網路安全管理與建置
暨CCNA證照輔導

課程大綱

一、Cisco IOS CLI介紹

二、基本指令

三、路由功能簡介

四、VLAN

五、封包傳遞過程

六、STP擴充樹

七、ACL

八、WAN廣域網路

九、各類型拓譜實務

第一章

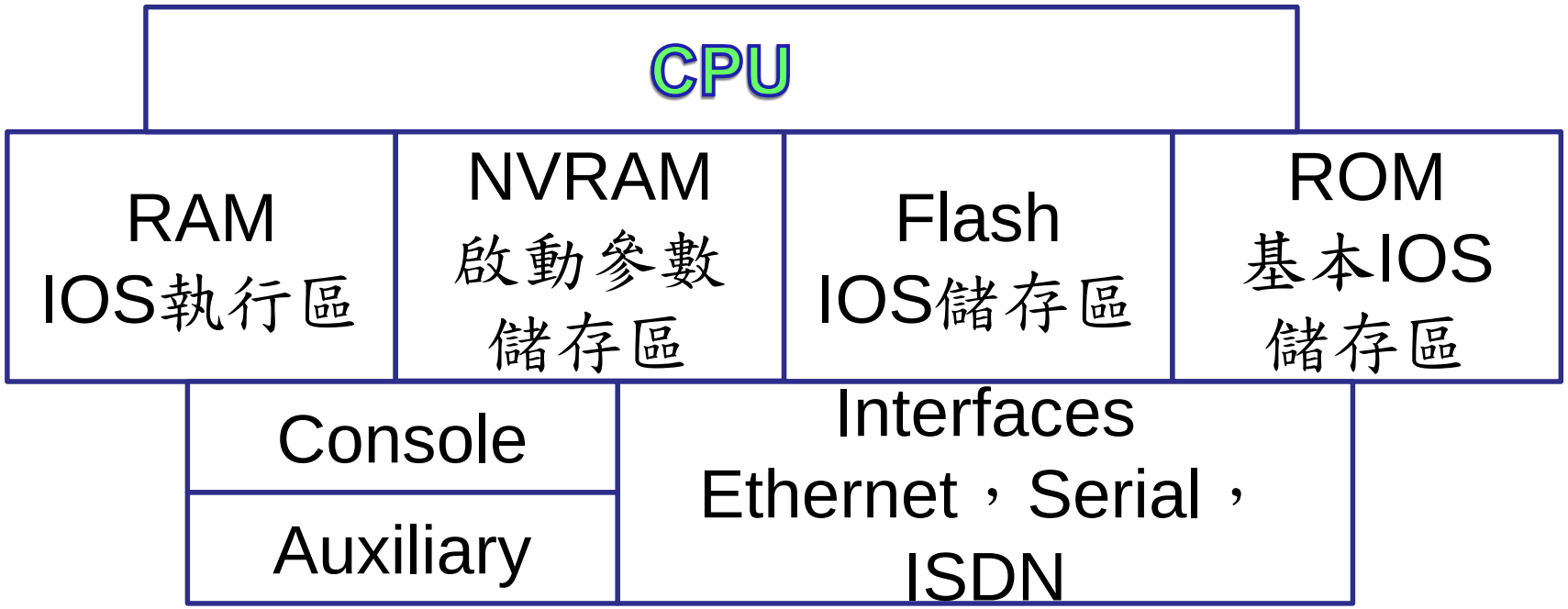
Cisco IOS CLI

CiscoIOS

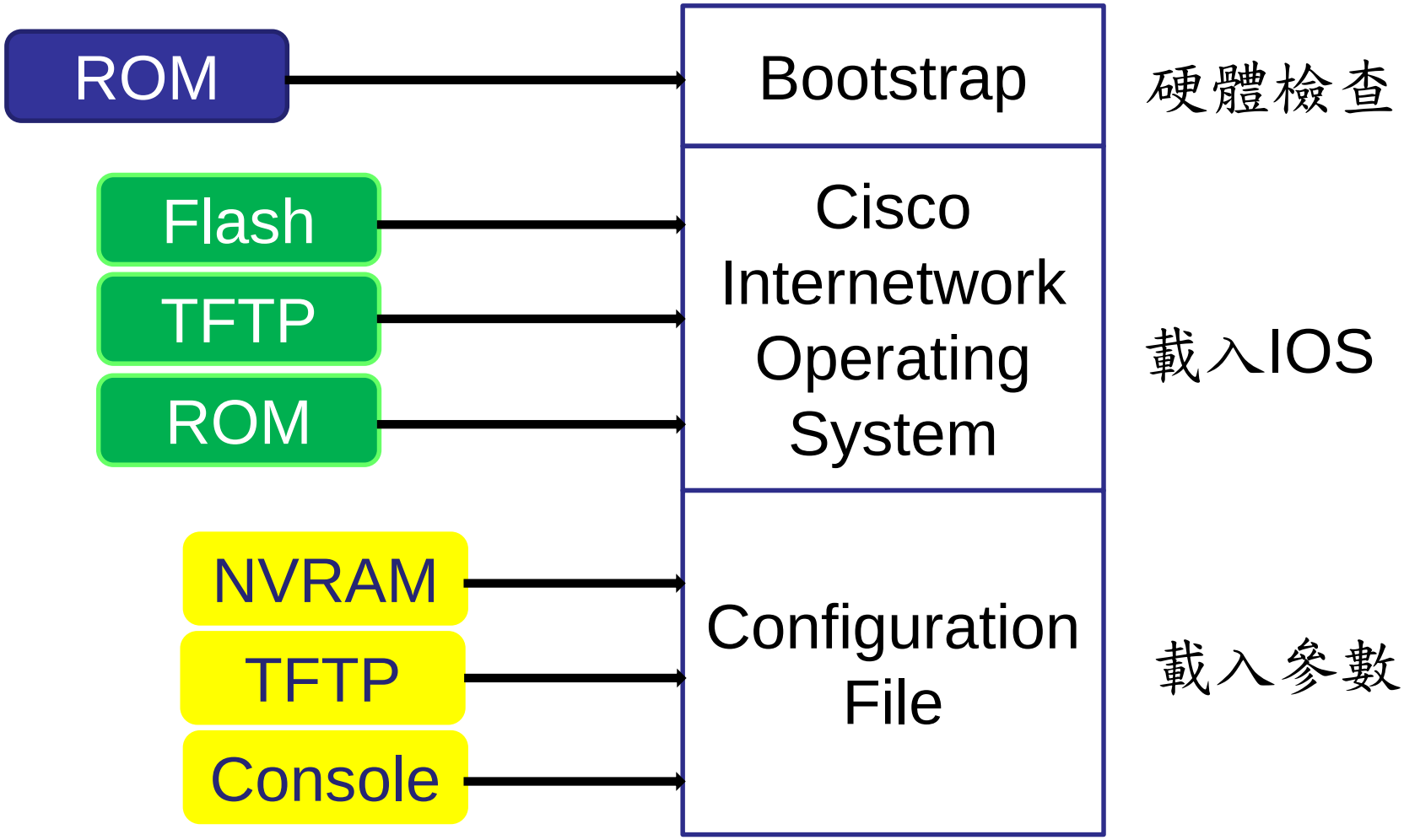
- CiscoIOS是Cisco路由器與大部分Cisco交換器的核心(kernel)，核心是作業系統中最基本的、不可或缺的部份，負責配置資源與管理諸如低階硬體界面與安全性等
  - Cisco已經建立了一個稱為CiscoFusion的東西，可以讓所有的Cisco裝置執行相同的作業系統。
  - 但實際上卻不是這樣，因為Cisco併購了一些不是他們自己設計與製造的裝置。幾乎所有的Cisco路由器都執行相同的IOS，不過大約只有一半的交換器執行相同的IOS－然而這個數目成長得很快。

開機程序

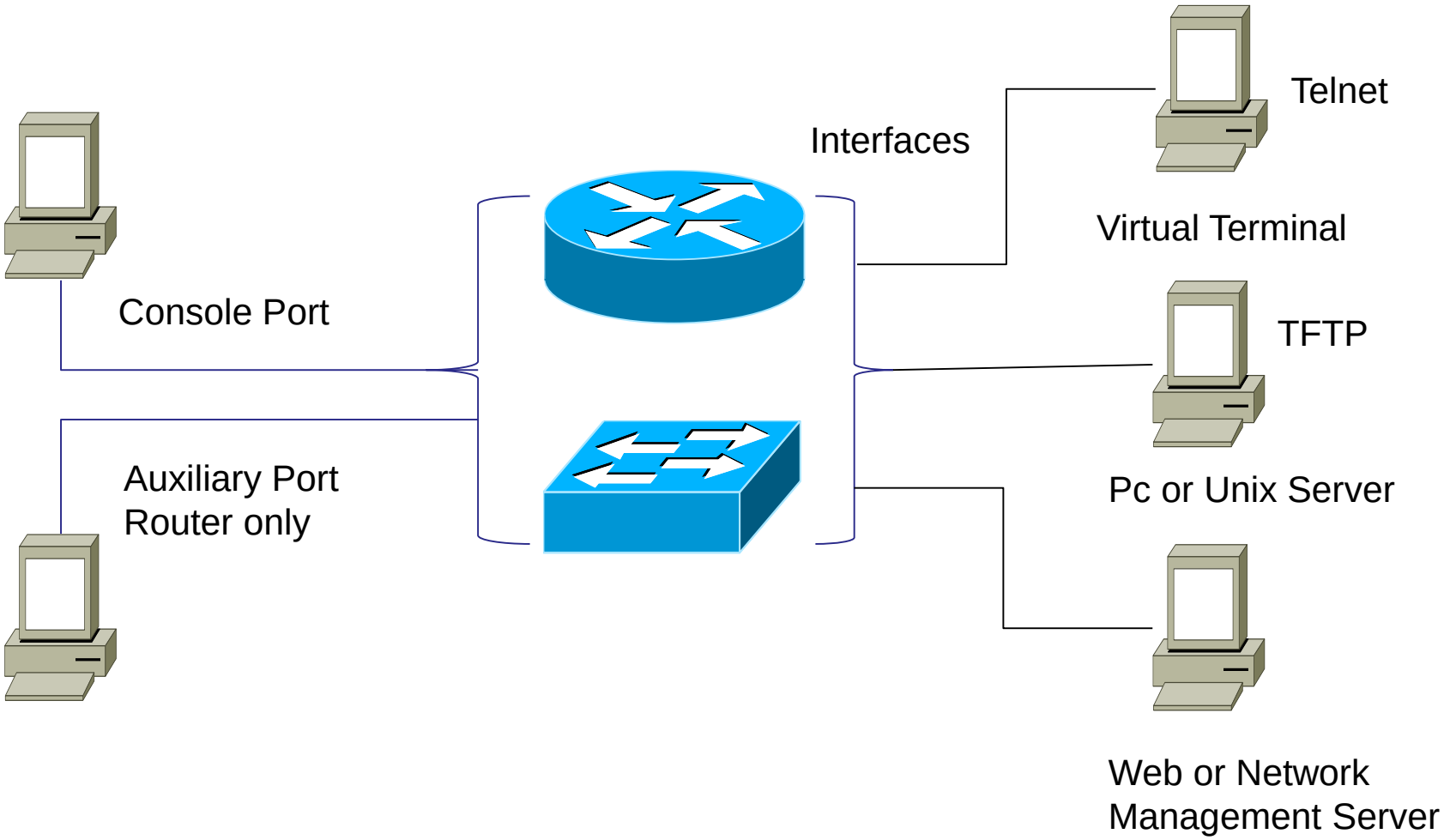
- 硬體-開機測試(PowerOnSelfTest，POST)
- 載入IOS映像檔IOS software image
- 載入設定檔Configuration



開機程序-續


ROM
Flash
TFTP
ROM
NVRAM
TFTP
Console
Bootstrap
Cisco Internetwork Operating System
Configuration File
硬體檢查
載入IOS
載入參數

連結介面


Interfaces
Telnet
Virtual Terminal
Console Port
TFTP
Auxiliary Port
Router only
Pc or Unix Server
Web or Network
Management Server

Consoleterminal

- RJ-45 to RJ-45 rollover cable
- RJ-45 to DB-9cable
- 超級終端機設定
  - Speed 9600：b/s位元速率
  - Data bits：8資料位元
  - Parity：None同位元檢查
  - Stop bit：1停止位元
  - Flow control：None流量控制

Remote Terminal

- Straight-through serial cable
- telnet，ssh
- Ip
  - Switch的VLAN1上要設定IP
  - Router的介面上要設定IP

例telnet 192.168.1.1明碼

Or ssh 192.168.1.1 secureshell有加密

IOSCLI

- IOS Internetwork Operating System
- CLI Command Line Interface
  - User EXEC：使用者模式
    - 僅能進行一般監視功能
    - SwitchX>
  - Privileged EXEC：特權模式
    - 可執行所有功能
    - SwitchX#

第二章

基本指令

登入路由器

- 以下是您要做的：

```
Router>
Router>enable
Router#
```

- 現在提示列是**Router#**，這表示您正處於特權模式中，在這種模式下可以檢視與更改Cisco路由器的組態。您可以使用**disable**命令從特權模式退回使用者模式，操作畫面如下：

```
Router#disable
Router>
```

登入路由器

- 此時可以輸入**logout**離開主控台：

```
Router>logout

Router con0 is now available
Press RETURN to get started.
```

- 或者在特權模式提示列只要鍵入**logout**或**exit**即可登出：

```
Router>en
Router#logout

Router con0 is now available
Press RETURN to get started.
```

路由器模式概觀

```
Router#config
Configuring from terminal, memory, or network
    [terminal]?    Enter
Enter configuration commands, one per line. End with
```

```
  CNTL/Z.
Router(config)#
```

- 因為是整體設定模式，此時您所作的變更會影響整個路由器。

？語法

- ？　指令的說明
  - 所在介面指令的說明，
    - 輸入?，按Enter
    - 千萬不要輸入help，因為沒有這個指令
  - 忘了指令全名不知怎麼拼?以terminal為例
    - Switch#te?注意3個字元是沒有間隔的
    - 此時會出現所有te開頭的指令terminal，telnet
  - 忘了指令後面要加什麼參數
    - Switch#telnet?注意指令跟問號間要有空白
    - WORDIPaddressorhostnameofaremotesystem(說明參數要加IP或主機名稱)

錯誤訊息

錯誤訊息	範例	除錯
Ambiguous command 不明確的指令	Switch#co %Ambiguouscommand:"co “	Switch#co? Configure connect copy
Incomplete command 未完成的指令	Switch#show %Incomplete command.	Switch#show?
Invalid input detectedat ‘^’ marker 指令在 ‘^’ 產生錯誤	Switch#showvlanbriof ^ %Invalid input detectedat’^’marke	Switch#show vlan? briefVTPallVLANstatusinbrief idVTPVLANstatusbyVLANid nameVTPVLANstatusbyVLANname

懶人輸入法

- CiscoIOS只要輸入指令或參數的縮寫就可以執行
  - Switch#show clock
  - *0:44:38.440UTC???11993
  - Switch#sh cl
  - *0:44:41.497UTC???11993
  - 這2個指令的結果都一樣沒有差別
  - Switch#show running-config
  - Switch#sh r
  - 你會使用哪種方式呢?

懶人輸入法-續

- Tab鍵的妙用
- 如果只知道指令或參數的縮寫，但忘了全名，可以在輸入指令或參數的縮寫後直接按Tab鍵，此時，系統會自動幫你完成，前提是這個指令的縮寫必須是唯一的，如果縮寫跟別人相同，則無法使用此功能
- Switch#sh ＋Tab鍵➔Switch#show
- Switch#te＋Tab鍵➔Switch#te
  - 因為sh開頭的只有show
  - te開頭的有telnet，terminal

Command History

- 按上鍵可以找出前一個輸入的指令
- 按下鍵可以找出後一個輸入的指令
- showhistory秀出之前輸入過的指令
- Terminal history size0~255設定buffer大小
  - Switch#show history

    show clock

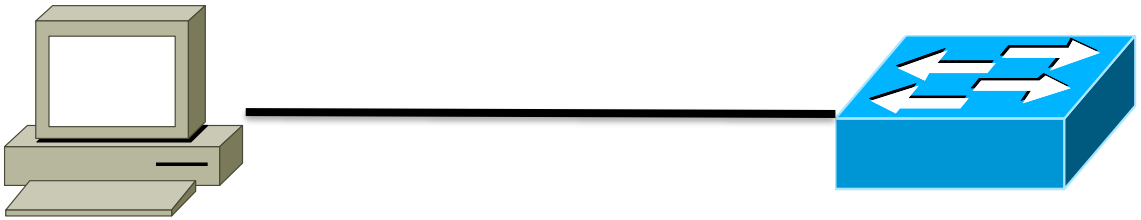
    sh cl

    show vtp

設定檔

- Cisco Router具備下列3種格式的記憶體
  - RAM：running configuration目前的設定
  - NVRAM：startup configuration開機的設定
  - Flash：IOSimage，backup configuration
- running-config自Router開機後的設定，關機後會消失，如果希望重開機後設定依然保留，則必須將設定儲存至startup-config。
- Show running-config
- Show startup-config

登入Switch



Console

Switch>	UserModePrompt
Switch>enable	進入特權模式指令
Switch#	PrivilegedModePrompt
Switch#disable	退出特權模式
Switch>	

設定模式

- Configuration modes
  - Global configuration mode全域模式所作設定會影響整個設備，指令如下
    - Switch#configure terminal
    - Switch(config)#
  - Interface
  - Subinterface
  - Controller
  - Line
  - Router

更改設備名稱

- Switch#configure terminal
- Switch(config)#hostname SwitchXXX
- SwitchXXX(config)#exit回上一層
- Ctrlz回最底層同end
- 一直打錯指令，不想讓設備進行名稱解析
- Switch(config)#no ip domain-lookup
- Switch#exit or logout退出此連線

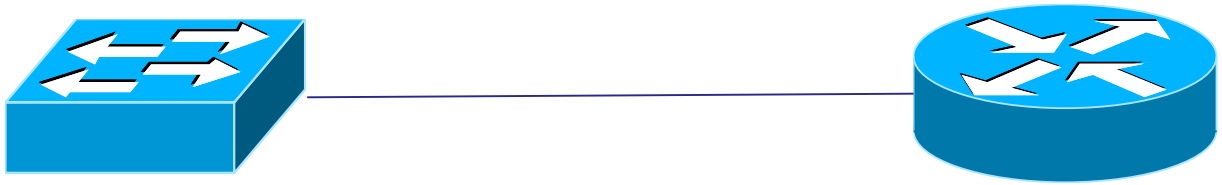
設定IP與主機名稱

- Switch#configure terminal
- Switch(config)#interface vlan1
- Switch(config-if)#ipaddress192.168.1.1255.255.255.0
- Switch(config-if)#no shutdown啟動

- Switch(config)#hostname Switch主機名稱

DefaultGateway

- Switch#configure terminal
- Switch(config)#ip default-gateway 192.168.1.254



Vlan 1
192.168.1.1/24

Default gateway
192.168.1.254/24

儲存設定

- 我們在Switch及Router上所作的設定皆存在於RAM中的running-config
- 若下次開機也要套用這些設定，必須將變更的設定儲存在NVRAM中的startup-config
- Switch#copy running-config startup-config
- 反之，若設定被亂改，想回復原始設定
- Switch#copy startup-config running-config

show

- Switch#在命令提示列打指令
- Show version版本
- Show running-config目前設定檔
- Show startup-config開機設定檔
- Show interfaces介面
- Show ip int brief介面的IP
- Show cdp neighbors鄰近的設備
- Show vlan brief vlan設定
- show?其他指令

密碼-1

- Console password
- Switch#conft
- Switch(config)#lineconsole0
- Switch(config-line)#password cisco(密碼)
- Switch(config-line)#login登入需要密碼

不打login就算有設定密碼，系統也不會要求要輸入

密碼-2

- Virtual Terminal password遠端連線
- Switch#conft
- Switch(config)#line vty 0 4(session0-4)
- Switch(config-line)#password cisco(密碼)
- Switch(config-line)#login

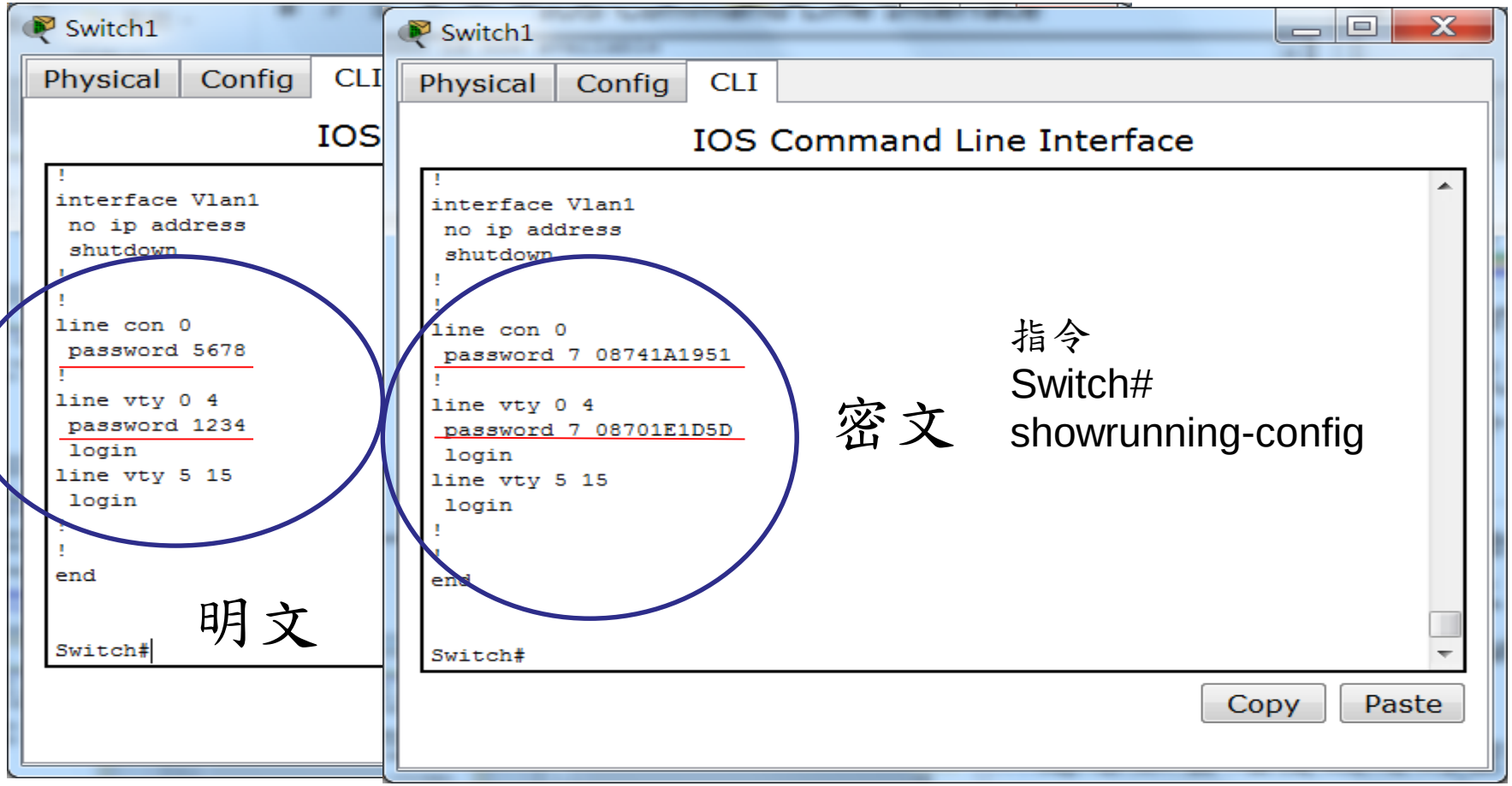
密碼-3

- Enable password與enable secret(優先)
- Switch#conft
- Switch(config)#enable password cisco
- Switch(config)#enable secret ryan
- Switch(config)#end
- Switch#show running-config
- Enable secret 5 **1mERr$hx5rVt7rPNoS4wqbXKX7m0**
- Enable password **cisco**看出差異了嗎

密碼-4

- Service password-encryption
- 許多密碼以明文的方式儲存，安全性低，所以可以使用這個指令來加密
- Switch#conf t
- Switch(config)#service password-encryption明文變密文　無法復原
- Switch(config)#no service password-encryption還原
- 還原加密之後設定的密碼，才不會變密文

加密前後對照


Switch1
Physical
Config
CLI
IOS
!
interface Vlan1
 no ip address
 shutdown
!
!
line con 0
 password 5678
!
line vty 0 4
 password 1234
 login
line vty 5 15
 login
!
!
end
明文
Switch#
Switch1
Physical
Config
CLI
IOS Command Line Interface
!
interface Vlan1
 no ip address
 shutdown
!
!
line con 0
 password 7 08741A1951
!
line vty 0 4
 password 7 08701E1D5D
 login
line vty 5 15
 login
!
!
end
Switch#
Copy
Paste
密文
指令
Switch#
showrunning-config

PortSecurity

- 透過電腦MAC的權限設定，鎖定電腦
- Switch#conft
- Switch(config)#interface fastetherne t0/5
- Switch(config-if)#
- Switchport mode access
- Switchport port-security
- Switchport port-security maximum1
- Switchport port-security mac-address sticky
- Switchport port-security mac-address 0008.aaaa.bbbb
- Switchport port-security violation restrict(shutdown，protect)

