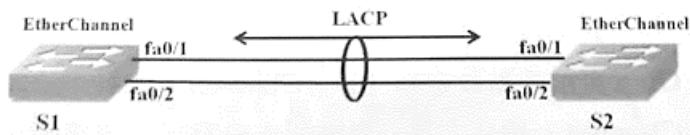
手動設定。

2. Passive :

被動協商。

3. Active :

主動協商。



Channel 能否建立	On	Active	Passive
On	YES	NO	NO
Active	NO	YES	YES
Passive	NO	YES	NO

▲EtherChannel 常用指令

指令	說明
Switch(config-if-range)#switchport trunk encapsulation dot1q/isl	在設定 EtherChannel 之前，要先為介面建立 trunk
Switch(config-if-range)#switchport mode trunk	
Switch(config-if-range)#channel-group <u>z</u> mode <u>active</u> p.s. 以後要進 port-channel 的指令為 int po <u>x</u>	設定要綁繩的介面在 channel-group z 中，並使用 LACP active 協商 使用 LACP 可用 active/passive 使用 PAgP 可用 auto/desirable 命令
Switch(config)#int port-channel <u>z</u> Switch(config-if)#switchport trunk encapsulation dot1q Switch(config-if)#switchport mode trunk Switch(config-if)#switchport mode trunk allowed vlan a,b,c	建立通道介面，並在該虛擬介面下設定 trunk 和 vlan(同實體介面)
Switch#show etherchannel port-channel	查詢埠通道介面的資訊
Switch#show etherchannel summary	查詢每個 Channel-group 狀態

Switch#show ip int brief	查詢 Port-Channel 執行狀態
Switch(config)#port-channel load-balance ?	修改交換器 EtherChannel 負載平衡模式 #注意 L3 交換器才能使用 ip 相關功能
Switch#show etherchannel load-balance	查詢交換器 EtherChannel 負載平衡模式

· Channel-group 狀態說明

```
S2#show etherchannel summary
Flags: D - down P - in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
----+-----+-----+-----+
1 Po1 (SU) LACP Fa0/1 (P) Fa0/2 (P)
```

Port-channel :

Po1 代表 Port-Channel 1

S 代表為 L2 EtherChannel ,

U 代表為 in use 。

Ports : P 為 in port-channel(使用於 Po1 中)

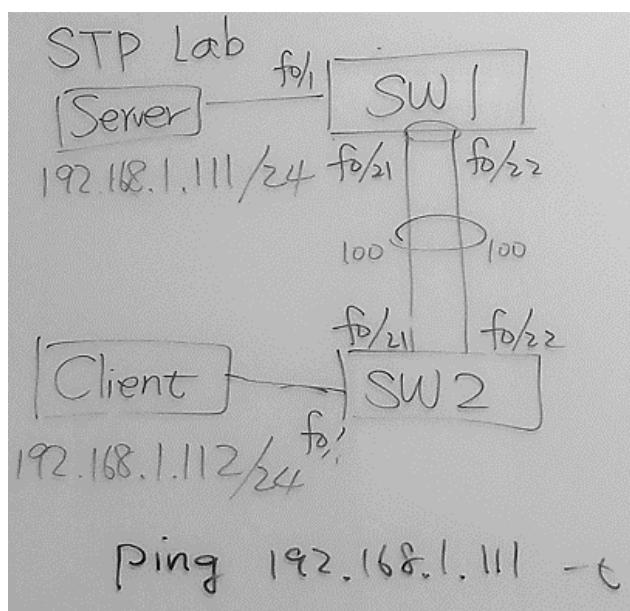
L3 EtherChannel

將交換器連到路由器上多個埠的時候，就可以使用 L3 EtherChannel，將整束的 IP 位址設定到邏輯埠通道介面上。

Router(config)#int port-channel x

Router(config)#int range fx/x-y

Router(config-if-range)#channel-group x → 實體介面不需設 ip



Ether Channel Lab

① 設定下圖架構，且 Server 可達 Client

② 設定 EtherChannel 為 LACP Protocol

```

Switch2(config)#int range f0/21-22
Switch2(config-if-range)#channel-group 1 mode active
Switch2(config)#int port-channel 1
Switch2(config)#switchport trunk encapsulation dot1q
Switch2(config)#switchport mode trunk
※這個 Lab 配合 Filezilla 傳檔案來觀察

```

檢視 ether channel 狀態

Switch2(config)#show etherchannel summary

Server 端會顯示

Group	Port-channel	Protocol	Ports
1	Po1(SD)	LACP	Fa0/21(I) Fa0/22(I)

Client 端會顯示

Group	Port-channel	Protocol	Ports
1	Po1(SU)	LACP	Fa0/21(P) Fa0/22(P)

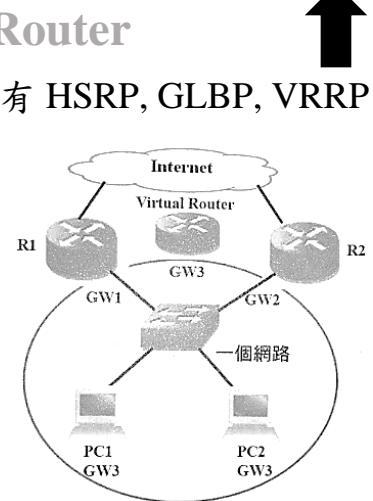
重點在 SUPP，才會是通的

FHRP(First Hop Redundancy Protocol) on Router

Default Gateway 備援機制，讓一個網路有多個 GW，GW 備援協定有 HSRP, GLBP, VRRP 三種。

沒有 FHRP 的狀態下，其中一條 GW 斷掉，必須手動設定另一條 GW。

(範例)R1 與 R2 合成一個 Virtual Router，該虛擬路由器有虛擬 IP & MAC，而電腦的 GW 設為虛擬路由器 IP，虛擬 MAC 位址則是在主機送出 ARP 請求時回傳的位址。由於虛擬路由器由 R1 及 R2 共同負責，故只要其中一個活著電腦就可透過 GW 連線。



決定由哪台實體路由器轉送交通、哪台備援，是冗餘協定的主要功用，即使作用中的路由器故障，主機也不用改變預設閘道。

#容錯提供裝置故障時持續運作的能力，而負載平衡則會將工作分散在多台裝置之間。

常用冗餘協定

- 热备援路由器協定(HSRP) Cisco 專屬，提供冗餘閘道，沒有負載平衡。可將多台路由器設定為備援群組，共享 IP 和 MAC。當使用虛擬 IP 和 MAC 後，就可在實際作用中的路由器故障時，進行位址置換。

利用 HSRP 負載平衡—透過 TRUNK，使用多個 VLAN，指定特定路由器作用在特定 VLAN。這當然不是真正的負載平衡，而且也不如使用 GLBP 那麼實在。

- **虛擬路由器冗餘協定(VRRP)** 提供冗餘閘道，沒有負載平衡，**VRRP** 是開放標準協定。
- **閘道負載平衡協定(GLBP)** 提供負載平衡，每個轉送群組最多 4 台路由器，會將主機的交通，依照輪序方式導向到群組中的每一台路由器，GLBP 會依序將下一台路由器之 MAC 位址傳給主機，將主機要傳送的交通導向特定的路由器。

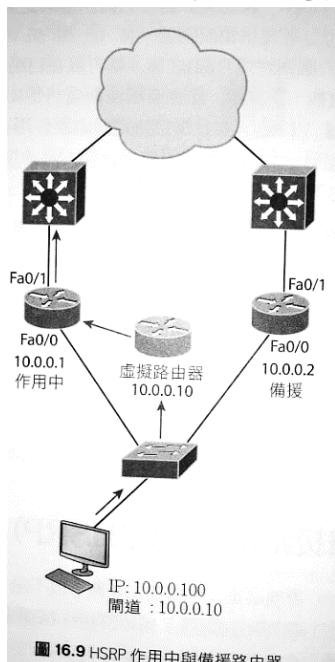
HSRP



HSRP 備援群組包含下列角色：

- **作用中路由器(active router)**
- **備援路由器(standby router)**
- **虛擬路由器(virtual router)**

HSRP 的缺點是很浪費。範例圖中，HSRP 群組一次只使用到 1 台路由器。



HSRP 群組透過多點傳播 Hello 訊息溝通。Hello 訊息包含用來決定作用與備援路由器所需的選舉資訊，也是故障移轉過程的關鍵。如果備援路由器沒有收到作用中封包，就會變成作用中路由器，並且開始回應主機請求。。

HSRPv2 的 Hello 封包使用群播 IP 為 224.0.0.102。

HSRP 虛擬 MAC

HSRP 虛擬路由器的虛擬 IP 必須是與主機同網段內的 IP。虛擬 MAC 則會建立全新的虛構 MAC。

HSRP 的 MAC 中只有 1 個變數，前 24 位元仍是 OUI，之後的 16 位元是 HSRP 的 MAC 位址，最後的 8 位元位址則是以 16 進位表示的 HSRP 群組編號。

HSRP MAC 範例：

0000.0c07.ac0a—CCNA 考過

- 前 24 位元(0000.0c)是 OUI；因為 HSRP 是 Cisco 協定，所以 ID 指定為 Cisco。
- 中間 16 位元(07.ac)是 HSRP ID。這是 Cisco 在協定中指定的值。所以很容易辨識這是 HSRP 使用的位址。
- 最後 8 位元(0a)是唯一的變動位元，用來表示群組編號，本例的群組編號 10，轉換為 16 進位放入 MAC 中成為 0a。

HSRP 群組中所有路由器的 ARP 快取中的每個 MAC 都伴隨該位址

QUESTION 405

Which one of these is a valid HSRP Virtual Mac Address?

- A. 0000.0C07.AC15
- B. 0000.5E00.01A3
- C. 0007.B400.AE01
- D. 0007.5E00.B301

哪一个是有效的 HSRP 虛擬 Mac 地址？

Correct Answer: A

HSRP V1 v.s. V2

HSRP V1 只支援 0-255 個群組, V2 可支援 0-4095 個群組, 主要應用在 VLAN 可以支援到 4094

Active Router 的選擇

所有 FHRP 的 Active Router 都一樣，先比較路由器的 Priority，Priority Max 為 Active Router(Priority default 100)，若 priority 相同，則比較介面 IP，大者為 Active Router。

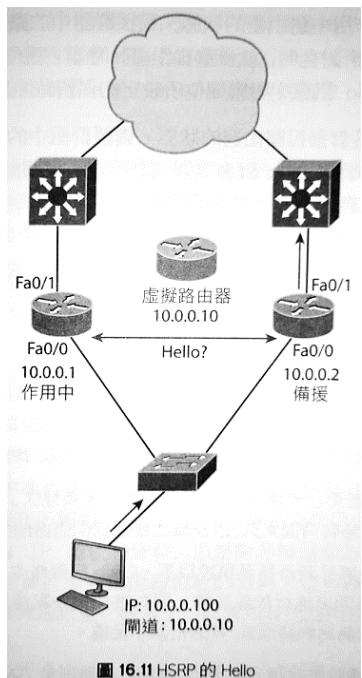
※VRRP 可使用路由器 IP 作為虛擬 IP，且該路由器優先為 Active Router，另兩種協定不可使用路由器 IP。

指定 Active Router

已有 Active Router 且未啟用 premmpt 時，Active Router 取決於設定的順序(先搶先贏)。因此要開啟 preempt 才能由優先權決定 Active Router

HSRP 計時器

用來確保路由器間通訊，如果出了問題，它們會讓備援路由器取而代之。有 Hello、保留(hold)、作用(active)、和備援(standby)四種。



- **Hello** 定義每台路由器送出 Hello 訊息的時間間隔，預設為 3 秒，用來辨識每台路由器的狀態。使用 Hello 計時器，在發生故障時可讓網路保持流動。這個計時器可以變更，但是一般認為降低 hello 值會為路由器增加不必要的負擔。HELLO 可以使用毫秒 ms 為單位。
- **保留計時器** 判斷作用中路由器是否故障的時間間隔。預設 10 秒，是 hello 的 3 倍。設定為 hello 計時器的 3 倍，可以確保備援路由器不會在每次發生短暫通訊問題時，就轉為作用中。
- **作用計時器** 監督作用中路由器的狀態。備援路由器每次從作用中路由器接收到 Hello 封包，就會重置作用計時器，這個計時器是否逾時是根據 HSRP Hello 訊息中對應欄位所設定的保留時間值。
- **備援計時器** 監督備援路由器的狀態。備援路由器每次從備援路由器接收到 Hello 封包時，就會重置該計時器。這個計時器是否逾時是根據對應 Hello 訊息中設定的保留時間值。

#現今企業網路狀態下，Hello 計時器通常設 200ms，保留計時器 700ms。命令如下
(config-if)#standby 1 timers msec 200 msec 700

HSRP 群組角色

- **虛擬路由器** 一個供封包傳送的獨立 IP 和 MAC。
- **作用中路由器** 實體路由器，負責接收傳送給虛擬路由器、以及通往相關目的地的資料。作用中路由器會處理要轉送的資料，以及回應對虛擬路由器 IP 的 ARP 請求。

- 備援路由器** 監督 HSRP 群組狀態，在作用中路由器故障時，迅速接管封包轉送的任務。作用中和備援路由器都會傳送 Hello 訊息，通知群組中其他路由器它們的角色和狀態。
- 其它路由器** HSRP 群組中可以包括其它的路由器：它們是群組的成員，但是不會扮演作用中或備援角色。這些路由器會監督作用中與備援路由器的 Hello 訊息，確保在所屬的 HSRP 群組中存在有作用中及備援路由器。它們會轉送針對本身 IP 位址的資料，但是除非被選舉為作用中或備援狀態，否則它們不會轉送屬於虛擬路由器位址的資料，這些路由器會根據 hello 計時器的時間間隔傳送訊息「發言」，以通知其他路由器它們在選舉中的位置。

設定及認證 HSRP

常用指令(設在對內網的埠)

指令	說明
Router(config-if)#standby <u>x</u> ip <u>y.y.y.y</u>	將介面加入一個 HSRP 群組 x 及其虛擬 IP y.y.y.y #屬於 HSRP 群組的所有路由器必須共用相同編號
Router(config-if)#standby group name <u>xxx</u>	承上，設定 HSRP 群組名稱，可省略
Router(config-if)#standby group priority <u>z</u>	設定該群組優先序，可省略，預設值為 100
Route#show standby	檢視 HSRP 所有參數 #注意群組編號為 Trouble shooting 重點，必須相同
Route#show standby brief	查詢 HSRP 狀態 查詢每個介面的 HSRP 角色
Router(config-if)#standby <u>x</u> preempt Router(config-if)#standby priority <u>z</u>	啟動該介面可插隊功能(preempt)，並設定優先權為 z。 #preempt 的意思是當 HSRP 收到對方的 hello 會重新選舉 Active Router 功能 #優先權預設 100，設為比 100 大就可以插隊為 active，負載平衡用得到。

介面追蹤 interface tracking

HSRP 提供內部網路的 GW 自動切換服務，但是對外網的連線就無法提供服務，介面追蹤功能可以監視外網的連線狀態。當 R1 對 Internet 的連線失效時，R1 對 PC1 的 GW 還是持續連線，HSRP 不會自動切換到 R2。

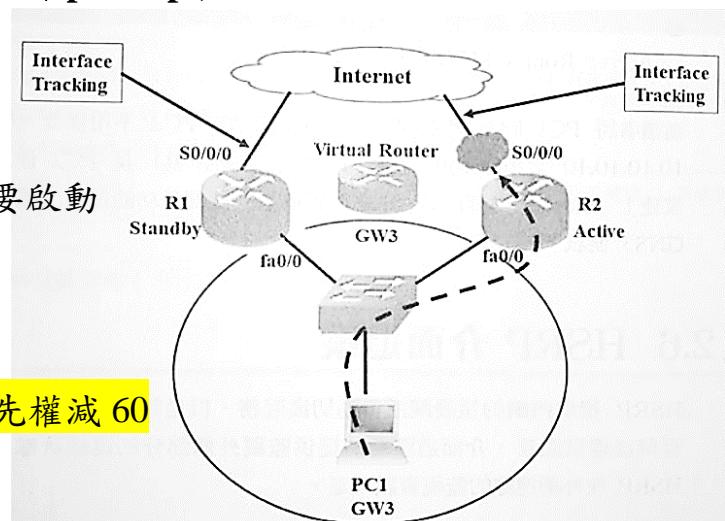
使用 interface tracing 偵測，當對外連線斷掉時對內的連線也一起斷掉，並且自動扣優先權讓另一台路由器作 Active。(注意：另一台要啟動 preempt)

◎介面追蹤指令(右圖為例)

```
R2(config)#int f0/0
R2(config-if)#standby 10 ip ....
R2(config-if)#standby 10 preempt      →另一台也要啟動
R2(config-if)#standby 10 priority ....
R2(config-if)#standby 10 track s0/0/0 60
```

s0/0/0 欲追蹤的介面

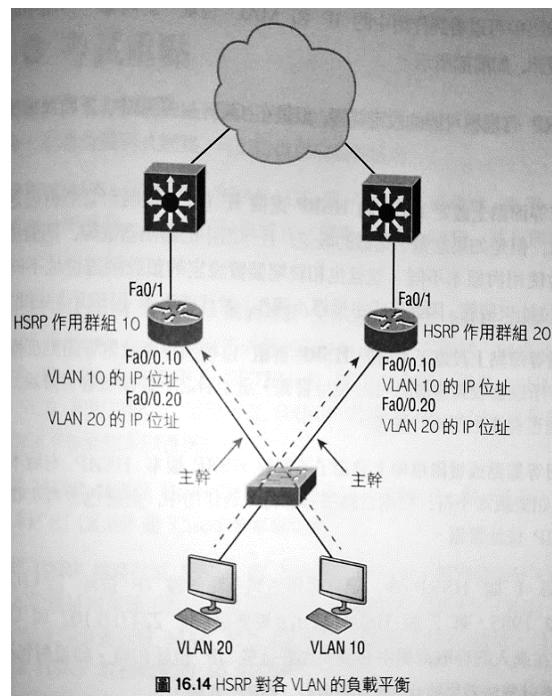
60-當該介面故障，R2 在 Group 10 的優先權減 60



p.s.HSRP 進階追蹤：可設定追蹤 Internet 中特定 IP 的連線狀態，或追蹤 Internet 中特定物件(IP SLA)的連線狀態，HSRP 再根據這些追蹤標的調整優先權，CCNP。

△HSRP 狀態 HSRP 介面會經歷五個狀態，最後只有 Active 和 Standby。

狀態	說明
初始(INIT)	HSRP 尚未運作。當組態設定異動或介面第一次轉變為可用時，會進入 INIT。
學習(Learn)	尚未產生虛擬 IP，也還沒看到作用中路由器的 HELLO。仍在等著聆聽作用中路由器 hello。
聆聽(Listen)	已經產生虛擬 IP，但該路由器不是作用中也不是備援。它會聆聽來自路由器的 HELLO。(非作用及備援的其他路由器狀態)
發言(Speak)	路由器定期傳送 HELLO，並積極地參與作用中/備援路由器的選舉。路由器必須有虛擬 IP 才能進入發言狀態。
備援(Standby)	會定期傳送 HELLO。一個 HSRP 群組只有一個路由器處於備援。
作用中(Active)	該路由器負責轉送傳給虛擬 MAC 的封包，並定期傳送 HELLO。一個 HSRP 群組只有一個作用中路由器。



HSRP 負載平衡

要讓 2 台 HSRP 路由器同時作用，可藉由在每台路由器間建立 TRUNK，並設定為 ROAS，每台路由器會成為不同 VLAN 的預設閘道，但是每個 VLAN 只有 1 台作用中路由器，通常，在更進階的設定中不會使用 HSRP 來做負載平衡；而會使用 GLBP，但是 HSRP 仍舊可以用來分擔負載，而且這也是認證目標。

HSRP 故障檢測

`show standby` 可以看到作用中 IP 和 MAC、計時器、作用中路由器等。

常見問題

- 在對等節點上設定不同虛擬 IP 備援路由器會使用與原本不同、與終端裝置預設閘道位址不同的虛擬 IP，造成主機停止運作。
- 在對等節點上設定不同的 HSRP 群組 導致對等節點都變成作用中，會收到 IP 衝突。

- 在對等節點或被阻擋埠上設定了不同的 HSRP 版本 HSRP 有版本 1 和 2。如果版本不符，則兩台路由器都會成為作用中，也會收到 IP 衝突。

在第 1 版 HSRP 中，HELLO 訊息會傳送到多點傳播位址 224.0.0.2 與 UDP 埠 1985。第 2 版 HSRP 使用 224.0.0.102 與 UDP 埠 1985。在 ACL IN，要允許這些 IP 位址和埠。

HSRP LAB

R1(config)#int f0/0

R1(config-if)#standby 102 ip 192.168.102.254 → 指定 virtual IP Group 編號及其虛擬 ip
R1(config-if)#standby 102 priority 120 → 指定 priority(預設或不設定是 100，比預設值大就好)
R1(config-if)#standby 102 preempt → 固定為 Active 角色(斷線後再連回還是該 Router 為 active，如果多個 Router 都打 preempt，那就比 priority 大小，建議如果兩台互備份可以都打 preempt，這樣另一台連回時就不會網路再斷一次)

你以為這樣備援就做好了嗎？太天真了少年！！

★假如 R1 的 f0/0 那條 segment 斷了，PC1 還是會 ping 不到 PC2，因為 HSRP112 的 active 還在 R1，這種狀況的專有名詞叫做 **Asymmetric Path**(去回不同路徑)

解法 1：把 f0/5 那條 segment 也拔掉(呵呵?)