查看設定

- Switch#show port-security int fa0/5

shutdown

- shutdown用不到的port可以用這個指令將其關閉。就算電腦網路線都接妥，還是無法連線。
- No shutdown　啟動已關閉的port。
- 記得養成習慣，在介面上做完相關設定後要使用no shutdown。
- 預設沒用的port都是關閉的。

雙工

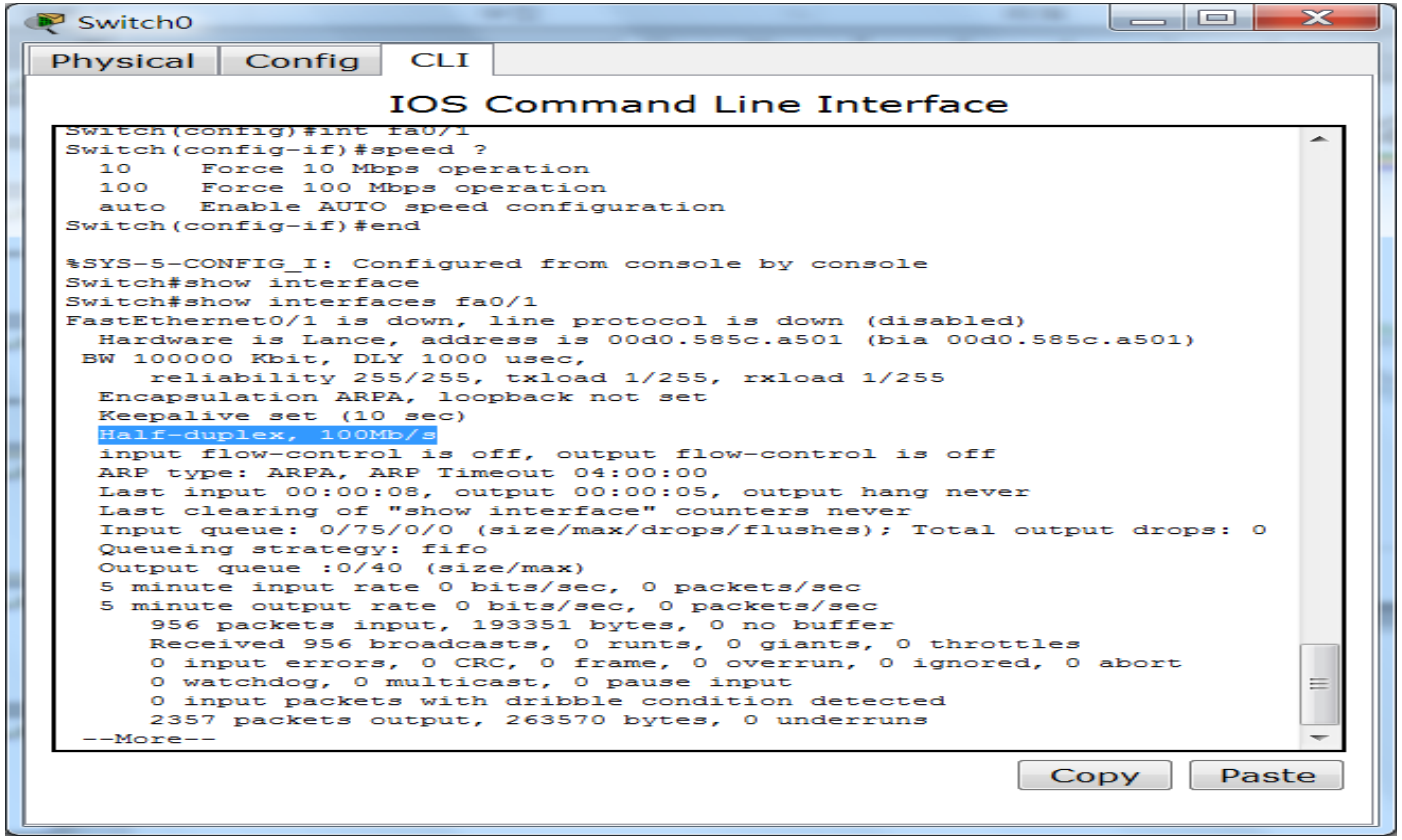
- Switch#conft
- Switch(config)#interface fa0/1
- Switch(config-if)#duplex?
  - Auto Enable AUTO duplex configuration
  - Full Force full duplex operation
  - Half Force half-duplex operation
- auto雙方“橋”出最佳模式

傳輸率

- Switch#conft
- Switch(config)#int fa 0/1
- Switch(config-if)#speed?
  - 10 Force 10Mbp soperation
  - 100 Force 100Mbp soperation
  - Auto Enable AUTO speed configuration

查看設定

- Show interface fastethernet 0/1



Line console

- RouterX(config)#line console0
- RouterX(config-line)#exec-timeout2030
  - 自動登出20分30秒內無任何動作即自行登出
- RouterX(config-line)#nologgingsynchronous
  - 當我們在輸入資料時，系統會不定期顯示系統訊息，造成資料輸入中斷，下此指令可將訊息抑制

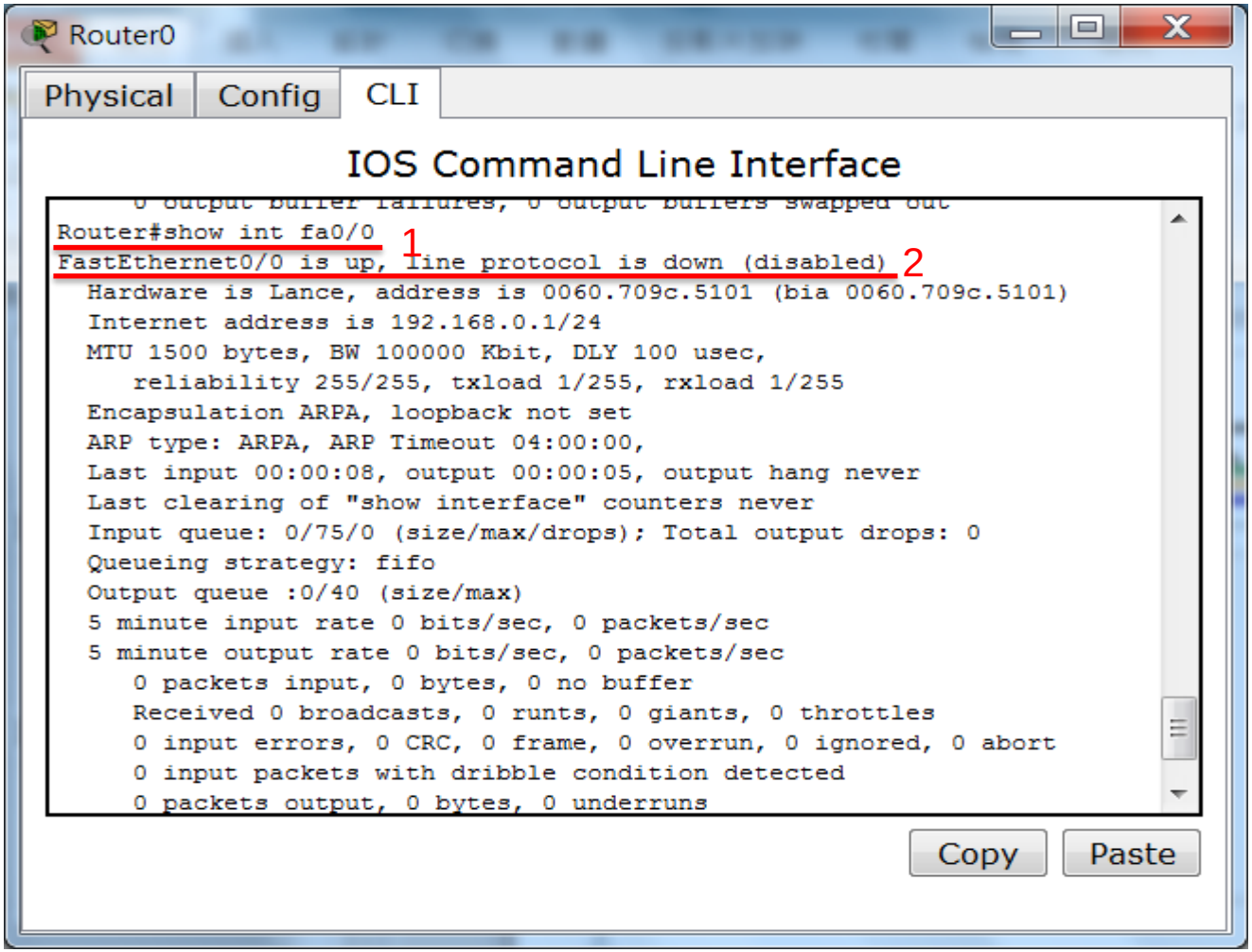
子介面

- RouterX(config)#interface type number
  - type
    - serial，ethernet，tokenring，fddi，hssi，loopback，dialer，null，async，atm，bri，tunnel，fastethernet
  - number(slot/port)
    - slot插槽
    - port埠數
- RouterX(config)#interface fa0/0

RouterIP設定

- Router#conft
- Router(config)#int fa0/0
- Router(config-if)#ipaddress192.168.1.254255.255.255.0
- Router(config-if)#no shutdown
- %LINK-5-CHANGED:Interface FastEthernet 0/0，changed stateto up

- Router#showintfa0/0



1up實體線路OK

2lineprotocolisdown
軟體設定有問題

up，up才有作用

介面狀態

- fa0/0 is up，line protocol is up
  - 正常運作
- fa0/0 is up，line protocoli s down
  - 資料格式不同，或收不到keepalives
- fa0/0is down，lineprotocolisdown
  - 硬體故障或線沒接好
- fa0/0is**adminis tratively down**，lineprotocolisdown
  - 介面被關閉(shutdown)使用noshutdown開啟

故障排除

- Show ip interface brief
- Show int fa0/0
- Show controllerss 0/0
- Show cdp neighbors detail

實作練習

- Switch vlan 1 ip address，default gateway
- Line console密碼設定
- Line vty密碼設定
- enable密碼設定
- port-security設定
- 故障排除

第三章

路由功能簡介

路由的基本原理

- 路由一詞是指將取自某裝置的封包，透過網路傳送給位於不同網路上的另一裝置
- 路由器實際上並不太在意主機，而只關心網路和通往每個網路的最佳路徑
- 目的主機的邏輯網路位址是用來讓封包能透過路由網路抵達某個網路，然後再用主機的硬體位址將封包從路由器送往正確的目的主機

路由的基本原理

- 要能夠路由封包，路由器就至少必須知道下列資訊
  - 目的位址
  - 能夠取得遠端網路資訊的鄰接路由器
  - 通往所有遠端網路的可能路徑
  - 通往每個遠端網路的最佳路徑
  - 如何維護與驗證路由資訊

路由的基本原理

- 路由器會從鄰接路由器或管理者取得遠端網路的資訊，然後建立起如何找到遠端網路的路徑表
  - 如果某個網路是直接相連，則該路由器本來就會知道要如何抵達這個網路
  - 如果該網路不是直接相連，路由器就必須透過2種方式取得如何抵達該遠端網路的資訊
    - 透過靜態路由，亦即由某人手動將所有網路位置輸入路徑表
    - 透過所謂的動態路由。

路由的基本原理

- 在動態路由時，某台路由器上的協定會與相鄰路由器上執行的相同協定溝通，接著這些路由器再相互更新彼此所知道的網路資訊，並且將資訊放入路徑表中
- 如果網路中發生變化，動態路由協定會自動通知所有路由器這個事件，而如果是使用靜態路由，管理者就要負責手動為所有路由器更新所有的改變
- 通常在大型網路中會同時使用動態與靜態路由。

路由器功能

- Path deter mination路徑選擇
  - Static routing靜態路由-管理者設定
  - Dynamic routing動態路由-藉不同的路由協定從其它路由器更新本身的路由表
  - Default routing預設路由-路由表找不到資訊的都會從預設路由路由0.0.0.00.0.0.0
- Packet for warding封包交換
  - 依照路由表及IP位址轉送封包

Routing Metrics

- Bandwidth頻寬
- Delay取決於頻寬、路由器暫存、網路流量、實際距離
- Hop count經過的路由器數量
- Cost成本由管理者依據各項可測量之數值進行設定，例如，頻寬

RoutingMethods

- DistanceVector距離向量
  - 距離hopcount
  - 向量方向，從哪一個路由器
  - RIPv1，RIPv2
  - 30秒更新一次
- Link-State鏈路狀態
  - triggeredupdates網路有異動立即更新路由表
  - periodicupdates定期更新(30分鐘)路由表
  - OSPF，EIGRP

第四章

VLAN

VLAN

- 方便管理與故障排除並減少錯誤發生機率
- 每個VLAN都是獨立的BroadcastDomain
- 每個VLAN都是獨立的Subnet
- VLAN存在於1個switch，也可以同時跨多個switches工作
- 支援VLSM Variable length subnetmasks
- 不同VLAN之間除非透過Router，否則無法溝通

網路設計

- 一家擁有約250名員工的公司如下

部門	使用者	位置
IT	15	A辦公大樓
HumanResource	10	A辦公大樓
Sales	102	B辦公大樓
Marketing	29	B辦公大樓
Finance	18	C辦公大樓
Accounting	26	C辦公大樓

1.部門人數最多的為102人的Sales
2./24即可滿足所需每個網路254IP
3.各部門屬不同VLAN
4.需考量未來成長

網路設計

部門	VLAN	IPSubnetaddress
IT	VLAN11	10.1.1.0/24
HumanResource	VLAN12	10.1.2.0/24
forfuturegrowth		10.1.3.0-10.1.255.0

部門	VLAN	IPSubnetaddress
Sales	VLAN21	10.2.1.0/24
Marketing	VLAN22	10.2.2.0/24
forfuturegrowth		10.3.3.0-10.3.255.0

部門	VLAN	IPSubnetaddress
Finance	VLAN31	10.3.1.0/24
Accounting	VLAN32	10.3.2.0/24
forfuturegrowth		10.3.3.0-10.3.255.0

- VALN11(A大樓第1個)
- 未使用到的Subnet可保留作其它用途，如IP tele phony

網路流量種類

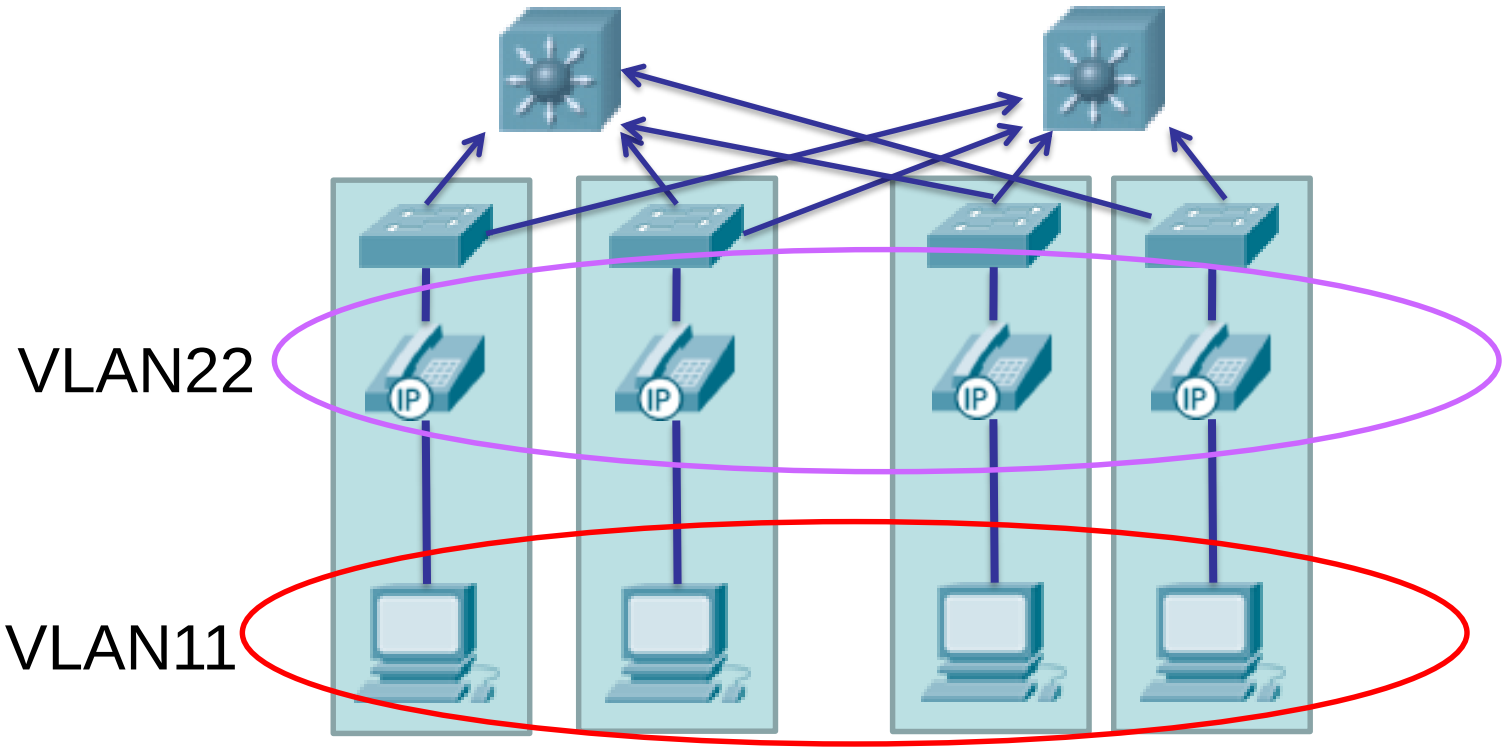
- 網路管理Networkmanagement
- 網路電話IPtelephony
- 多重傳播IPMulticast
- 資料傳輸Normaldata
- 清道夫Scavengerclass

網路管理

- 網路上存在許多用於網路管理的流量，管理者在網路規劃時，會將這些流量獨立在一個VLAN中，例如
  - BridgeProtocolDataUnits，BPDUs
  - SimpleNetworkManagementProtocol，SNMP
  - RemoteMonitoring，RMON

網路電話

- IPtelephony流量區分信號與語音等2部分，將語音獨立在VLAN中可有效管控流量
- 管理者可有效區分流量做好Qos與故障排除

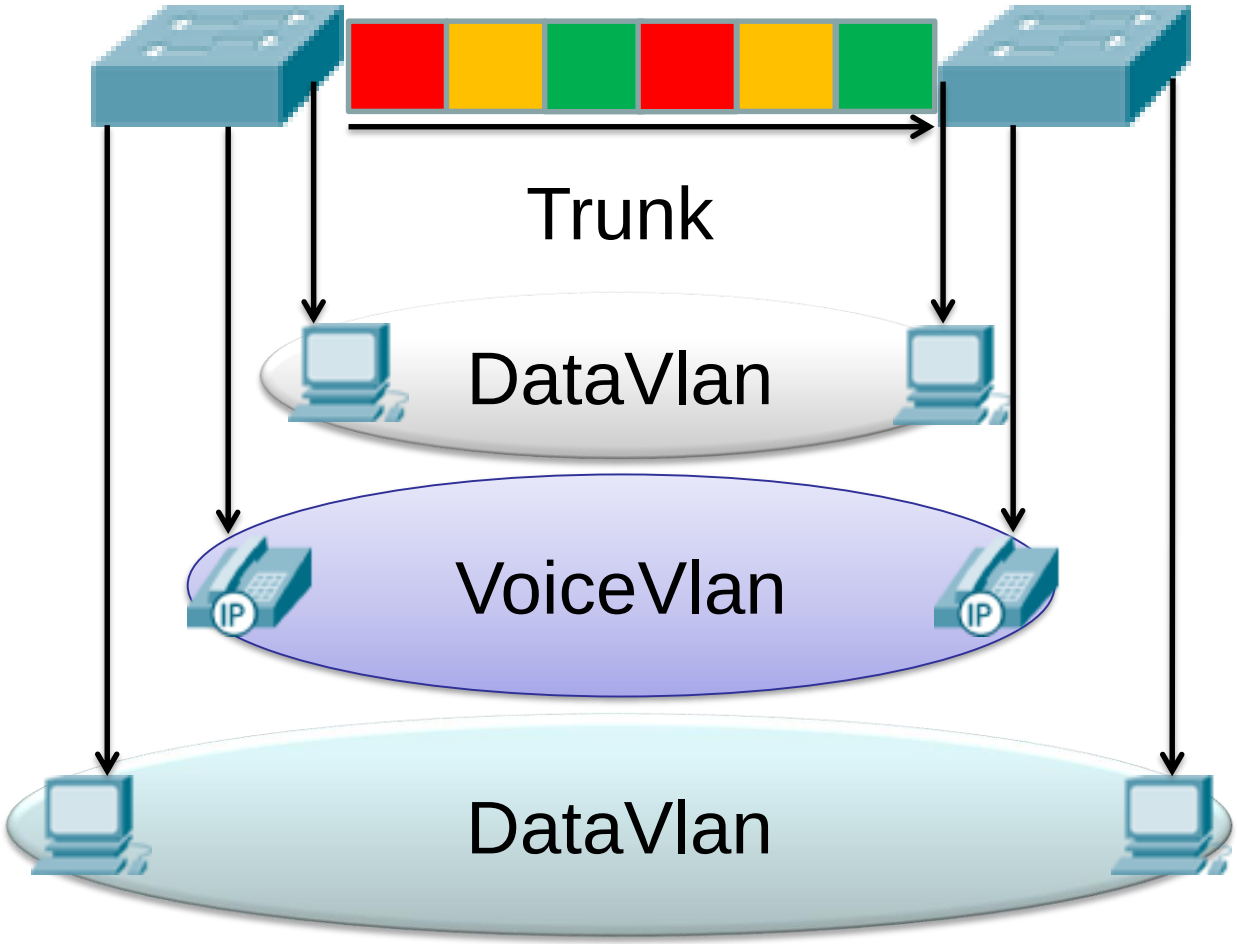


多重傳播

- 1個來源傳送至多重傳播的群組(具單一的IP及MAC為代表)
- 線上教學、視訊會議、安全性軟體及串流視訊(電影)
- 因為會產生相當大的流量，如果不加以區隔，將會影響正常資料傳送的流量

Trunk

Trunk作為不同VLAN在不同Switch間溝通的橋樑
frame到達Switch後，Switch會將其分配給所屬VLAN

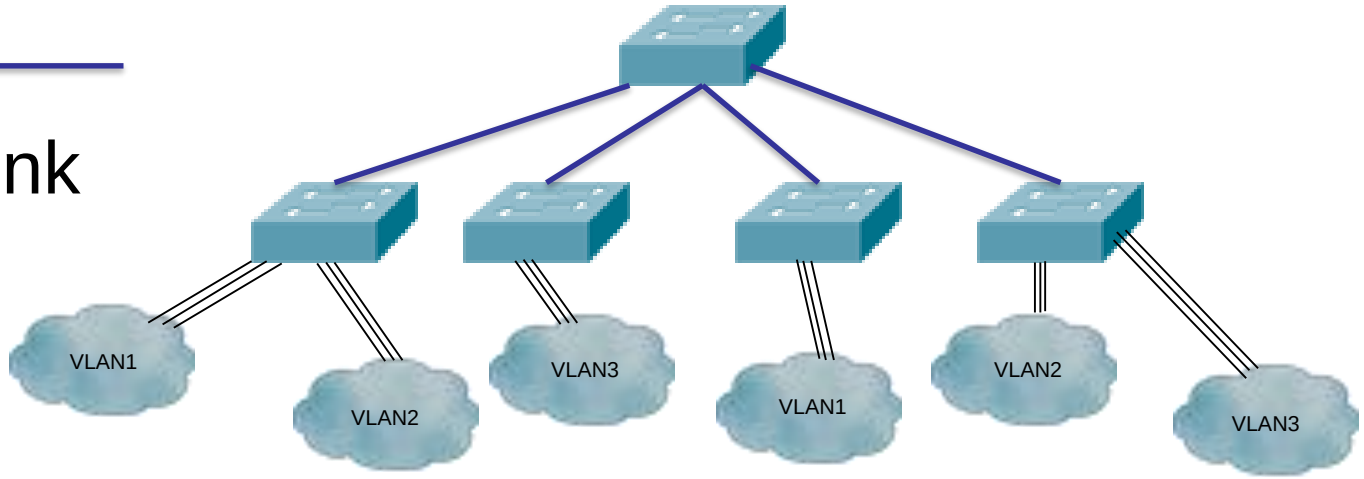


VLAN成員

- StaticVLAN
  - 管理自訂
- DynamicVLAN
  - VLAN Management Policy Server，VMPS
  - VMPS具有MAC位址與VLAN對映的功能
  - 依照到達switch的frame裡的來源MAC位址決定分配至哪個VLAN
- VoiceVLAN
  - 連接至IPphone

802.1QTrunking

Trunk



- trunk為點對點的連結，作為switch與switch、switch與router之間的橋樑，不同VLAN透過單一的trunk進行溝通
- 所有802.1Q的port皆為trunk
- 在trunk中的所有port皆屬於原生nativeVLAN
- nativeVLAN預設為VLAN1
- 所有未貼標籤的frames(不屬於任何VLAN)，皆為VLAN1
- 802.1Q不會在nativeVLAN上貼標籤，屬nativeVLAN的電腦無法讀取已貼標籤的frames

VTP

- VLAN Trunking Protocol，VTP
  - L2 messaging protocol
  - 自動更新VTP domain內所有switch的VLAN設定，避免發生錯誤，例如VLAN名稱重覆
  - switch在從trunk link接受到更新資訊前，預設不會加入任何的VTP domain
  - VTP server每隔5分鐘，會透過trunklink自動派送更新訊息至其它switch上

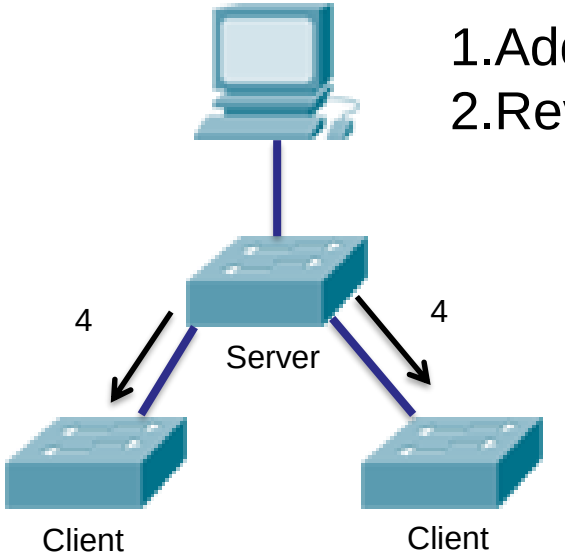
VTPmodes

- Server
  - 預設值，但除非自行設定或學習到VTPdomainname，server並不會自動派送自動更新訊息，可新增、刪除、修改VLANs、傳送與轉送更新訊息，同步。
- Transparent
  - 可新增、刪除、修改VLANs(本地)、轉送更新訊息。
- Client
  - 僅能傳送與轉送更新訊息，同步。

VTPoperation

- VTP以multicast frames進行更新
- VTPServer與Cient依照revision號碼進行更新，號碼越大的版本較新
- VTP的5分鐘更新一次，或有異動時會立即更新

Transparentre vision
永遠=0



1.Add new VLAN
2.Rev3->Rev4

3.Rev3->Rev4
4.Synnew VLAN information

3.Rev3->Rev4
4.SynnewVLANinformation

VTPoperation

- VTPdomain內所有switches的domainname與password要完全一樣，才能進行更新，不一樣就代表2台switch屬於不同VTPdomain，當然就無法實施更新了。
- switch在加入網路環境前，要先檢查
  - 是否為server模式
  - Domain name、password與現有環境是否相同
  - Revision number是否為最大，如果未檢查即將switch加入現有網路環境中，可能會造成新加入的switch會將其本身的設定，覆蓋掉網路現有的設定，而造成部分網路發生問題。

VTP實作練習

- VTP設定
- 802.1Qtrunks設定
- 在VTPserverswitch上新增或修改VLAN
- 分配switchport給VLAN
- 儲存VLAN設定

VTP設定實作

- CiscoCatalystswitchVTP預設值
  - VTPdomainname：none
  - VTPmode：Servermode
  - VTPpassword：null
  - VTPpruning：EnabledorDisabled
  - VTPversion：none
- domainname無法移除但可以修改
- domainpassword要相同否則無法正常工作

VTP設定實作

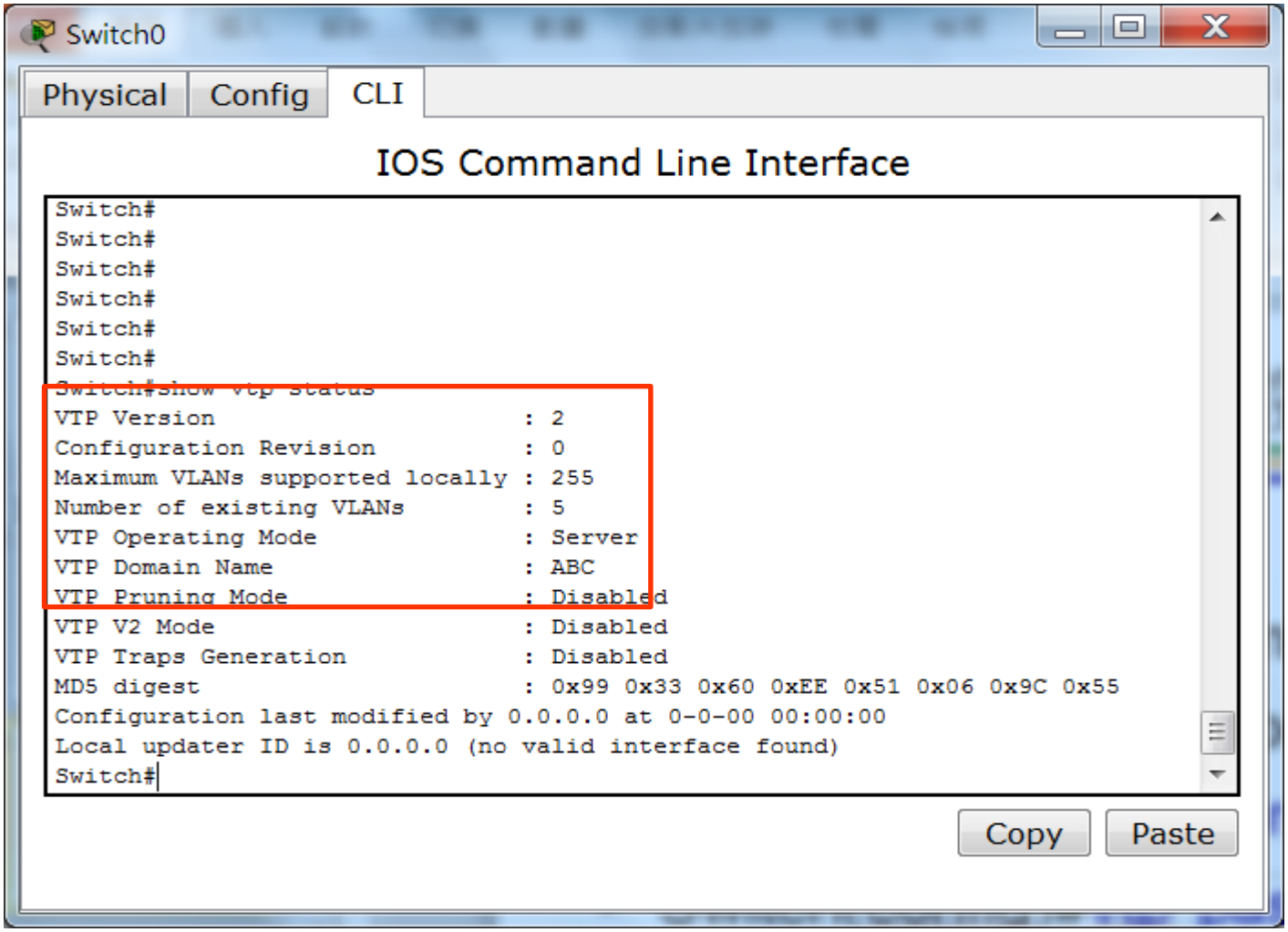
- Switch>enable
- Switch#configureterminal
- Switch(config)#vtpmodeserver
- Switch(config)#vtpdomain**ABC**
- Switch(config)#vtppassword**ABC**
- Switch(config)#vtpversion2
- Switch#copyrunning-configstartup-config

domainname跟password大小寫要完全一樣

存檔前先轉成transparent模式

VTP設定實作

- Switch#showvtpstatus



802.1Qtrunks設定

- 設定trunkport就無法成為secureport
- Switch(config-if)#
  - Switchport mode
    - access存取port(非trunk模式)
    - dynamic{auto|desirable}協商機制
      - dynamicauto+trunkordynamicdesirable才會變trunk
      - dynamicdesirable+dynamicautoordynamicdesirableortrunk才會變trunk
    - trunk(永久的trunk)
  - Switchport nonegotiate不協商，除非雙方都是trunk才會變trunklink

802.1Qtrunks設定

	trunk	desirable	auto	access
trunk	trunk	trunk	trunk	access
desirable	trunk	trunk	trunk	access
auto	trunk	trunk	access	access
access	access	access	access	access

- Switch#show interface fa0/1 switchport
  - 查trunk模式
- Switch#show interface fa0/1trunk
  - 查通過turnk的VLAN

VLAN設定

- 設定前先確認VTPmode為server mode or transparent mode
- 新增VLAN
  - Switch(config)#vlan2
  - Switch(config-vlan)#name switchlab88
  - VIDs1-1005(1，1001，1002~1005保留)
  - extended-rangeVLANsVIDs1006-4094
  - Switch#show vlan brief
  - Switch#show vlan id2
  - Switch#show vlan names witch lab88

VLAN設定

- 分配switchport給VLAN
  - Switch(config)#int fa0/1
  - Switch(config-if)#switchport mode access
  - Switch(config-if)#switchport access vlan11
  - 指定多個port
  - Switch(config)#int range fa0/1-9 or
  - Switch(config)#int range fa0/1，fa0/3，fa0/5
  - Switch(config-if-range)#switchport mode access
  - Switch(config-if-range)#switchport access vlan22
- showinterfacefa0/1switchport

no移除

VLAN新增、移除與變更設定

- VTPserver與transparent模式下執行
- 當在VTPserver上變更VLAN設定時，會在VTPdomain內傳播(5分鐘)
- 當1個port被指配給新的VLAN時，將自動從之前的VLAN中移除。
- 當移除1個VLAN時，原本在此VLAN中的所有port需重新指配給其它VLAN，否則無法使用。

VLAN移除設定

- 重新分配switchport給VLAN1
  - Switch(config)#**no**vlan2 ***1.移除vlan***
  - Switch(config)#intfa0/1 ***2.自vlan移除某個port***
  - Switch(config-if)#**no**switchportaccessvlan2

    3.重新將此port指配給vlan1
  - Switch(config-if)#switchportmodeaccess
  - Switch(config-if)#switchportaccessvlan1

VLAN設定

- router設定
  - config#intfa0/0.1(虛擬介面)
    - Encapsulation dot1q11(vlan編號)
    - Ip address 192.168.1.254 255.255.255.0(閘道)
    - No shutdwon
  - config# int fa0/0.2
    - Encapsulation dot1q22
    - Ip address192.168.2.254255.255.255.0
    - No shutdwon

故障排除

- #showvlanbrief
- #showvtpstatus
- #show int fa0/1switchport
- #show in ttrunk
- #show ip intbrief
- Noswitch port access vlan
- 將已被移除的介重新回歸到VLAN1
- 不然show vlan brief會看不到

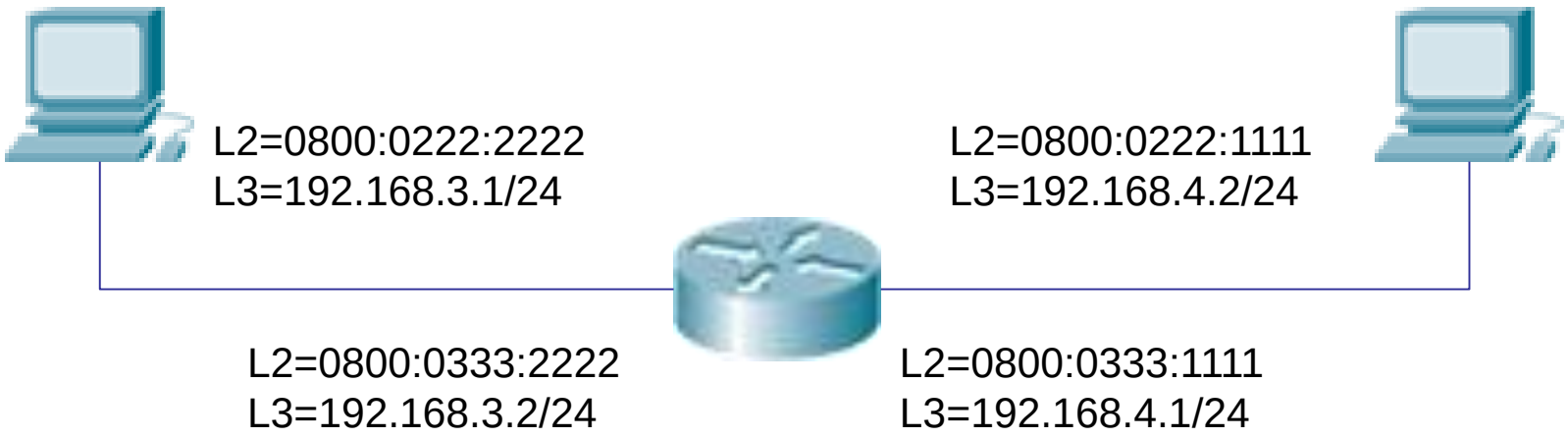
第五章

封包傳遞過程

定址

- Layer 2 Addressing
  - MAC
- Layer 3 Addressing
  - IP

每台電腦及路由器上的每個介面最少要有2個位址



封包傳遞

- 封包在傳遞的過程中，雖然會經由路由器傳送，但是其第3層的IP位址是不會變的，惟一會變的只有第2層的MAC位址。
- 相關指令
  - Show ip arp
  - ping
  - traceroute

IP路由流程

- IP的路由流程相當簡單，而且不會因為網路的規模不同而有所改變，我們將以圖為例，逐步地描述Host_A如何與不同網路上之Host_B通訊的過程。

圖 5.1　2 台主機與 1 台路由器之 IP 遞送範例

IP路由流程

- 在本例中，Host_A上的使用者對Host_B的IP位址進行ping的動作；這是最簡單的路由，但是仍然涉及許多步驟，包括：
  - 1.ICMP(Internet Control Message Protocol)產生echo請求的有效負載(payload)。
  - 2.ICMP將該有效負載傳給IP以建立封包；這個封包中至少包含IP來源位址、IP目的位址、和內容為01h的協定欄位。當封包抵達目標時，這些資訊就能告訴接收端主機應該將此有效負載交給誰。

IP路由流程

3. 一旦建立封包後，IP會判斷目的IP位址是位於本地網路或遠端網路。
4. 由於IP判定這是遠端請求，所以封包必須送往預設閘道以便路由至遠端網路。藉由解析Windows中的Registry，以找出設定的預設閘道。

IP路由流程

5. 主機172.16.10.2(Host_A)的預設閘道是172.16.10.1，為了要將該封包送到預設閘道，必須先知道路由器界面Ethernet0的硬體位址。為什麼呢？因為如此該封包才能往下送給資料鏈結層來建立訊框，並且送往路由器連到172.16.10.0網路的界面。本地LAN上的主機間只會透過硬體位址進行通訊—您一定要瞭解，當Host_A要與Host_B進行通訊時，必須將封包送往本地網路上預設閘道的MAC位址。

IP路由流程

6.接著檢查ARP快取記憶體，看預設閘道的IP位址是否已被解析為硬體位址：

- 如果已有資訊，就可以立即送往資料鏈結層建立訊框(硬體目的位址也會隨著該封包向下傳)。
- 如果該主機的ARP快取記憶體中還沒有該硬體位址，則會對區域網路送出ARP廣播，以搜尋172.16.10.1的硬體位址。路由器會回應這個請求，並且提供Ethernet0的硬體位址，而該主機則會將此位址放入快取中。同時，路由器也會將Host_A的硬體位址放入自己的ARP快取中。

IP路由流程

7. 當封包與目的硬體位址傳給資料鏈結層後，就會利用LAN驅動程式透過所使用的區域網路類型來提供媒介存取。接著使用控制資訊封裝這個封包而產生訊框；在本例中，該訊框除了包含硬體的目的與來源位址外，還包含Ether-Type欄位，用來描述將該封包傳給資料鏈結層的網路層協定－在此為IP。訊框的結尾是訊框查核序列(Frame Check Sequence，FCS)欄位，存放循環冗餘檢查(CRC)的結果。

IP路由流程

8.一旦完成訊框的裝填，就會交由實體層逐一將每個位元放入實體媒介中(本例為雙絞線)。

9.碰撞網域中的每個裝置都會收到這些位元，建立訊框，執行CRC，並檢查FCS欄位中的結果。如果結果不符，訊框就會被丟棄。

- 如果CRC相符，則檢查硬體目的位址，判斷是否也符合(在本例為路由器的界面Ethernet0)。
- 如果符合，則檢查Ether-Type欄位以找出網路層所使用的協定。

IP路由流程

10.將封包由訊框中取出，傳給Ether-Type欄位中所指定的協定(亦即IP)，並且將訊框的剩餘部份丟棄。

11.IP收到封包，並且檢查IP目的位址。因為該封包的目的位址並不符合接收之路由器本身所設定的任何位址，該路由器會在它的路徑表中尋找目的IP的網路位址。

IP路由流程

12.路徑表必須包含網路172.16.20.0的資料，否則封包會立刻被丟棄。並且將包含「**destination network unreachable**」訊息的ICMP訊息送回給最初的裝置。

13.如果路由器在表中找到目的網路，則封包會被交換到離開的界面－在本例為Ethernet1。

14.路由器透過封包交換，將封包送入Ethernet1的緩衝區。

IP路由流程

15.Ethernet1緩衝區必須知道目的主機的硬體位址，所以會先檢查它的ARP快取。

- 如果過去已經解析過Host_B的硬體位址，則將封包與硬體位址向下傳給資料鏈結層建立訊框。
- 如果尚未解析過該硬體位址，路由器會從E1送出ARP請求，以尋找172.16.20.2的硬體位址。

Host_B會回應自己的硬體位址，接著封包與目的位址會送往資料鏈結層建立訊框。

IP路由流程

16. 資料鏈結層建立訊框，包含目的與來源硬體位址、Ether-Type欄位、與訊框尾端的FCS欄位。將該訊框送往實體層以便逐一將位元送到實體媒介中。

17. Host_B收到訊框，並且立即執行CRC。如果結果與FCS欄位相符，就檢查硬體目的位址。如果仍然相符，就檢查Ether-Type欄位以判斷封包應該送往網路層的哪個協定－在本例為IP。

IP路由流程

18.在網路層中，IP會接收這個封包，並且檢查IP目的位址。當確定符合後會檢查協定欄位，以找出其有效負載要交給誰。

19.將有效負載交給ICMP；它能瞭解這是個echo請求，並且加以回應－立即丟棄這個封包，並且產生新的有效負載作為echo的回應。

20.接著建立封包，包含來源與目的位址、協定欄位、以及負載；現在的目的裝置為Host_A。

IP路由流程

21.IP接著檢查目的IP位址是位於本地LAN或遠端網路上的裝置。因為目的裝置是位於遠端網路，所以該封包必須送往預設的閘道。

22.在Windows裝置的Registry中找到預設的閘道IP，並且檢查ARP快取以檢查該IP位址是否已經解析為硬體位址。

23.一旦找到預設閘道的硬體位址，將封包與目的硬體位址向下傳給資料鏈結層以建立訊框。

IP路由流程

24. 資料鏈結層的訊框標頭中包含下列資訊：
    - 目的與來源硬體位址
    - 值為0x800(IP)的Ether-Type欄位
    - 包含CRC結果的FCS欄位
25. 將訊框下傳給實體層以逐一將每個位元送到網路媒介上。
26. 路由器的Ethernet1界面會接收這些位元並且建立訊框，執行CRC，檢查FCS欄位以確保結果相符。

IP路由流程

27.如果CRC正確，接著檢查硬體目的位址。因為符合路由器的界面，所以將封包由訊框中取出，並且檢查Ether-Type欄位，以找出應該將封包遞送給網路層的哪個協定。

28.判定協定為IP，所以由它取得封包。IP會先對IP標頭執行CRC檢查，然後檢查目的IP位址。因為IP目的位址並不符合路由器的任何界面，所以會檢查路徑表以找出是否有通往172.16.10.0的路徑。

IP路由流程

如果沒有通往目的網路的路徑，封包就會立刻被丟棄(這是許多管理者發生混淆的地方－當ping失敗時，大多數人會認為是因為封包並沒有抵達目的主機。但是在此可以看出，事實上未必如此。它可能只是因為某個遠端路由器中少了一條回到原始主機網路的路徑罷了！此時，封包是在回程、而不是前往主機的途中被丟棄的)。

IP路由流程

29.路由器知道如何抵達網路172.16.10.0－離開的界面是Ethernet0－所以封包被交換到界面Ethernet0。

30.路由器檢查ARP快取以判斷是否已經解析過172.16.10.2的硬體位址了。

31.因為172.16.10.2的硬體位址已經在原本前往Host_B的旅程中就放入快取了，所以將硬體位址與封包傳給資料鏈結層。

IP路由流程

32. 資料鏈結層使用目的硬體位址與來源硬體位址建立訊框，並且將IP放入Ether-Type欄位。對訊框執行CRC，將結果放入FCS欄位中。

33. 接著將訊框傳給實體層，以便逐一將每個位元送入區域網路中。

34. 目的主機收到訊框，執行CRC，檢查目的硬體位址，並且檢視Ether-Type欄位以找出要將封包傳給誰。

IP路由流程

35.IP是被指定的接收者；當封包傳給網路層的IP時，它會檢查協定欄位尋求更進一步的指示。IP根據指示將有效負載交給ICMP，而ICMP接著判斷出這個封包是ICMP的echo回應。

36.ICMP送出驚歎號(!)到使用者界面以確認它已經收到回應，接著再嘗試傳送另外4個echo請求給目的主機。

靜態路由

- Static route
  - 手動輸入
  - 小型網路
- Dynamic route
  - 由路由協定自己學習路由
  - 大型網路

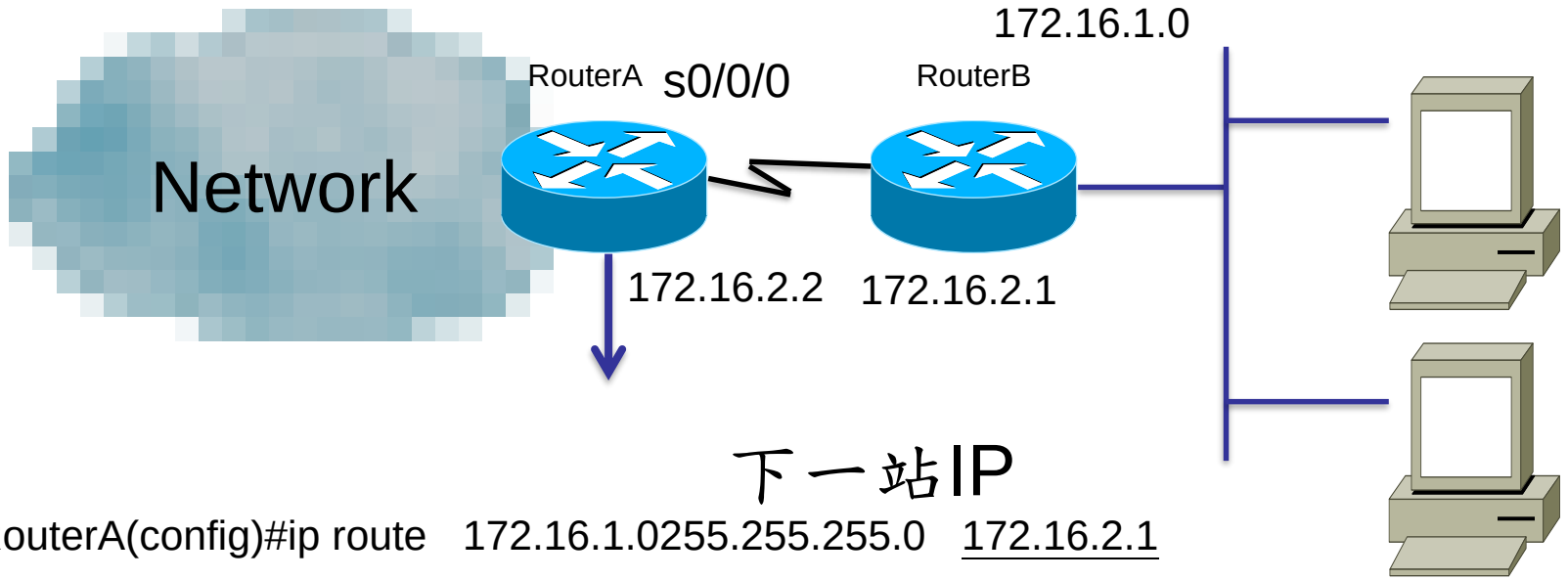
靜態路由

- 靜態路由是指在每台路由器的路徑表中手動加入路徑。靜態路由有其優點與缺點，不過每種路由程序都是如此。
- 靜態路由具有下列優點：
  - 不會造成路由器CPU的額外負擔；這意謂著您購買路由器所花的錢可能比使用動態路由時便宜。
  - 路由器間沒有使用額外的頻寬；這意謂著您可能可以節省花在WAN線路上的錢。
  - 增加安全性；因為管理者可以選擇只讓路由得以存取一些特定的網路。

靜態路由

- 靜態路由具有下列缺點：
  - 管理者必須確實熟悉整個互連網路，以及每台路由器的連結方式，才能正確地設定路由器。
  - 如果要新增網路到互連網路中，管理者必須手動在所有路由器中加入通往該網路的路徑。
  - 在大型網路中並不可行，因為它的維護本身就是個全天候的工作。

StaticRoute



下一站IP

RouterA(config)#ip route 172.16.1.0255.255.255.0 172.16.2.1

出口介面

RouterA(config)#ip route 172.16.1.0 255.255.255.0 s0/0/0

預設路由

RouterB(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2

靜態路由

– 下面是在路徑表中加入靜態路徑的命令語法：

```
ip route [destination_network] [mask] [next-hop_address or exitinterface] [administrative_distance] [permanent]
```

- 下面的清單是字串中每個命令的解說：
  - **iproute**—用來建立靜態路徑的命令。
  - **destination_network**—要放在路徑表中的網路。