解法 2：用 Interface Tracing(介面追蹤)

Interface Tracing Lab

※Interface Tracing- track，若要啟用則對應的多台 Router 都要啟用可插隊功能(Preempt)

1. 設定 track

Router(config)#track 1 interface fx/x line-protocol/ip

Router(config)#track 2 interface fy/y line-protocol/ip track 後數字代表編號

(track line 是對介面，track ip 要注意有可能 ip 還是可以路由)

2. 套用 track

Router(config)#int f0/0

Router(config-if)#standby 102 track x decrement 30 → 套用 track x，若生效 priority -30(有其它設定方式在 CCNP 有)

int f0/1 比照套用另一個 track

測試 track：拔除 switch 的 f0/1，確認 R1 的 HSRP Group 112 的 active 是否交給 R2，且 PC1 可持續 ping 到 pc2

*****R1 設定檔參考*****

interface FastEthernet0/0

ip address 192.168.102.1 255.255.255.0

duplex auto

speed auto

standby 102 ip 192.168.102.254

```
standby 102 priority 105  
standby 102 preempt  
standby 102 track 2 decrement 250
```

!

```
interface FastEthernet0/1  
ip address 192.168.112.1 255.255.255.0  
duplex auto  
speed auto  
standby 112 ip 192.168.112.254  
standby 112 priority 105  
standby 112 preempt  
standby 112 track 1 decrement 250
```

*****R1 設定檔參考*****

◎取消 HSRP Standby

Router(config-if)#no standby XX →XX 為 group 號碼

◎在 telnet 模式下讓 log 同步顯示(telnet 模式預設不顯示)

#terminal monitor

以下是很重要但考試基本不會考的 VRRP(Virtual Router Redundancy Protocol)

- IEEE defined，功能和用法類似 HSRP，PC 端 GW 也是設在虛擬 IP。
- HSRP v.s. VRRP(下頁)

比較項目	HSRP	VRRP
開發廠商	Cisco, 1994	IETF 1998-2005, RFC3768
群組數目	0-255	0-255
角色定義	1 Active, 1 Standby, Other Listen	1 Master, Other Backups
虛擬 IP 位址	VIP 位址不能跟同組 HSRP 路由器的 IP 位址相同	VIP 位址可以跟同組 VRRP 路由器的 IP 位址相同
群播位址	224.0.0.2	224.0.0.18
追蹤功能	可追蹤介面與物件	只能追蹤物件
預設 Hello time	Interval 3s, delay 10s	Interval 1s, delay 3s

※Master 的虛擬 MAC 00-00-5E-00-01-XX，XX 為 VRRP Group number。

- VRRP 指令和 HSRP 一樣，把 standby 換成 vrrp 就好。



GLBP (Gateway Load Balancing Protocol)

- 顧名思義，重點在 GW Load Balancing，並且兼有 GW 自動備援機制，Cisco only。
- 運作原理：

GLBP 中路由器有兩種角色，AVG(Active Virtual Gateway) & AVF(Active Virtual Forwarder)。AVG 類似 HSRP 的 Active，一個 GLBP Group 中只有一個 AVG，選 AVG 的原則和 HSRP 選 Active 一樣，根據優先權與路由器介面 IP 大小決定，至於 AVF 則是每台路由器都可當(包含 AVG)。

AVG 負則虛擬路由器的請求，但實際傳送資料的路由器由 AVF 擔任，由 AVG 來挑選哪台要作 AVF。

GLBP 中一樣有虛擬 IP，但虛擬 MAC 則是每個 AVF 都有，GLBP 虛擬 MAC 格式為 0007:B400:XXYY，XX 為群組號碼，YY 為 AVF 的路由器 ID。AVG 回應 PC 端的 ARP 就是回應給它 AVF 的 MAC。

· GLBP 負載平衡方式

即 AVG 挑選 AVF 的方法，注意 AVG 自己也可以當 AVF。

1. Weighted load-balancing :

設定每台 AVF 的權重，權重越大的 AVF 就越容易被 AVG 挑到，要使用此種方式最好把性能較好的路由器權重設大一點，如此可把大部份流量送往性能較佳的路由器。

2. Host-dependent load-balancing :

根據電腦決定 AVF，固定的電腦配固定的 AVF。

3. Round-Robin load-balancing :

輪迴方式，AVG 輪流挑選 AVF，可以平均用到每台 AVF。

- GLBP 指令：把 HSRP 的 standby 換成 glbp，其它細節設定在 CCNP。



廣域網路協定—HDLC, PPP, PPPoE, MLPS, DSL, CABLE, GRE, BGP

區域網路 v.s. 廣域網路：

通常您會擁有區域網路的基礎建設，但卻會從 ISP 租用廣域網路的基礎建設。

需要 WAN 的原因：

LAN 提供高網速(10/40/1000 Gbps)，並且很便宜。但只能在小區域中運作。更大的通訊環境中就需要 WAN(因為某些商業需求必須要能連結到遠方)，比如員工在外要連結內網，或是分公司要連到總公司。

WAN 的主要特徵：

- 連接的裝置間距離遠大於 LAN。
- 使用諸如電信公司、有線電視、衛星系統、或網路供應商等服務供應商所提供的服務。
- 使用序列式連線來提供大區域的網路。

Serial port

路由器中有一種網路介面為 **serial port**(序列埠)(s0/0/0)，主要用來連接 WAN 線路，與 LAN 使用 Ethernet port 不同(f0/0)。

LAN 使用乙太網路埠的 L2 協定(固定為乙太網路協定)，會有 MAC；但 WAN 的 L2 協定並不固定，視連線方式採用不同協定，故 WAN 的 L2 沒有 MAC。

廣域網路拓樸

實體拓樸指網路的實體配置，邏輯拓樸指信號穿越實體拓樸時的路徑。

星狀或軸幅(hub-and-spoke) 有一個單獨的中心(中樞路由器)，提供從遠端網路到核心路由器的存取。

所有通訊都會穿越核心路由器。優點是成本較低並且容易管理，但缺點也很嚴重：

- 中樞路由器代表有單點故障的可能。
- 中樞路由器限制了對集中式資源的存取效能。所有交通都是經由單一管道。

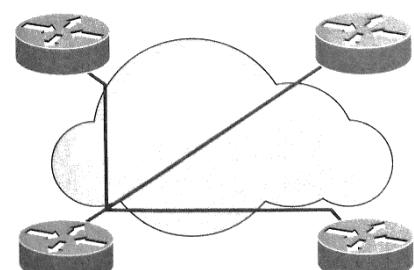


圖 21.1 軸幅式

全網狀(fully meshed) 封包交換網路邊緣的每個繞送節點都擁有直接連到網路中其他任意節點的路徑。

高度冗餘，但成本也最高。所以在實務上沒辦法使用全網狀拓樸，全網狀的缺點：

- 需要許多虛擬電路—每個連線都需要一條，高成本。
- 非廣播式環境中，對不支援多點傳播的路由器設定會更複雜。

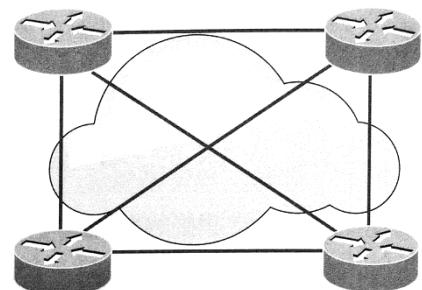


圖 21.2 全網狀拓樸

部分網狀(partially meshed) 可減少全網狀網路中的路由器數量。路由器不會全部直連，但優於軸輻式設計的冗餘。是最平衡的設計，提供更多的虛擬電路、冗餘性、效能。

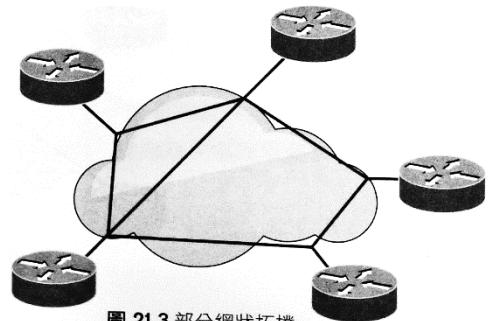


圖 21.3 部分網狀拓撲

廣域網路術語

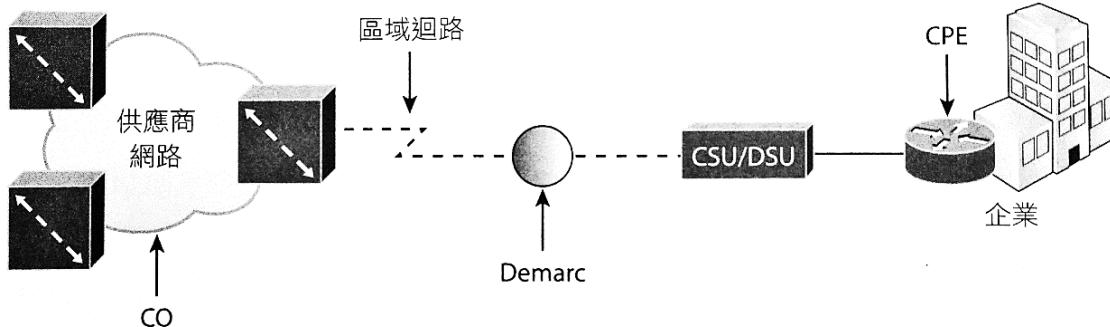


圖 21.4 WAN 術語

- **用戶端設備(Customer Premises Equipment, CPE)** 通常為用戶端，且位於用戶場所。
- **頻道服務單元/資料服務單元(channel service unit / data service unit, CSU/DSU)** CSU/DSU 會提供對 DTE 的時脈，資料終端設備(DTE)透過它連接到數位電路，例如 T1/T3 專線。即數位資料的來源或目的地，例如 PC、伺服器、和路由器。以上圖為例，路由器被是 DTE，因為傳送資料給 CSU/DSU，由 CSU/DSU 再轉送給服務供應商。CSU / DSU 使用電話線或同軸電纜(如 T1 或 E1)連到 ISP，但對路由器則使用序列式纜線。
- **責任分界點(Demarcation Point)** ISP 的責任終點，CPE 的責任起點。通常是一個放在 ISP 所擁有與安裝的通訊箱中的一個裝置。用戶從這個箱子接線到 CPE，它通常是一條連到 CSU/DSU 或 ISDN 介面的連線。
- **區域迴路(Local Loop)** 連接責任分界點到最近的一個中央(交換)機房。
- **中央機房(Central Office, CO)** 連結用戶網路與 ISP 的交換網路，有時又稱為 POP(Point of Presence)。
- **長途網路(Toll Network)** ISP 內部的主幹鏈路，由一群 ISP 擁有的設備組成。
- **光纖轉換器(Optical fiber converter)** 在光纖線路端點都有光纖轉換器，負責光學信號與電子信號間的轉換。

WAN 線路頻寬

- **數位信號 0(Digital Signal 0, DS0)** 基本的數位信號單位，速率 64 Kbps，相當於一個條通道；歐規稱為 E0、日規稱為 J0，是最小容量的數位電路，一個 DS0 就等於一條語音/資料電路。
- **T1** 又稱 DS1，包含 24 條 DS0，頻寬 1.544 Mbps。
- **E1** 歐規 T1，包含 30 條 DS0，頻寬 2.048Mbps。

- T3 又稱 DS3，包含 28 條 T1，頻寬 44.736Mbps。
- OC-3 光纖負載 3(Optical Carrier 3)，這種電路使用光纖，包含 3 條 T3，頻寬 155.52Mbps。
- OC-12 包含 4 條 OC-3，頻寬 622.08Mbps。
- OC-48 包含 4 條 OC-12，頻寬 2488.32Mbps。
- OC-192 包含 4 條 OC-48，頻寬 9953.28Mbps。

廣域網路連線類型—分為 Dedicated & Switched

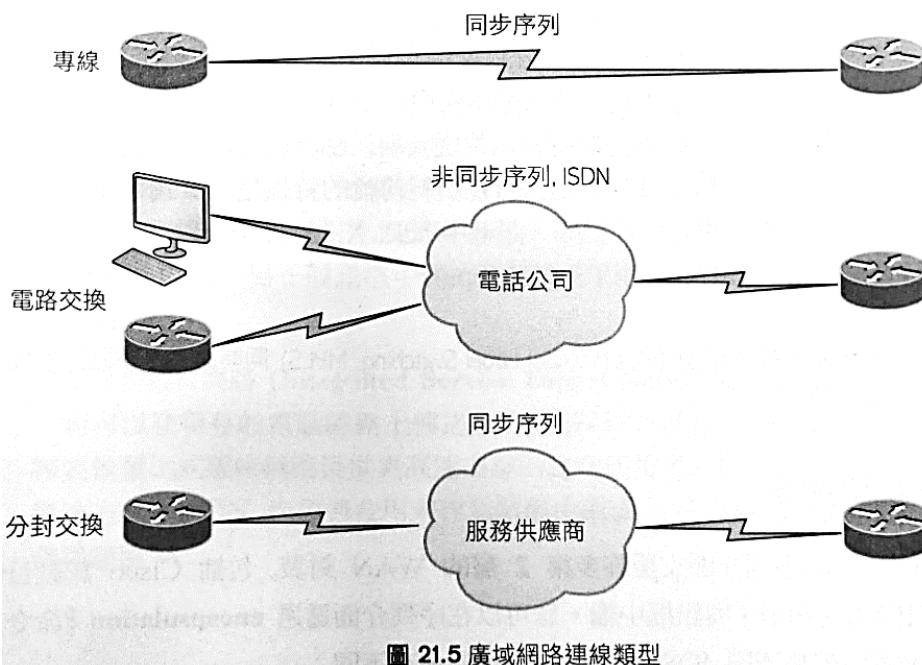
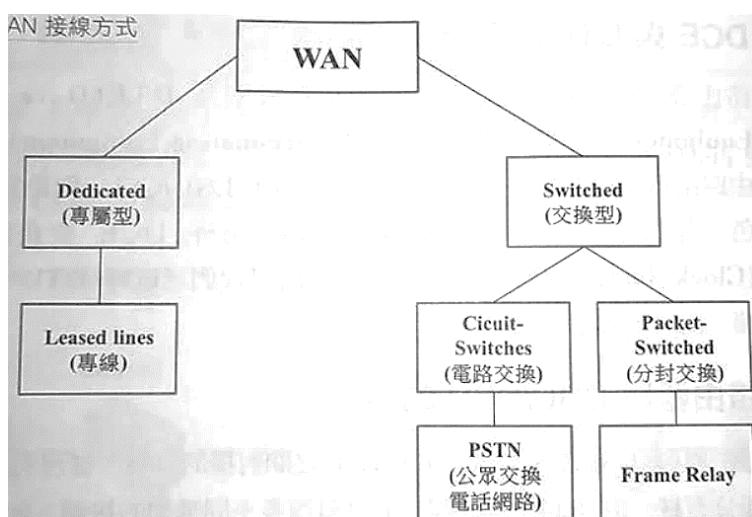


圖 21.5 廣域網路連線類型



Dedicated—專線

又稱為 point-to-point，如下圖，R1 與 R2 的實體連線是跟 ISP 租用線路，該線路是端點兩台路由器專用，不會有其他人使用，也稱為 Leased Line(專線)。

下圖中 R1-R2 使用 s0/0/0 序列埠來連接專線，R1 & R2 的 s0/0/0 IP 要規劃在同一網路，且該網路只有這兩個 IP，所以專線連線產生的網路規劃上都以/30 子網路為主。Leased line 的 WAN L2 協定有 HDLC, PPP 等。



- **租用專線(leased line)** 通常稱為點對點 P2P 連線或專線。是從 CPE 經 DCE 到遠端的 CPE，且事先建置好的 WAN 線路，傳送資料之前不需要準備，因為它使用同步的序列線路，速率最高可達 45Mbps，租用專線上最常使用的封裝是 HDLC 與 PPP。

#P2P 價格很貴

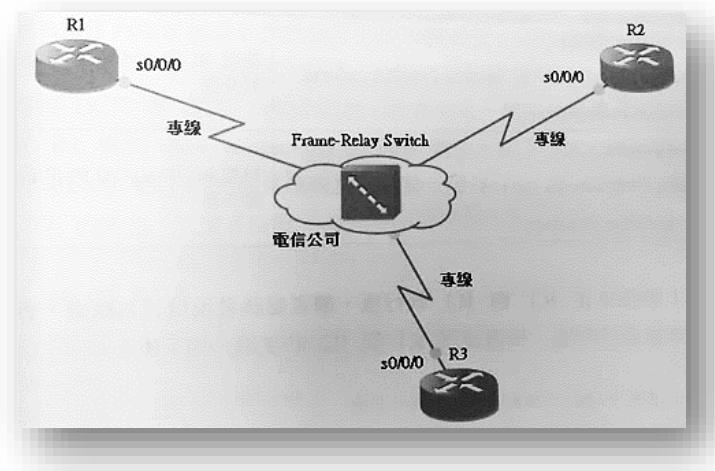
交換型—分為電路交換和分封交換

- **電路交換(circuit switching)** 電路交換使用現有電話系統，當電路交換的線路建立連線後，其行為類似專線，故專線可用的協定在電路交換中大部份都可使用。類似電話—計時收費，成本也低。在建好端點對端點的連線之前，不能傳送資料。電路交換利用撥接數據機或 ISDN，供低頻寬需求的資料傳輸使用。

- **分封交換(packet switching)** ISP 會在 WAN 中建置快速交換器，再將交換器的頻寬租給企業，由於頻寬共享，故可降低租用成本，類似 P2P，但付費的方式(與成本)比較像電路交換。下圖的台路由器使用專線接到 ISP 的 Frame-Relay Switch，共同使用一台交換器頻寬。分封交換的 WAN L2 協定有 ATM, Frame-Relay, X.25 等。

分封交換只有在資料傳輸的特性是爆發式(burst)、不連續時，才運作得很好。速度為 56Kbps 到 T3(45Mbps)。

#多重協定標籤交換(MultiProtocol Label Switching, MPLS)同時結合了電路交換與分封交換。



廣域網路封裝

L2 的 WAN 封裝可在序列介面透過 **encapsulation ?** 指令來檢視：

```
Corp # config t  
Corp(config)# int s0/0/0  
Corp(config-if)# encapsulation ?
```

atm-dxi	ATM-DXI	eneapsulation
frame-relay	Frame Relay	networks
hdlc	Serial	HDLC synchronous
lapb	LAPB	(x.25 Level 2)
ppp	Point-to-Point	protocol
smds	Switched	Negabit Data Service (SMDS)
x25	.25	

如果路由器上有其他種類的介面，就會有其他的封裝選項。序列介面上不能設定 Ethernet 的封裝。

WAN 封裝包含：訊框中繼、ISDN、HDLC、PPP、PPPoE、cable、DSL、MPLS、ATM、3G/4G、VSAT 與都會乙太網路(Metro Ethernet)。常用的 WAN 協定是 HDLC、PPP 與訊框中繼。

#序列埠連線的擴充性和成本效益都比不上連到 ISP 的快速乙太網路。

- **訊框中繼(Frame Relay)** 早期的分封交換技術，是 L1、L2 的規格，提供較高的效能。訊框中繼接替 X.25 的任務，移除了大部分 X.25 用來補救實體層錯誤(雜訊很多的線路)的技術。訊框中繼比 P2P 更便宜，運行的速度是 64Kbps 到 45Mbps。另外它提供動態頻寬配置與壅塞控制的功能。
- **整合服務數位網路(Integrated Service Digital Network, ISDN)** 可在現存的電話線路上傳送語音與資料的數位服務，連線速度較類比式撥接鏈路更高。ISDN 可用來作為訊框中繼或 T1 專線等其他鏈路的備援。
- **高階資料鏈結控制(High-Level Data-Link Control, HDLC)** 從同步的資料鏈結控制 (Synchronous Data Link Control, SDLC)衍生，SDLC 是 IBM 的一種資料鏈結連線協定。HDLC 為 L2 的協定，與 LAPB(Link Access Procedure, Balanced)比較起來，它的額外負擔非常少。HDLC 不會在相同的鏈路上封裝多個 L3 協定，其標頭沒有記載 HDLC 封裝內部的協定類型識別資訊，因此每個用 HDLC 的廠商都有自己識別 L3 協定的方式，即每個廠商的 HDLC 都具有專屬性。
- **點對點協定(Point-to-Point Protocol, PPP)** PPP 是 IEEE 標準，因為所有多重協定版的 HDLC 都是專屬，只有 PPP 可在不同廠商的設備之間產生 P2P。PPP 為 L2 協定，使用資料鏈結標頭中的 L3 控制協定欄來識別 L3 協定，允許認證與多重鏈路連線，且可以在同步與非同步鏈路上運作。
- **乙太網路上的點對點協定(Point-to-Point Protocol over Ethernet, PPPoE)** 將 PPP 訊框封裝在乙太網路訊框中，與 ADSL 服務搭配使用。一樣有 PPP 常用功能—驗證、加密、壓縮，但缺點為最大傳輸單位(MTU)比標準乙太網路的 MTU 小；如果您的防火牆設定不夠牢靠，這個小小的特性確實會造成一些問題！
- 主要功能是加入對乙太網路介面的直接連線，同時提供 DSL 支援，通常由許多台主機在共用的乙太網路介面上使用，透過至少一台橋接數據機開啟對各種目的地之 PPP 會談。
- **有線電視網路(cable)** HFC(Hybrid Fibre-Coaxial，光纖同軸混合電纜—同時使用光纖和同軸電纜建立的寬頻網路)中，通常會有 500 到 2,000 名用戶連到特定的纜線網段，共享上/

下行的頻寬，在有線電視(CATV)上的真實頻寬最高可達 27Mbps 的下載速率及 2.5Mbps 上傳速率。一般使用者可以取得 256Kbps 到 6Mbps 的存取速度。

- 數位用戶線路(Digital Subscriber Line, DSL) 傳統電話公司在雙絞式電話線上提供進階服務(高速資料、有時還有影像)時所使用的技術。傳輸能力較 HFC 網路低，速度受限於線路長度和品質。DSL 不是完整的 P2P 解決方案，而是像撥接、cable、或無線之類的 L1 傳輸技術。DSL 建置在區域迴路(Local loop)。連線建立在一對數據機之間，而數據機則位於 CPE 和 DSLAM(DSL Access Multiplexer)。DSL 存取多工器)間的銅線兩端。

#DSLAM 是位於 CO 的裝置，並且匯集來自多個 DSL 用戶的連線。

- 多重協定標籤交換(Multiprotocol Label Switching, MPLS) 在分封交換網路上模擬電路交換網路特性的資料傳輸機制。可將封包加上標籤(編號)，然後使用標籤來轉送封包，這些標籤是在 MPLS 網路的邊緣指定，標籤通常對應到 L3 目地位址的路徑(相當於以目地 IP 為基礎的遶送)。MPLS 的目的是要支援非 TCP / IP 之其他協定的轉送。因此，不論 L3 協定為何，網路內的標籤交換方式都相同。在較大的網路中，加上 MPLS 標籤的結果是只有邊緣路由器會去檢視遶送。所有核心路由器都是根據標籤來轉送封包，這使得封包在服務供應商的網路中能有更快的轉送速度。這也是為什麼今日大部分公司都使用 MPLS 來取代他們的訊框中繼網路。

#運用有 MPLS 的乙太網路來連接 WAN，稱為 MPLS 上的乙太網路，或 EoMPLS

- 非同步傳輸模式(Asynchronous Transfer Mode, ATM) ATM 的設計是為了對易受時間影響的交通，同時提供語音、視訊、資料傳輸。ATM 使用細胞(cell)來取代封包，細胞長度是固定的 53 個位元組，也可利用等時的(isochronous)時脈(外部時脈)來幫助資料移動得更快。現今採用訊框中繼，通常就會執行 ATM 上的訊框中繼(Frame Relay over ATM)。

- 蜂巢式(Cellular)3G/4G 對涵蓋區域內的小型遠端辦公室很有用。

- VAST 小型衛星地面站 有許多據點分散在很大的區域中，可以考慮使用。VAST 比數據機下載快 10 倍，上傳速度為下載速度 1/10。

- 都會乙太網路(Metro Ethernet) 一種都會區域網路(Metropolitan area network, MAN)，以乙太網路為標準。

WAN 的實體線路



←這張圖少了 demarc point

• DSU/CSU v.s. MODEM Data Service Unit/Channel Service Unit/Modulator and DEModulator

DSU/CSU 視備可視為兩種介面，DSU 連接路由器，負責管理路由器輸出、入訊號，CSU 連接電信公司實體線路，負責傳送、接收與電信公司連線的數位訊號，並可測試另一端 CSU 是否正常運作。

DSU/CSU & MODEM 的比較，這兩種設備都是用來介接路由器與電信公司的線路。

當電信公司線路是專線(傳送數位訊號)，此時就需要 DSU/CSU 來和路由器對接，路由器送出數位訊號給 DSU/CSU，DSU/CSU 再將數位訊號轉送到專線上給遠端的 DSU/CSU。

當電信公司線路走電話線(傳送類比訊號)，此時就需要用 MODEM 來與路由器對接，路由器一樣送出數位訊號給 MODEM，MODEM 再將數位轉成類比，透過電話線傳給遠方的 MODEM 。

• DCE & DTE

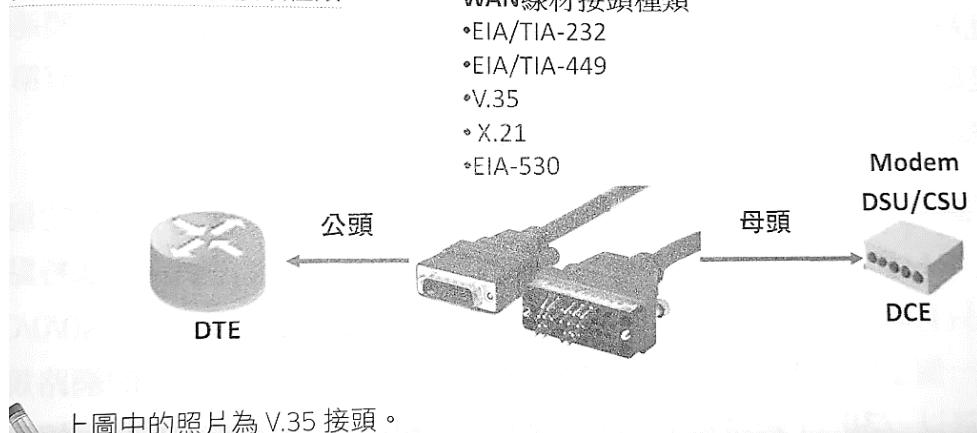
路由器與 DSU/CSU 扮演的角色分別為 DTE(Data Terminal Equipment)、DCE(Data Circuit-Terminating Equipment), DTE 為路由器擔任，作為資料終端設備，DCE 則為 DSU/CSU，作為電信公司通訊設備的末端，此外 DCE 要送出 Clock Rate(時脈)給 DTE 以保持同步，簡單說，DTE 為 User 端，DCE 為電信業者端。

• 路由器與 DSU/CSU、MODEM 的線材沒有像網路一樣統一 RJ45，而是有各種不同的接頭

表 13-2 WAN 線材接頭種類

WAN線材接頭種類

- EIA/TIA-232
- EIA/TIA-449
- V.35
- X.21
- EIA-530



上圖中的照片為 V.35 接頭。

Clock Rate Configuration on Router



前提：在沒有 ISP 供應商的環境中，DCE 端設定。

• Serial port s0/0/0 設定

路由器使用序列埠連接 WAN 時，需要做一些額外設定，和 FastEthernet 埠接 LAN 略有不同。



- 進入兩端 int s0/0/0 介面設定 IP 並 no shutdown，燈號會變綠燈，但 show int s0/0/0 會看到仍是 protocol down。綠燈不代表網路連線正常，只代表 L1 運作正常。

設定時脈

承上，序列埠 L2 有問題是因為沒設定時脈，時脈決定序列埠的傳輸頻寬，要設定在 DCE，DTE 則只接收時脈，要查詢哪邊是 DCE 使用 show controllers int 指令。

◎查詢 DCE/DTE、時脈

#show controllers s0/0/0 → 只提供 L1 資訊

◎在 DCE 上設定時脈—如果沒有自動設定的話，DTE 要和 DCE 設一樣

#Router(config-if)#clock rate ? 在 WAN 中 ISP 的 DSU/CSU 永遠是 DCE

#show int s0/0/0 會看見 BW xxxKbit，但這是用來算路由協定的成本參考頻寬，WAN 的實際頻寬還是要看時脈設定。



圖 21.10 Cisco 的 HDLC 訊框格式：每個廠商的 HDLC 都有一個專屬的資料欄位，以支援多重協定的環境。

位元導向的 L2 協定、用於專線上的 P2P 協定，不提供認證。

#位元導向協定有 SDLC/HDLC，位元組導向有 TCP/IP。

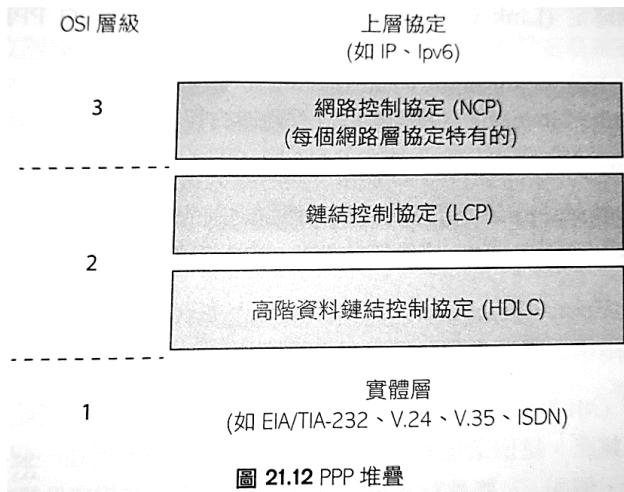
show int s0/0/0，其中 **Encapsulation** 後面顯示目前使用的 WAN L2 協定封裝，思科預設為思科版 HDLC。

#show run 沒有哦

HDLC 有兩種版本，IEEE 和 Cisco 版，表頭檔完全不同，差別在處理 L3 協定，IEEE 版只能處理 IP 協定，而 Cisco 版可處理多種 L3，如 IP, IPX, Apple Talk 等。當 Cisco 路由器與他牌路由器 WAN 對接時，HDLC 版本不相容(他牌的只能用 IEEE 版)，要使用其他 WAN L2 封裝協定。↓ PPP

PPP

為 WAN L2 協定，可用在非同步序列(撥接)或同步序列(ISDN)的傳輸媒介面，使用 LCP 建與維護資料鏈結的連線。



PPP 包含四個組成：

- **EIA / TIA-232-C、V.24、V.35、ISDN** 序列通訊的 L1 國際標準。
- **HDLC** 在序列鏈路上封裝資料包的方法。
- **LCP (Link Control Protocol)** 建立、設定、維護與結束點對點連線的方法。也提供壓縮、**認證**、錯誤偵測、多連結(Multilink)的封裝選項。

LCP 的設定選項

認證 (Authentication) 告訴鏈結的呼叫端要傳送可用以識別用戶的資訊，認證的方法有 PAP、CHAP。

壓縮 (Compression) 資料或負載在傳送之前先壓縮，以增加 PPP 連線的產出 (throughput)，然後接收端的 PPP 會對資料訊框進行解壓縮。

錯誤偵測 (Error Detection) PPP 利用品質 (Quality) 和神奇數字 (Magic Number) 確保可靠且無迴圈的資料鏈結。

多重鏈路 (Multilink) Cisco 路由器從 11.1 版的 IOS 開始在 PPP 鏈結支援多重鏈路，這個選項允許多個個別實體線路出現在一個第 3 層邏輯線路上，例如，2 條執行多重鏈路 PPP 的 T1 看起來像是 1 條第 3 層遶送協定的 3Mbps 線路。

PPP 回呼 (PPP callback) PPP 可以設定為成功認證之後就回頭呼叫，可以記錄使用量，作為帳務的記錄，或許多其他的用途，若啟用回呼，呼叫端路由器 (客戶端) 聯繫遠端路由器 (伺服器) 並進行認證，並且這 2 部路由器都必須設定回呼。完成認證後，遠端路由器會結束連線，重新啟始一條連線到呼叫端。

- **NCP(Network Control Protocol)** 建立/設定不同 L3 協定的方法。NCP 的設計是將協定封裝在 PPP 資料鏈結上，以允許多種網路層協定時通訊。例如網際網路協定控制協定 (Internet Protocol Control Protocol, IPCP) 與 Cisco 發現協定控制協定 (Cisco Discovery Protocol Control Protocol, CDPCP)。

△PPP 協定堆疊只規定在 L1, L2

建立 PPP 會談—PPP 連線建立過程有三個階段

- **L2 連線建立** 該階段主要建立 PPP 協定與 L2 的連線，每個 PPP 裝置會發送 LCP 封包，其中包含一個「設定選項」(Configuration Option)欄位，允許每部裝置檢視資料大小、壓縮、認證。如果沒有「設定選項」欄，就使用預設值。
- **認證** L2 連線建立後，檢查是否有啟動認證，此階段也是在 LCP 執行，使用 PAP 或 CHAP 認證鏈路。認證發生在讀取 L3 協定前，若無設定認證則跳至下一階段。
- **L3 協定階段** PPP 利用 NCP 以封裝多個網路協定，並透過一條 PPP 資料鏈結來傳送。每個 L3 協定(如 IP、IPv6 被遠送協定)會與 ncp 建立一個服務，PPP 會發送 NCP 協定封包來選擇，且設定一個以上的網路層協定，決定 L3 的協定後，PPP 連線就建立完成。

· PPP 常用指令

指令	說明
Router(config-if)#encapsulation ppp	更改 WAN L2 封裝為 PPP #很重要，有 PPP 才能接下去
Router(config-if)#ppp authentication pap	啟動 PAP 認證功能
Router(config-if)#ppp pap sent-username cisco password ccna	送出 PAP 認證使用者帳密
Router(config)#username cisco password ccna	建立使用者帳密
Router(config-if)#ppp authentication chap	啟動 CHAP 認證功能
Router(config-if)#ppp authentication chap pap	啟動 PAP+CHAP 混合認證功能
Router#show int s0/0/0	查詢 s0/0/0 的 L2 封裝
Router#debug ppp authentication	啟動 PPP debug(可看到三方/二方交握過程)

PPP Configuration



選擇性啟用，預設關閉。

PPP 提供兩種認證：Password Authentication Protocol(PAP) & Challenge Handshake Authentication Protocol(CHAP)。

- **PAP** 基本的 2-way handshake，未加密，用戶帳密以明文發送，且只能在建立初始鏈路時進行。當建立 ppp 鏈路時，遠端節點會傳回帳密給認證路由器。
- **CHAP** 較安全，透過 3-way handshake 交換 pre-share key(共用金鑰)，可在鏈路啟始時進行，也可用於定時查核鏈路(確認是否由同主機進行通訊)。認證路由器傳送詢問請求給遠端，遠端則傳回用 MD5 單向雜湊函數計算出來的值，再由認證路由器檢查是否匹配。

PAP 設定

指令	說明
Router(config-if)#encapsulation ppp	啟用 PPP
Router(config)#username <u>對方主機名</u> password <u>雙方相同</u>	為連結到自己的遠端路由器設定帳密(對方要先有 hostname)
Router(config-if)#ppp authentication pap	設定認證方式可同時設定兩種，前者優先使用
Router(config)#ppp pap sent-username _____ password _____	對遠端裝置驗證自己的身份(對

方成為 server)，對方路由器上要有相同帳密

有啟動 PAP 功能的路由器稱為 PAP Server，此時會等待 PAP Client 發送使用者帳密，直到確認帳密或終止連線。

※首先發送封包的就是 PAP Client，也即有執行 PAP sent-username 的那台。

※也可以雙方都啟動 PAP 互相傷害。

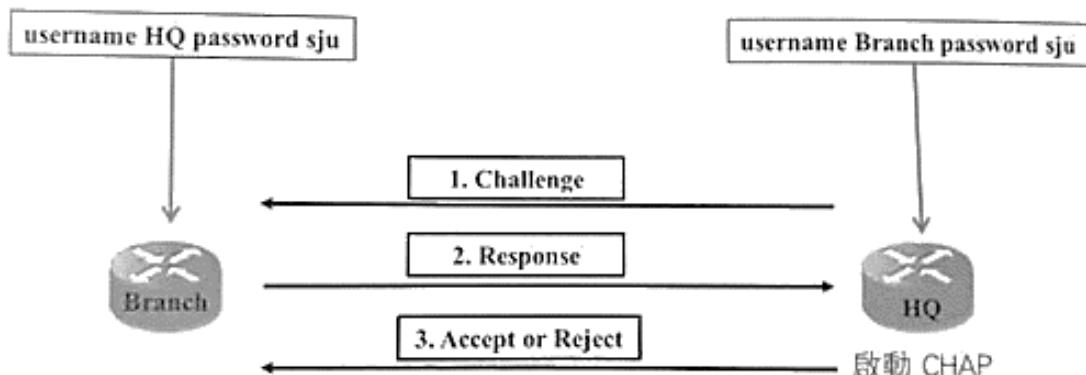
CHAP Configuration—NA 不會考



- CHAP 需要三方交握才能完成，不同於 PAP 直接帳密認證，CHAP 使用 hash(雜湊函數)進行加密，不會將使用者帳密傳送，安全性高。

發送第一個交握封包的是 CHAP Server，即啟動 CHAP 認證功能的路由器，PAP 則相反。HQ 送出的第一個交握封包有一個字串，Branch 利用這個字串與密碼 sju 做 md5 的 hash 運作得到一個結果，將該結果在第二個交握封包送出，HQ 收到後會跟自己的 md5 hash 運算結果比對，相同就發同意連線的第三個交握封包，不同的話 HQ 就拒絕 PPP 連線。

#CHAP 的密碼兩台路由器一定要設一樣，使用者名稱則為對方主機名稱，另外 CHAP 跟 PAP 一樣都有單向及雙向認證。



- CHAP 基本指令—單向認證(以上頁圖為例)這裡好像有問題，username 應是 local hostname

HQ(config)#username Branch password <u>cisco</u>	設定認證資料，使用者名稱必須為對方主機名稱
HQ(config)#int s0/0/0 HQ(config-if)#encapsulation ppp	設定 s0/0/0 介面的 L2 為 PPP 協定
HQ(config-if)#ppp authentication <u>chap</u>	啟用 PPP 協定的 CHAP 認證

Branch(config)#username HQ password <u>cisco</u>	設定認證資料，使用者名稱必須為對方主機名稱
Branch (config)#int s0/0/0 Branch (config-if)#encapsulation ppp	設定 s0/0/0 介面的 L2 為 PPP 協定

Router#debug ppp authentication

啟動 PPP debug (可看到 CHAP 三方交握訊息)

- CHAP 雙向認證—把 Branch 也啟用 ppp authentication chap。

◎混合式 PPP 認證—可將 PAP 和 CHAP 混合使用

```
Router(config-if)#ppp authentication chap pap
    #ppp authentication pap chap
```

哪個放在前面就是先用哪個認證，第一道認證過了之後就不用第二道。
或是連進來的 client 只有啟用其中一種就會使用相對應的驗證。

PPP Troubleshooting

步驟	檢查方向	使用指令
1	檢查網路模型哪層出問題	#show ip int brief
2	L1 的連線問題，確認網路線種類	--
3	檢查是否設定 Clock Rate	#show controller s0/0/0
4	檢查兩邊路由器的 WAN 封裝是否一致	#show int s0/0/0
5	檢查是否啟用 PPP Authentication	#show run #debug ppp authentication
6	確認兩邊路由器的 IP 在同網段	ping

★WAN 鏈路兩端雖然啟用認證，並且 IP 都設正確，但雙方 IP 若在不同子網路，會顯示一切正常，甚至 PING 得到，但實際上網路交通、遶送協定會出問題

MLP(Multilink PPP)

WAN 的負載平衡機制很多，但 MLP 不用錢！而且是標準協定，所以支援多廠商，其規範在 RFC1990，其中詳述封包分割和序列化規格。

p2p 連線備援，最簡單的方法是多一條專線，但這樣的備援和 HSRP 類似，沒有負載平衡。使用動態路由協定時，因為 COST 不同所以路由表只會列出一條，另一條為隱藏備援(無流量)。另外，兩條專線共需要四個 IP，造成 IP 浪費。

LCP 模組提供多條點對點連線的 Bundle 功能，稱為 MLP，類似 EtherChanel 將兩條線路綁成一條邏輯線路。所以在鄰居表中只會有一筆；另外 MLP 用一個虛擬介面來代表多個序列埠，只要一個虛擬 IP。

MLP 優點

● **負載平衡** MLP 提供隨選頻寬，可在最多 10 條鏈路上進行負載平衡，甚至可以計算特定網點間的交通負載，這些鏈路不需要相同頻寬，但是建議最好能這樣。另一項優勢是它能切割封包，並將封包碎片透過所有鏈路傳送，以降低 WAN 上的延遲。

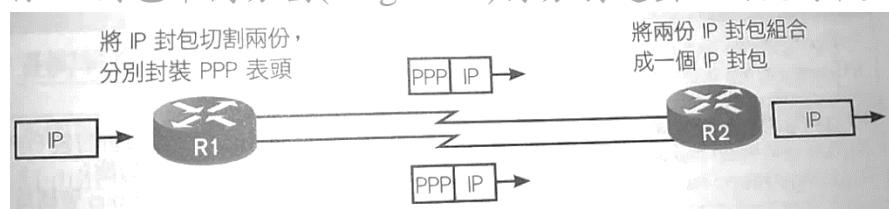
● **增加冗餘性** 若某條鏈路故障，其他鏈路仍可以收送。

● 鏈路切割和穿插 (interleaving) MLP 切割大型封包，將封包碎片透過多條點對點鏈路傳送，較小的即時封包不會被切割。因此即時性封包會插在切割過的非即時性封包之間傳送，以降低延遲。

• MLPPP 路徑平衡

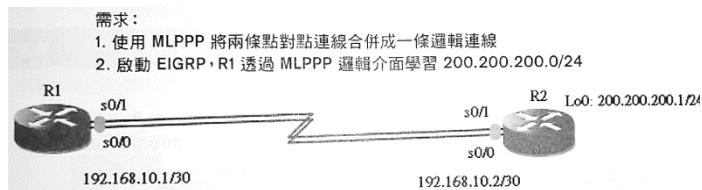
在 EtherChannel 的路徑平衡不會切割 Frame，而是以 Frame 為單位，根據 EtherChannel 的演算法將 Frame 將某條路徑送出，因此 EtherChannel 的路徑平衡只是偽・平衡。

MLPPP 路徑平衡則是以封包為單位，將 IP 封包平衡分割(Fragments)再分別送出，因此可做到真正的路徑平衡，詳見右圖。



• MLPPP 設定

△注意 multilink number &multilink group 號碼要相同才能建立成功。



指令	說明
(config-if)#no ip add	取消要設為 MLP 的序列介面上原有 IP
R1(config)#int multilink <u>x</u> R1(config-if)#ip add <u>x.x.x.x y.y.y.y</u> R1(config-if)#encapsulation ppp R1(config-if)#ppp multilink R1(config-if)#ppp multilink group <u>x</u>	建立 MLP 邏輯介面並給定 MLP 介面一個 ip Multilink 告知邏輯介面封裝 ppp(原有則省略) 啟動 ppp multilink 功能 設定 ppp multilink group number 為 x
R1(config)#int s0/0 R1(config-if)#no sh R1(config-if)#encapsulation ppp R1(config-if)#ppp multilink R1(config-if)#ppp multilink group <u>x</u>	啟動 s0/0 介面 宣告封裝 ppp 啟用 ppp multilink 功能 設定 ppp multilink group number 為 x
R1(config)#int s0/1 以下省略	在 s0/1 完成重覆設定一次
#show int multilink 1	查詢 multilink 介面資訊
#show ppp multilink	查詢 ppp multilink 狀態及設定細節 #包含介面編號，綁繩的實體介面資訊

※將本例中的 R1 & R2 建立為 EIGRP 鄰居後，會看到 eigrp neighbor 只有一筆，out interface 為 Mu1。

Show ip route 路由表中會有一筆直連(D)，出口介面也是 Mutilink 1。

=====



PPPoE

概念

在乙太網路中封裝 PPP 資料，目前廣用於 ADSL / Cable modem。

用戶端向 ISP 租用 ADSL Modem，並使用 RJ45 連到 ADSL Modem，ISP 為了計量收費，搭配一個 L2 PPP 協定以方便帳戶管理、驗證用戶端資訊。

簡言之，乙太網路接口不需驗證，但要通過 ISP 業者要有帳號密碼，也就必須用 PPP 協定，在乙太網路上的 PPP 就叫做 PPPoE。

PPPoE 封裝 PPP 封包封裝在 Ethernet 表頭裡，因此在傳送過程中 12 資料使用 Ethernet 網路的 MAC 位址，類似 Tunnel 但不用指定 source & destination，如下圖。

ISP 端收到 Ethernet Frame 後解封裝就會看見 PPP 表頭，如此客戶與 ISP 就可建立 PPP Session，進而使用驗證等功能。

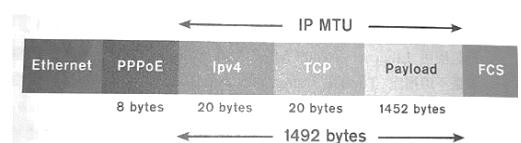
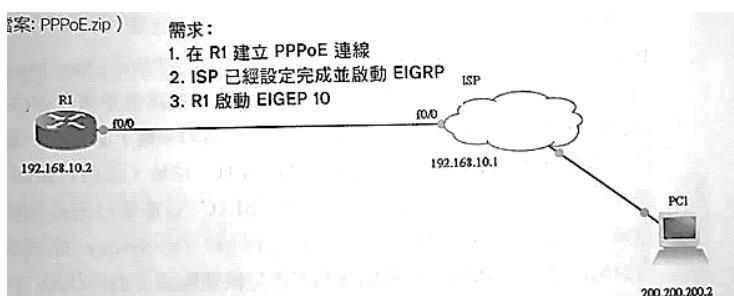
PPPoE 運作過程

分為 PPPoE Discovery & PPPoE Session 兩階段。PPP 是運作在 P2P 的連線上，而乙太網路則是多重存取(Multi-access)架構，所以 PPP 協定封包要在乙太網路架構上運作，必須先找到乙太網路封包中目的端和來源端 MAC 再封裝到 PPP 封包中，代表這個 P2P 連線兩端的 MAC 位址都已經定位，上面這麼長一串指的就是 PPP Discovery。當 Discovery 階段完成，就可開始進行 PPPoE 資料傳輸及帳號驗證，此即 PPPoE Session 階段。

調整 IP Packet 的 MTU

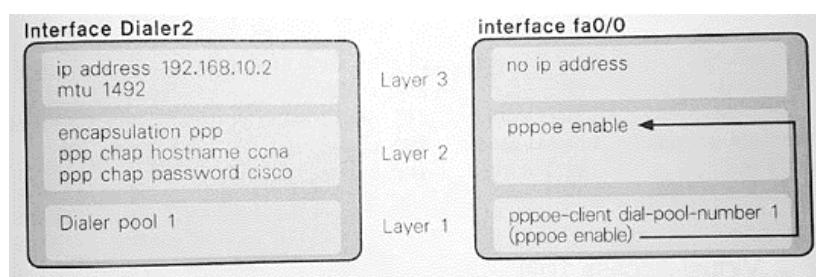
PPPoE 封包如圖，由於 IP 封包的 MTU(maximum transmission unit)為 1500bytes，當 PPPoE 表頭插入 Ethernet Frame 中會多出 8bytes，故要將 IP 封包 MTU 調整為 1492，這樣 PPPoE 表頭插入時才不會超過 1500。