靜態路由

- **mask**－該網路使用的子網路遮罩。
- **next-hop_address**－負責接收封包並轉送至遠端網路之下一中繼站路由器位址－這是位於直接相連網路的路由器界面。在新增路徑前，必須先能夠ping到該路由器界面；如果輸入錯誤的下一中繼站位址，或是通往該路由器的界面沒有啟動，則路由器組態中會包含該靜態路徑，但路徑表中卻不會有這條路徑。

靜態路由

- **exitinterface**－您也可以用它來取代下一中繼站位址，但是它必須是點對點的鏈結，例如WAN。這個命令在諸如乙太網路等LAN上無法作用。
- **administrative_distance**－根據預設，靜態路徑的管理性距離為1(如果您使用離開界面取代下一中繼站位址，則管理性距離甚至為0)。您可以在命令最後面加入管理權重以改變預設值。

靜態路由

- **permanent**—如果界面被關閉，或者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，選擇這個選項能夠在無論什麼情況下，都將這個項目保留在路徑表中。

路由狀態

- Router#show ip route
- Codes:C-connected，S-static，I-IGRP，R-RIP，M-mobile，B-BGPD-EIGRP，EX-EIGRPexternal，O-OSPF，IA-OSPFinterareaN1-OSPFNSSAexternaltype1，N2-OSPFNSSAexternaltype2E1-OSPFexternaltype1，E2-OSPFexternaltype2，E-EGPi-IS-IS，L1-IS-ISlevel-1，L2-IS-ISlevel-2，ia-IS-ISinterarea*-candidatedefault，U-per-userstaticroute，o-ODRP-periodicdownloadedstaticroute

- R代表RIP路由協定
- 120/1120代表AD值，1代表metric值

預設路由

- 我們使用預設路由將目的網路不在路徑表中的封包送往下一中繼站路由器。您只能在殘根型網路(stubnetwork)上使用預設路由；殘根型網路是只有一條離開路徑的網路。

預設路由

- 當設定預設路徑時，靜態路徑中的網路位址與遮罩位置都要以通配字元(wildcard)取代。事實上，您可以將預設路徑視為是使用通配字元來取代網路與遮罩資訊的靜態路徑。

預設路由

```
Lab_C(config)#no   ip   route   192.168.10.0   255.255.255.0
    192.168.40.1
Lab_C(config)#no   ip   route   192.168.20.0   255.255.255.0
    192.168.40.1
Lab_C(config)#no   ip   route   192.168.30.0   255.255.255.0
192.168.40.1
Lab_C(config)#ip   route   0.0.0.0   0.0.0.0   192.168.40.1
```

- 如果現在檢視路徑表，只會看到2個直接相連的網路，加上S*表示這個項目是候補的預設路徑。

AD值

- AdministrativeDistance
  - 0~255路由協定用來比較，較小的優先使用
  - 例路由器A使用2個路由協定RIP(AD=120)、EIGRP(AD=90)，均可到達目的地，此時路由器A會優先使用EIGRP

Route source	DefaultDistance
Connected interface	0
Static route address	1
EIGRP	90
OSPF	110
RIPv1，RIPv2	120
External EIGRP	170
Unknow or unbelievable	255

路由協定

- 路由協定共有3類，包括：
  - **距離向量** — 距離向量協定(distance-vector protocol)會根據距離找出通往遠端網路的最佳路徑。封包每經過一台路由器，稱為一個中繼站(hop)。向量會指示通往遠端網路的方向。RIP與IGRP都是距離向量路由協定；它們會將整個路徑表傳送給直接相連的鄰居。

路由協定

- **鏈路狀態**—鏈路狀態協定(link-stateprotocol)又稱為最短路徑優先協定(shortest-path-first protocol)；在這種協定中，每台路由器會建立3個獨立的表格，其中之一會追蹤直接相連的鄰居，一個會決定整個互連網路的拓樸，而最後一個則是路徑表。鏈路狀態路由器對互連網路的資訊瞭解得比距離向量路由協定清楚。OSPF是完全屬於鏈路狀態的IP路由協定。鏈路狀態協定會傳送包含它們自己鏈路狀態的路徑更新資訊給網路上所有其他的路由器。

路由協定

- **混合式**－混合式協定同時使用距離向量與鏈路狀態，例如EIGRP。

- 沒有一種路由協定的設定方式適合所有情況，您只能視情況見招拆招。如果瞭解不同路由協定的運作方式，就能夠做出真正符合任何情況之獨特需求的良好決策。

距離向量路由協定

- 距離向量路由演算法會將完整的路徑表內容傳送給鄰接的路由器，鄰接路由器則會將收到的路徑表項目與自己的路徑表合併成為該路由器的完整路徑表－這稱為謠傳式路由(routingbyrumor)，因為路由器會相信從鄰接路由器收到的遠端網路路徑資訊更新，而沒有自行驗證。
- 網路可能會有多條通往相同遠端網路的路線，此時協定會先檢查管理性距離。如果AD相同，則會使用其他的衡量指標來判斷通往遠端網路的最佳路徑。

距離向量路由協定

- RIP只使用中繼站數目來判斷通往特定網路的最佳路徑。如果RIP找到不只一條路徑可通往相同的遠端網路，並且具有相同中繼站數目，則會自動執行輪流式負載平衡(round-robinloadbalancing)。RIP最多能進行6條相同成本線路的負載平衡(預設為4)。

距離向量路由協定

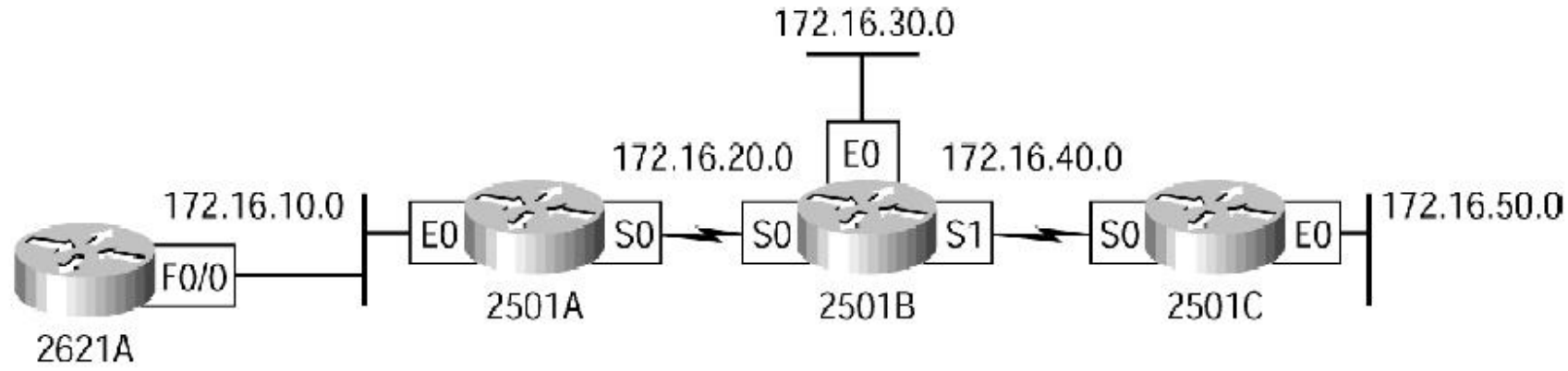
- 不過，當2條通往遠端網路的線路具有不同的頻寬，但是相同中繼站數目時，這種路由衡量指標就會出問題。圖是2條線路可通往遠端網路172.16.10.0的範例。

圖 5.3 針孔式壅塞

距離向量路由協定

- 因為172.16.30.0網路是頻寬為1.544Mbps的T1鏈結，而172.16.20.0網路是56K的鏈結，您自然希望路由器優先選擇T1。但是因為RIP路由只使用中繼站數目作為唯一的衡量指標，這2條路徑被視為具有相同的成本－這種小麻煩稱為針孔式壅塞(pin hole congestion)。

距離向量路由協定



路徑表		
172.16.10.0	F0/0	0

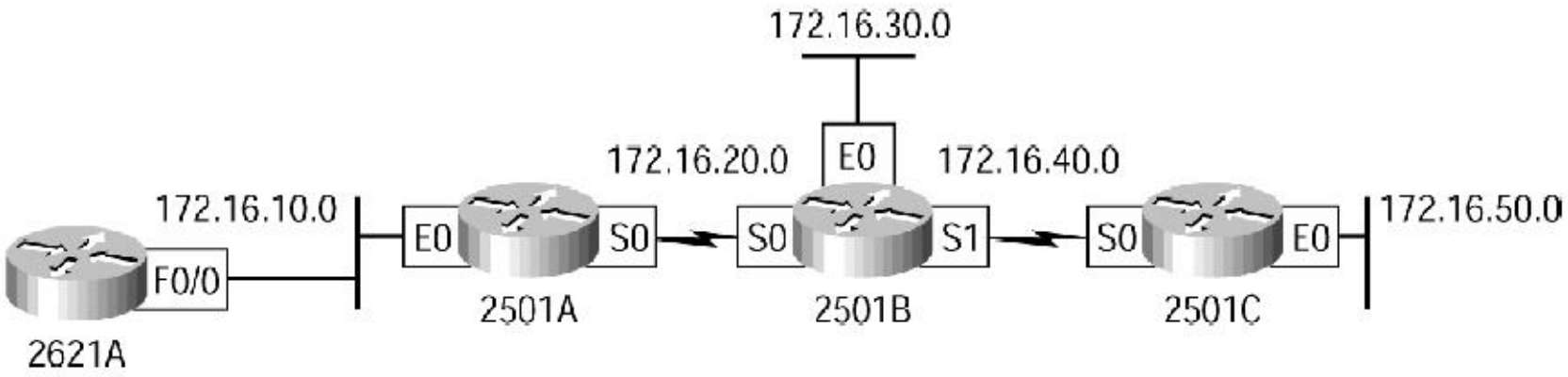
路徑表		
172.16.10.0	E0	0
172.16.20.0	S0	0

路徑表		
172.16.20.0	S0	0
172.16.30.0	E0	0
172.16.40.0	S1	0

路徑表		
172.16.40.0	S0	0
172.16.50.0	E0	0

圖 5.4 用距離向量遞送的互連網路

距離向量路由協定



路徑表		
172.16.10.0	F0/0	0
172.16.20.0	F0/0	1
172.16.30.0	F0/0	2
172.16.40.0	F0/0	2
172.16.50.0	F0/0	3

路徑表		
172.16.10.0	E0	0
172.16.20.0	S0	0
172.16.30.0	S0	1
172.16.40.0	S0	1
172.16.50.0	S0	2

路徑表		
172.16.20.0	S0	0
172.16.30.0	E0	0
172.16.40.0	S1	0
172.16.10.0	S0	1
172.16.50.0	S1	1

路徑表		
172.16.40.0	S0	0
172.16.50.0	E0	0
172.16.10.0	S0	2
172.16.20.0	S0	1
172.16.30.0	S0	1

圖 5.5 收斂後的路徑表

路由迴圈

- 距離向量路由協定會藉由定期從所有作用中的界面廣播路徑更新資訊，以追蹤互連網路中的任何變動。這種廣播中會包含完整的路由表，雖然可運作得不錯，但是很消耗CPU資源與線路頻寬。如果網路發生重大變動，就會產生問題。此外，距離向量路由協定的收斂時間緩慢，也會導致路徑表的不一致和路由迴圈(routing loop)。

路由迴圈

- 當每台路由器沒有同時或接近同時地更新，就可能產生路由迴圈。例如假設圖中的網路5故障。在此互連網路中，所有路由器都是從路由器E處取得網路5的資訊，而路由器A的表格中，則包含通過路由器B抵達網路5的路徑。

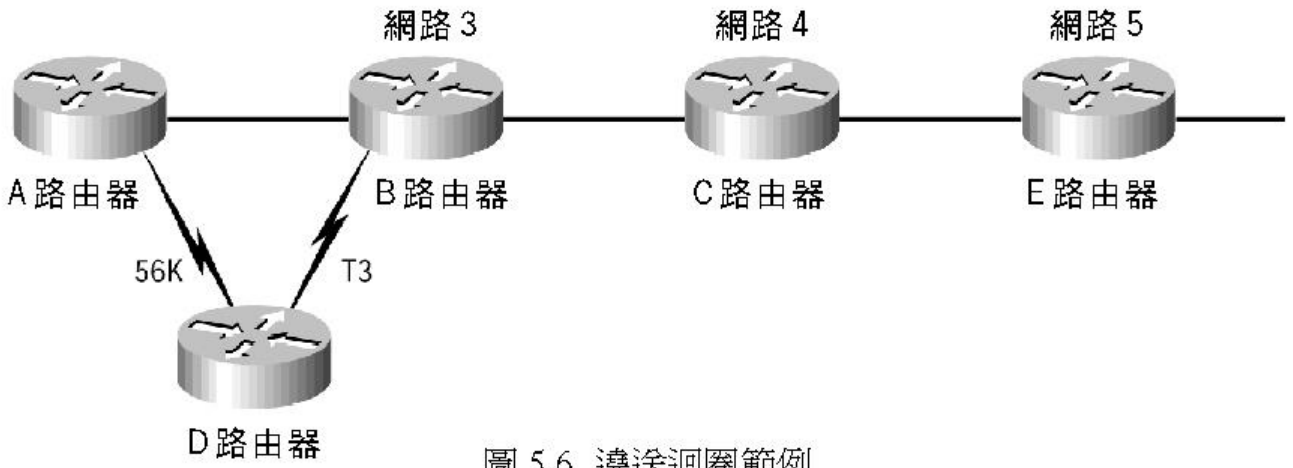


圖 5.6 遞送迴圈範例

路由迴圈

- 但是A、B、與D路由器還不知道網路5的狀況，所以它們仍舊繼續傳送更新資訊。C路由器最後終於送出更新，並且讓B路由器停止路由到網路5，但是A與D路由器仍舊尚未更新。對它們而言，網路5似乎仍舊可以在衡量指標為3的情況下，透過B路由器抵達。

路由迴圈

- 問題發生在當A路由器送出定期的30秒更新：“**嗨！我的鏈結還是老樣子喔！**”時，表示它仍舊具有抵達網路5的能力。B與D路由器收到這個好消息，發現可以從A路由器處抵達網路5，於是送出可以抵達網路5的資訊。任何要送往網路5的封包都會先到A路由器，再到B路由器，然後再送回A路由器—這就是路由迴圈。

最大中繼站數目

- 前述的路由迴圈問題稱為“**算到無限**”(counting to infinity)問題；這是因為在互連網路上宣傳的閒話與錯誤資訊所造成。如果沒有某種形式的干預，中繼站計數將會在封包每次經過一台路由器時就無限地增加。

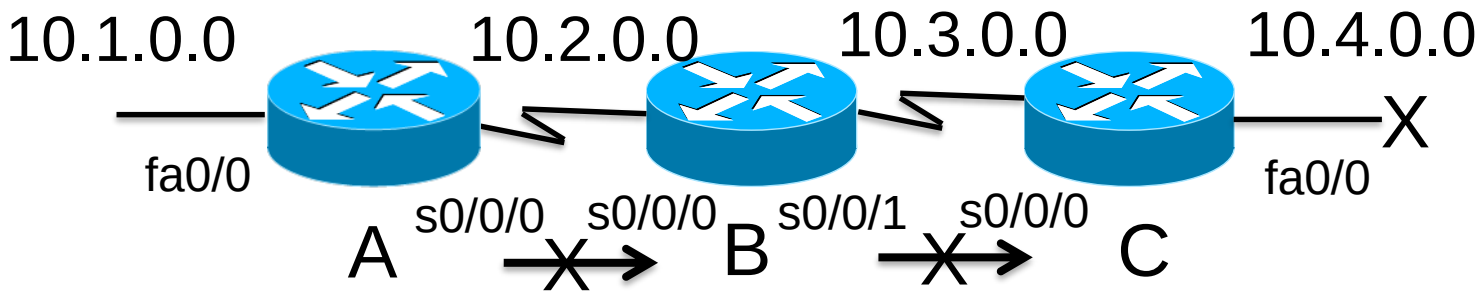
最大中繼站數目

- 解決這個問題的一個方式是定義最大中繼站數目(maximum hop count)。RIP的中繼站計數最高可以到15，所以需要16個中繼站的路徑會被視為無法抵達。換句話說，在巡迴了15個中繼站後，網路5將被認為故障。因此，最大中繼站數目會決定路徑表中的項目需要多久才會被視為無效或有問題。
- 雖然這是個解決之道，但是並無法移除路由迴圈。每個封包還是會進入迴圈，只是它們不再永遠不受檢查地在其中旅行，而只會來來回回16次，然後消滅。

分割視野

- 另一種解決路由迴圈的方法稱為“**分割視野**”(split horizon)，它會強制實施路由資訊不得往接收方向回傳的規則，以降低距離向量網路中不正確的路徑資訊與路由成本。易言之，路由協定會區別網路路徑是從哪個界面取得，一旦決定之後，它就不會從相同界面將該路徑宣傳回去。這可以防止A路由器將B路由器送來的更新資訊再回傳給B路由器。

Routing Loops-Split horizon



RoutingTableA		
10.1.0.0	fa0/0	0
10.2.0.0	s0/0/0	0
10.3.0.0	s0/0/0	1
10.4.0.0	**s0/0/0**	**2**

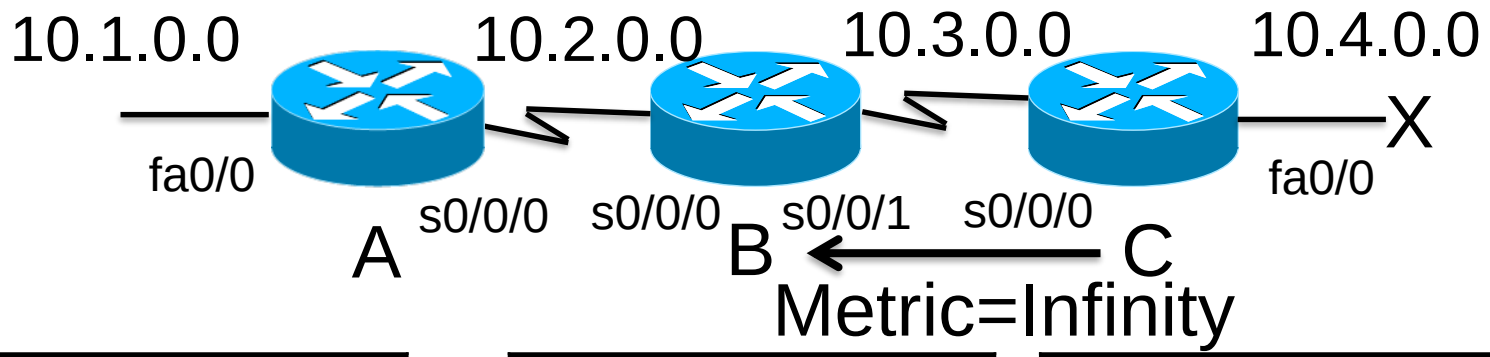
RoutingTableB		
10.2.0.0	s0/0/0	0
10.3.0.0	s0/0/1	0
10.4.0.0	**s0/0/1**	**1**
10.1.0.0	s0/0/0	1

RoutingTableC		
10.3.0.0	s0/0/0	0
10.4.0.0	**fa0/0**	**0**
10.2.0.0	s0/0/0	1
10.1.0.0	s0/0/0	2

路徑毒害

- 另一種避免不一致路徑更新與停止網路迴圈的方法稱為“**路徑毒害**”(route poisoning)。例如當網路5故障時，E路由器會宣傳網路5為16或無法抵達(有時也稱為無限大)，以開始實施路徑毒害。
- 這項路徑的毒害資訊可以讓C路由器避免受到關於網路5之路徑的不正確更新資訊所影響。

Routing Loops-Route poisoning



RoutingTableA		
10.1.0.0	fa0/0	0
10.2.0.0	s0/0/0	0
10.3.0.0	s0/0/0	1
10.4.0.0	**s0/0/0**	**2**

RoutingTableB		
10.2.0.0	s0/0/0	0
10.3.0.0	s0/0/1	0
10.4.0.0	**s0/0/1**	**1**
10.1.0.0	s0/0/0	1

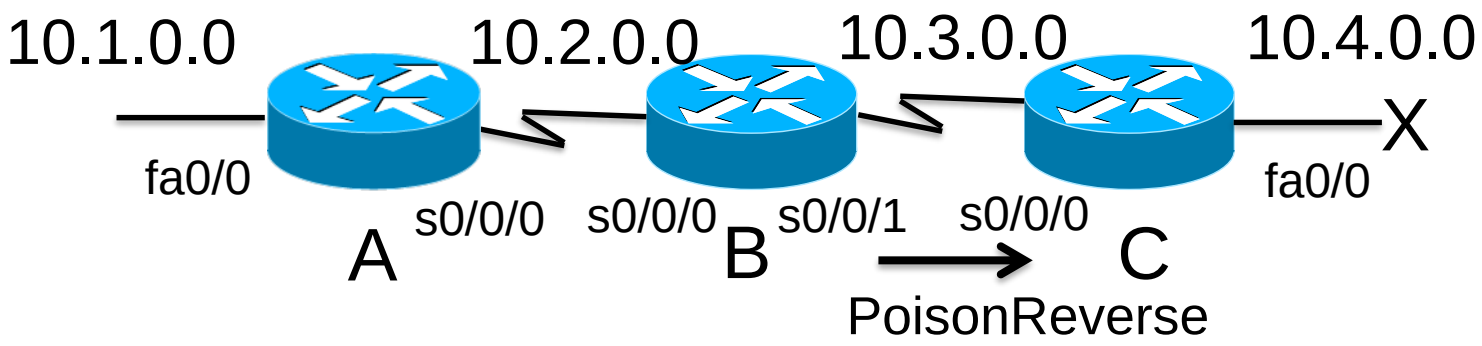
RoutingTableC		
10.3.0.0	s0/0/0	0
10.4.0.0	**fa0/0**	**down**
10.2.0.0	s0/0/0	1
10.1.0.0	s0/0/0	2

路徑毒害

當C路由器從E路由器處收到路徑毒害資訊時，會將“**逆向毒害**”(poisonreverse)的更新資訊傳回給E路由器－這能確保該網段上的所有路徑都收到此路徑毒害資訊。

- 路徑毒害與分割視野都能建立比較有活力、也比較可依靠的距離向量網路，並且在預防網路迴圈方面很有效。

Routing Loops-Poison reverse



RoutingTableA		
10.1.0.0	fa0/0	0
10.2.0.0	s0/0/0	0
10.3.0.0	s0/0/0	1
10.4.0.0	**s0/0/0**	**2**

RoutingTableB		
10.2.0.0	s0/0/0	0
10.3.0.0	s0/0/1	0
10.4.0.0	**s0/0/1**	**possibly down**
10.1.0.0	s0/0/0	1

RoutingTableC		
10.3.0.0	s0/0/0	0
10.4.0.0	**fa0/0**	**infinity**
10.2.0.0	s0/0/0	1
10.1.0.0	s0/0/0	2

抑制

- “**抑制**”(holddown)能夠防止一條時好時壞(稱為反覆，flapping)之路徑的定期資訊更新—這通常發生在斷線後再接上的序列鏈結上。如果沒有辦法將它穩定下來，網路將一直無法收斂，而這個反覆的界面將會讓整個網路當掉！

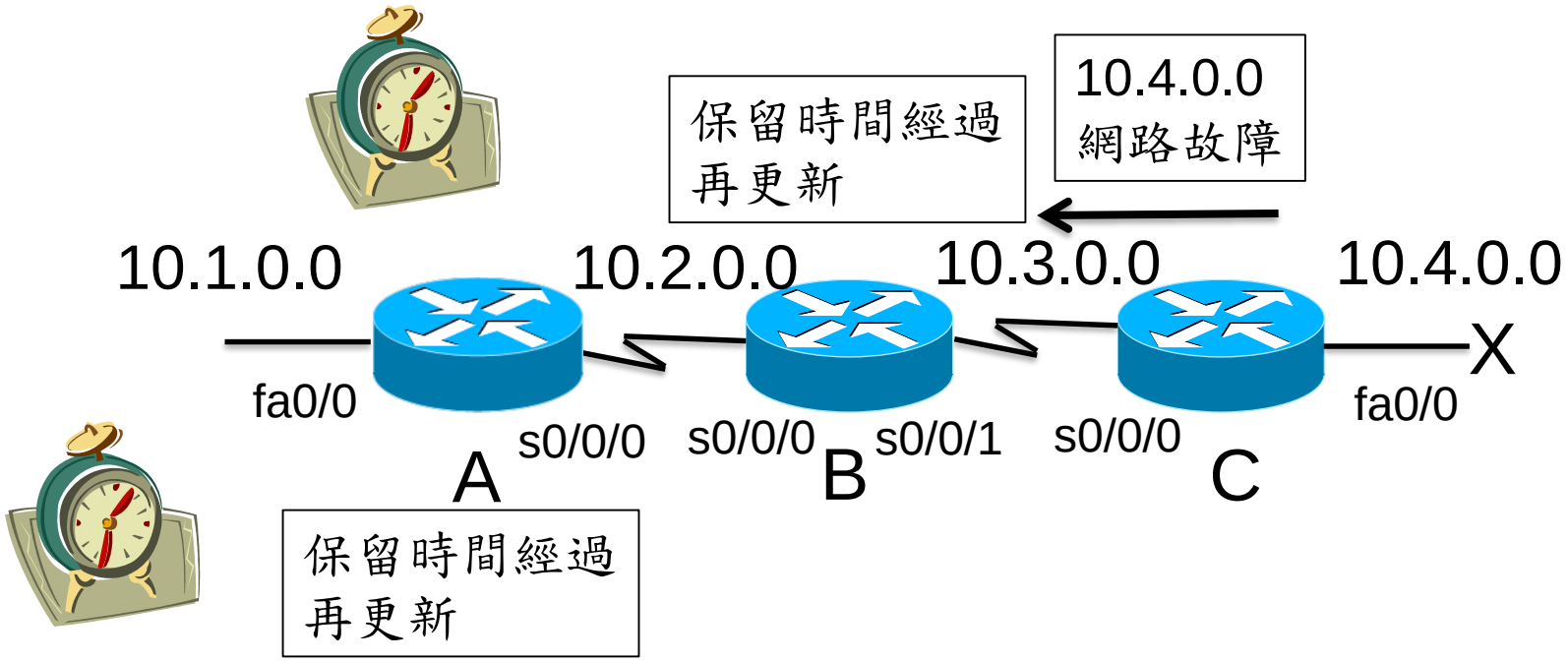
抑制

- 抑制這種機制在改變到次佳路徑之前，會先給當掉的路徑一些復原的時間，或是讓網路能夠先比較穩定，以防止路徑變動得太快。這也告訴路由器在特定期間內，要限制可能會影響到最近才移除之路徑的變動。它能讓無作用的路徑不要貿然地回復到其他路由器的表格中。