• 設定



PPPoE 必須從兩種介面設定，第一種介面為 interface dialer(撥號介面)，第二種為 interface fa0/0(乙太網路介面)。

如圖，撥號介面是個虛擬介面，此介面需給定 IP 與 PPP 相關設定，分別表示撥號介面的 L2 & L3 設定，另在撥號介面還要調整 MTU 為 1492 與宣告 dialer pool 號碼給乙太網路介面使用，dialer pool 號碼可視為 PPP 使用的 L1 封裝介面；在乙太網路的設定只要啟動介面、指



定使用哪個 dialer pool 號碼並啟動 PPPoE，乙太網路介面不需設定 IP，所以乙太網路介面沒有 L3 設定，即沒有繞送能力，乙太網路介面的 L1 使用撥號介面定義的 dialer pool 號碼。

p.s. dialer pool number 不用和 interface dialer number 一樣。

p.s. 在乙太網路介面使用 dialer pool 號碼後，PPPoE 自動啟用。

- R1 啟動 PPPoE 的指令

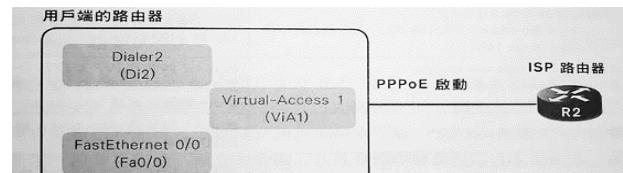
ISP 部份已設定(包含 CHAP 認證資訊 ccna/cisco)，故 R1 的認證資訊也要設定為 ccna/cisco。

指令	說明
R1(config)#int dialer 2	
R1(config-if)#ip add <u>x.x.x.x y.y.y.y</u>	建立虛擬介面 dialer2 並給定 IP
R1(config-if)#mtu <u>1492</u>	設定其 mtu 值為 1492
R1(config-if)#encapsulation ppp	設定 L2 封裝為 PPP
R1(config-if)#ppp chap hostname ccna	設定 CHAP 認證帳號
R1(config-if)#ppp chap password cisco	設定 CHAP 認證密碼
R1(config-if)#dialer pool 1	設定 L1 封裝為 dialer pool 1(給下面 int f0/0 用)
R1(config)#int f0/0	
R1(config-if)#no sh	啟動 int f0/0
R1(config-if)#pppoe-client dial-pool-number 1	使用 dialer pool 1 作為 L1
R1(config-if)#pppoe enable	啟動 PPPoE，此指令在宣告 dialer pool 時會自動執行，可省略

◎查詢 pppoe 運作狀態

R1#show ip int brief

會看到有一個 Dialer 2 介面，還會有一個 Virtual-Access 1 介面，有看到該介面產生並運作正常才是 pppoe 有啟用成功，下面說明。



Virtual-Access 介面(virtual template interface)

運作狀態如右圖，三個介面雖然分開，但是一起合作啟動 PPPoE，可以將 Virtual-Access 視為 PPPoE 運作的介面，而 PPPoE 的介面由撥號介面與乙太網路界面運作產生。

設定 PPPOE Client

建立撥接介面，然後將它連結到實體介面。步驟如下：

1. 使用 interface dialer number 命令建立撥接介面
2. 使用 ip address negotiated 命令指示 client 使用 PPPoE Server 提供的 IP
3. 設定封裝 PPP
4. 設定撥接池、編號
5. 在實體介面上使用 pppoe-client dial-pool number ____命令

最後用 show ip int br / show pppoe session 檢查

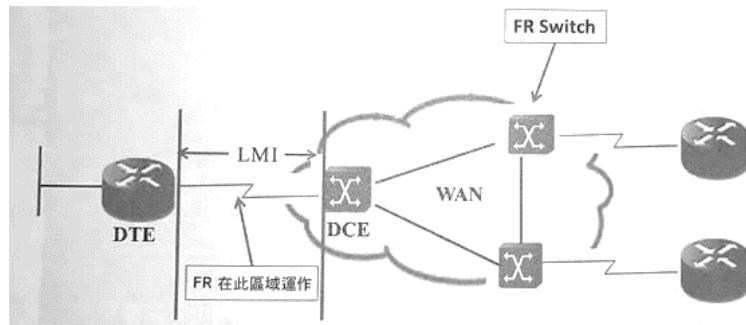
```
R1(config)#int dialer __  
R1(config-if)#ip address negotiated  
R1(config-if)#encapsulation ppp  
R1(config-if)#dialer pool __  
R1(config-if)#int f __  
R1(config-if)#no ip address  
R1(config-if)#pppoe-client dial-pool-number __  
R1#show ip int br  
R1#show pppoe session
```



Advanced WAN protocol—Frame-Relay, VPN, GRE

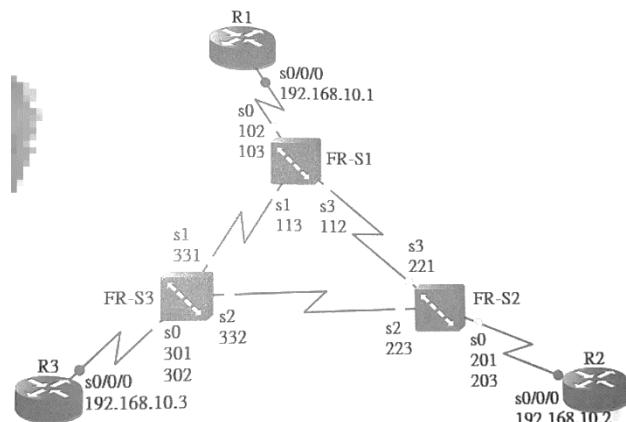
Frame-Relay

- 範例圖中有三個 FR 交換器，ISP 建立 FR 交換器所形成的交換器網路再租給(企業)用戶，而用戶端路由器的連線只到 FR 交換器，之後走哪條由 ISP 動態決定，故企業用戶會共享該 FR 頻寬，不同於專線方式，但價格也較便宜。



DLCI 號碼

FR 的 L2 位址就是 **Data Link Connection Identifier(DLCI 號碼)**，如同乙太網路的 L2 位址為 MAC，FR 就是靠 DLCI 對應出一條虛擬線路 VC(Virtual Circuit)。DLCI 的設定由 ISP 規劃，設定在 FR 交換器的介面中，以下圖為例，FR-S3 的 S0 介面有設定兩個 DLCI 號碼 301、302，S1 介面中設定 DLCI 號碼為 331，S2 介面中設定為 332。



Virtual Circuit

FR 網路共享，因此沒有任何線路作為專線使用，當企業用戶要使用 FR 網路時，會在 FR 網路中產生一條虛擬線路傳遞資料，虛擬線路的產生是依靠 DLCI 的對應。

以上圖為例，R1—R2 間的 VC 線路規劃為：

R1 s0/0/0 → FR-S1 s0/102 → FR-S1 s3/112 → FR s3/221 → FR s0/201 → R2 s0/0/0

所以 R1 中使用 DLCI=102 就會產生此條 VC 線路，DLCI 的規劃是由 ISP 業者，因盤在 R1 對應的 FR-S1 中 S0 有兩個 DLCI，表示 R1 將有兩條 VC 線路從 S0/0/0 連出去。因此，可以將 VC 線路視為一條連到 FR 服務的路由器之間的邏輯路徑。

LMI 運作

Local Management Interface，是一種 keepalive 的機制，提供本地路器 DTE 和 FR 交換器 DCE 間的 FR 連接的狀態資訊，以下圖為例，R1 和 FR-S1 間使用專線連接，LMI 協定就是在此連線上運作來檢查 R1 與 FR-S1 的連線狀況，另外 R1 也會透過 LMI 協定從 FR-S1 得到 DLCI=100

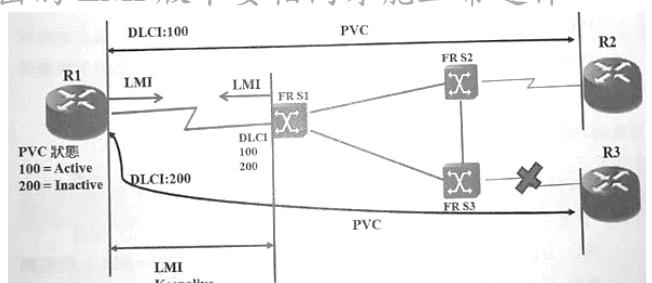
& 200，所以 R1 就有兩條 VC 連線，R1 使用 DLCI 100 連到 R2，DLCI 200 連到 R3，當 R3 或 FR-S3 連線有問題，R1 的 DLCI 200 VC 線路就會變成 Inactive。

LMI 協定的版本有三種，路由器與 FR 交換器送出的 LMI 版本要相同才能正常運作。

-Cisco：預設 LMI

-ANSI：對應於 ANSI 標準 T1.617 Annex D

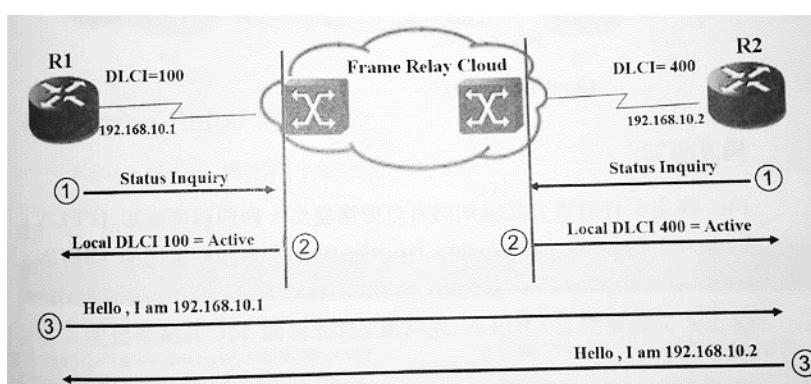
-Q933a：對應於 ITU 標準 Q93



Inverse-ARP

Inverse-ARP 的用途類似 ARP，只是 ARP 是將 IP 對應 MAC，Inverse-ARP 則是將 IP 對應到 DLCI，運作過程異於 ARP，但功能都是透過 L3 位址找 L2 位址。以下圖為例，R1 使用 DLCI 100 產生一條 VC 到 R2，相對的 R2 使用 DLCI 400 會產生一條 VC 到 R1，在 R1 先使用 LMI 詢問 DLCI 狀態(步驟 1 與步驟 2)，當 R1 確定 VC 沒問題後，在步驟 3 就是 Inverse-ARP 的動作，R1 會將自己的 192.168.10.1 送到 R2，在 R2 收到 192.168.10.1 就對應到本地的 DLCI=400 並存儲此筆對應，一樣的動作，R1 收到 R2 對應本地的 DLCI 100。

※Inverse-ARP 為對應本地 DLCI 到遠端 IP 位址



VPN(Virtual Private Network)

VPN 重點是「安全」，在網際網路上建立私密網路，提供私密性和非 TCP / IP 協定的隧道，VPN 是日常用來提供遠端使用者或分離的網路，能透過網際網路之類的公共媒介來連結，而不需要使用更昂貴的永久性措施。介於 LAN 和 WAN，且通常用 WAN 來模擬 LAN 鏈路-因為本地 LAN 上的電腦，必須連到遠端 LAN 並且使用它的資源。

VPN 聽起來像是將 LAN(或 VLAN)連到 WAN，但不止於此。主要差異在於：典型 WAN 使用路由器和其他人的網路（例如 ISP），將更多 LAN 相連。本地主機/路由器視之為遠端網路，而非本地網路。

VPN 使用 WAN 鏈路將本地與遠端相連，讓本地成為遠端的一部分。聽起來很像 VLAN 的定義，且觀念相同：「讓我的主機對遠端而言，看起來像是位於它的區域內」，主要差異在於：對實際上位於本地的網路而言，使用 VLAN 很好；但是對於實際上橫跨 WAN 的遠端網路而言，則選擇使用 VPN。

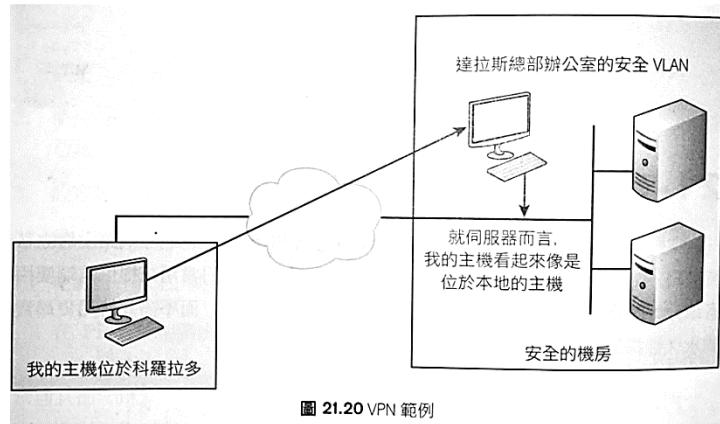


圖 21.20 VPN 範例

VPN 的效益

CCNA 中提到的優點包括：

- **安全性** VPN 使用先進的加密和認證協定，可以提供非常優良的安全性，有助於保護網路免於未經授權的存取。
- IPsec 和 SSL 加密都屬於這個類別，SSL (Secure Socket Layer) 是用於瀏覽器的加密技術，具有原生的 SSL 加密，稱為網站 VPN (Web VPN)。您也可以使用安裝在 PC 上的 Cisco AnyConnect SSL VPN 客戶端，以提供 SSL VPN 解決方案和 Clientless Cisco SSL VPN。
- **節省成本** 將遠端辦公室連到最近的 ISP，然後建立具有加密和認證的 VPN 隧道，比傳統 P2P 專線便宜，且提供較高頻寬。
- **延展性** 可在新地點快速啟用，或讓行動用戶在外安全連線。
- **寬頻技術相容性** 對遠端用戶而言，任何網際網路存取都可以提供對 VPN 的連線。它讓用戶可以利用 DSL 或纜線數據機的高速網際網路存取。

企業與供應商管理型 VPN

公司管理自己的 VPN，就叫企業管理型 VPN。

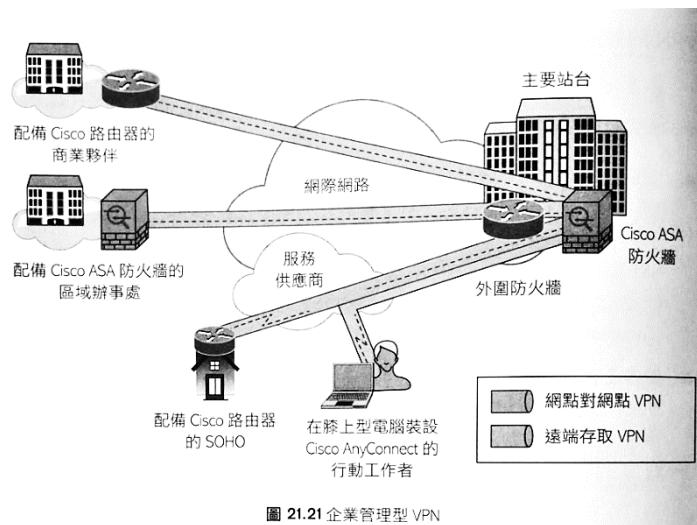


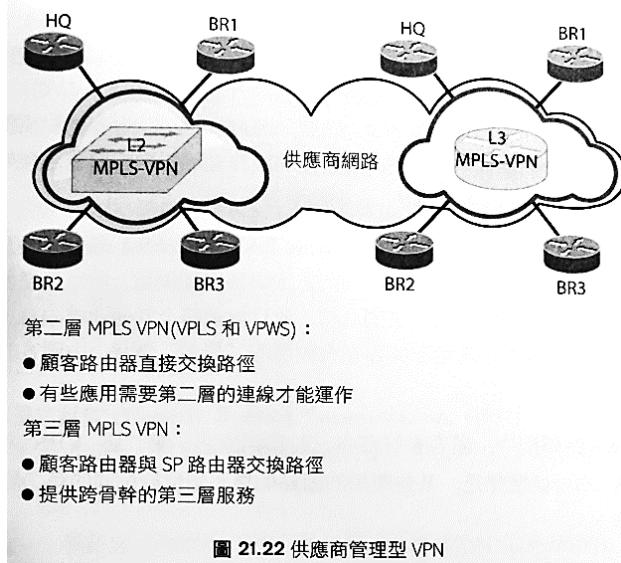
圖 21.21 企業管理型 VPN

企業管理型 VPN 有三類：

- **遠端存取 VPN (remote access VPN)** 遠端使用者（如在家上班者）隨時隨地可安全存取企業網路。

- **網點對網點 VPN (site-to-site VPN)** 又稱為企業內網路 VPN (intranet VPN)，讓公司能安全地透過網際網路之類的公共媒介，從遠端安全連到公司骨幹，不使用像訊框中繼等更昂貴的 WAN。
- **企業間網路 VPN (extranet VPN)** 讓組織的供應商、合作夥伴、顧客能以受限方式連到企業網路進行企業對企業 (B2B) 通訊。

供應商管理型 VPN



第二層 MPLS VPN 使用 MPLS 標籤來傳輸資料。溝通發生在供應商邊緣路由器 (PE, provider edge router) 間，PE 緊接著顧客的網路。

已經擁有第二層網路的網際網路供應商，在其他常見的第三層 MPLS VPN 之外，也可以選擇使用這種 VPN。

第二層 MPLS VPN 有兩種典型的技術：

- **虛擬私有線路服務 (Virtual Private Wire Service, VPWS)** 也稱 ETHoMPLS (Ethernet over MPLS)，或 VLL (虛擬專線，Virtual Leased Line)。VPWS 在附加虛擬電路 (attachment-virtual circuit) 和模擬虛擬電路間具有固定的關係。VPWS 為基礎的服務是點對點的服務，例如在 IP/MPLS 上的訊框中繼/ATM /乙太網路服務。
- **虛擬私有 LAN 交換服務 (Virtual Private LAN Switching service, VPLS)** 多個服務實例會虛擬共享相同乙太網路廣播網域，是虛擬點對點服務。然而每條連線都是獨立的，並且與網路上其他連線隔離。附加的虛擬電路和模擬的虛擬電路間存在有動態的“學習”關係，由顧客的 MAC 位址決定。

VPLS 中，顧客會管理自己的繞送協定。相對第三層 MPLS 的優點是，某些應用若不位於相同的第二層網路，就無法運作。

第三層 MPLS VPN 提供跨骨幹的第三層服務，不同子網路再連到各自網點。通常會在 VPN 上使用繞送協定，所以必須跟 ISP 溝通，以交換路徑。您的路由器 (稱為 CE) 和供應商路由器 (稱為 PE) 間會建立緊鄰關係。ISP 有很多 P 路由器(核心路由器)，其任務是提供 PE 間連線。

設定 VPN 常見的方法有兩種，IPsec、隧道協定。

四種常用隧道協定：

- **第二層轉送 (L2E Layer 2 Forwarding, L2F)** Cisco 專屬。也是它為虛擬私密撥接網路 (Virtual Private Dial-up Network, VPDN) 所建立的第一種隧道協定。VPDN 允許裝置使用撥接連線來建立連到企業網路的安全連線。L2F 後來被 L2TP 所取代，但 L2TP 仍然對 L2F 有向後的相容性。
- 點對點隧道協定 (PPTP, Point-to-Point Tunneling Protocol) 微軟建立的協定，可讓遠端網路安全地傳送資料到企業網路
- 第二層隧道協定 (L2TP, Layer 2 Tunneling Protocol) 由 Cisco 和微軟共同建立。用來取代 L2F 與 PPTP。L2TP 將 L2F 和 PPTP 合併在單一的隧道協定中。
- 通用遶送封裝 (Generic Routing Encapsulation, GRE) Cisco 專屬，會形成虛擬的點對點鏈結，可將多種協定封裝在 IP 隧道中。



Cisco IOS IPsec

是一組產業標準的協定和演算法，可在 OSI L3 運作，在 IP 網路上進行安全的資料傳輸。

「IP 網路」？★★ IPsec 只能加密 IP 交通。對非 IP 交通，必須先為它建立 GRE，再用 IPsec 來加密通道。

IPsec 轉換 (IPsec transform) 指定單一安全性協定和它對應的安全性演算法；沒有這些轉換，IPsec 將無法運作。

安全性協定

IPsec 使用的兩個主要安全性協定 AH 和 ESP

AH 驗證標頭 (Authentication Header)

使用單向雜湊 (one-way hash) 來提供封包資料和標頭驗證，運作方式如下：傳送端產生單向雜湊；然後接收端產生相同單向雜湊，若封包發生改變，就不能通過驗證，並會被丟棄。IPsec 依賴 AH 鑑別來源端。AH 檢查整個封包，但不提供加密服務。ESP 則不一樣，它只提供封包資料的完整性查核

ESP 封裝安全性有效負載 (Encapsulating Security Payload)

提供機密性 (confidentiality)、資料來源驗證、無連線式完整性 (connectionless integrity)、防封包重送服務 (anti-replay service)，藉由破壞交通流分析以達到有限的交通流機密性-ESP 有五個部分：

- **機密性 (加密)** 使用諸如 DES 或 3DES 等對稱式加密演算法提供機密性，其他所有服務都可個別選擇所要的機密性，但 VPN 所有端點選的機密性必須相同。
- **資料完整性** 能確認資料在傳送過程中沒有被竄改。IPsec 使用 checksum 做簡單的資料檢查。

- **認證** 確保和正確對象建立連線。接收端透過確保和授權資訊的來源，以認證封包來源正確。
- **防封包重送服務** 只有在已選擇資料來源認證服務的情況下，才能使用該服務。防封包重送的選擇是以接收端為基礎，只有接收端檢查序號時，這項服務才會有效。封包重送攻擊就是駭客攔截一份認證過的封包，並在稍後將它傳送給預期目的地。當該重複的已認證 IP 封包抵達目的時，可能會破壞服務或做其他的壞事。序號（sequence number）欄位的目的就是要應付這種攻擊。
- **交通流** 若要進行交通流的保密，則必須選擇隧道模式如果是在累積大量交通的安全性閘道中實作，則最為有效-因為在這種大量交通的情況下最容易遮蔽掉真正的來源-目的模式，也就是壞蛋嘗試要破壞網路安全性所要的東西

加密

VPN 在公共網路上建立私密網路，若要維持機密性、安全性，則需要 IPSec 使用各種協定加密，目前使用的加密演算法有下列幾種：

- **對稱式加密** 需要一個共享的金鑰來進行加/解密，在傳送前先加密資料。對稱式加密的標準有資料加密標準（Data Encryption Standard，DES），triple DES（3DES），以及先進加密標準（Advanced Encryption Standard，AES）等。
- **非對稱式加密** 使用不同金鑰來加/解密，這些金鑰稱為私密金鑰與公開金鑰。

私密金鑰用來對訊息的雜湊值（hash）加密，以產生數位簽章，再用公開金鑰解密。公開金鑰可將對稱式金鑰加密，以安全分送給接收主機，然後接收主機再用它獨有的私密金鑰解開該對稱式金鑰。最佳例子就是 RSA（Rivest，Shamir，Adleman）。