抑制

- 當路由器收到鄰居的更新資訊，表示之前可以存取的網路現在無法運作與存取時，就會啟動抑制計時器。如果鄰居送來新的更新中對於某個網路項目有比原先更好的衡量指標時，路由器就會移除這項抑制，並且送出資料。但是如果在抑制計時器逾期之前從鄰接路由器中收到更新，且具有比原本路徑更差或相等的衡量指標，則路由器會忽略這個更新，並且繼續抑制計時器的計時動作。這可以讓網路在嘗試收斂前有更多的時間達到穩定。

Routing Loops-Hold down timer



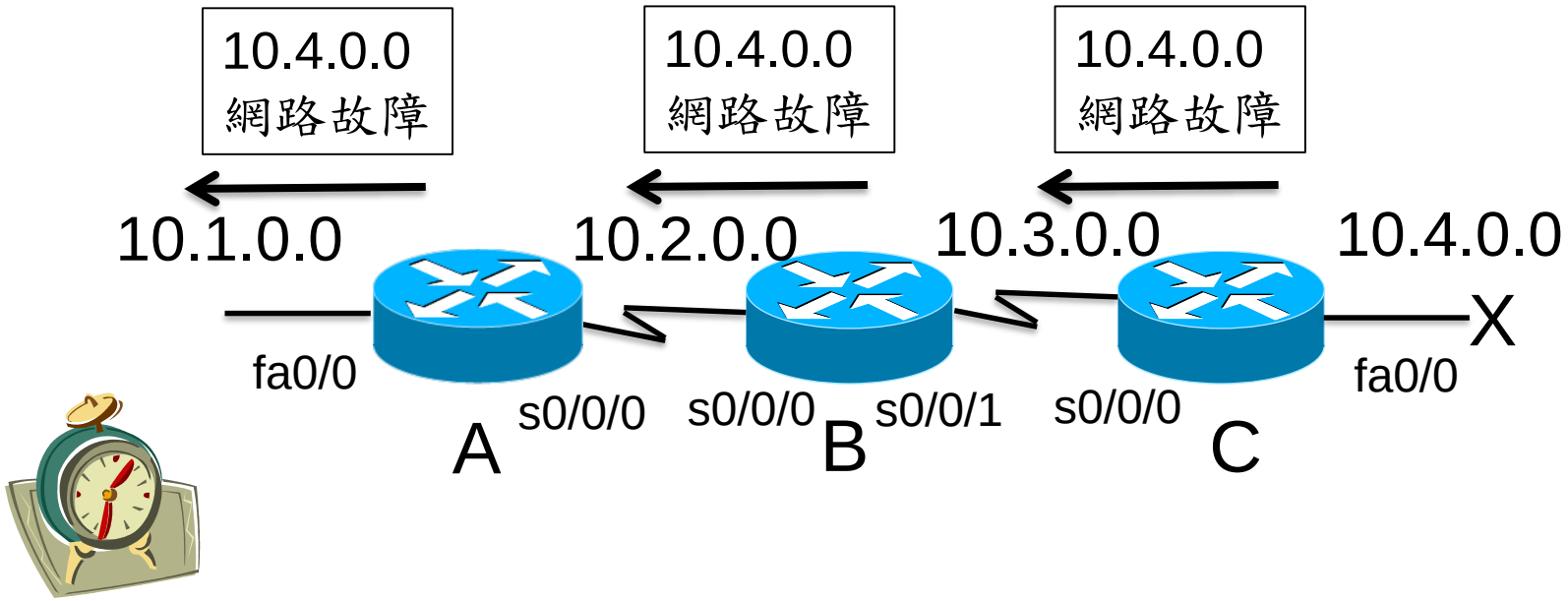
抑制

- 抑制使用觸發式更新(triggered update)來重置抑制計時器，以警告鄰接路由器關於網路的變動。觸發式更新與鄰接路由器的更新訊息不同，它是因為偵測到互連網路中的變動，而建立新的路徑更新資訊，並立即傳送給鄰接路由器。

抑制

- 觸發式更新在下列3種情況下會重置抑制計時器：
  - 抑制計時器逾時。
  - 收到具有較佳衡量指標的更新資訊。
  - 在沖刷時間(flushtime，路徑在被移除前所保留的時間)逾時後從路徑表中移除路徑。

RoutingLoops-Triggeredupdates

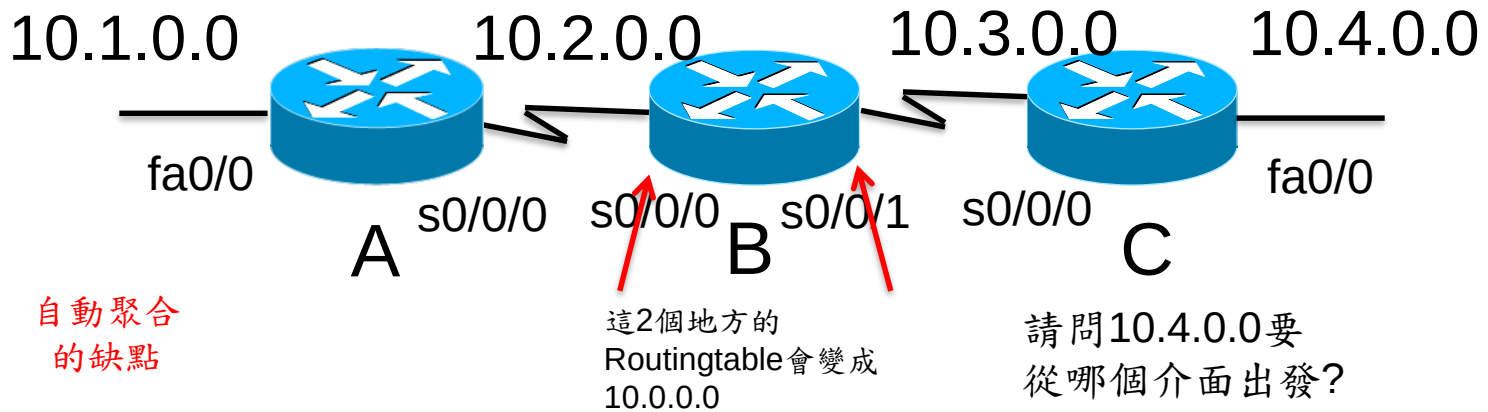


RIP

- Distancevect or routing protocol
- **Hop count** is used as the **metric** for path selection
- Maximumal low able **hop countis15**
- Routing updates are broad cast every **30s**
- RIPv1 classful，broadcast 255.255.255.255
- RIPv2classless，multicast 224.0.0.9
- UDP port520

RIP

- Router(config)#routerrip
- Router(config-router)#version2
- Router(config-router)#network10.2.0.0
- Router(config-router)#network10.3.0.0
- Router(config-router)#**noauto-summary**
  - 不希望網路自動聚合要下此指令



IGRP

- 內部閘道路由協定(Interior Gateway Routing Protocol，IGRP)是Cisco專屬的距離向量路由協定，也就是說，要在網路中使用IGRP，所有的路由器都必須是Cisco的路由器。Cisco建立這個路由協定以克服RIP的相關問題。
- IGRP的最大中繼站數目為255，而預設值為100。這在較大型網路中很有用，並且能夠解決RIP網路中最多只能有15個中繼站的問題。

IGRP

- IGRP使用的衡量指標也與RIP不同；它的預設是使用線路的頻寬與延遲來做為決定互連網路最佳路徑的指標，稱為“**複合式衡量指標**”(composite metric)。它也可以使用可靠性、負載、與最大傳輸單元(MTU)等，不過在預設中並沒有包括這些指標。

IGRP

- 下面是IGRP特徵中，RIP所沒有的部份：
  - IGRP可以使用在大型的互連網路中。
  - IGRP使用自治系統編號來啟動。
  - IGRP每隔90秒提供一次完整的路徑表更新。
  - IGRP使用線路的頻寬與延遲做為衡量指標(最低的複合指標)。

IGRP計時器

- IGRP使用下列計時器(含預設值)來控制效能：
  - **更新計時器(update timer)**－指定路徑更新資訊的傳送頻率；預設為90秒。
  - **無效計時器(invlaid timer)**－指定路由器因為沒有收到特定路徑的更新，而宣告一條路徑無效之前所應該等待的時間；預設為更新週期的3倍。

IGRP計時器

- **抑制計時器(hold down timer)**－指定抑制的時間；預設為更新計時器值的3倍加上10秒。
- **沖刷計時器(flush timer)**－將路徑自路徑表中清除之前，應該等待的時間；預設為路徑更新週期的7倍。如果更新計時器是預設的90秒，則路徑在從表中移除前要先經過7*90=630秒。

設定IGRP路由

- 設定IGRP的命令與設定RIP路由的命令大致相同，只有一個重要的差異：IGRP使用自治系統(automous system，AS)編號。自治系統中的所有路由器必須使用相同的AS編號，否則將無法溝通路徑資訊。啟用IGRP路由的方法：

```
Lab_A#config  t
Lab_A(config)#router   igrp   10
Lab_A(config-router)#network      192.168.10.0
```

檢查狀態/除錯

- Show ip protocols
- Show ip int brief
- Show ip route
- Debug ip rip➔可以看到更新的訊息
- No debug all

OSPF基礎

- 開放式最短路徑優先(Open Shortest Path First，OPSF)是一種開放的路由協定標準，受到網路廠商的廣泛支持，包括Cisco。如果您有多部路由器，而且不全部是Cisco的設備，則不能使用EIGRP。剩下能用的大概就是RIPv1、RIPv2、或OSPF。但如果是大型網路，則選擇只剩下OSPF，或所謂的路徑重分送－在路由協定之間的轉換服務。

Link-State

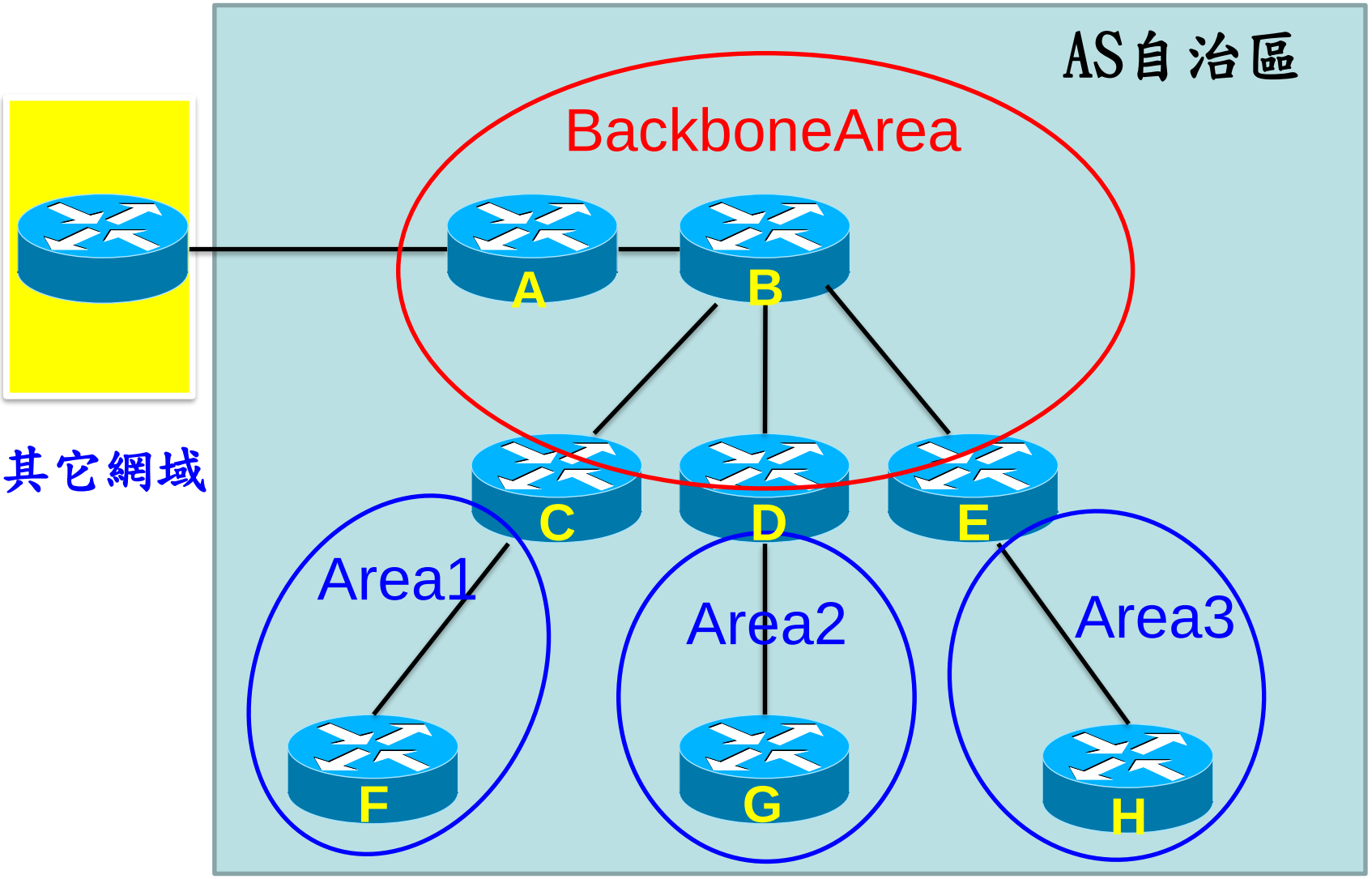
- OSPF Open Shortest Path First
- Classless interior gateway protocol
- Single-Area OSPF
- 透過LSA的傳播來更新路由表
  - Link：路由器介面
  - State：介面的述敘與其鄰接路由器的關係
  - Advertisement宣告
- 所有相同Area內的路由器都會收到LSA
- 224.0.0.5 224.0.0.6 30分鐘傳播一次

OSPF基礎

表 6.3　OSPF 與 RIPv1 的比較

特性	OSPF	RIPv1
協定類型	鏈路狀態	距離向量
無級別的支援	是	否
VLSM的支援	是	否
自動總結	否	是
手動總結	是	否
路徑的散播	異動時多點傳播	定期廣播
路徑衡量指標	頻寬	中繼站
中繼站計數限制	無	15
收斂	快	慢
對等節點的認證	是	否
階層式網路	是(利用區域)	否(展平的)
路徑的計算	Dijkstra	Bellman-Ford

Autonomous System

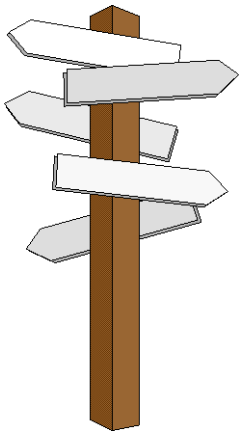


Autonomous System(Cont)

- RouterA-(Autonomous System Boundary Router，ASBR)
- RouterB-Backbone router
- RouterC，D，E-Area Border Routers，ABRs
- Router F，G，H-nonbackbone，internal routers

OSPF術語

- **鏈路(link)**—鏈路是一個網路或指定給某個網路的路由器界面。當我們增加一片界面到OSPF程序時，OSPF就會將該片界面視為一條鏈路。這條鏈路或界面就會有相關的狀態資訊(開啟或關閉)，以及一或一個以上的IP位址。



OSPF術語

- **路由器ID**－路由器ID(RID)是用來識別路由器的IP位址。Cisco挑選路由器ID的方式是使用所有設定之回繞界面中IP位址最高的一個，如果沒有設定位址的回繞界面，就選擇所有運作中之實體界面中，IP位址最高的一個。
- **鄰居(neighbor)**－鄰居是有界面在相同網路上的2部或更多部路由器，例如連到點對點序列鏈路的2部路由器。

OSPF術語

- **緊鄰關係(adjacency)**－緊鄰關係是能直接交換路徑更新的兩部OSPF路由器之間的關係。OSPF在分享路徑資訊方面真的非常挑剔－不像EIGRP就直接與所有的鄰居分享路徑。相對地，OSPF只與那些也建立緊鄰關係的鄰居直接分享路徑。並非所有的鄰居都可建立緊鄰關係，要根據網路的類型與路由器的組態而定。

OSPF術語

- **鄰居關係資料庫(neighbor ship database)**—這是從一份Hello封包看到的所有OSPF路由器的清單，資料庫維護了每部路由器的各種細節，包括路由器ID與狀態。
- **拓樸資料庫(topology database)**—拓樸資料庫包含從路由器為某個區域所接收之所有鏈路狀態宣傳(LinkStateAdvertisement，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。

OSPF術語

- **鏈路狀態宣傳(LinkState Advertisement，LSA)**—這是一種OSPF資料封包，包含要與其他OSPF路由器分享的鏈路狀態與路徑資訊。LSA封包有好多種，稍後我們會加以解釋。OSPF路由器只與那些與它已經建立緊鄰關係的路由器交換LSA封包。

OSPF術語

- **委任路由器(designated router，DR)**—每當OSPF路由器連到相同的多重存取網路時就會選出一部DR，Cisco喜歡稱這些為廣播網路，但其實他們是有多個接收者的網路，請試著不要混淆了多方存取(multiaccess)與多點(multipoint)，有時候他們非常容易令人混淆。
- **備份委任路由器(backup designated router，BDR)**—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熱備援，BDR只會從OSPF緊鄰路由器接收所有的路由更新，但不會散播LSA更新。

OSPF術語

- **OSPF區域(OSPF area)**－OSPF區域是一群鄰近的網路與路由器。相同區域中的所有路由器共享一個區域ID，但因為路由器可以同時屬於一個以上的區域，所以區域ID要關連到路由器上的界面。於是就有可能同一部路由器上的某些界面屬於區域0，而其餘的界面屬於區域1。同一個區域內的所有路由器會有相同的拓樸表。在設定OSPF時，必須記住一定要有區域0，而這通常會設定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。

OSPF術語

- **廣播(多方存取)**－廣播(多方存取)網路如乙太網路，可允許多個裝置連結(或存取)相同的網路，並提供廣播的能力，可將單個封包傳送給網路上的所有節點。在OSPF中，每個廣播多方存取網路必須選出一部DR與一部BDR。

HelloPacket

- RouterID：32bits，loopback interface優先，若沒有loopback interface則IP最大的優先。
- Hello and dead intervals
- Neighbors：鄰居
- Area ID：2個Router需分享相同網段(介面)
- Router priority：0-255決定designated router DR及Backup DR，BDR
- DR and BDRIP

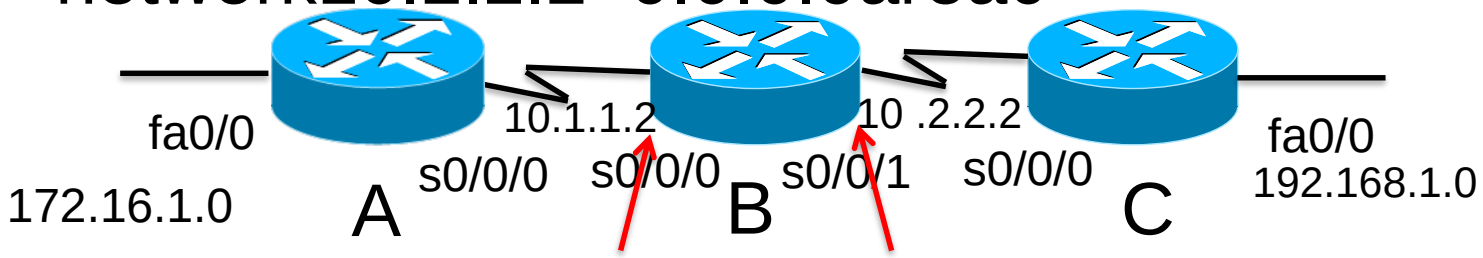
OSPFCOST

- cost(metric)=
  - Reference bandwidth/interface bandwidth(bps)
- 預設reference bandwidth=10^8bps
- Fastethernet=100Mbps
  - cost=10^8/100M=1
- T1=1.544Mbps
  - cost=10^8/1.544M=64
- Fastethernet<T1所以會選擇Fastethernet

OSPF設定實作

- Router(config)#router ospf process-id
- Router(config-router)#
  - Network address wildcard-mask area area-id
- RouterB
  - routerospf100
  - Network 10.1.1.2 0.0.0.0 area0
  - network10.2.2.2 0.0.0.0area0

area-address=
1.network
2.subnet
3.interface address



OSPF與回繞界面

- 設定回繞(loopback)界面對於OSPF路由協定是很重要的，Cisco建議您在路由器上設定OSPF時最好使用他們。
- 回繞界面是一種邏輯界面，這表示他們並非實體的路由器界面。他們可作為診斷的用途，或用來設定OSPF。在路由器上設定回繞界面的理由是因為如果不這樣做，路由器上的最高IP位址就會變成路由器的RID，而RID的目的是為了宣傳路徑，以及選出DR與BDR。

OSPF與回繞界面

- 假設有部路由器沒有設定回繞界面，而路由器的序列界面是路由器的RID，因為它的IP位址最高。如果該界面故障，就得重新選舉該網路上的DR與BDR。也許這並不嚴重，但如果這是一條常常啟動/關閉的鏈路，情形會如何？這部路由器將無法收斂，因為DR/BDR的選舉從來都沒有完成。
- 在OSPF這顯然會是個問題，而回繞界面能解決這個問題，因為回繞界面從不會當掉，路由器的RID也就不會變動。

設定回繞界面

- 設定回繞界面是OSPF設定中最容易的部份，輕鬆一下！
- 首先，讓我們以**showipospf**命令檢視一下Lab_A路由器的RID：

```
Lab_A#sh ip ospf
  Routing Process "ospf 132" with ID 192.168.20.1
[output    cut]
```

設定回繞界面

- RID是192.168.20.1或路由器的序列0/0界面，因此，讓我們以完全不同的IP位址結構來設定回繞界面：
- 這裡使用什麼樣的IP結構其實無關緊要，但每部路由器得屬於不同的子網路才行。

```
Lab_A#config  t
Enter configuration commands, one per line.  End with CNTL/Z.
Lab_A(config)#int  loopback  0
Lab_A(config-if)#ip  address  172.16.10.1  255.255.255.0
Lab_A(config-if)#no  shut
Lab_A(config-if)#^Z
Lab_A#
```

設定回繞界面

- 剩下的問題就是我們是否要讓OSPF宣傳這些回繞界面，宣傳或不宣傳其實各有優缺點，使用不宣傳的位址可節省真正的IP位址空間，但因為這些位址不會出現在OSPF表中，所以也就ping不到。所以這裡的考量就是要讓網路的除錯比較容易，或是要節省位址空間，怎麼辦呢？最好的策略就是使用之前所說過的私有IP位址，這樣做，兩者都可兼顧！

除錯指令

- #show ip route ospf
- #show ip protocols
- #show ip ospf
- #show ip ospf interfaces
- #show ip eigrp neighbors
- #show ip route
- #show ip int fa0/0

EIGRP的功能與運作

- EIGRP是一種無級別(classless)、加強版的距離向量(distance-vector)協定，提供另一個比IGRP更好的Cisco專屬繞送協定，這也是為什麼稱它為加強版IGRP的原因。就像IGRP一樣，EIGRP使用自治系統(autonomous system)的觀念來描述一組鄰近的路由器，並執行相同的繞送協定，與分享路徑資訊。

EIGRP的功能與運作

但與IGRP不同的是，EIGRP在路徑更新中包含了子網路遮罩的資訊。子網路資訊的宣傳讓我們得以在設計網路時使用VLSM與路徑總結！

- EIGPR有時又稱為混合式繞送協定(hybrid routing protocol)，因為它同時有距離向量與鏈路狀態協定的特性。

EIGRP

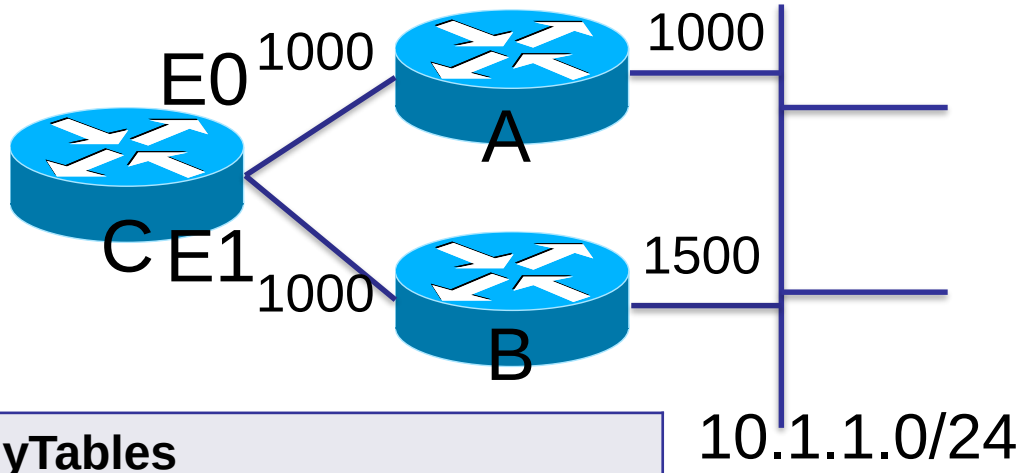
- Enhanced Interior Gateway Routing Protocol
- 快速收斂
- 降低使用頻寬
- 支援多重網路協定IPX，IPv4，IPv6
- Classless routing
- Less overhead使用unicast及multicast
- Load balancing
- Easy summarization