GRE(Generic Routing Encapsulation) Tunnel

一種隧道協定，可將許多協定裝在 IP 隧道中。（例如遶送協定 EIGP, OSPF，被遶送協定 IP, IPv6）

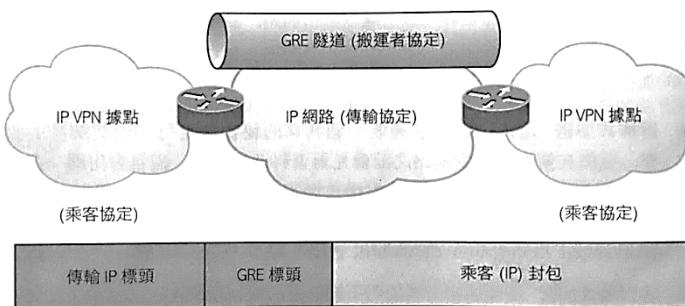


圖 21.23 GRE 隧道結構

思科開發的通道協定之一，可封裝任何 L3 協定，支援傳送 multicast 封包，是少數可支援路由協定的通道協定，GRE 通道將原始 IP 封包再封裝一層新 IP，不管用何種 L3 協定(IPv4 or IPv6)，經過 GRE 時會再封裝一層新的 IP 表頭。GRE Tunnel 又稱 **Carrier Protocol(承載協定)**，負責將原始 IP 封包裝起來送往目的端，傳遞過程不進行任何解封裝動作。

GRE 使用 47port，無加密功能，只能算是 VN 沒有 P。

GRE 隧道支援的標頭：

- 被封裝協定、乘客協定(passenger protocol) IP、IPv6，即 GRE 封裝的協定。
- GRE 封裝協定
- 傳輸協定 通常是 IP

GRE 隧道特徵：

- 使用標頭中的協定類型(TYPE)欄，故任何 L3 協定均可用在 GRE 中。
- Stateless，無流量控制
- 無安全性
- 隧道內的封包產生額外負載，至少 24bytes。

GRE over IPsec

GRE 沒有任何的有效負載（payload）機密性或加密能力，如封包在公共網路上被監聽，它們的內容都是明碼：雖然 IPsec 提供在 IP 網路上用隧道形式傳輸資料的安全方法，但仍然有其限制。

IPsec 不支援 IP 廣播或 IP 多點傳播，所以需要這些功能的協定（如繞送協定）無法使用。IPsec 也不支援使用多重協定的交通，GRE 是可以“承載”其他乘客協定（如 IP 廣播，IP 多點傳播，以及其他非 IP 協定）的協定，因此使用 GRE 隧道搭配 IPsec，就可以執行繞送協定、IP 多點傳播、多重協定交通。

在一般的軸輻式拓樸（例如企業對分公司），可在總部和分公司間做靜態隧道，通常是在 IPsec 上的 GRE。要在網路上增加新輻條時，只要在中樞路由器上設定。輻條間交通必須經由中樞路由器，先離開一條隧道，再進入另一條。靜態隧道是小型網路的解決方案，但輻條數量增加後，就不可行了。

Cisco DMVPN (Cisco 專屬)

DMVPN（動態多點虛擬私有網路。Dynamic Multipoint Virtual Private Network）可以輕鬆建置 IPsec VPN。為了降低成本、易於設定、有彈性的連線，Cisco 提出 DMVPN。DMVPN 有一台中樞路由器，例如總部路由器，稱為中軸（hub），而分公司稱為輻條（spoke）。所以企業對分公司的連線才稱為軸輻式互連。這種設計類似訊框中繼。DMVPN 在 hub 設定單一 GRE 隧道界面和單一 IPsec 基本資料，以管理所有 spoke，並讓 hub 上的組態不因更多 spoke 加入而增加。DMVPN 也讓資料在 spoke 間互傳時，能動態地在其間建立 VPN 隧道。

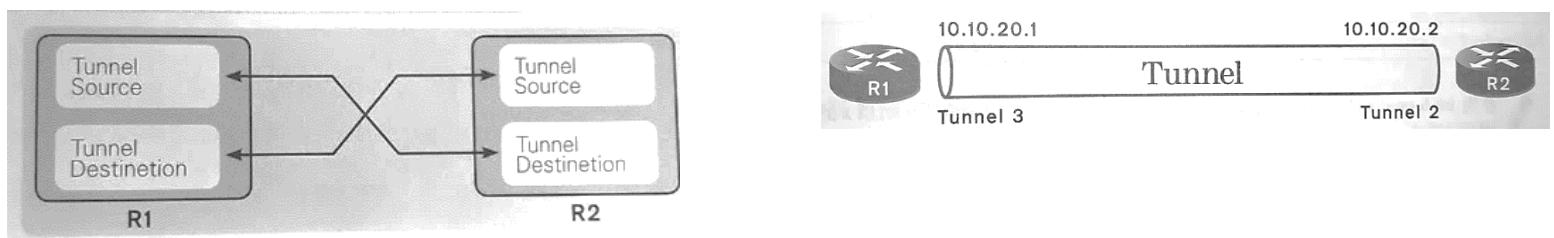
Cisco IPSec VTI (Cisco 專屬)

IPsec 組態的虛擬隧道介面(VTI, Virtual Tunnel Interface)模式可在遠端存取需要保護時，簡化 VPN 組態。它提供比 GRE 或 L2TP 更簡單的 IPsec 封裝與加密地圖。它像 GRE 一樣會傳送繞送協定和多點傳播交通，但不需要 GRE 協定及其相關的額外負擔。所有交通都經過加密，並只支援一種協定-IPv4 或 IPv6，就像標準的 IPsec。

建立 GRE 通道介面

GRE 通道需要在兩端各建一個通道介面(Tunnel Interface)，靠這兩個虛擬介面(類似 Loopback，使用 int tunnel 指令建立)溝通，

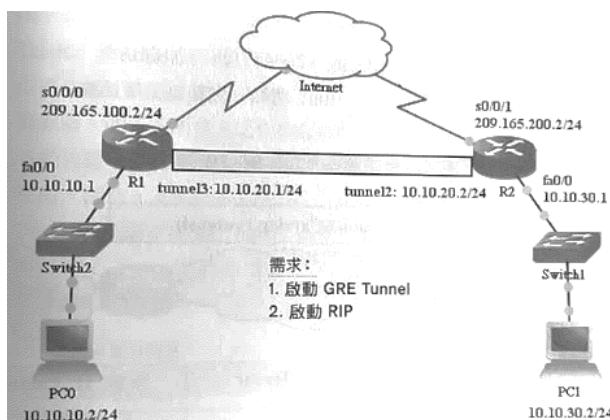
要通過 internet 來連線，需指定通道 Source & Destination，以下圖 R1 通道介面為例，來源 S0/0/0，目的 R2 S0/0/1，R2 通道介面則反過來。GRE 通道建立後，通道是網路連線，視為虛擬線路，所以要有 IP。Tunnel source IP & Tunnel destination IP 作為新的 IP Header，為封包在 Internet 繞送的依據。



兩台路由器的 Tunnel Source & Destination IP 對應關係

- 常用 GRE Tunnel 指令(參考下圖)

指令	說明
Router(config)#int tunnel <i>x</i>	建立 tunnel <i>x</i> 介面，並給予 IP
Router(config-if)#ip add 略	#tunnel 兩邊的編號可以不同
Router(config-if)#tunnel mode gre ip	設定 tunnel 使用的模式為 gre ip
Router(config-if)#tunnel source s0/0/0	設定 tunnel 的來源、目的(以 R1 為例)
Router(config-if)#tunnel destination 209.165.200.2	(目的設實體 ip，不是 tunnel ip)
#show run int tunnel <i>x</i>	如題
#show ip int br	檢查是否有 tunnel 介面
#show int tunnel <i>x</i>	檢查 tunnel 組態設定、介面狀態(up/up)、IP、來源/目地、協定 GRE/IP
#show ip route	如題



- 通道建立好後，R1 可以 PING 到 R2 的 Tunnel IP，但 PC0 還是 ping 不到 PC1，因為 R1 並不會有 10.10.30.0/24 的路由資訊。所以要在 R1、R2 啟用路由協定來讓它們互學遠端路由，所以在 R1、R2 都啟用動態路由協定後 network 10.0.0.0 宣告出去就可，但不可宣告 209.165.100.0/24 以及 209.165.200.0/24(IP 實體介面的網段)，不然就不會經過通道，而是經由 Internet 實體介面。



單宿主 EBGP(Exterior Border Gateway Protocol)

BGP 使用於 ISP 業者，是常見的遠送協定，ISP 間使用 BGP 跨網路交換路由。

外部 v.s. 內部閘道協定—以 ospf 比較

特性	BPG	OSPF
遠送演算法	路徑向量	鏈路狀態
無級別支援	是	是
VLSM 支援	是	是
路徑總結	所有 BGP 路由器	ASBR/ABR
衡量指標	多種	頻寬
階層式	否	是
建構單位	自治系統	區域
基礎協定	TCP 179	協定值 89
交通類型	單點傳播	多點傳播
鄰居	特別設定	發現/設定
路徑交換	僅限鄰居	僅限緊鄰的鄰居
初始更新	同步資料庫	同步資料庫
更新頻率	遞增	60 分鐘計時器遞增
Hello 計時器	60 秒	10 / 30 秒
Hold 計時器	180 秒	40 / 120 秒
內部路徑交換	內部 BGP 會談	LSA TYPE 1、2
外部路徑交換	外部 BGP 會談	LSA TYPE 3、4、5
路徑更新	含網路、屬性、AS 路徑	含網路、衡量指標(LSA TYPE 3、4)
網路敘述	宣傳網路	在介面上啟動 OSPF
特殊功能	路徑反射器	殘根、完全殘根、NSSA 區域

在演算法部份 BGP 使用路徑向量(Path Vector)，其在學習遠端網路部份類似距離向量，由 BGP 路由器通報路由給 BGP 鄰居。

在決定最佳路徑上是根據不同路徑屬性(Path Attributes)，與其它的動態路由協定完全不同。

BGP 屬於 EGP(Exterior Gateway Protocol)分類。

BGP 鄰居若在同 AS(設定 BGP peer)，稱為 IBGP(internal)鄰居，IBGP 不必共用同網路，且可被其它未執行 BGP 的路由器分隔(但每個 IBGP 路由器必須設定為同區域中所有 IBGP 路

由器的鄰居)。;若在不同 AS(顧客網路-ISP)，稱為 EBGP(external)鄰居。EBGP 要共用同網路，且可直接彼此存取，每個 EBGP 不必互為鄰居。

BGP 可宣傳經由動/靜態、重分送(redistribution)所學到的網路。

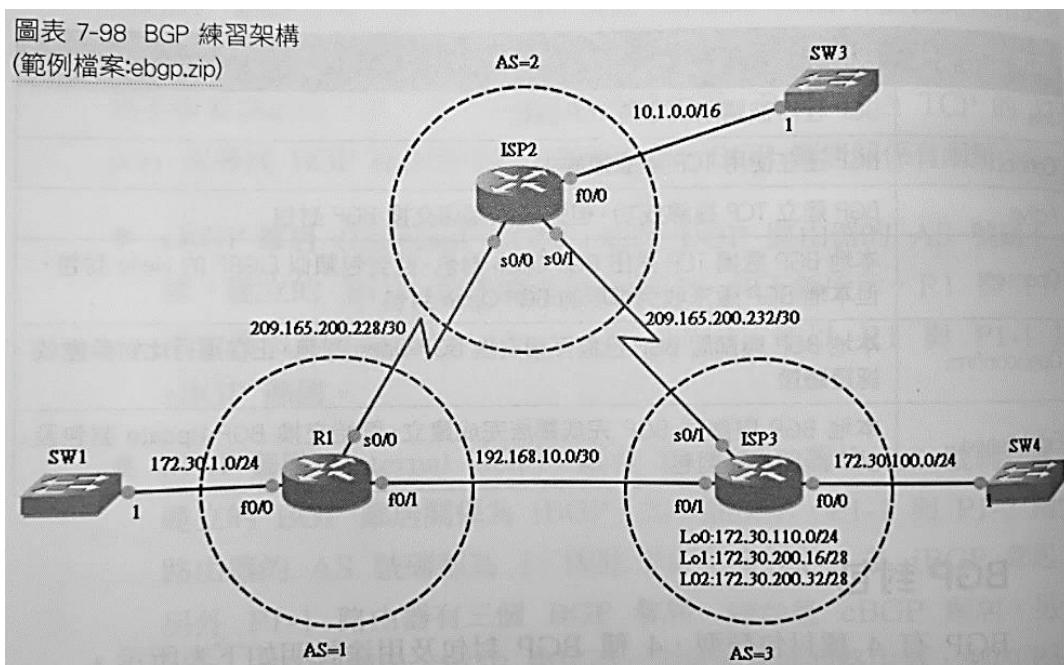
BGP 以 AS(Autonomous System 自治區)為單位，BGP 在 AS 間交換路由資訊，所以 BGP 路由器必須屬於一個 AS 才能運作，如下圖，路徑是以 AS 為主，而不是以路由器作路徑。

ASN(AS Number)：由 IANA 統一管理，像 IP 一樣分公私有。

AS Number Range	Purpose
0	保留
1-64,495	公有 ASN，由 IANA 分配
64,496-64,511	保留
64,512-65,534	私有 ASN，無須申請即可使用
65,535	保留

CCNA 拖圖題考過

eBGP Configuration



設定 EBGP 需要：

- AS 編號(自己及所有遠端的，不能重覆)
- BGP 中的所有鄰居(對等節點)及其 IP
- 要宣傳到 BGP 的網路



BGP 指令(以上圖為例)

指令	說明
R1(config)#router bgp 1 #AS=1-65535	啟動 BGP 程序，AS=1 #一台路由器只能有一個 BGP 程序，

	只屬於一個 AS。
R1(config-router)#neighbor <u>290.165.200.230</u> remote-as 2	宣告鄰居及其要使用的介面 IP， remote-as 為鄰居 BGP AS #router 沒有自動發現鄰居功能，需手動設定 ISP3 同上
R1(config-router)#neighbor 192.168.10.2 remote-as 3	
Router(config-router)#network <u>網段</u> mask ____ ※BGP 的 network 指令為 no auto-summary	設定 BGP 通報路由
#show ip bgp	查詢 BGP 表(所有路徑的資訊)
#show ip bgp summary	查詢 BGP 狀態，包含鄰居、鄰居 IP、 鄰居 AS、會談狀態
#show ip bgp neighbors	查詢 BGP 鄰居資訊，包含 TCP 會談 資訊、BGP 參數、TCP 計時器/計數器
#show ip bgp neighbors <i>ip</i> advertised-routes	查詢通報給 BGP 鄰居的路由
#debug ip bgp	觀察 bgp 運作
Router(config-router)#neighbor <i>ip</i> shutdown --啟動用 no...shutdown	關閉 BGP neighbor(開啟用 no)

p.s. 一個路由器只能有一個 BGP ASN

#show ip bgp summary

圖表 7-101 R1 查詢 BGP 鄰居

```
R1# show ip bgp summary
BGP router identifier 209.165.200.229, local AS number 1
BGP table version is 1, main routing table version 1
Neighbo      V   AS  MsgRcvd  MsgSent  TblVer  InQ OutQ Up/Down State/PfxRcd
192.168.10.2  4    3     0       0        0       0     0 never   Active
209.165.200.230 4    2     0       0        0       0     0 never   Active
```

--Neighbor : R1 宣告 BGP 鄰居路由器的 IP

--AS : BGP 鄰居的 ASN

--Up/Down : 鄰居建立後維持的時間，時間越久表示 BGP 鄰居關係越穩定，never 表示未建立鄰居。

--State/pfxRcd : State 表示 BGP 鄰居建立的狀態，Active 表示鄰居 tcp 連線建立成功，未交換 bgp 封包。pfxRcd 表示收到的 bgp 更新封包數，當 bgp 開始通報路由時就會有數字。

#show ip bgp

BGP 表，類似 EIGRP Topology table，重點：

- ① 最左邊「>」代表最佳路徑(若有備援路徑會顯示在另一行)



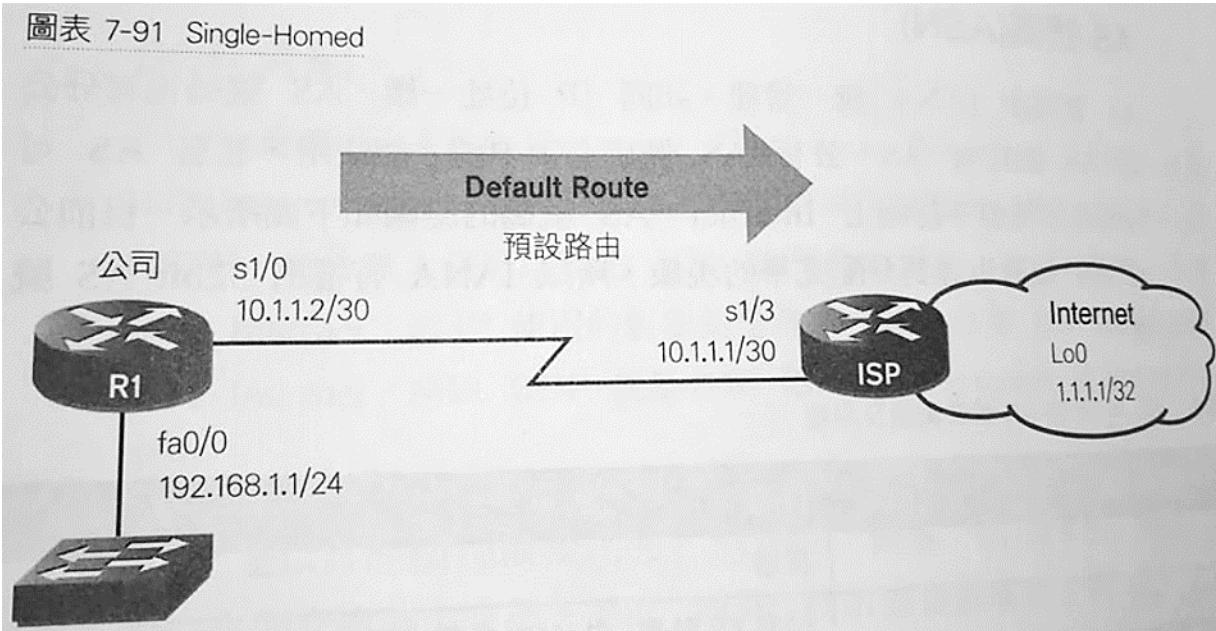
② 路徑表中 next hop 0.0.0.0 那行代表為本機宣傳的路徑

③ 最右邊 path 表示經過的 ASN

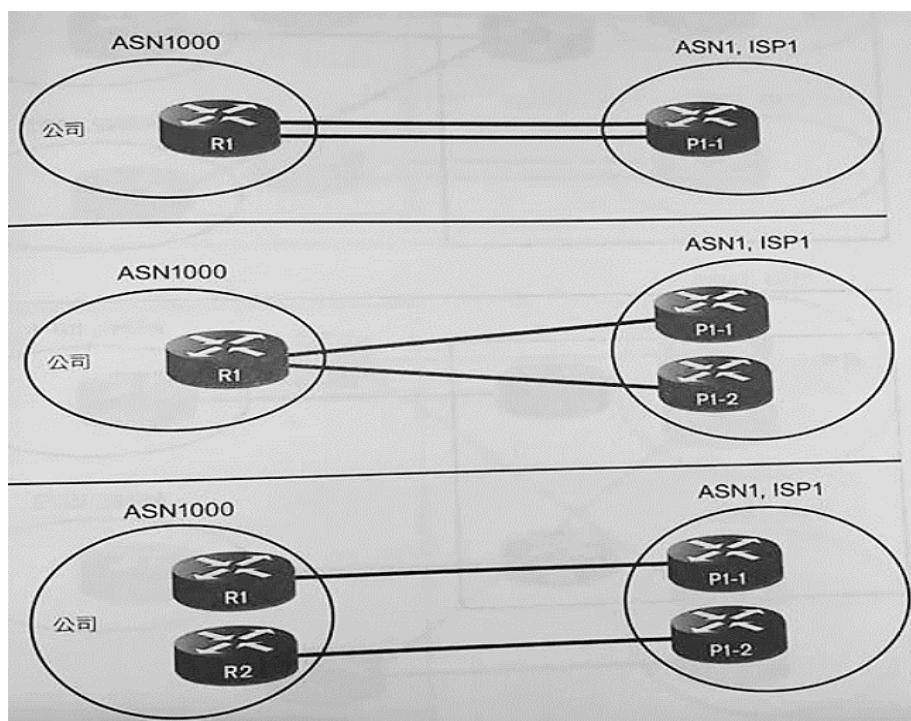
公司/企業常見 BGP 使用狀況分類

- 公司與 ISP 間有四種連線接法：Single-homed, Dual-homed, Single-multihomed, Dual-multihomed。Single 為單一線路連接，Dual 為多條線路連接，Home 為單一 ISP 業者，Multihome 為多個 ISP 業者。