EIGRPTables

- Advertised distanceAD宣告成本
  - 鄰居到達特定網路的成本metric
- Feasible distanceFD合理成本
  - 自己到達鄰居的成本metric+AD
- Success or router
  - 具有最小FD之neighbor
- Feasible successor
  - 具有AD<至目的地最小FD路徑的neighbor

EIGRPTables

IPEIGRPTables	
Next-HopRouter	Interface
RouterA	Ethernet0
RouterB	Ethernet1



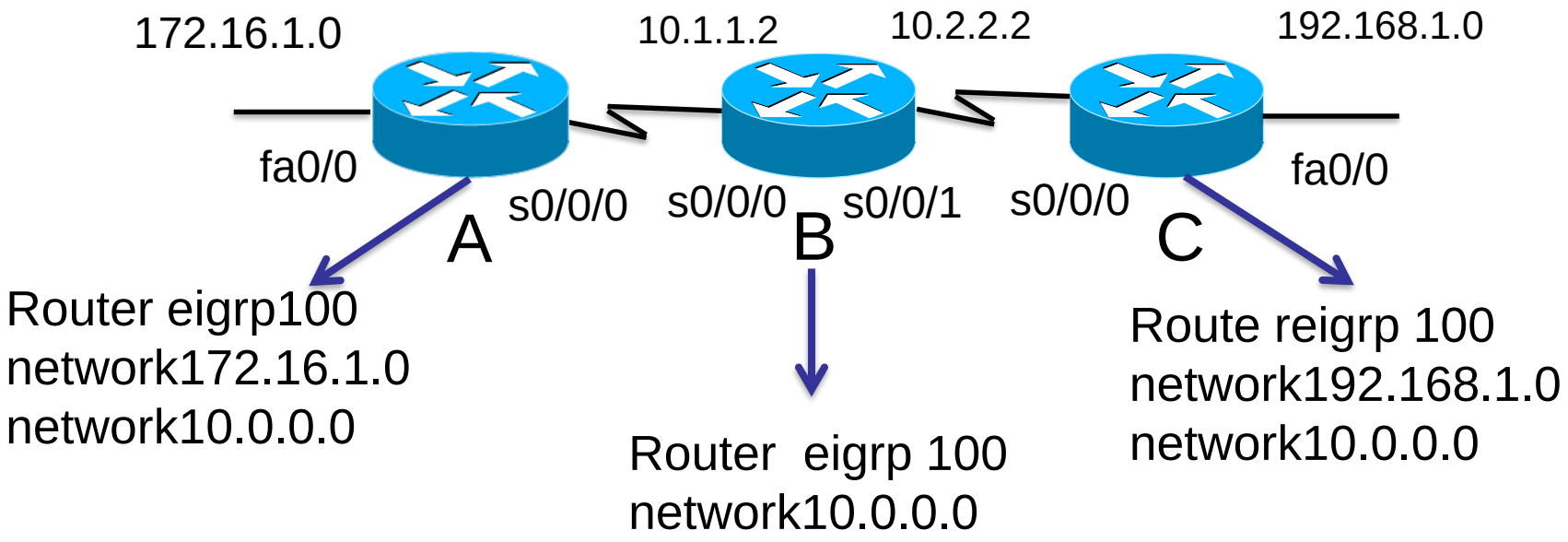
IPEIGRPTopologyTables			
Network	FeasibleDistance (EIGRPMetric)	Advertised Distance	EIGRP Neighbor
10.1.1.0/24	2000	1000	RouterA(E0)
10.1.1.0/24	2500	1500	RouterB(E1)

TheIPRoutingTables			
Network	Metric FeasibleDistance	Outbound Interface	NextHop EIGRPneighbor
10.1.1.0/24	2000	Ethernet0	RouterA

A:Successor
B:Feasiblesuccessor

EIGRP設定實作

- Router(config)#
  - Router eigrp autonomous-system
- Router(config-router)#
  - Network network-number



除錯指令

- #show ip route eigrp
- #show ip protocols
- #show ip eigrp interfaces
- #show ip eigrp neighbors
- #show ip route
- 在相同的AS裡才能交換路由資訊
- #show ip eigrp topology可查AS及FD

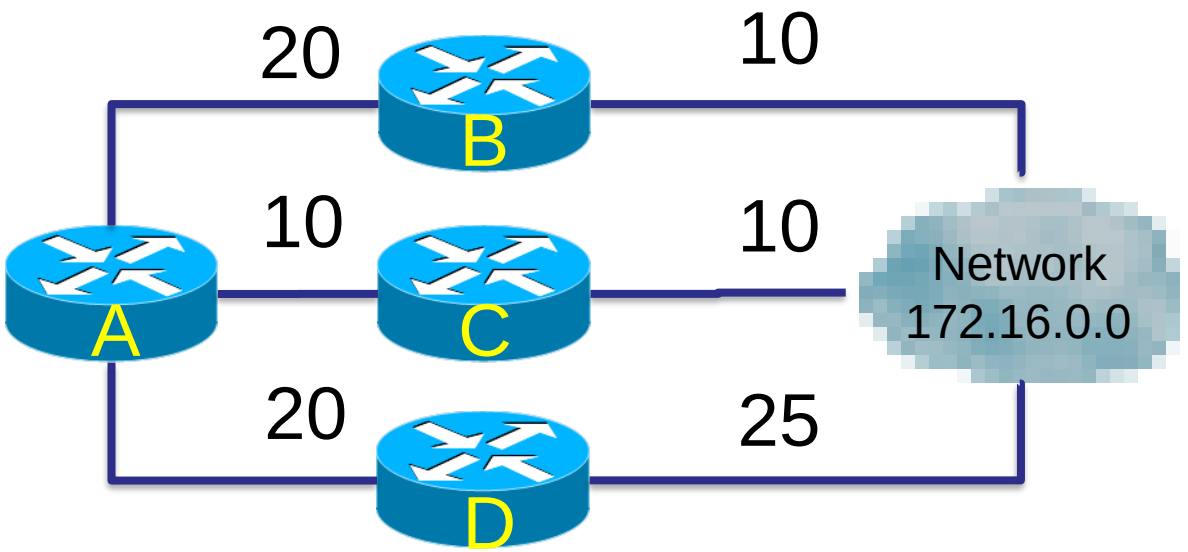
Load banancing with EIGRP

- Router(config-router)#
  - maximum-paths16**最大16條路徑**
  - Variance multiplier 1 **equal-cost**
  - Variance multiplier1-128
  - rule1其它path之AD<Successor之FD
  - rule2其它path之FD一定要<Successor之FDX variance

LoadBalancing

C為Successor
1.AD<Successor之FD
B-AD(10)<C-FD(20)
2.B-FD<C-FDxvariance
30<20x**2**

備援路徑為B



Network	Neighbor	FD	AD
172.16.0.0	B	30	10
	C	**20**	10
	D	40	25

除錯指令

- #show ip eigrp neighbors
- #show ip protocols
- #show ip eigrp interfaces
- #show ip route
- #debug eigrp packets
- #show ip eigr ptopology

第六章

STP擴充樹

第2層之3個交換功能

- 第2層 交換有3個不同的功能：
  - **學習位址**－第2層 交換器與橋接器會記住它從界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。

第2層之3個交換功能

- **決定轉送或過濾**－當交換器從界面收到訊框時，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界面，該訊框只會從特定的目的埠轉送出去。
- **避免迴圈**－如果為了達到冗餘的目而在交換器之間建置多重連線，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。

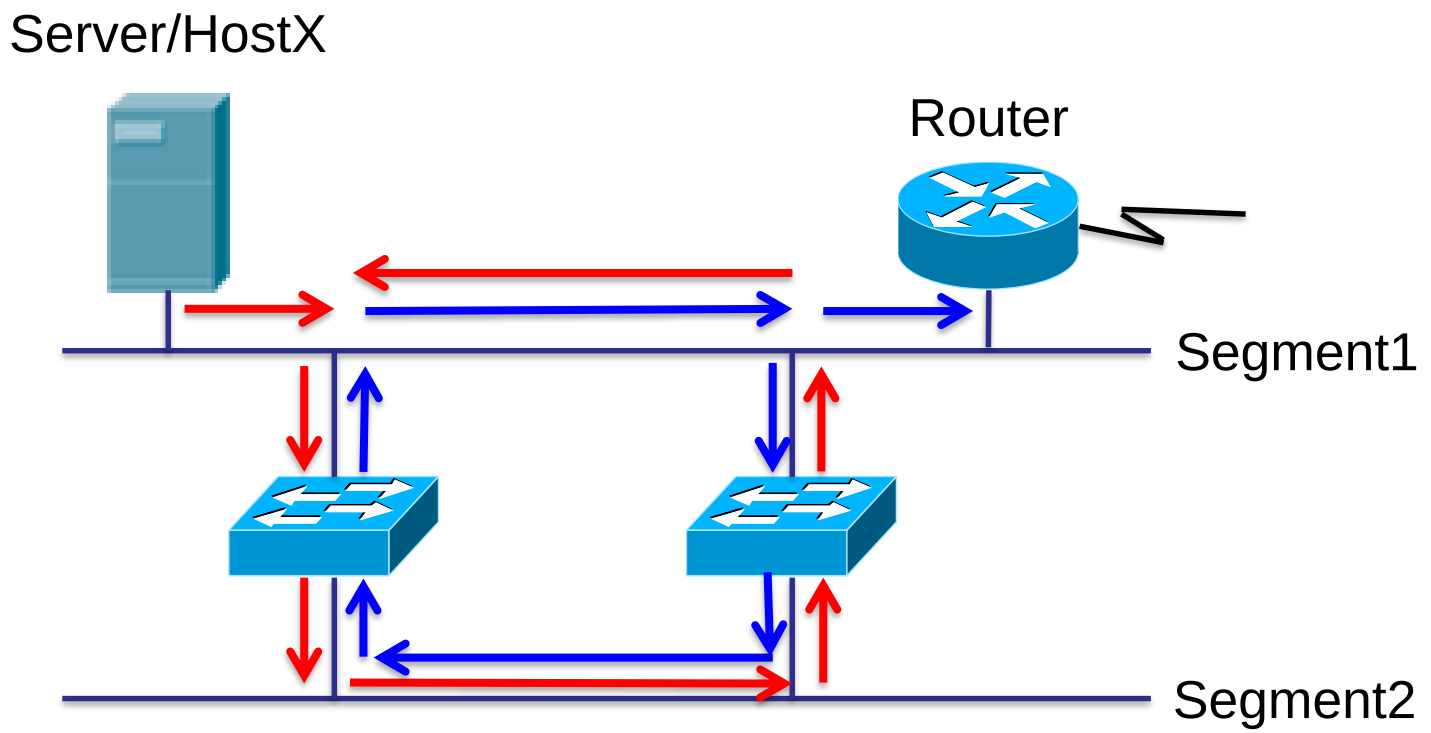
STP

- Spanning Tree Protocol
  - 在複雜的網路環境中，會有備援裝備以避免單點故障，雖然備援的裝備可以解決問題，但是又會衍生其它額外的問題。
  - STP為第二層路徑備援的協定，同時可以防止某些問題的產生。

擴展樹協定(STP)

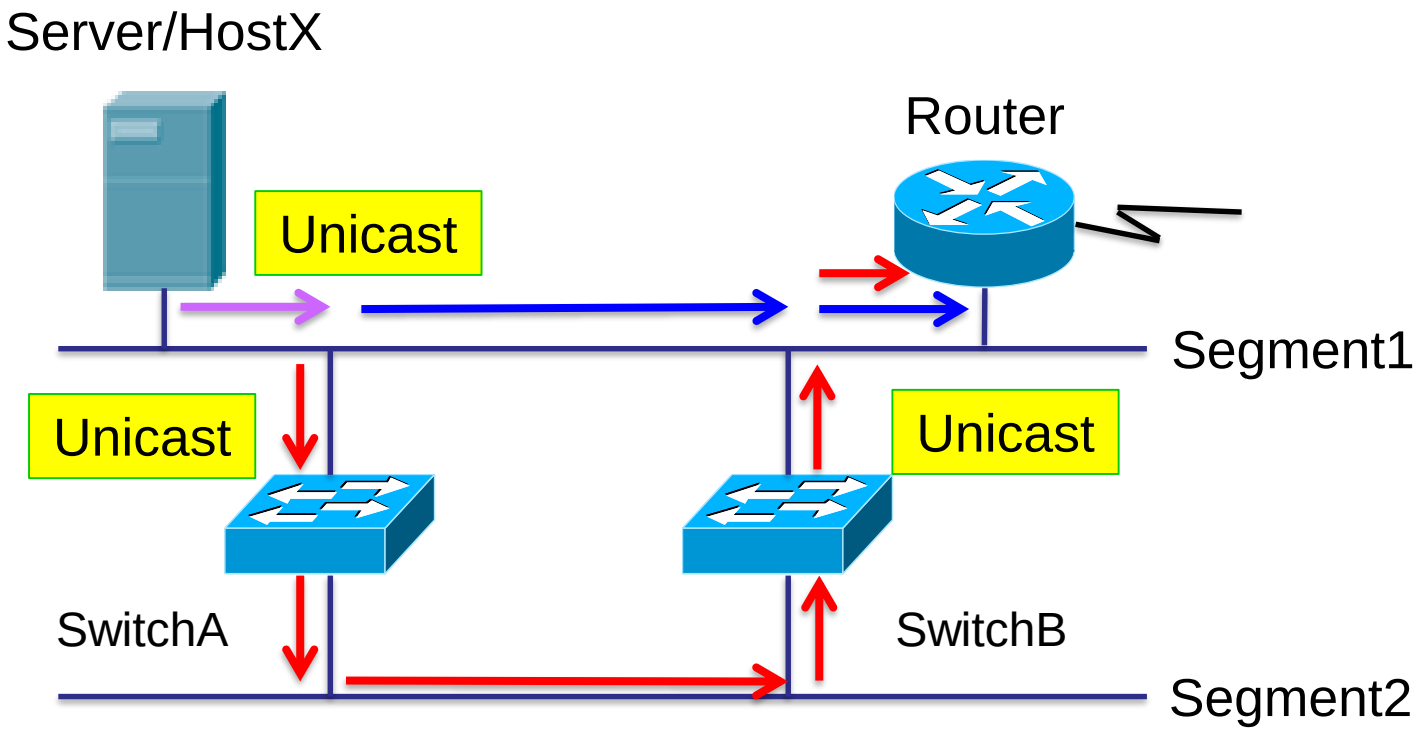
- STP的主要任務是要預防在第2層的網路上發生網路迴圈，它警覺地監視網路以找尋所有的鏈路，藉由關閉冗餘的鏈路來確定迴圈不會發生。STP使用擴展樹演算法(Spanning-Tree Algorithm，STA)，首先產生一個拓樸資料庫，然後搜索出冗餘鏈路，並拿掉它。執行STP之後，訊框只能在良好的、由STP挑選的鏈路上轉送。

廣播風暴



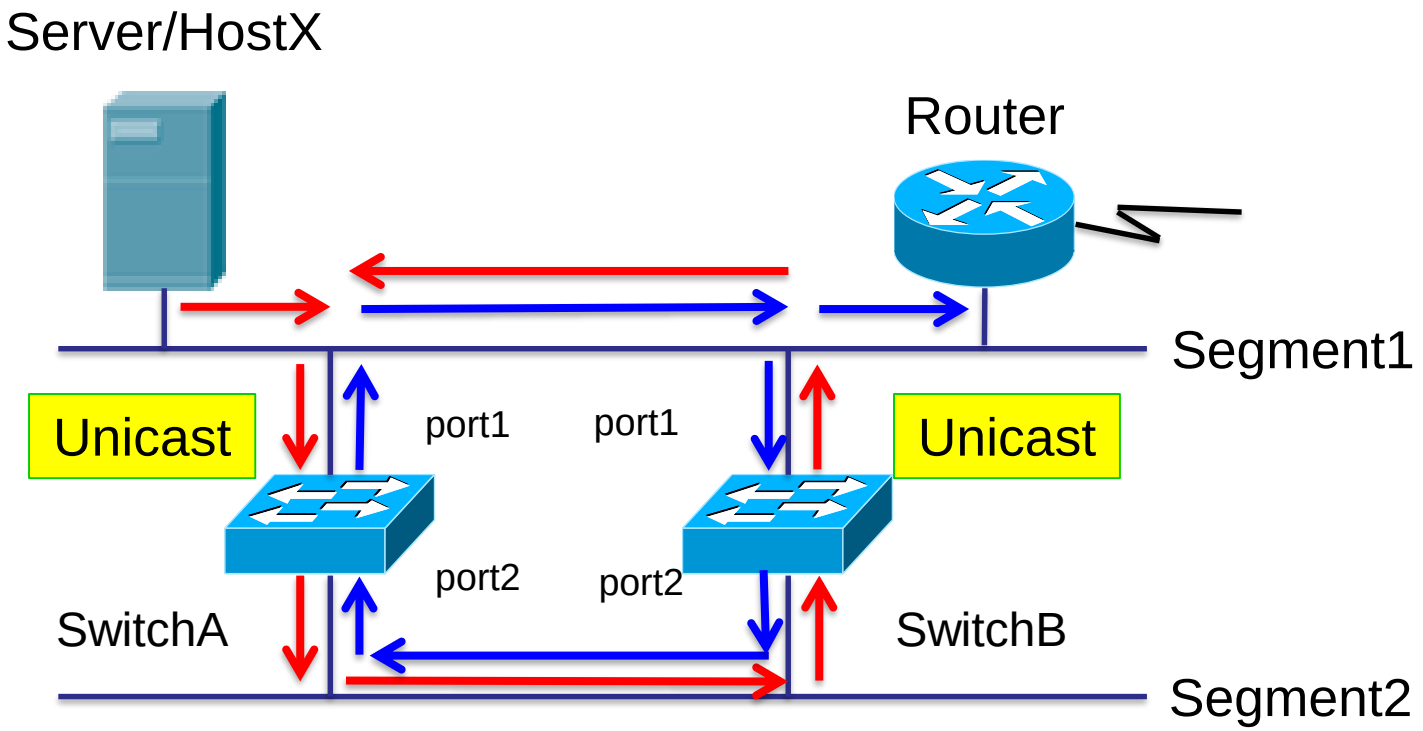
- HostX傳送broadcast，在這個環境中會一直存在無法消除
- 廣播越多，就會形成廣播風暴，會耗盡頻寬及Switch的CPU等資源，即造成網路無法正常工作

重覆複本資料



- HostX傳送unicast frame給Router，由於SwitchA並未學習到HostX的MACaddress，所以會採用all port flooding
- SwitchB會再傳送給Router1個unicast frame
- Router會收到2個複本不解?你在一天內收到2份相同的公文，怎麼辦？

不穩定的MAC資料庫



- HostX傳送unicast frame給Router
- SwitchA、B尚未學習到HostX的MAC，所以SwitchA、B的port1均會學習到HostX的MAC all port flooding
- SwitchA、B的port2亦會學到HostX的MAC

SpanningTree

- One root bridge per broadcast domain
  - 每個廣播網域選出一台root bridge
  - Root bridge上的所有port皆為designated port
- One root port per nonroot bridge
  - 從其它非root bridge各選出一個root port
- One designated port per segment
  - 每個區段選出一個designatedport
- Nondesignated port sareunused
  - 其它沒被選到的port，皆列為未使用，須關閉

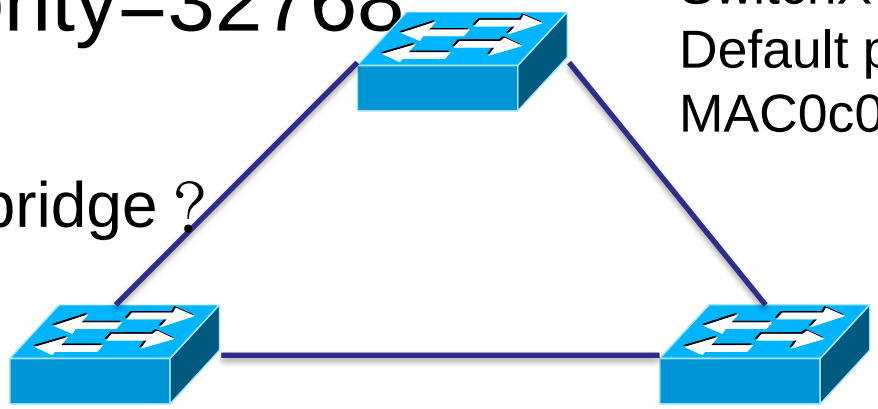
SpanningTree

- 具有最小BID者為ROOT Bridge
  - 0~65535預設32768+MAC共8bytes
- Nonroot bridge至ROOT Bridge最小成本者為ROOT PORT:forwarding.
- 在LAN區段具有最小成本至ROOT SWITCH者為designated port:forwarding.
- 其它設定為Blocking.

STP Root bridge選舉

- Bridge Protocol Data Unit，BPDU每2秒傳送1次，比BridgeID，BID大小，最小的獲勝
- BID=priority(2bytes)+MAC(8bytes)
- 預設priority=32768

請問誰是Root bridge？



SwitchX
Default priority32768
MAC0c00.1111.0000

SwitchY
Default priority32768
MAC0c00.1111.1111

SwitchZ
Default priority32768
MAC0c00.1111.2222

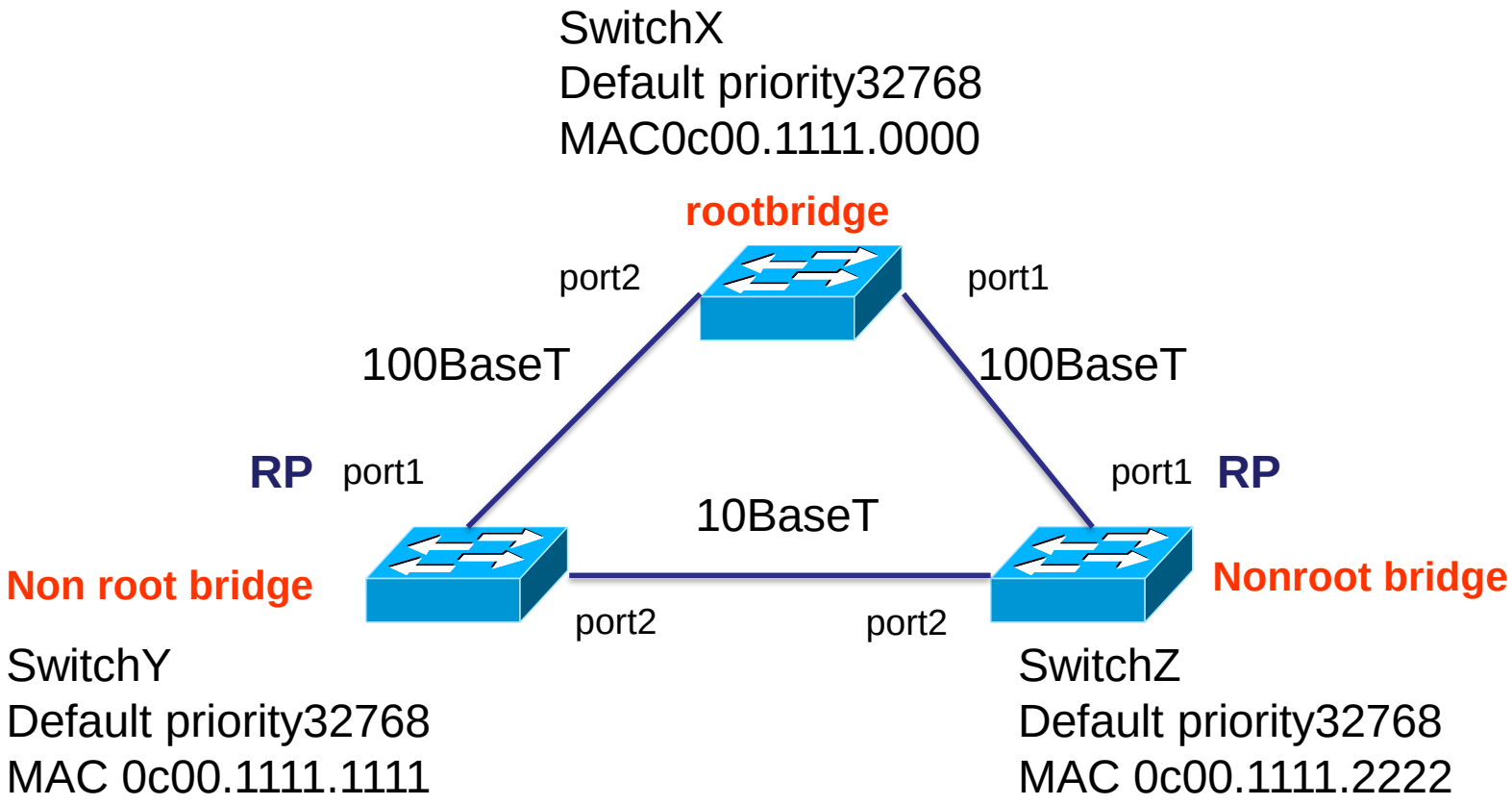
路徑成本

- 比較下表之路徑成本，若相同則依序比較
  - 最低的BID
  - 最低的路徑成本
  - 最低的傳送設備BID
  - 最低的傳送port priority(MAC)
  - 最低的傳送設備portID

LinkSpeed	CostIEEE現在版本	CostIEEE先前版本
10Gb/s	2	1
1Gb/s	4	1
100Mb/s	19	10
10Mb/s	100	100

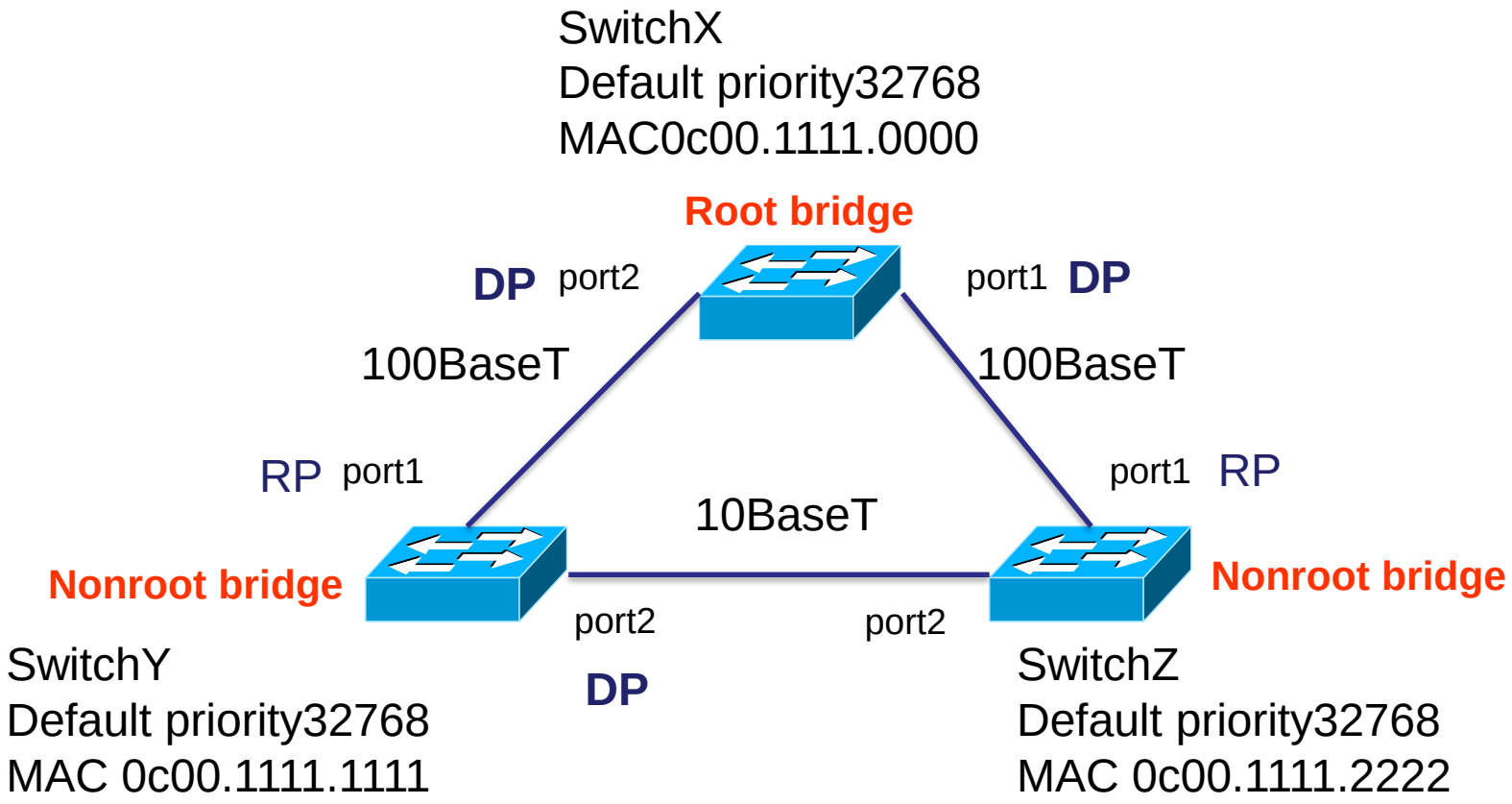
Rootport

- Nonroot bridge上具有回到root bridge最小成本的介面為root port



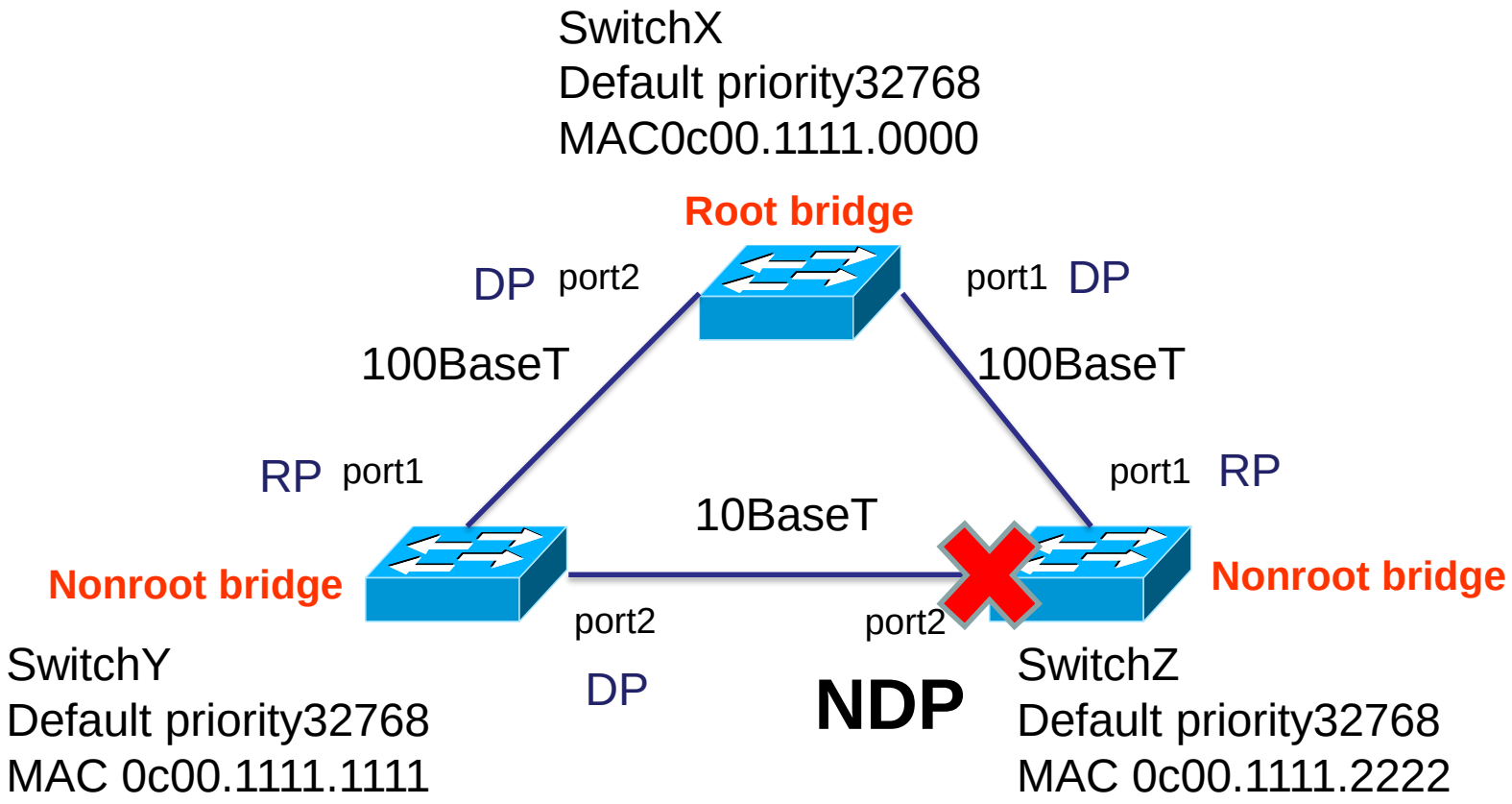
Designated port

- 每個區段具有回到root bridge最小成本的介面為designated port



Nondesignated port

- 每個區段具有回到root bridge最小成本的介面為designated port，其餘為NDP



STPportstates

- designatedport與rootport皆為forwarding
- nondesignatedport為blocking

NDP未收到BPDU20秒時，即進入Listening狀態

重新選舉(rootbridge，RP，DP的選舉)，無法傳送任何資料

此階段RP，DP會變Forwarding

NDP則變成Blocking狀態

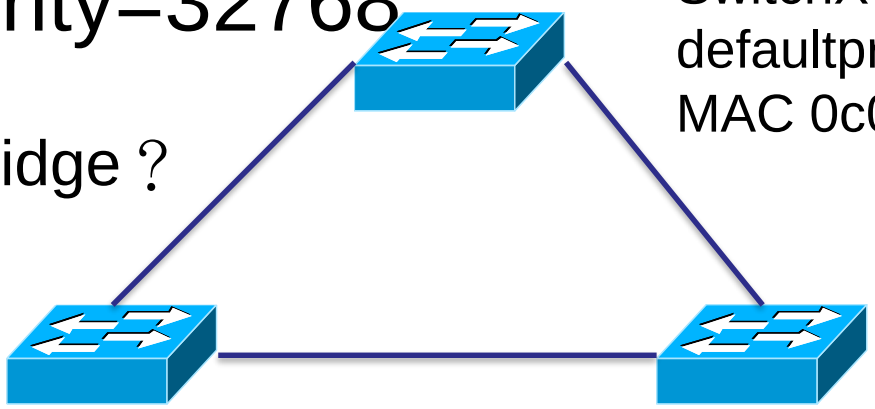
PortFast

- 當Switch的port直接接到終端設備而非其它的Switch時，可以使用PortFast加快速度
- 直接從blocking狀態轉換為forwarding狀態
- 只能在Accessport上設定
- BPDUguard收到BPDU直接變Blocking
- 指令
  - SwitchX(config-if)#spanning-treeportfast
  - SwitchX(config)#spanning-treeportfastdefault
  - SwitchX#showrunning-configintfa0/0

PortFast

- Bridge Protocol Data Unit，BPDU每2秒傳送1次，比Bridge ID，BID大小，最小的獲勝
- BID=priority(2bytes)+MAC(8bytes)
- 預設priority=32768

請問誰是Rootbridge？



SwitchX
defaultpriority32768
MAC 0c00.1111.0000

SwitchY
Default priority32768
MAC 0c00.1111.1111

SwitchZ
Default priority32768
MAC 0c00.1111.2222

第七章
ACL

存取清單簡介

- 存取清單其實就是一個對封包進行分類的條件清單，當您需要控制網路交通時，他們可能非常有幫助。存取清單將會是供您選擇用來進行決策的工具。
- 存取清單最常見、也最容易瞭解的用途之一就是用來實作安全原則時，過濾不想要的封包。

存取清單簡介

一旦建好清單，可應用在任何界面上進入或離開方向的交通。應用存取清單會使路由器分析以特定方向通過界面的每個封包，並採取適當的動作。

- 比對封包與存取清單時，必須遵循幾個重要的規則：
  - 總是循序地比對存取清單的每一列－也就是說總是從存取清單的第1列開始，然後比對第2列，然後第3列，依此類推。

10-1存取清單簡介

- 不斷地比對存取清單，直到符合為止。一旦封包符合存取清單上某列的條件，就會對封包起作用，並且不再進行任何比對。
- 每個存取清單的結尾都會有一列隱含的“**拒絕**”—這表示如果封包無法符合存取清單中任何一列的條件，則會被丟掉。

- 以存取清單過濾IP封包時，這些規則的每一條都蘊含很強的意義。請記住，若要建立有效的存取清單，真的要不斷地練習。

AccessControlLists

- Filtering-過濾封包將不必要的流量隔離
  - Permit or deny packets
  - Permit or deny vty access
  - 被過濾的封包，路由器會丟棄並回傳
    - ”Destination unreachable”(ping)
    - ”Administratively prohibited”(traceroute)
- Classification-分類給予特定網段權限

ACL Operation

- Inbound ACLs
  - 先經由ACL條件判斷後，再進行路由處理
- Outbound ACLs
  - 先進行路由處理，再送至ACL條件判斷
- ACL為循序式條件判斷，前面的條件優先執行，且後面的條件無法覆蓋前面的條件
- ACL最終的條件判斷為deny any any
- 因此最少要有一個permit

ACLOperation

- 例1
- deny192.168.1.10.0.0.0
- Permit IP any

差別?

- 例2
- Permit IP any
- Deny 192.168.1.1 0.0.0.0 此行與前面衝突因此無效

存取清單簡介

- 存取清單主要有2種：
  - **標準式存取清單(standard access list)**—這些只使用IP封包中的來源IP位址當作檢驗條件，所有決定都是根據來源IP位址進行的。這表示標準式存取清單基本上允許或拒絕整組的協定，他們無法分辨IP交通的類型，例如WWW、Telnet、UDP等等。

10-1存取清單簡介

- **延伸式存取清單(extended access list)**—延伸式存取清單可以比對IP封包之第3層與第4層標頭中的許多其他欄位。他們可以比對網路層標頭中的來源與目的IP位址與協定欄位，以及傳輸層標頭中的埠號。這使得延伸式存取清單有能力在控制交通時進行更細緻的決策。

Type of ACLs

- Standard ACL
  - 1-99，1300-1999(來源位址)
  - 靠近目的地
- Extended ACL
  - 100-199，2000-2699(來源、目的位址和埠)
  - 靠近來源

萬用字元Wildcard mask

- 0 match
  - 完全符合
- 1 don’t care
  - 位元可變動
- 單一IP
  - 172.30.16.29 **0.0.0.0**= **host** 172.30.16.29
- 任何IP
  - **0.0.0.0 255.255.255.255** = **any**

萬用字元Wildcardmask

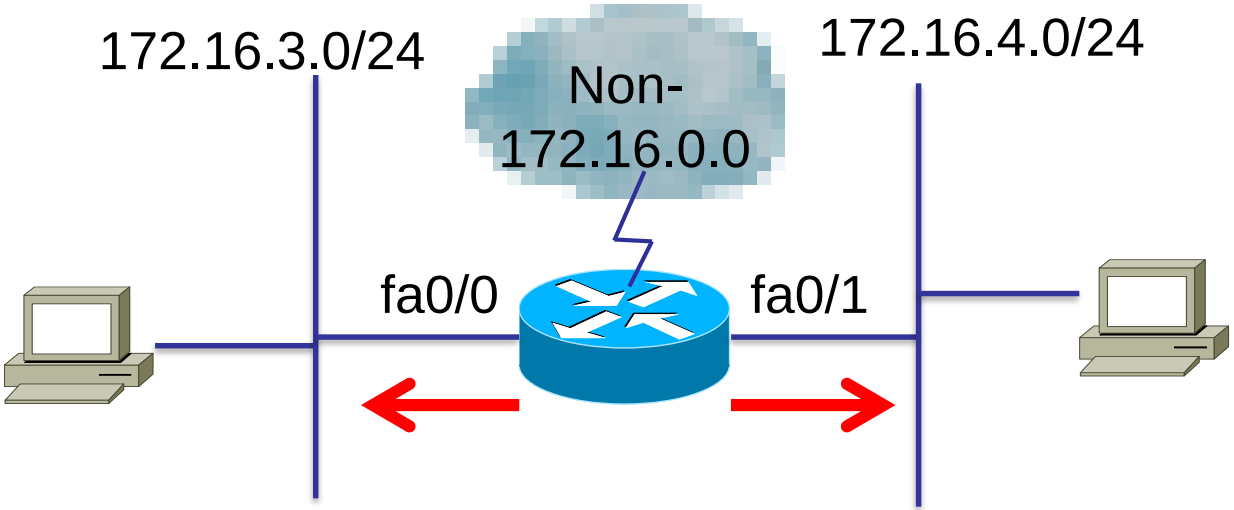
- 例172.30.16.0/24~172.30.31.0/24
  - 172.30.16.00.0.15.255
- 10101100.00011110.00010000.00000000
- 10101100.00011110.00010001.00000000
- 10101100.00011110.00010010.00000000
- 10101100.00011110.00010011.00000000

- 10101100.00011110.00011111.00000000
- ==========
- 00000000.00000000.00001111.11111111

NumberedStandardACL

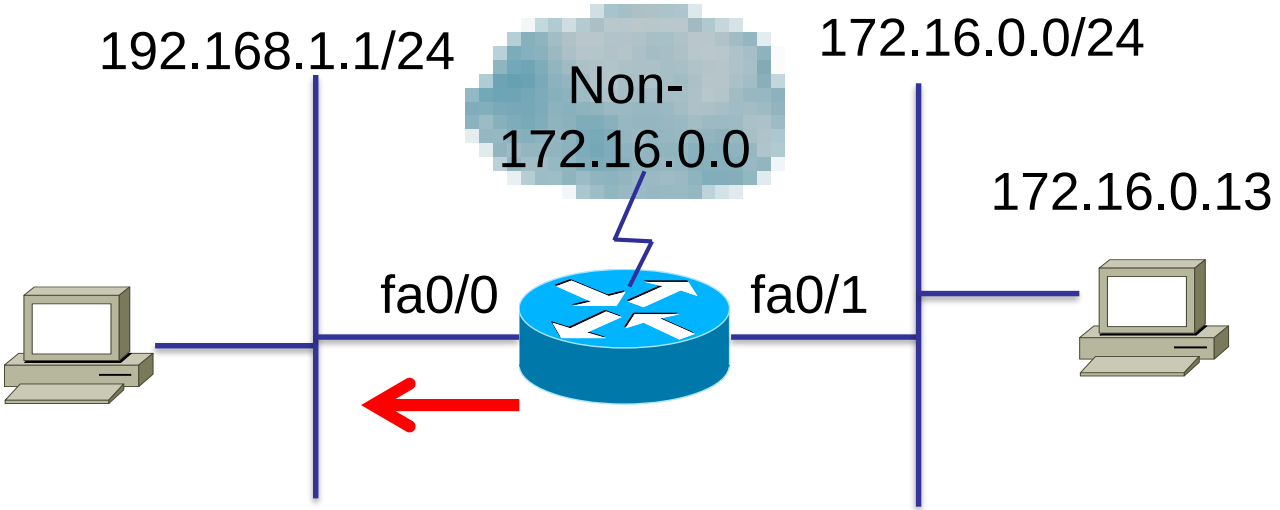
- RouterX（config）#access-list access-list number｛permit｜deny｜remark｝source ｛mask｝
- RouterX（config-if）#ip access-group access-list-number｛in｜out｝
- RouterX（config）#access-list 1 permit 172.16.0.0 0.0.255.255
- RouterX（config）#interface Ethernet 1
- RouterX（config-if）#ip access-group 1 out

StandardACL設定實作1



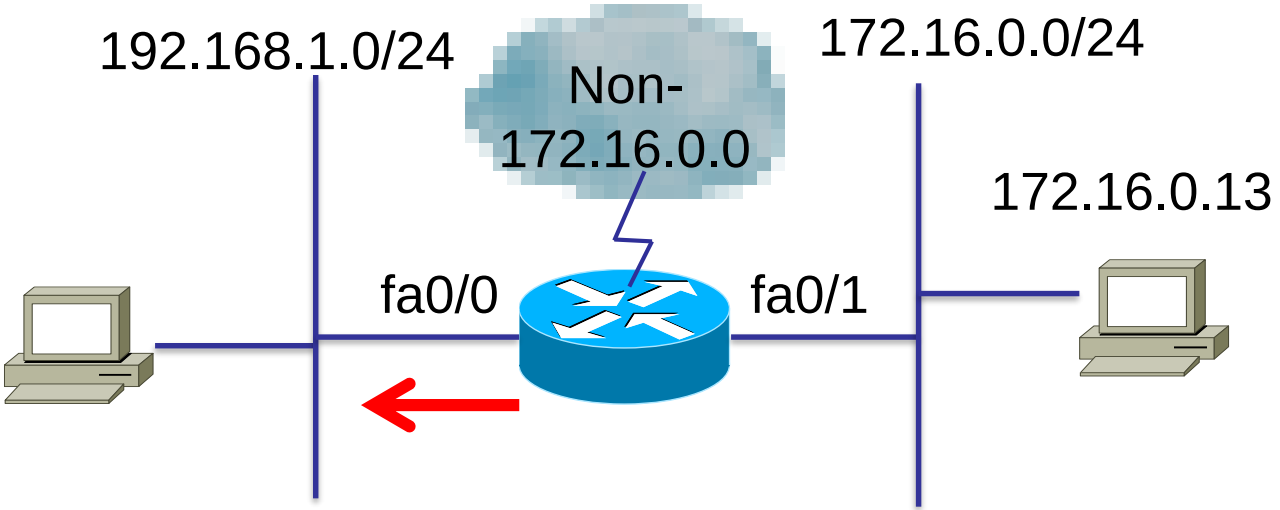
- Router(config)#access-list**1**permit172.16.0.00.0.255.255
- Router(config)#intfa0/0
- Router(config-if)#ipaccess-group**1**out
- Router(config)#intfa0/1
- Router(config-if)#ipaccess-group**1**out

StandardACL設定實作2



- Router(config)#access-list**1**deny172.16.0.130.0.0.0
- Router(config)#access-list**1**permitany
- Router(config)#intfa0/0
- Router(config-if)#ipaccess-group**1**out

StandardACL設定實作3



- Router(config)#access-list**1**deny172.16.0.00.0.0.255
- Router(config)#access-list**1**permitany
- Router(config)#intfa0/0
- Router(config-if)#ipaccess-group**1**out

Vty Access

- RouterX(config-line)#
  - access-class access-list-number{in|out}
  - access-list 12 permit 192.168.1.0 0.0.0.255
  - Line vty 0 4
  - access-class 12 in

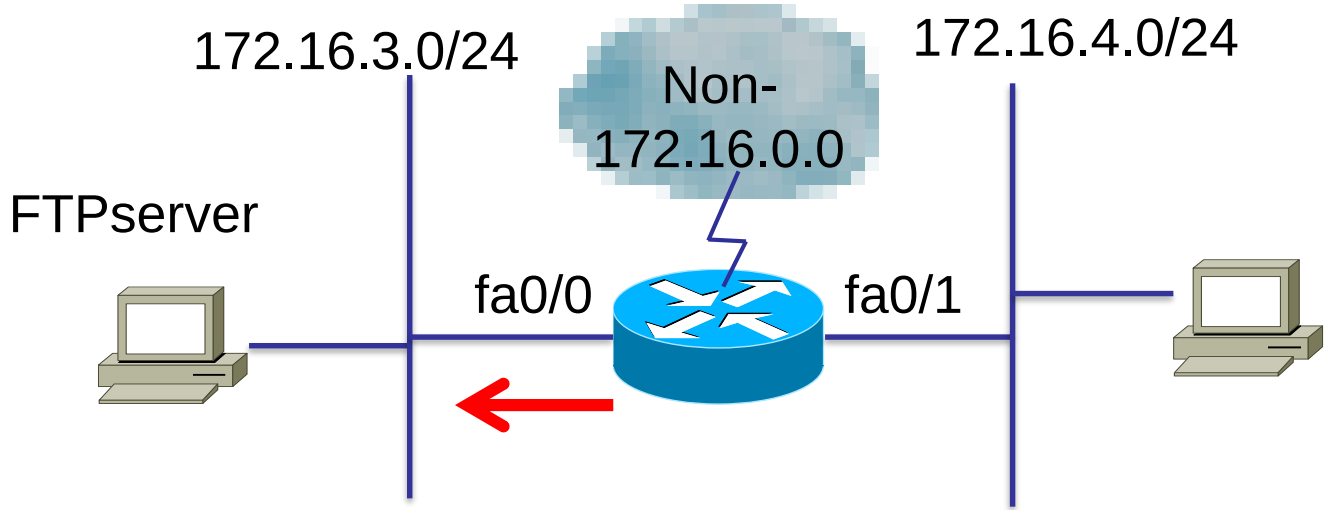
Numbered Extended ACL

- Router(config)#
  - access-list access-list-number{permit|deny}protocolsourcesource-wildcard[operatorport]destinationdestination-wildcard[operatorport][established][log]
  - ipaccess-group access-list-number{in|out}
  - operator
    - lt（lessthan）
    - gt（greaterthan）
    - eq（equal）
    - neq（notequal）

NumberedExtendedACL

- access-list 101 permit tcp any host 128.88.1.2 established
- access-list101 permit tcp any host 128.88.1.2 eq smtp
- Interface fa 0/0
- Ip access-group101 in
- extended靠近來源