1. Single-homed – 單純的靜態路由，無備援，所以有其它三個備援方式

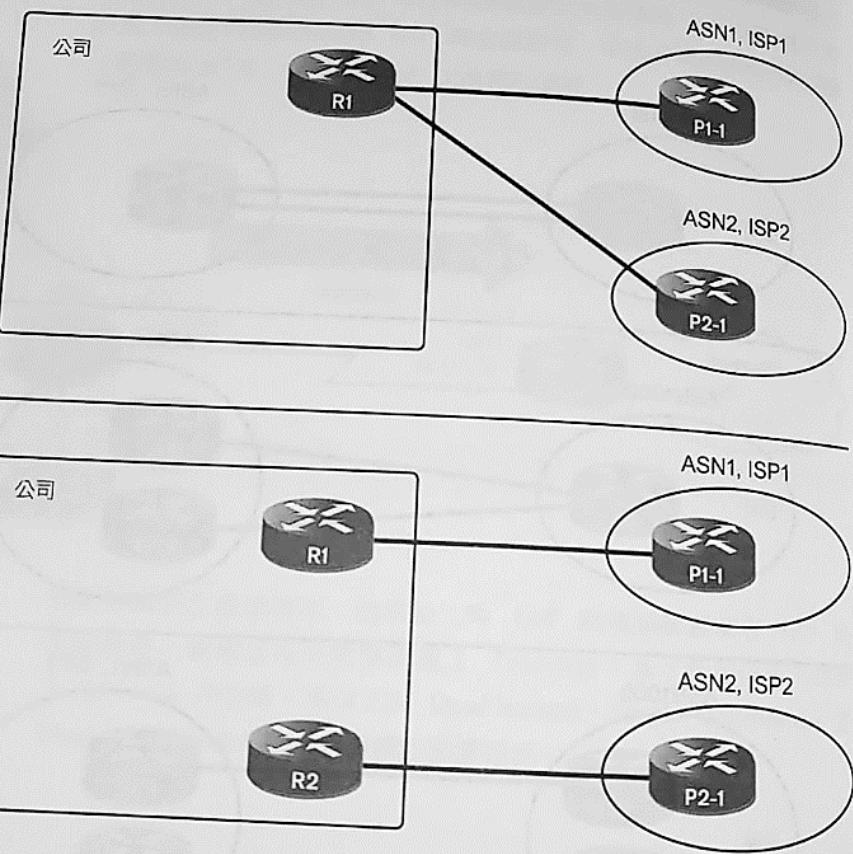


2. Dual-homed – 對單一 ISP 的連線做備援，但 ISP 業者掛掉就沒辦法了



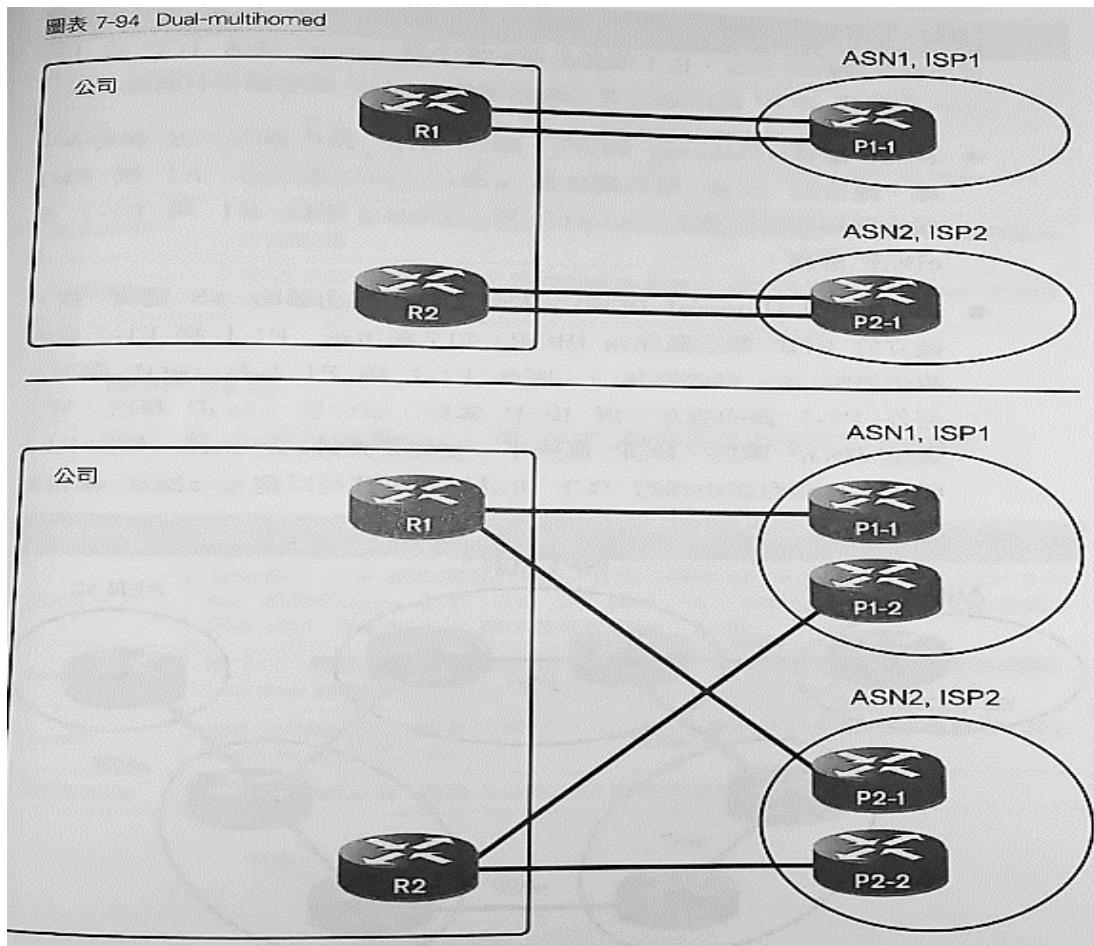
3.Single-multihomed – 公司對多個 ISP，但公司本身沒有做備援

圖表 7-93 Single-multihomed



4.Dual-multihomed – 公司對多個 ISP，且對單一 ISP 都有備援

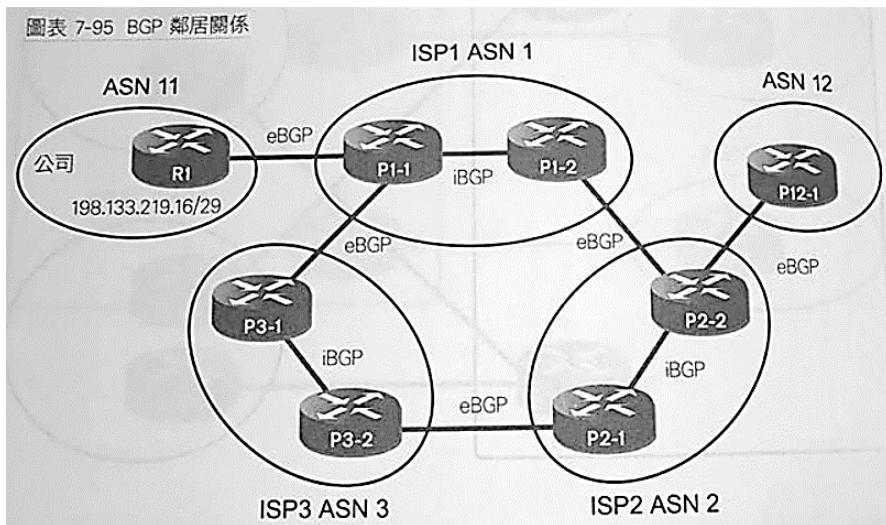
圖表 7-94 Dual-multihomed





BGP 的鄰居關係

- Like OSPF/EIGRP，BGP 在通報路由資訊前也要建立鄰居關係。
- EIGRP/OSPF 發 HELLO 封包建立鄰居關係；BGP 則不用封包建立，也不需要直接路由器，BGP 透過 TCP 179 port 來尋找 BGP 路由器並建立鄰居關係。
- BGP 鄰居不一定是要直連的路由器，比如下圖 P3-1 可與 P2-1 TCP 互通便可建立 BGP 鄰居
- BGP 鄰居關係有兩類(範例如下)：
 - eBGP(External BGP)：兩台不同 ASN 的 BGP 路由器建立起來的關係。
 - iBGP(internal BGP)：兩台相同 ASN 的 BGP 路由器建立起來的關係。



- BGP 鄰居狀態
建立 BGP 鄰居的過程中會有 6 種狀態轉換：

BGP 鄰居狀態	說明
Idle	BGP 程序被關閉或等待 TCP 連線
Connect	BGP 使用 TCP 建立連線中
Active	BGP 建立 TCP 成功，但未和鄰居交換封包
Opensent	本地 BGP 透過 TCP 送出 BGP Open 封包，類似 EIGRP 的 Hello 封包，但本地 BGP 尚未收到鄰居的 BGP Open 封包
Openconfirm	本地與鄰居已完成交換 BGP Open 封包，進行參數比對、驗證中
Established	本地與鄰居已完成鄰居建立，開始交換 BGP Update 封包及 BGP Keepalive 封包

- BGP 封包類型 4 種

BGP 封包	說明
Open	用來建立 BGP 鄰居關係的封包，類似 EIGRP 的 Hello 封包，當收到鄰居的 Open 封包，本地 bgp 要和該封包中的參數、密碼驗證做比對，通過後就可以建立鄰居。
Keepalive	BGP 鄰居建立後，會發送此封包維繫鄰居關係，功能也類似 EIGRP 的 Hello 封包。

	包
Update	包含通報的網路 IP 位址、MASK、相關的路徑屬性，類似 EIGRP 的 Update 封包
Notification	當 BGP 有錯誤時，使用此封包通知 BGP 鄰居

=====



大原則

1. 檢查實體層(纜線及介面)，並確認介面的統計資訊(L1、L2)
2. 確定裝置有正確路徑，視需要修改增刪路由表。
3. 確認預設閘道
4. 確認 DNS
5. 確認有無 ACL

Show interface 的詳細解說

R2#sh int fa0/0

FastEthernet0/0 is up, line protocol is up

[output cut]

Full-duplex, 100Mb/s, 100BaseTX/FX

ARP type: ARPA, ARP Timeout 04:00:00

Last input 00:00:05 , output 00:00:01, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

 1325 packets input, 157823 bytes

 Received 1157 broadcasts (0 IP multicasts)

 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

 0 watchdog

 0 input packets with dribble condition detected

 2294 packets output, 244630 bytes, 0 underruns

0 output errors, 0 collisions, 3 interface resets

 347 unknown protocol drops

 0 babbles, **0 late collision**, deferred

 4 lost carrier, 0 no carrier

 0 output buffer failures, 0 output buffers swapped out

速度與雙工設定 介面錯誤最常見的原因是鏈路兩端雙工模式不符。雙工設定不符會收到大量的錯誤、間歇的斷線、甚至完全掛掉。(預設自動協商速度和雙工)

#如果雙工不符合通常會看到碰撞計數器增加

● **Input queue drops** 如果輸入佇列丟棄計數器增加，表示送到路由器的交通超過它的處理能力，如果持續很高，嘗試這些計數器增加的時間點，以及這些事件與 CPU 使用狀況的關係。ignored 和 throttle 計數也會增加。

- **Output queue drops** 這個計數器表示封包因介面壅塞而丟棄，導致併列延遲。當它發生時，諸如 VoIP 之類應用會發生效能問題，如果您觀察到它持續增加，請考慮 QoS。
- **Input errors** 通常表示高錯誤率，例如 CRC。它可能是纜線問題、硬體問題、或是雙工不 符合。
- **Output errors** 在碰撞之類問題發生時，該埠嘗試傳送的訊框總數。

用 IP SLA 進行故障檢修



IP 服務等級協定(Service- Level Agreement, SLA)，使用 IP SLA ICMP 的 echo 來偵測遠端裝置，而不需要手動執行 ping。

使用 IP SLA 的理由如下：

- 邊緣對邊緣(edge-to-edge)網路可用性的監測。例如封包遺失統計
- 網路效能監控/可視性。例如網路延遲時間和回應時間
- 基本網路運作的故障檢測。例如端點對端點的網路連線

指令	說明
Router(config)#ip sla <u>1</u>	啟用 sla 運算，可使用 1-21 億做為運算編號
Router(config-ip-sla)#icmp-echo <u>目的 IP</u>	設定 IP SLA ICMP echo 檢測和目的地
Router(config-ip-sla-echo)#frequency <u>10</u>	設定檢測頻率(秒)
Router(config)#ip sla schedule ? <1-2147483647> Entry number Router(config)#ip sla schedule <u>1</u> life ? <1-2147483647> Life seconds (default 3600) Forever continue running forever Router(config)#ip sla schedule <u>1</u> life forever start-time ? 省略 Router(config)#ip sla schedule 1 life forever start-time now	安排 SLA 檢測排程
#show ip sla configuration #show ip sla statistics	檢查 ip sla 運算

QUESTION 474

Which two criteria must be met to support the ICMP echo IP SLA? (Choose two)

- The destination device must support the echo protocol
- default gateway must be configured for the source and destination devices
- The source device must be running Layer 2 services.
- The source and destination devices must be Cisco devices
- The source device must be a Cisco device but the destination device can be from any vendor

Correct Answer: AE



使用 SPAN 進行故障檢測

網路交通的嗅探器 sniffer 是網路監控和故障檢測的好工具。在有交換器之前，我們是使用集線器；而當集線器在某個埠接收到數位信號時，它會把信號送給其他所有的埠。因此，連接在集線器埠上的 sniffer 就可以接收到網路上所有的交通。

交換器開機後，會根據接收到的不同封包來源 MAC 建立第二層轉送表。這種預設做法會讓連接在另一個埠的 sniffer 無法收到其他單點傳播的交通。交換器中引入了 SPAN 功能以協助解決這個問題(參見圖 20.2)。

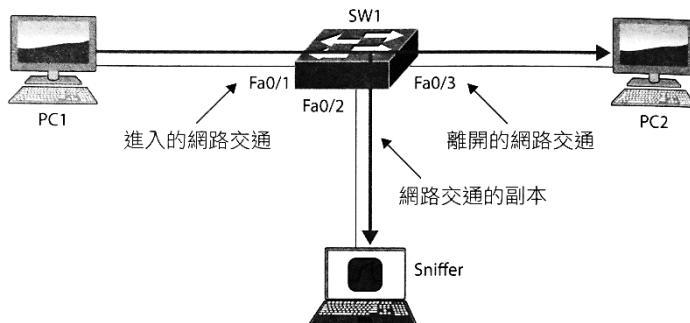


圖 20.2 使用 SPAN 進行故障檢測

SPAN 功能讓你可以分析流經該埠的網路交通，並且將該網路交通的副本送往交換器上連接有網路分析器或其他監控裝置的埠。SPAN 會複製來源埠對目的埠所傳送或接收的網路交通，以做為分析之用。

例如，假設想要分析從 PC1 流到 PC2 的網路交通，如圖 20.2，必須先指定想要用來擷取該資料的來源埠。您可以設定介面 Fa0/1 以捕捉進入的交通，或是設定介面 Fa0/3 以捕捉離開的交通。接著指定 sniffer 要連接、並捕捉封包的目的埠介面，在本例中為 Fa0/2。從 PC1 流到 PC2 的網路交通就會被複製到該介面，之後就可以使用網路交通的 sniffer 來進行分析。

指令	說明
S1(config)#monitor session 1 source interface f0/1	在想要監控的來源埠上指定一個 SPAN session number
S1(config)#monitor session 1 dest interface f0/2	在 sniffer 的目的埠上指定一個 SPAN session number
#show monitor	檢查 SPAN session 的設定



IPv6 troubleshooting

常用指令	
Show ipv6 int br	
Show ipv6 neighbors	檢視鄰居解析表(mac-IP)

被解析位址的可能狀態：

- **INCOMPLETE(incomplete，未完成)** 該項目已經執行了位址解析。送出鄰居召喚訊息，但是還沒有收到鄰居的訊息。
- **REACH(reachable，可抵達)** 已經收到確認，通往鄰居的這條路徑運作正常。REACH 是好的狀態！
- **STALE(呆滯)** 當介面在鄰居可抵達時間範圍(neighbor reachable time frame)內沒有進行通訊時，就是 STALE 狀態。下次鄰居進行通訊時，狀態就會變回 REACH。
- **DELAY(延遲)** 發生在 STALE 狀態之後；在所謂 **DELAY-FIRST PROBE TIME** 時間內都沒有收到可抵達確認的時候。這表示這條路徑之前運作正常但是在鄰居可抵達時間範圍內沒有任何通訊。
- **PROBE(探測)** 在 PROBE 狀態下，設定的介面會回應鄰居召喚，並且等待鄰居的可抵達確認。

VLAN 連線的故障檢測



VLAN 故障檢測的步驟：

1. 檢查所有交換器上的 VLAN 資料庫
2. 檢查 CAM(內容可定址記憶體)表
3. 檢查 VLAN 埠的指派是否設定正確

會用到的指令	
Show vlan brief	檢查是否有正確的 VLAN
Show mac address-table	檢查 CAM
Show interfaces interface switchport	確認該埠的設定、狀態
Switchport access vlan vlan	略

Trunk troubleshooting

當相同 VLAN 上，位於不同交換器的主機間無法連線時，就必須檢查 TRUNK。Cisco 將該象稱為 Vlan leaking，就像是在交換器間流失了某 VLAN 設定。

下為檢測 VLAN TRUNK 的步驟：

1. 確認介面組態設定了正確的 TRUNK 參數
2. 確認埠的設定正確
3. 確認每台交換器上的原生 VLAN

會用到的指令	
Show interfaces trunk	檢查交換器間的 trunk 連線
Show vlan brief	檢查是否有正確的 VLAN
Show interfaces interface trunk	確認該埠的主幹設定，是/不是主幹

Show interfaces <u>interface</u> switchport	確認該埠的 mode(dynamic auto/其他)
Show dtp interface <u>interface</u>	查詢 dtp 狀態
Switchport mode	
Switchport mode dynamic	
Switchport trunk native <u>vlan</u>	

網管工具—NTP, Syslog, Netflow, SNMP, SLA, SPAN, QoS



NTP(Network Time Protocol)網路時間校時

- 使用 UDP123 讓主動與 NTP 設備進行時間校時
- 為了防止非法 NTP，可以做 Authentication，ccnp 範圍

NTP Server(Switch)

↓stratum 的值從 1-15，預設 8，16 為無接收 ntp

首先要有一台 ntp master(如果是在 LAN 之內)

比如說以上課的 lab，在 switch 的 conf t 底下>>**ntp master x** x 為層數預設為第 8 層

NTP Client

(config)#ntp server ntp master IP version4

(config)#service timestamps log datetime msec →syslog 加入時間戳記

◎確認向哪台主機同步

#show ntp associations

◎查詢同步狀態

#show ntp status

◎在題庫看到沒用過的指令，大概是驗證用的

#ntp authentication-key 1 md5 0822455D0A16 7

#ntp authenticate

Syslog



· IOS 訊息格式

一個 IOS 訊息主要有三部份，如下所示為一個 IOS 訊息，此訊息為 f0/0 shutdown 時產生。訊息中第一部份為 IOS 訊息產生時間，此部份也可使用序列號(Sequence No.)，第二部份為 IOS 訊息摘要，產生來源、嚴重等級及簡易說明，『%LINEPROTO-5-UPDOWN』中 LINEPROTO 為訊息產生來源，5 為嚴重等級，UPDOWN 為該訊息的簡易說明，第三部份為該訊息的詳細內容。

Oct 29 10:00:01 EST: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

IOS 訊息嚴重等級分類 --考點

分 8 級，數字越小越嚴重，比如 Lv0 的訊息表示系統無法運作、Lv5 的訊息為一般通知訊息、Lv7 表示使用者啟動 debug 指令產生的訊息。(設定為 3 級可看到 0123，以此類推)

等級	關鍵字	說明
0	Emergencies	System is unusable 系統無法使用
1	Alerts	Immediate action is needed 需要立即採取行動
2	Critical	Critical conditions exist 危急狀況
3	Errors	Error conditions exist 錯誤狀況

4	Warnings	Warning conditions exist 警告狀況
5	Notification	Normal but significant condition 正常但重大狀況
6	Informational	Informational messages only 正常資訊訊息(預設)
7	Debugging	Debugging messages 偵錯訊息

IOS 訊息輸出

IOS 訊息可輸出到 **Console** 畫面、**VTY** 畫面、記憶體緩衝區及 **Syslog** 伺服器等，預設 IOS 的訊息只會記錄(**Log**)在 Console 畫面或 VTY 畫面。若要將 IOS 訊息記錄下來，可選在記憶體衝區或伺服器儲存。

- **Syslog** 預設等級 7，會顯示在控制台(console)並送入緩衝區(buffer)，(取消)可使用指令
(config)#(no) logging ?(console/buffered...)

p.s.**(config)#logging console/buffered** 為預設值

◎查詢緩衝區資訊

#show logging

◎VTY 預設不顯示 IOS 訊息，要在管理者模式下 **terminal monitor** 來顯示

1. syslog→事件管理

軟體如 kiwi syslog 等

2. SNMP→設備效能與狀態監控

軟體如 MRTG, PRTG

3. Netflow→內部網路流量分析，可得知哪些 IP 與服務

SNMP Lab—工具在 ccna share 裡的軟體

Router(config)#snmp-server community **public** rw

→基本上有支援 SNMP 的裝置都用 public 為預設群組名稱

#Snmp 軟體--PRTG !!!要配合 udp 161/162 port 有時防火牆會擋

配合 syslog 軟體—kiwi syslog 做事件管理 !!!要配合 udp 514 port 有時防火牆會擋

Router(config)#loggin **192.168.1.100** →將 syslog 存在該位置(伺服器 ip)

Router(config)#logging trap **debugging/7** →debugging 代表 Lv7，用?可看到選項

Router(config)#service timestamps log datetime msec →取得時間戳記訊息，配合 NTP 使用

使用序列標號而不使用日期時間：

(config)#no service timestamps

(config)#service sequence-numbers

p.s.最後的 lab 有個指令是 **ip route ip mask ip/int track ...** 當 track 的對像掛掉時該筆路由將不執行，一種浮動路由的作法



QoS 的模式

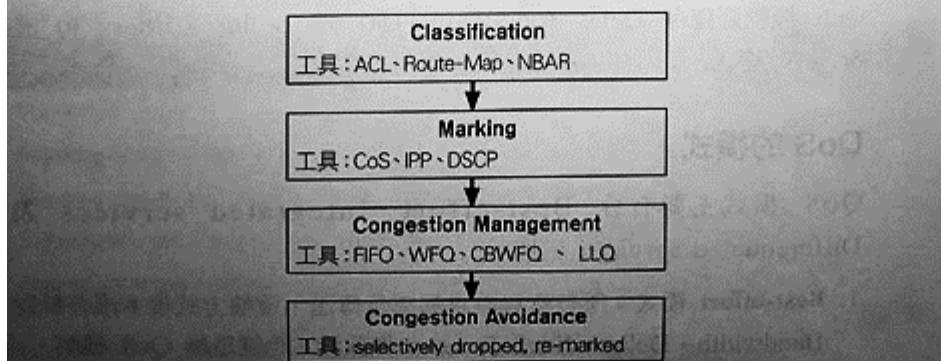
QoS 模式主要有分 Best-effort、Integrated services 及 Differentiated services 三種。

1. **Best-effort 模式**：所有資料流量都盡量傳送，這種方式根本沒有針對 Bandwidth、Delay、Jitter 及 Loss 做保證，也就是無 QoS 機制。
2. **Integrated services (IntServ)模式**：QoS 的保證是從來源端到目的端所經過路由器都要能確保有足夠的資源保留給 QoS 後，應用程式的資料封包才會傳送出去，如何確定經過的路由器都要保留資源來符合 QoS 的參數要求，就需要使用 Resource Reservation Protocol (RSVP)來詢問每台路由器並保留頻寬給 QoS 使用。IntServ 模式在 Internet 比較難實作。
3. **Differentiated services (DiffServ)模式**：此模式會先將資料封包分類 (Class)與標記(Mark)，路由器根據封包的標記來給於資料封包不同的 QoS 等級，每一台路由器各自根據封包中的標記來做 QoS 行為稱為 PHB(Per Hop Behavior)，這點 IntServ 模式不一樣。本單元將針對此種模式的 QoS 做法進行探討。

DiffServ 模式運作

DiffServ 模式的 QoS 運作流程如下圖所示，當一台路由器收到資料流量時，第一步要將資料流量分類(Classify)，分類後的封包要做標記(Mark)，此標記是為了可以辨識分類的流量封包，之後根據封包中的標記來將封包分優先等級；接下來要做壅塞管理(Congestion Management)，壅塞管理主要是佇列(Queueing)的技術，讓優先權較高的封包可以優先送出；當佇列已經快滿了，就要執行壅塞避免(Congestion Avoidance)，壅塞避免主要就是將封包丟棄，以避免佇列溢出(Overflow)。

圖表 17-46 DiffServ 模式 QoS 的處理步驟



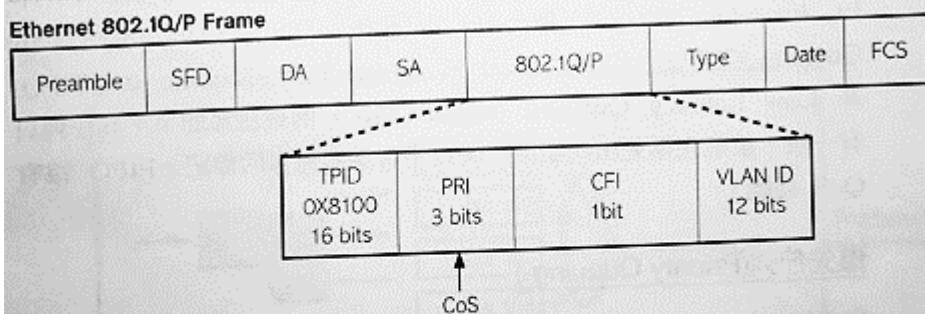
分類(Classification)

將資料流量分類是做 QoS 的第一步，可以使用 ACL 或 Route-Map 根據封包中的 L2、L3 及 L4 的表頭檔資訊來進行分類，如果要使用封包的 L7 的表頭檔來進行分類就要使用 Network Based Application Recognition (NBAR)協定。

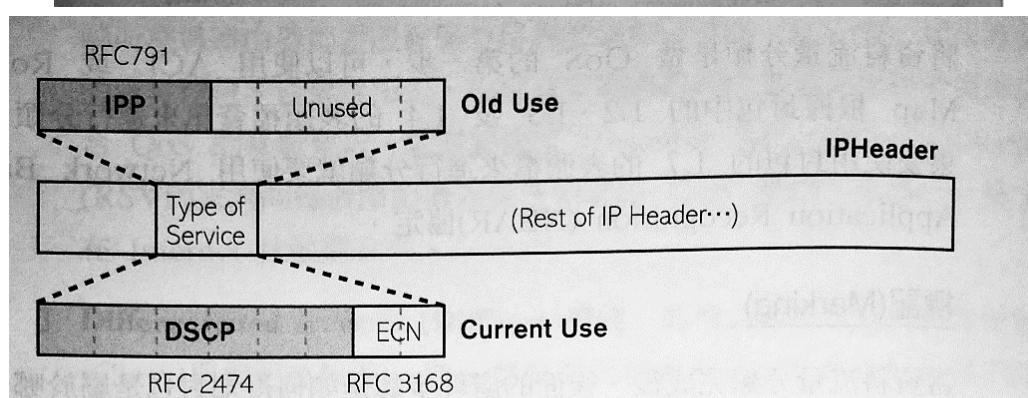
標記(Marking)

當資料流量分類完成後，後面的處理步驟是如何得知封包是屬於哪一個分類，所以要在一個封包完成分類後，在封包中做個標記以便後續的辨識，標記的資訊可以記錄在 L2 或 L3 的表頭檔。以 L2 Ethernet 表頭檔中會有一個欄位 CoS(Ethernet Class of Service)，如下圖所示，CoS 有三個 3bit，所以有 8 種分類可以將封包做標記，其他 L2 協定的標記欄位有 Frame Relay 使用iscard Eligibility (DE)、ATM 使用 Cell Loss Priority (CLP)及 MPLS 使用 Traffic Class (TC)。

圖表 17-47 Ethernet 表頭檔的 CoS 欄位



在 L3 以 IP 表頭檔的標記欄位有 ToS(Type of Service)，如下圖所示，ToS 有 8bits，在 IPP(IP Precedence) 定義使用前面 3bits 來將做標記使用，3bits 可以有 8 種分類可以標記；後來又定義 DSCP(Differentiated Services Code Point) 標記規格，DSCP 使用 ToS 欄位前面 6 bits，共有 64 種標記方式。



當資料封包設定標記後，如果下一台路由器還要使用封包的標記，此時就要設定信任邊界(Trust Boundary)，當路由器設定屬於信任邊界，則該路由器繼續使用上一台路由器的封包標示，如果不是，則需要重新在做一次分類再標記，所以如何定義 Trust Boundary 的範圍也是在做標記要考慮。

QoS 機制

根據封包欄位區分交通型態，送給政策實施機制(policy enforcement mechanism)，進行管制(policing)。

政策實施機制包含**標記、排隊、管制、塑型**。(訊框/封包中的欄位可用來標記交通)

● CoS(Class of Service) L2 訊框標記，**3 位元**。使用 802.1Q VLAN tagging 時，它在訊框標頭中稱為 PCP(Priority Code Point)。

● ToS(Type of Service) **8 位元**，L3 封包標頭中做 IP 優先序判別。

● DiffServ/DSCP(Differentiated Service Code Point) 用來分類、管理交通，並提供服務品質。在 IP 標頭的 **8 位元 DS(Differentiated Services field)** 中使用 **6 位元 DSCP**。

DSCP 可以理解為 IP 交通類別優先序判別的新方法，具有向後相容性，可替代 **ToS**。

● Class Selector 使用與 IP 優先序相同的 3 位元，用來指示 DSCP 值的 3 位元子集合。

● TID(Traffic Identifier) 使用在無線訊框，描述 802.11 中 QoS 控制欄中的 3 位元。

Cos 用在有線網路，**TID** 用在無線網路。

分類標記工具

盡量在靠近信任邊界的地方進行交通標記，交通分類常見三種：

● **標記** 檢查現有 L2/L3 標頭，並根據已有標記分類。

● **定址** 使用標頭中的來源/目的 **L2 位址/L3 位址/L4 埠號**。可以用 IP、埠號將交通分類。

● **應用簽章** 檢查有效負載裡的資訊，稱為 deep packet inspection。

NBAR—應用簽章中的重要部份

Network Based Application Recognition，提供 L4-L7 的深度封包檢查，但比單純的定址分類或 ACL 消耗更多 CPU。因為 L3-L4 不能識別應用，所以 NBAR 會深入檢查封包有效負載，並與其簽名資料庫(PDLM, Packet Description Language Model)比對。NBAR 使用兩種運作模式：

--被動 提供應用協定、介面、位元速率、封包、位元組數量即時統計。

--主動 將應用的交通分類，以便應用 QoS。



SNMP

Simple Network Management Protocol，應用層管理協定。

收集、修改各廠牌網路設備間的管理資訊，以便監視運作狀況。

原理

採用 client-server 架構，client 端裝 SNMP Agent 軟體，Agent 會維護一個 MIB(管理資訊資料庫)，MIB 紀錄設備資訊(介面、CPU 使用率、溫度)。Server 端裝 SNMP Management 軟體，定期向 Agent 收集 MIB。

可設定臨界值(Thresholds)，超過鄰界值會發送 Trigger(觸發)資訊給管理者。

#SNMP 的基本組成：MIB、Manager、Agent ccna 會考

版本

- SNMPv1 無加密、非可靠傳送 Trap(UDP)、不可大量獲取資訊
- SNMPv2 無加密、非可靠傳送 Trap(預設 UDP 可設 TCP)、可大量獲取資訊
- SNMPv3 加密、認證、完整性、可靠傳送 Trap(TCP)、可大量獲取資訊

#trap snmp 代理者用來傳送被觸發的資訊片段給 snmp 管理者

SNMP Configuration

R1(config)#snmp-server host ip	設定 trap 要送到哪裡
R1(config)#snmp-server community string ? R1(config)#snmp-server community string rw	開啟路由器的 snmp 讀寫存取並給個名字 #有 read only 和 read&write 兩種選項
R1(config)#snmp-server location ____ R1(config)#snmp-server contact ____	設定 snmp 位置、聯絡資訊(非必要)
R1(config)#ip access-list 略 R1(config-ext/std-nacl)#permit 略	設定 ACL 來限制對 NMS 主機的 SNMP 存取 (非必要)
R1(config)#snmp-server community ____ <u>ACL</u> <u>rw</u>	把 ACL 用在 SNMP 組態中的另一種寫法
#show snmp group	Show snmp security mode

QUESTION 410

which command do we use to see SNMP version

- A. show snmp pending
- B. show snmp engineID
- C. snmp-server something
- D. http://bbs.hh010.com

哪个命令我们用来查看SNMP版本

Correct Answer: A

SNMP 版本

Cisco 支援 SNMP 版本可分為 SNMPv1、SNMPv2c 和 SNMPv3，如下表所示。在 SNMPv1 只簡單使用 **Community** 名稱來當密碼作身分認證並且密碼在傳送過程無加密，在安全性上有相當大的疑慮，另外也無法一次傳送大量(**Bulk**)的資料，因此必須花費較多的時間重複地下達命令，才能夠取得 MIB 資料。

SNMPv2c 新增 **getbulkrequest** 命令，讓管理端只要下達一次命令即可取得大量相關資料，而不必藉由多次的存取來取得相關資料，可有效地增進傳送 MIB 資料的效能，另外 SNMPv2c 還新增 Inform request 類似 trap，Inform 有 ACK 機制，比 Trap 更 Reliable。SNMPv3 版本則是在 SNMP V2 的基礎上增強安全功能。

圖表 17-24 SNMP 版本差異

SNMP Version	安全性	Trap/Inform 訊息	大量獲取資訊
SNMP v1	沒加密	Trap	不行
SNMP v2c	沒加密	Trap 或 Inform	可以
SNMP v3	提供加密、認證與完整性三種	Trap	可以

MIB

標準的資料結構，將各廠牌設備資訊讀寫。每個 SNMP Agent 維護一個 MIB。

MIB 資料庫以樹狀結構儲存設備資訊，樹狀結構的節點會分配一組 OID(唯一物件識別碼)。

MIB 分標準、私有，就是通用和專屬的差別。

服務模型

雲端供應商可以根據您的需要和預算，提供不同的可應用資源。您可以選擇只提振網路平台，或是將整個網路、OS、和應用資源移往雲端。

圖 22.4 是根據您選擇的服務類型，可以使用的 3 種服務模型。

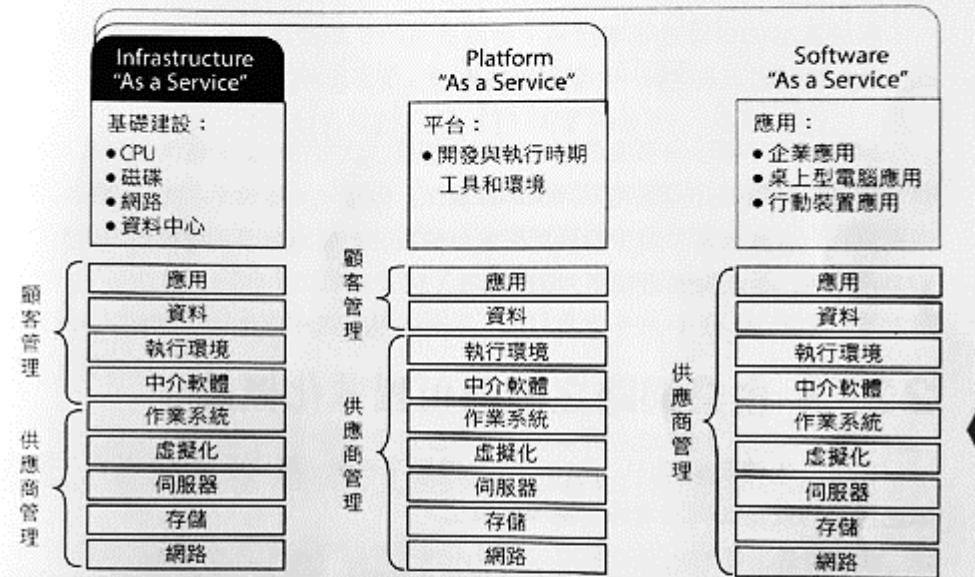


圖 22.4 雲端運算服務

IaaS 允許顧客管理大部分的網路，SaaS 不允許顧客做任何管理，而 PaaS 則介於兩者之間。顯然，主要的考量可能是成本，所以重點是顧客只需要為它們所使用的服務或基礎建設付費。

下面簡單說明每種服務：

- **IaaS (以基礎建設作為服務, Infrastructure as a Service)**：只提供網路交付顧客基礎建設—平台虛擬化的環境；顧客擁有主要的控制和管理能力。
- **SaaS (以軟體作為服務, Software as a Service)**：提供需要的軟體、作業系統與網路 SaaS 廠商會提供常見的應用軟體，例如資料庫、網站伺服器、和電子郵件軟體。顧客透過網際網路來存取這些軟體。使用者無需要在自己的電腦或伺服器上安裝軟體，而是由 SaaS 廠商安裝，並且在廠商的資料中心上執行。微軟的 Office 365 和 Amazon 的網路服務(AWS, Amazon Web Service)都是 SaaS 的最佳範例。

雲端服務的供應商市場提供了非常廣泛的雲端運算產品，從高度專業的產品，到大範圍的服務選擇，全都取決於您的企業需求和預算。

還有一項好處是每項服務都是固定的價格，讓您可以很輕鬆地規劃未來的預算。首先，您可能必須先花點錢來訓練員工，但是一旦自動化之後，因為管理變得更簡單，您就只需要更少的員工來進行維護。它能將企業資源釋放出來進行新的業務需求，並且能夠更有活力和彈性。

CCNP PART (ROUTING)

路由觀念

- IGP v.s. EGP；路由協定分類
- Route Summarization
- Traffic Types-Well-known IPv4/v6 multicast address.
- IPv6 address types.

Network Types

1. point to point：兩台路由器連在一起，沒什麼好說的。
2. Broadcast network：一台路由器廣播給其它同網段上的路由器，也沒什麼好說的。
3. NBMA：只能 unicast 的網路模式，一對多，常見在 ATM & Frame Relay。

Implementing RIPng

- RIPng：使用 **multicast FF02::9**

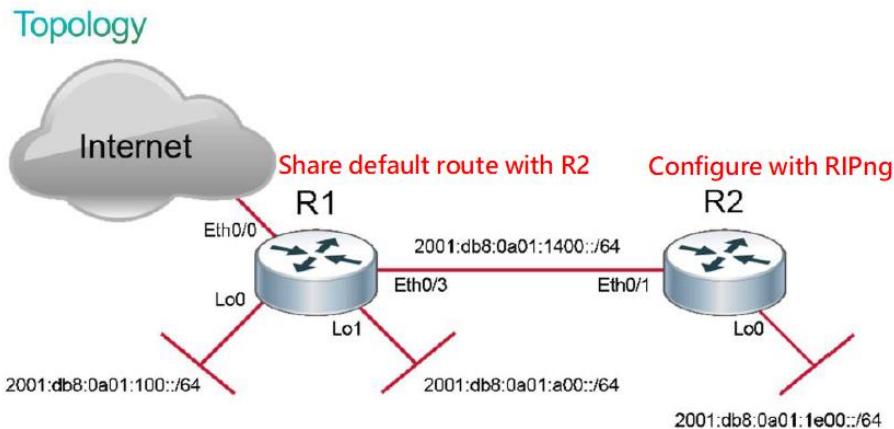
p.s.相對應的路由器 RIPng 程序號碼可不同

int 下的 ipv6 rip xx enable 取代 IPv4 的 network 宣告

- 支援相同成本負載平衡，最大 4 條。(maximum paths number=1 時不進行不載平衡)

RIPv2 v.s. RIPng

Feature	RIPv2	RIPng
Advertised routes	IPv4	IPv6
Transport protocol	UDP (port 520)	UDP (port 521)
Multicast address used	224.0.0.9	FF02::9
VLSM support	Yes	Yes
Metric	Hop count (maximum of 15)	Hop count (maximum of 15)
Administrative distance	120	120
Routing updates	Every 30 seconds and with topology change	Every 30 seconds and with topology change
Authentication support	Yes	Yes

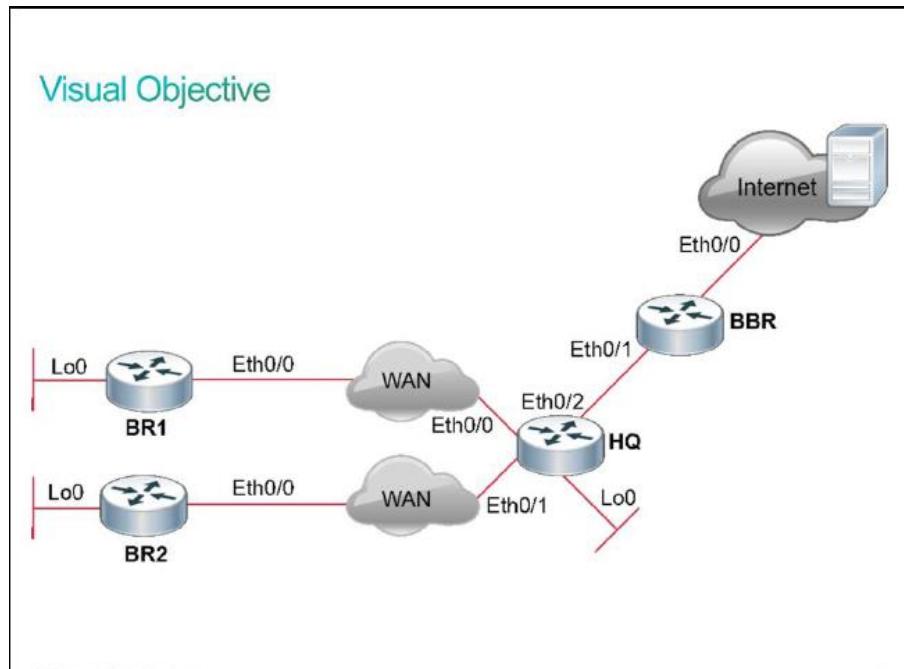


· RIPng 常用指令

指令	說明
R2(config)#ipv6 unicast-routing	啟用 ipv6 routing 功能
R2(config)#ipv6 router rip <u>CCNP RIP</u>	建立 RIPng 程序並命名(不同 router 可同 RIPng 名)
R2(config-if)#ipv6 rip <u>CCNP RIP enable</u>	在介面上啟用 RIPng
R1(config-if)#ipv6 rip <u>CCNP RIP</u> default-information originate only 在 R2 show ipv6 route rip 可以看到學到的預設路由	originate 放出本地所有路由(含預設)給所有鄰居 only 只放出本地預設路由給鄰居
R2(config-if)#ipv6 rip <u>CCNP summary-address</u> 2020:70:14:2::/63	RIPng 路徑彙總(設在和對方直連的介面上)
R2#show ipv6 rip RIP process "CCNP_RIP", port 521, multicast-group FF02::9, pid 208 Administrative distance is 120. Maximum paths is 16 Updates every 30 seconds, expire after 180 Holddown lasts 0 seconds, garbage collect after 120 Split horizon is on; poison reverse is off Default routes are not generated Periodic updates 47, trigger updates 5 Full Advertisement 1, Delayed Events 0 Interfaces: Loopback0	查詢 RIPng 的所有細節，包含： port 號、群/單播、程序名稱、AD 值、Update time、expire time、啟用介面、重分送。

Ethernet0/1 Redistribution: None	
R2#show ipv6 route rip R 2001:DB8:A01:100::/64 [120/2] via FE80::A8BB:CCFF:FE00:5F30, Ethernet0/1	查詢 RIPng 的 AD 值和 Hop Count 120 是 AD 值，2 是 Hop count
show ipv6 route 2001:db8:c0a8:c800::1 Routing entry for 2001:DB8:C0A8:C800::/64 Known via "rip BR2", distance 120, metric 2 Route count is 1/1, share count 0 Routing paths: FE80::A8BB:CCFF:FE00:CF10, Ethernet0/0 Last updated 00:04:08 ago	查詢特定路由的細節
R2#show ipv6 protocols IPv6 Routing Protocol is "connected" IPv6 Routing Protocol is "ND" IPv6 Routing Protocol is "rip CCNP_RIP" Interfaces: Loopback0 Ethernet0/1 Redistribution: None	萬用指令，可查詢已啟用協定類型、名稱、介面。

※Lab - Challenge 01



沒什麼重點，注意 step3 有陷阱，有人早就有 default route 要先 no 掉



複習(?)一下：Protocol ID

ICMP 1	TCP 6
UDP 17	GRE 47
EIGRP 88	OSPF 89

Advanced EIGRP 重要觀念

◎K-Value： 很重要，給我背起來啊口胡！

Constant	Metric
K1	Bandwidth
K2	Loading
K3	Delay
K4	Stablity
K5	MTU

◎EIGRP 常用名詞：FD、RD(AD)、Successor、Feasible Successor

◎EIGRP 使用 5 種封包：(透過 RTP 可靠傳輸協定)

- **Hello** 透過不可靠的多點傳播以發現 EIGRP 鄰居：這表示它不需要確認。有兩種計時方式 Interval time / Hold time，間隔時間為 Hello 封包送出週期，保留時間用以維持鄰居關係，若保留時間歸零時未收到 Hello 封包，判定鄰居陣亡，預設保留時間為間隔時間的三倍(5/15)。
p.s. 兩台路由器 Hello time 不同，在 EIGRP 沒影響，在 OSPF 會有差
- **更新(Update)** 包含傳送給鄰居的路徑資訊，不定期(必要時)送出。更新封包不會送出整個路由表，只包含需要的路由資訊，並且只發給需要的路由器，所以有多台需更新時使用多點傳播，只有單一鄰居需更新時使用單點傳播。
- **ACK** 使用單點傳播回應更新。ACK 不使用可靠傳送，否則它還需要另一個 ACK 來做確認。對於更新、查詢、回覆三種封包均使用 ACK 以作為可靠傳輸。當收到鄰居送來的這三種封包時，必須回一個 ACK 給鄰居以作為收到確認(Hello 封包不需要 Ack)。

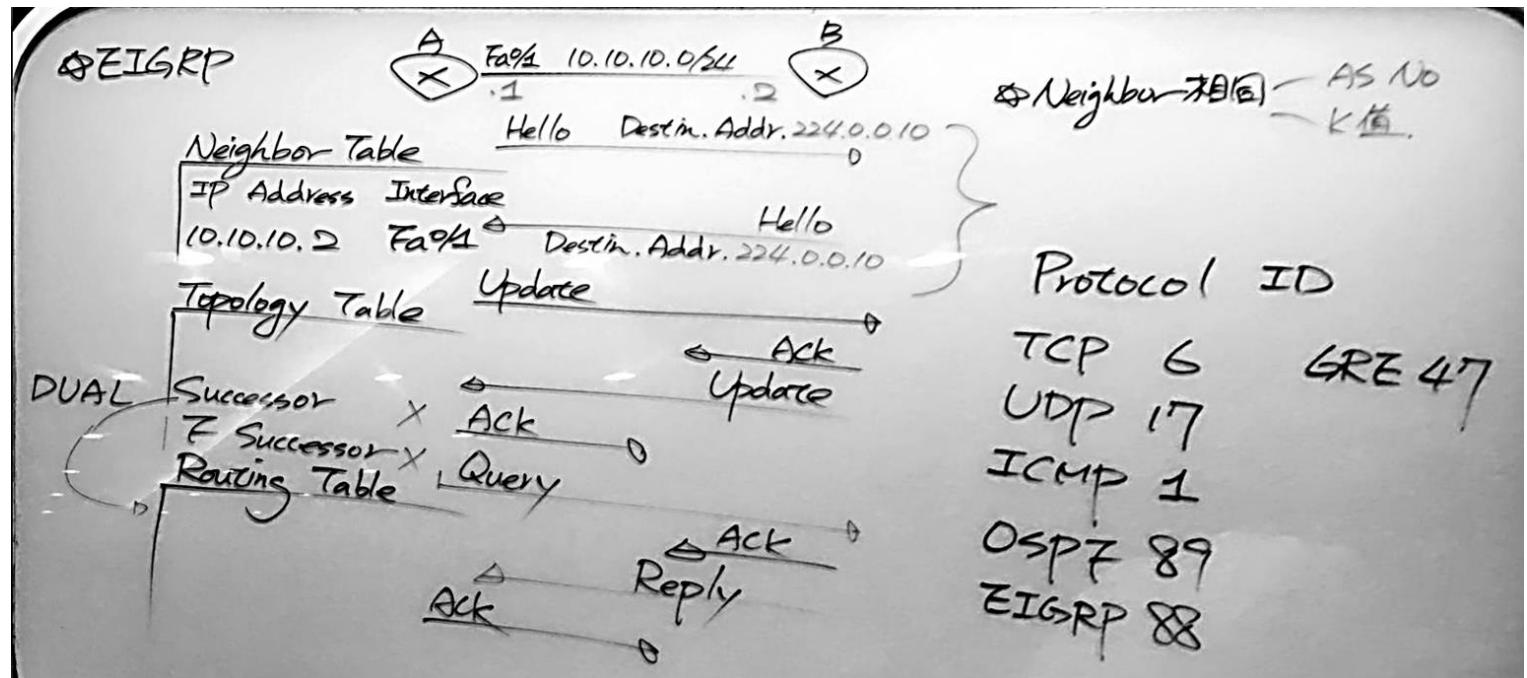
Query 和 Reply 是成對的

- **查詢(Query)** 在兩種情況下會發送多點傳播 Query：
 - ① 遺失路由(沒有該筆遠端路由) ② 沒有可用的 FS。
 鄰居若有該路由則使用 Reply 回覆。沒有則繼續往下一批鄰居問，直到產生 SIA(Stuck in Active)。當 SIA 等待時間(3 分鐘)到，會重新建立整個 EIGRP 鄰居關係，並重新計算路由表，導致收斂。
- 要減少 Query 的範圍有三種方式：

① Summary Route ② 設定備援 FS 路由 ③ 設定 Stub Router(s)

● 回應(Reply) 透過單點傳播來回應 Query。回應中包含通往被查詢目的地的特定路徑。

下圖為五種封包的發送過程，debug 也可以看到。



EIGRP 進階操作指令：

※Lab - Discovery 02、Discovery 03

指令	說明
BR1(config)#router eigrp 100 BR1(config-router)#network 172.16.1.0	基本的 EIGRP 宣告路由指令，重點在於 Network 後面其實不是放網段而是可以直接放 ip，比如我要宣告 192.168.5.254 這筆路由，我應該打 192.168.5.0 而不是 192.168.4.0。雖然我打的是 5.0，在別人的路由學到的實際上是 4.0
BR2(config-router)#network 172.16.2.0 0.0.0.3 BR2(config-router)#network 192.168.2.1 0.0.0.0	進階的 EIGRP 宣告路由指令，可加上 Wildcard，就可以限制要放出的網段 ip 數
BR3(config-router)#eigrp router-id 192.168.3.255	手動配置 EIGRP 的 router-id，通常沒啥卵用，但要注意不能和別人 id 衝突
BR1#show ip eigrp neighbors	查詢 EIGRP 鄰居表
BR1#show ip eigrp neighbors detail	進階查詢 EIGRP 鄰居表(見使用說明書) 重點在查詢 AS、該 AS 的鄰居 IP、與鄰居相連接的介面
Show ip eigrp interfaces	查詢 eigrp 介面
Show ip eigrp interfaces detail	進階查詢 EIGRP 介面，可以看到 Hello interval/Hold-time、已發送 Hello 數、重送

	封包數
HQ(config-router)#passive-interface default HQ(config-router)#no passive-interface e0/0	將所有介面設成 passive-interface，再啟用想加入 eigrp 的介面，這是一套連續技！常用在我有 100 個介面但只想啟用一個介面 eigrp 時，顯然一個一個 no 不太現實。
HQ#debug eigrp packets ? <u>Hello/</u>	EIGRP 的抓封包，選項多元自行問號用來觀察 eigrp 運作是否順心如意
HQ(config)#access-list 100 permit eigrp any any HQ#debug ip packet 100	只抓特定 EIGRP 程序的封包
HQ#no debug all HQ#undebug all	停用 debug 抓封包
BR3(config-if)#ip hello-interval eigrp <u>100 10</u> BR3(config-if)#ip hold-time eigrp <u>100 30</u>	指定單一介面上 EIGRP 100 的 Timer(hello-interval/hold-time)
HQ(config-router)#neighbor <u>172.16.2.2 e0/0</u>	手動指定介面對應鄰居，對該鄰居使用 Unicast
HQ(config)#access-list 10 permit any HQ(config)#router eigrp 100 HQ(config-router)#offset-list 10 out 500000 serial 1/0	用 ACL 指定某段的 FD，使 FS 偏好某台路由器，以 S1/0 出去的路由來說，FD=原始值+50 萬
BR#show ip eigrp traffic EIGRP-IPv4 Traffic Statistics for AS(100)以下省略	Verify EIGRP packet traffic statistics Hello/Update/Query/Reply/Ack SENT/RECEIVED Numbers
#show ip route eigrp	查詢 EIGRP 學到的路由。 D - EIGRP, EX - EIGRP external D EX 代表從其他協定學到的重分送路由
#show ip eigrp topology	1. 查詢 EIGRP Topology，CCNP 的重點放在觀察 FD 最小的會被選入路由表 2. EIGRP Topology 只會列出 Successor 和 FS
#show ip eigrp topology all-links 這裡原本有個無聊實驗，在持續 ping 的狀態下把某 FS 的介面 shutdown，會發現沒 FS 的收斂時間比有 FS 長…果然很無聊對吧	加上 all-links 後會把 non-FS 也列入，non-FS 指的是其 RD>Successor FD 的路由
#show interfaces fx/x	查詢該介面的 Bandwidth & Delay

BR1#show ip eigrp neighbors detail

使用說明書

EIGRP-IPv4 Neighbors for AS(100)

H	Address	Interface	Hold Uptime	SRTT	RTO	Q
Seq						

Num			(sec)	(ms)	Cnt
0	172.16.1.1	Se0/0	13 00:13:48	25	150 0 10
Version 10.0/2.0, Retrans: 0, Retries: 0, Prefixes: 5					
Topology-ids from peer - 0					

說明：

H 代表鄰居發現的順序

Address EIGRP 鄰居的 IP

Interface 與鄰居連接的介面

Hold 以秒為單位，表示路由器願意花多久等待特定鄰居的 Hello 封包

UP time 與鄰居建立關係的時間長

SRTT Smooth Round-Trip Timer 流暢來回計時器，代表從該路由器抵達鄰居，再繞回來的完成時間。當傳送多點傳播後，該值會限制鄰居回覆的等待時間。如前所述，路由器在沒收到回覆時，嘗試透過單點傳播來建立通訊。

RTO retransmission timeout 指定多點傳播嘗試隔；它是以 SRTT 值為基礎。

Q queue 指示佇列中是否有任何訊息。如果該值一直很大，表示有問題。

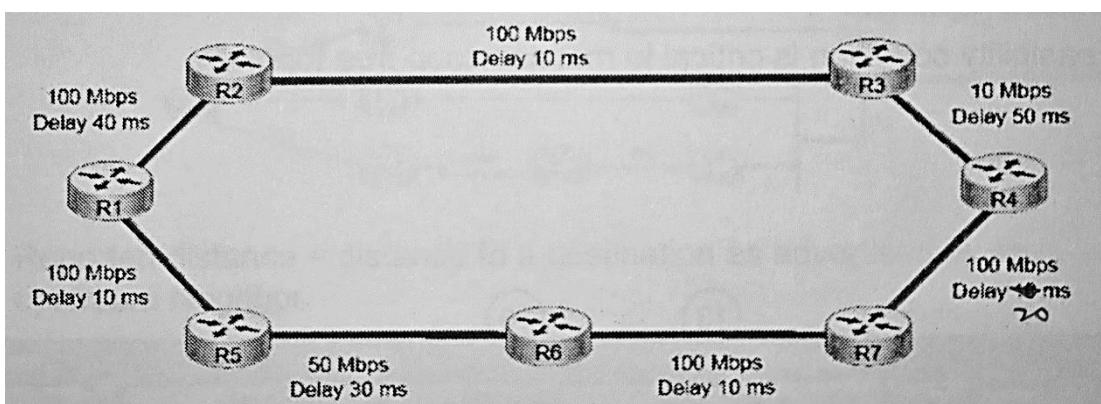
Seq 鄰居最後一次更新的序號，用來維護同步，並避免重覆訊息、失序訊息。

Retrans 重送的封包數

Retries 嘗試重送封包的次數

Prefix 從鄰居收到的 Prefix number

· EIGRP Metric Calculation



■ Bandwidth=10⁷/整段路徑中最小頻寬

以 R1-R2-R3-R4 來說，Bandwidth=10⁷/10⁴Kbps=1000

■ Delay=整段路徑 Delay 累加

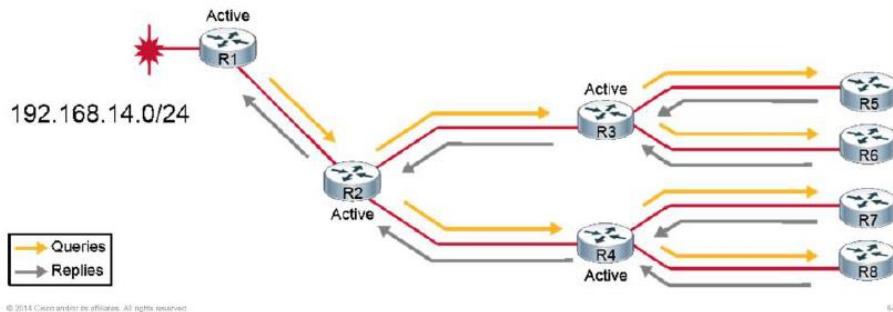
以 R1-R2-R3-R4 來說，Delay=4000+1000+5000=10000(tens of microseconds)

■ Metric=(Bandwidth+Delay)*256

範例省略

總之，經過一番蛋疼的計算後，選擇下面那條為 Successor，上面那條為 FS

• 新觀念 Stub Routers (of EIGRP)



繼承以前的 EIGRP 觀念，在①遺失路由②沒有 FS 的情況下，會發出 Query 封包，並且會往鄰居病毒式的擴散下去。

但 Query 會有個問題，如上圖，Active 的左邊路由遺失了，所以它會自主的發出 Query 封包來向完全無關的右邊詢問，很顯然右邊不會 Active 的左邊路由，於是整個右邊的網路會卡住，收斂時間會很長(直到產生 SIA 重新計算網路拓樸)。

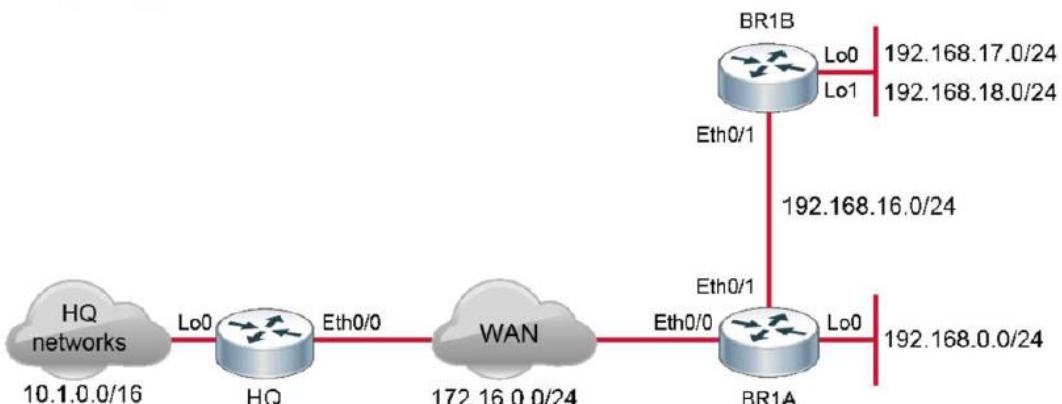
為了減少收斂範圍/時間，思科發明了 Stub Router，如上圖 R5-R8 末端路由器，並不需要被 Query 詢問，將其設定為 Stub Router 可有效降低收斂時間。

詳解版本：在大企業的網路拓樸中，Core Router 到 Branch Router 通常會有備援路徑，所以在沒有 stub router 的狀況下會造成 query 迴圈，最古早的做法是用 ACL 檔，所以後來才有了 stub router 的設計。Stub Router 的原理是其發出的 hello 封包中有一個 stub 參數，當下圖 HQ 收到 BR1A 的 hello 中帶有 stub 參數時，就不會再對它發出 query。另外在以下的 Discovery lab 中，eigrp stub 後接的參數代表 BR1A 會對 HQ 發出的路由類型，反正不管哪種，就是絕對不會發 query，如此第二重隔絕了 query loop。

#Travis 老師：receive-only 的用途，當這個 branch 太小，沒有必要發路由給 HQ 時使用。

Discovery 04

Topology



Stub Router 指令

指令	說明
HQ#debug eigrp packets <u>terse</u>	抓除了 Hello 之外的所有封包

(UPDATE, REQUEST, QUERY, REPLY, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)	(其實用 debug eigrp packets ?就看得到說明了) #lab 中用來觀察它發了一個 Query
<pre>BR1A(config-router)#eigrp stub ? -connected : Advertises connected routes included with a network command -summary : Advertises configured summary routes -static : Advertises static routes, if redistribute static command is configured -redistribute : Advertises redistributed routes, if redistribution is configured -receive-only : Prevents the stub from sending any type of route</pre>	設定本地 Router 為 EIGRP Stub Router 預設值為 connected+summary
<pre>#show ip eigrp neighbors detail Stub Peer Advertising (CONNECTED SUMMARY) Routes 括號裡面就是 Stub Router 設定的模式</pre>	1. 在 Stub Router 的鄰居查詢 Stub Router 設定狀態

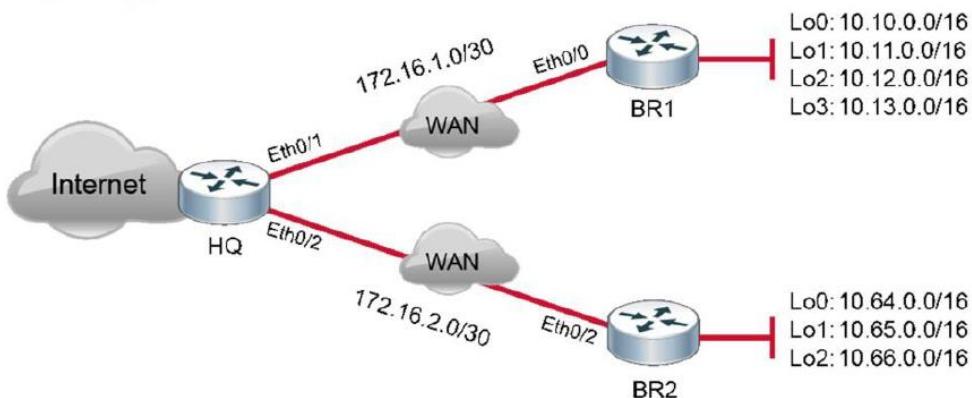
註：

設定 Stub Router(Receive only)後在鄰居 show ip route 不會學到路由

設定 Stub Router(connected/summary)後在鄰居 show ip route 不會學到 D EX 重分送路由

Discovery 05 Reducing Query Scope by Using Summary Routes

Topology



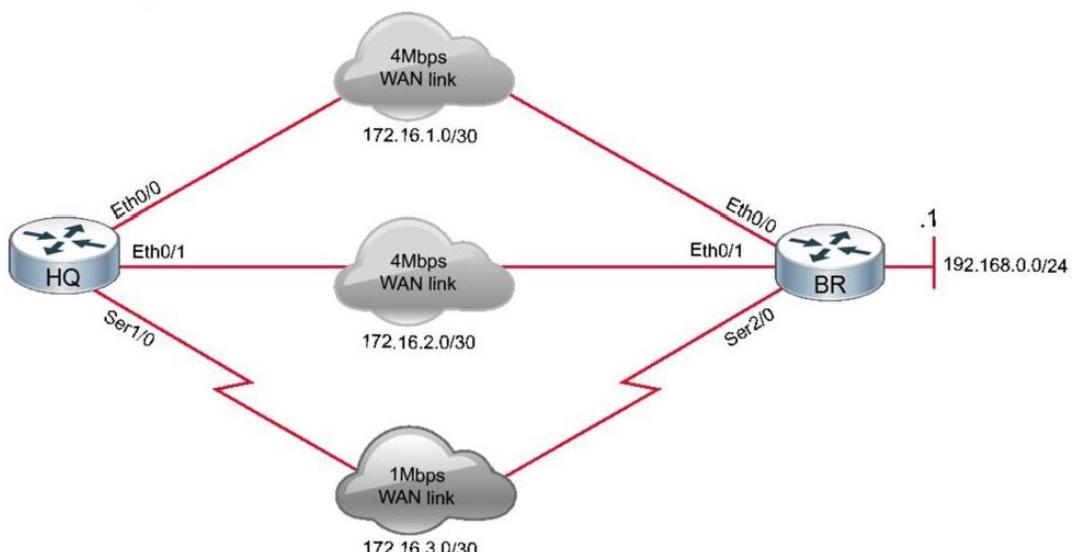
Summary route 常用指令

指令	說明
<pre>BR1(config)#router eigrp 1 BR1(config-router)#auto-summary</pre>	在 EIGRP 模式設定 BR1(BR2)使用自動匯總總路後： 1. 在 HQ 的路由表會將 BR1 學到的路由匯總成一筆

	<p>2. BR1 自己的路由表會有一筆 D 10.0.0.0/8 is a summary, 00:01:25, Null0 Null0 防止迴圈用 (null 中譯：空值)</p> <p>3. 從 HQ ping 10.10.0.1 或 2 其中有一個會 ping 不到，這是 auto-summary 的問題-去回不同路。所以 lab 的下一步是 no auto-summary，再手動匯總。</p>
BR1(config-if)#ip summary-address eigrp 1 10.8.0.0/13 BR2(config-if)#ip summary-address eigrp 1 10.64.0.0/14 #ip default-network IP IP 不用加 mask，會自動指定 classful	在介面上設定 EIGRP 手動路由匯總 此時 HQ ping 得到 10.10.0.1 或 2 了
HQ(config-router)#redistribute static	設定預設路由(等同 ip route 0.0.0.0...)並且 EIGRP 和 RIP 會自動發布
	設定 EIGRP 發布預設路由

Discovery 06 EIGRP Load Balancing

Topology



EIGRP Load Balancing 常用指令

指令	說明
HQ(config)#router eigrp 1 HQ(config-router)#variance 6	<p>設定 EIGRP unequal cost load balancing。</p> <p>1. 從路由表和 EIGRP 拓樸表可以看出有一筆 FD 值為 2297856 的並沒有列在路由表(所以為 FS)，因為 variance 值預設為 1，即 FD*1 範圍內的路徑才會列在路由表。 P 192.168.0.0/24, 2 successors, FD is 409600 via 172.16.1.2 (409600/128256), Ethernet0/0 via 172.16.2.2 (409600/128256), Ethernet0/1 via 172.16.3.2 (2297856/128256), Serial1/0</p> <p>2. 用 2297856/409600 得出其差距為至少整數 6 倍，variance 設為 6 可將該筆 FS 列入路由表。</p>
#show ip protocols	查詢 variance 及 Maximum Path 用此指令

註：EIGRP 預設 Maximum Path=4、Variance=1

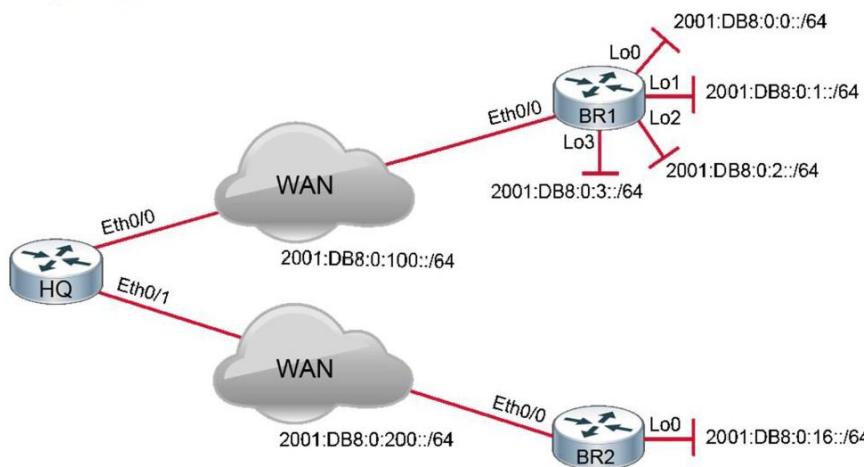


Discovery 07 EIGRP for IPv6

EIGRP for IPv6 Overview

Feature	EIGRP for IPv4	EIGRP for IPv6
Concept of the link-local address to establish EIGRP neighbor relationship	No	Yes
Automatic summarization possible	Yes	No
Layer 3 protocol for EIGRP messages	IPv4	IPv6
Authentication	EIGRP-specific	Uses IPv6 AH/ESP
Reserved multicast address	224.0.0.10	FF02::A
Layer 3 header protocol type	88	88
Uses composite metric, by default uses bandwidth and delay	Yes	Yes
Uses successor, feasible successor	Yes	Yes
Router ID format	IPv4	IPv4

Topology



EIGRP v6 常用指令

指令	說明
BR2(config)# ipv6 unicast-routing	啟用 ipv6 路由功能， ipv6 路由協定前置指令 ， 會考!!
BR2(config)# ipv6 router eigrp 100 BR2(config-rtr)# eigrp router-id 192.168.2.1	啟用 ipv6 EIGRP，並且在無 ipv4 的情況下需手動設置 router-id 。(v4 格式)
BR2(config-if)# ipv6 eigrp 100	在介面上啟用 EIGRP(來到 CCNP 要學會看 log ↓) *Oct 30 13:25:45.882: %DUAL-5-NBRCHANGE: EIGRP-IPv6 100: Neighbor FE80:200::1 (Ethernet0/0) is up: new adjacency
BR1(config-if)# ipv6 summary-address eigrp 100 2001:DB8::/62	在介面上手動設定 ipv6 路由匯總
#show ipv6 eigrp topology	查詢 EIGRPv6 拓撲表、鄰居表、路由表

```
#show ipv6 eigrp neighbors  
#show ipv6 route eigrp
```

註：IPv6 的路由匯總不像 IPv4 那麼複雜，只要算好要匯總幾筆，/後面的數字直接扣掉相對應的二次方就可以了。範例→

Prefixes
2001:DB8:0:0::/64
2001:DB8:0:1::/64
2001:DB8:0:2::/64
Summary route
2001:DB8:0:0::/62

要匯總三筆，只要借 2 位，所以 $64-2=62$