ExtendedACL設定實作1

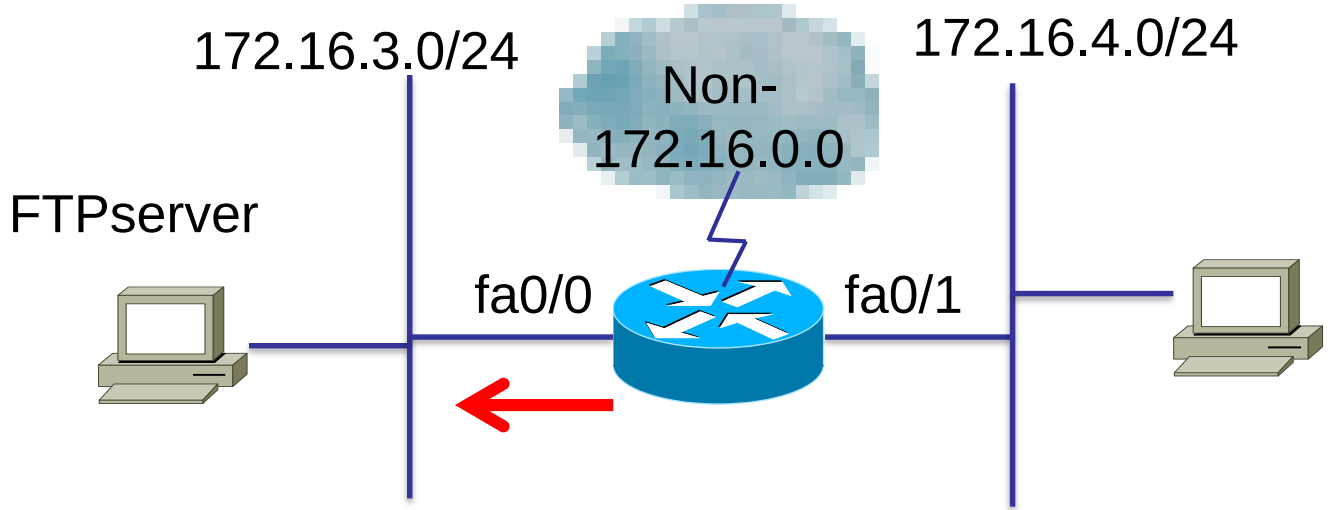


- Deny FTP traffic from subnet 172.16.4.0 to subnet 172.16.3.0 out fa0/0
- Permit all other traffic
- access-list101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
- access-list 101 permit ip any any

Extended ACL設定實作1

- Router(config)#
- access-list101deny tcp172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
- access-list 101 permit ip any any
- Router(config)#int fa 0/0
- Router(config-if)#ip access-group 101 out

ExtendedACL設定實作2



- Deny only Telnet traffic from subnet 172.16.4.0 out fa0/0
- Permit all other traffic
- access-list102 deny tcp 172.16.4.0 0.0.0.255 any eq 23
- access-list 102 permit ip any any

Extended ACL設定實作2

- Router(config)#
- access-list 101 deny tcp172.16.4.0 0.0.0.255 **any** eq **23**
- access-list 101 permit ip any any
- Router(config)#int fa 0/0
- Router(config-if)#ip access-group 101 out

第八章

WAN廣域網路

廣域網路簡介

- 到底是什麼構成廣域網路(Wide Area Network，WAN)，而使它不再是區域網路(Local Area Network，LAN)呢？距離是第一個令人想到的觀點，但目前無線的區域網路可以涵蓋相當程度的區域！所以是頻寬嗎？同樣地，很多地方都建置了大量的頻寬；所以這兩者都不是。那到底是什麼呢？

廣域網路簡介

- 也許區別區域網路與廣域網路最好的方式就是：通常您會擁有區域網路的基礎建設，但卻會從服務供應商租用廣域網路的基礎建設。雖然現代的技術甚至也漸漸地模糊了這個定義。我們已經討論過您通常會擁有的資料鏈結(乙太網路)，現在即將討論的是您通常不會擁有的資料鏈結，而是從服務供應商租來的。

定義廣域網路術語

- 在考量WAN服務類型之前，最好先瞭解以下的術語，這些是服務供應商經常使用的。
  - **用戶端設備(Customer Premises Equipment，CPE)**—用戶端設備是由用戶擁有，且位於用戶場所的設備。
  - **責任分界點(Demarcation Point)**—責任分界點是服務供應商責任終了、而CPE的責任開始的分野，它通常是一個放在由電信公司(電話公司)所擁有與安裝的通訊箱中的一個裝置。用戶要負責從這個箱子接線到CPE，它通常是一條連到CSU/DSU或ISDN界面的線路。

定義廣域網路術語

- **區域迴路(Local Loop)**—區域迴路連接責任分界點到最近的一個稱為中央機房的交換機房。
- **中央機房(Central Office，CO)**—這個點將連結用戶與供應商的交換網路，中央機房有時又稱為POP(PointofPresence)。
- **長途網路(Toll Network)**—長途網路是WAN供應商網路內部的主幹線路。這個網路由一群ISP擁有的交換機與設備所組成。

廣域網路連線類型

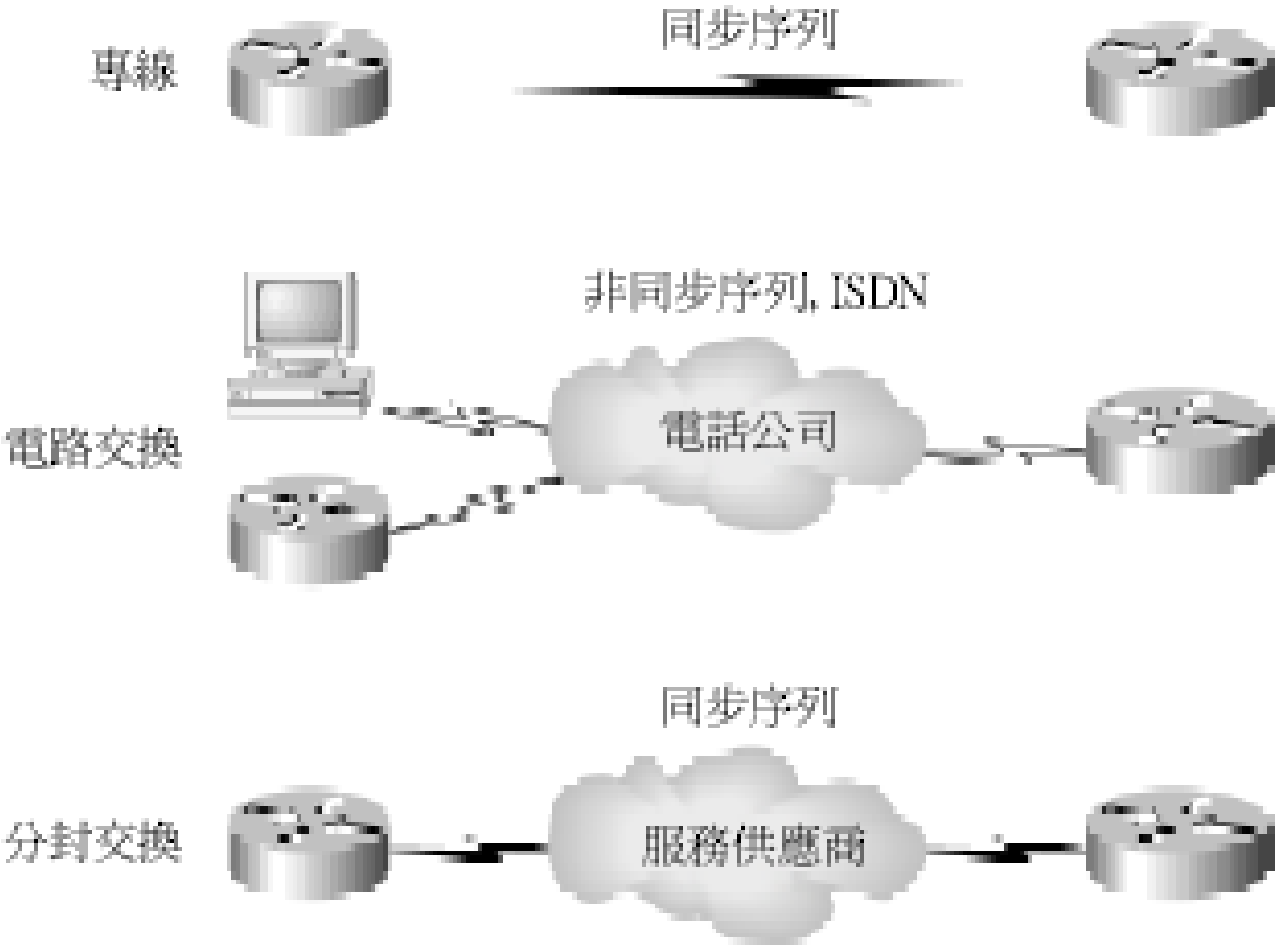


圖 11.1 廣域網路連線類型

廣域網路支援

- 定義網域網路協定：
  - **訊框中繼(FrameRelay)**－1990年代早期發展出來的分封交換技術，訊框中繼是資料鏈結與實體層的規格，提供較高的效能。訊框中繼接替X.25的任務，但大部分X.25用來補救實體層錯誤(雜訊很多的線路)的技術都移除了。訊框中繼比點對點鏈路更有經濟效益，運行的速度是64Kbps到45Mbps(T3)。訊框中繼提供動態頻寬配置與壅塞控制的功能。

廣域網路支援

- **整合服務數位網路(Integrated Service Digital Network，ISDN)**—ISDN是一組可以在現存的電話線路上傳送語音與資料的數位服務。ISDN為那些需要比類比式撥接鏈路所提供更高速之連線的遠端使用者，提供更有經濟效益的解決方案。ISDN也很適合用來作為訊框中繼或T-1專線等其他種鏈路的備份鏈路。

廣域網路支援

- **平衡式鏈路存取程序(Link Access Procedure ，Balanced，LAPB)**－LAPB的設計是要供X.25之資料鏈路層使用的連線導向協定，也可用來進行簡易的資料鏈路傳輸。LAPB會因為它嚴格的逾時與視窗技術而產生大量的額外負擔。
- **高階資料鏈結控制(High-LevelData-Link Control，HDLC)**－HDLC是從同步的資料鏈結控制(Synchronous DataLink Control，SDLC)衍生的

廣域網路支援

- **點對點協定(Point-to-Point Protocol，PPP)**
  —PPP是一種業界標準，因為所有多重協定版的HDLC都是專屬的，所以可利用PPP在不同廠商的設備之間產生點對點的鏈路。PPP使用資料鏈結標頭中的網路層控制協定欄來識別網路層協定，它允許認證與多重鏈路的連線，而且可以在同步與非同步的鏈路上運作。

廣域網路支援

- **非同步傳輸模式(Asynchronous Transfer Mode，ATM)**—ATM的設計是為了易受時間影響的交通，同時提供語音、視訊、與資料的傳輸。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。

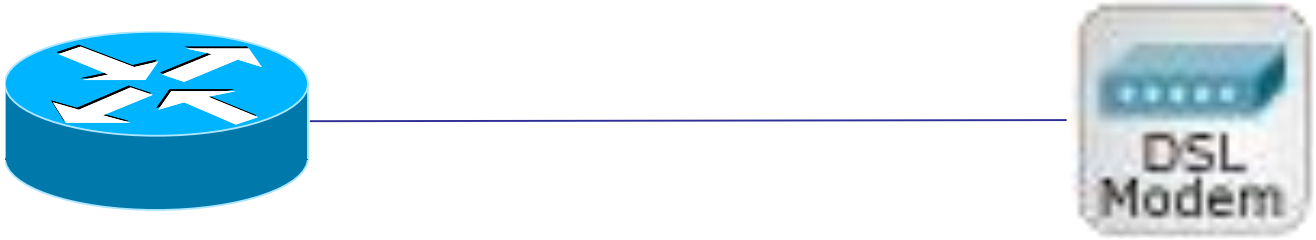
序列傳輸

- WAN序列接頭(serial connector)使用序列傳輸(serial transmission)，這種傳輸是在單一的通道上，一次放置1個位元。
- Cisco路由器使用專屬的60個接腳的序列接頭，您必須跟Cisco或Cisco設備供應商購買。

DTE/DCE

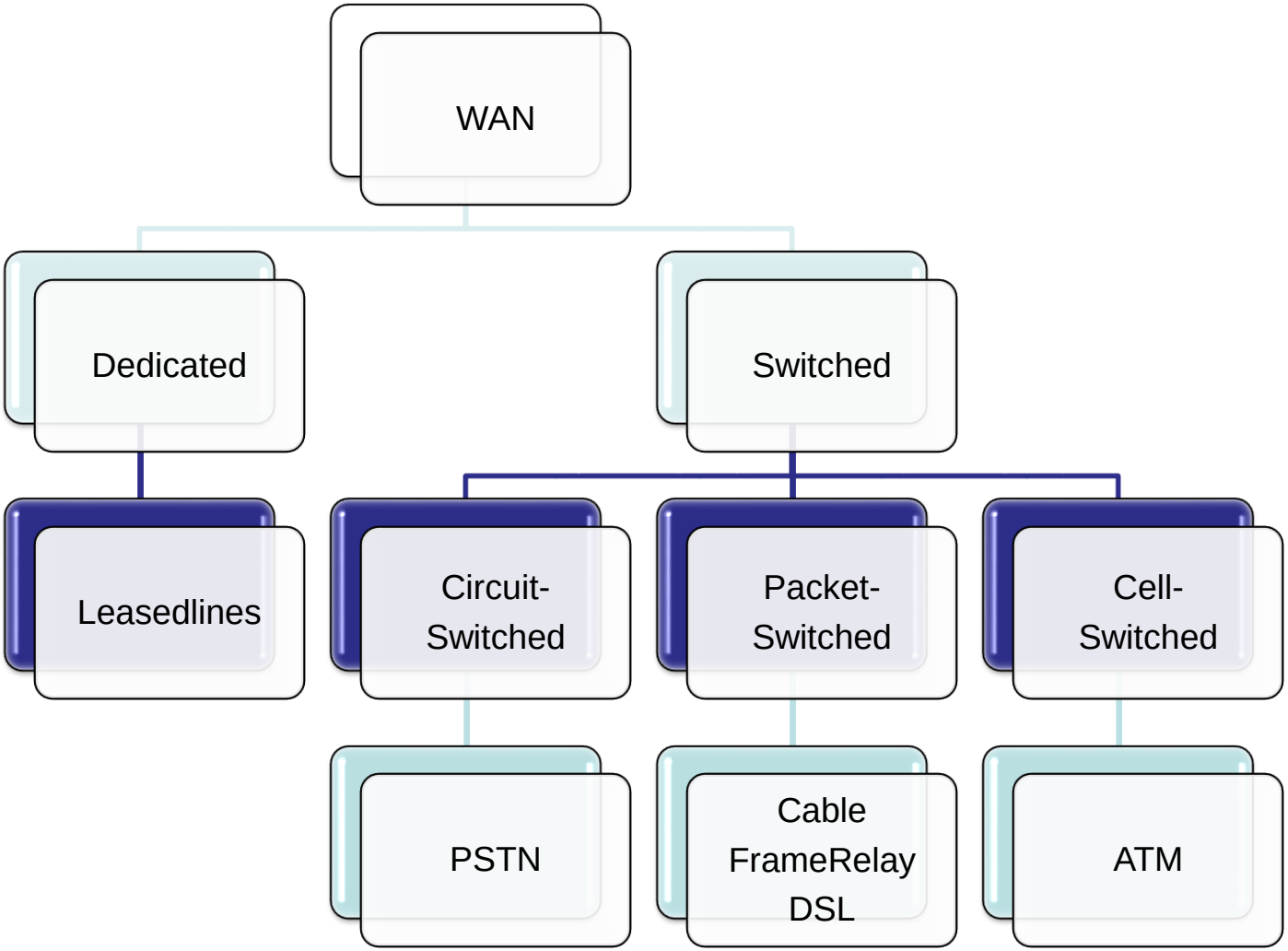
- DTE Data Terminal Equipment
  - 用戶端設備
- DCE Data Circuit-terminating Equipment
  - 負責連接DTE連線至Central Office CO
  - clockrate

DSU/CSU digital to digital
Modem digital to analog



DTE DCE

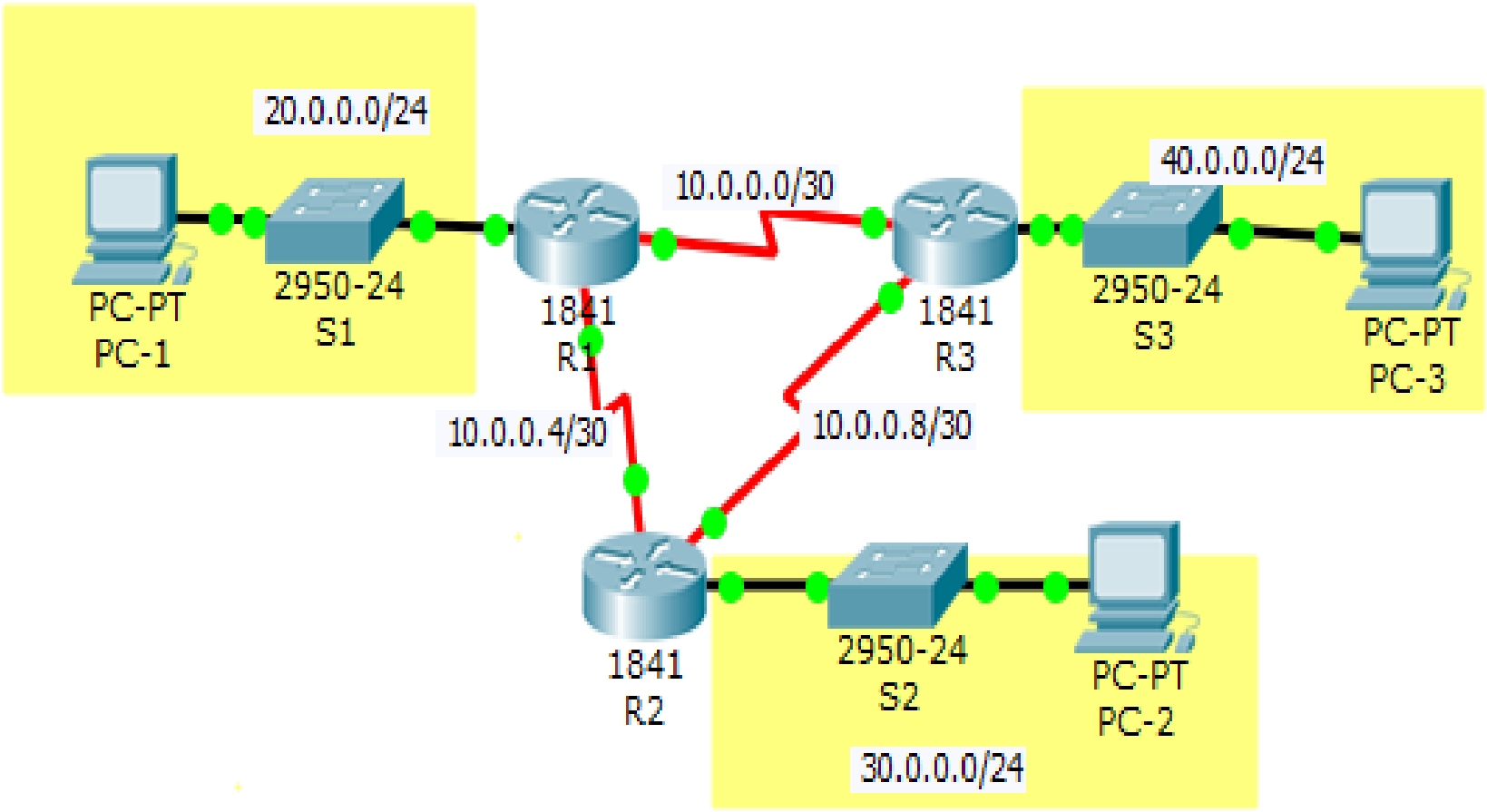
WAN communication Link



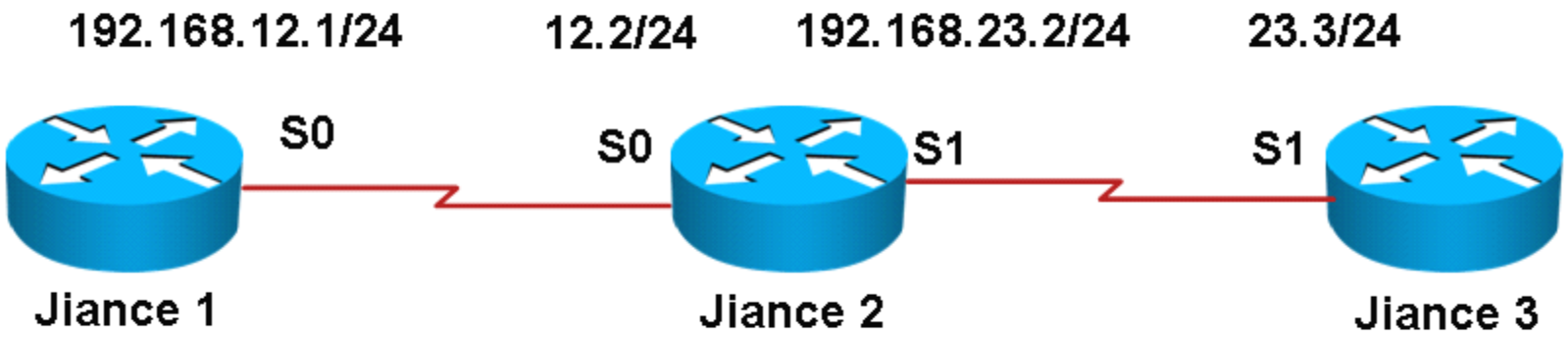
第九章

各類型拓譜實務

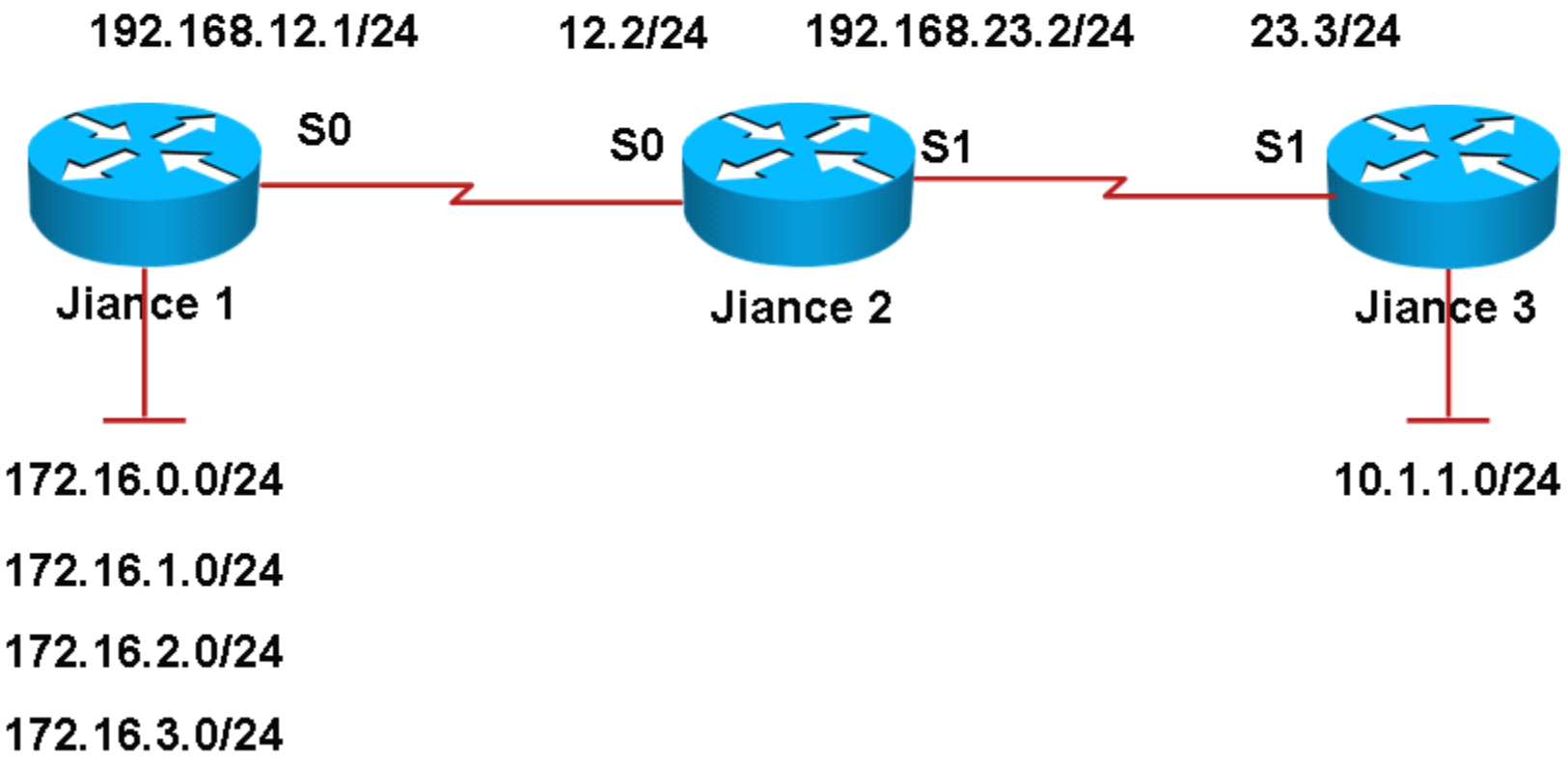
預設路由及靜態路由


20.0.0.0/24
PC-PT
PC-1
2950-24
S1
1841
R1
10.0.0.0/30
1841
R3
40.0.0.0/24
2950-24
S3
PC-PT
PC-3
10.0.0.4/30
10.0.0.8/30
1841
R2
2950-24
S2
PC-PT
PC-2
30.0.0.0/24

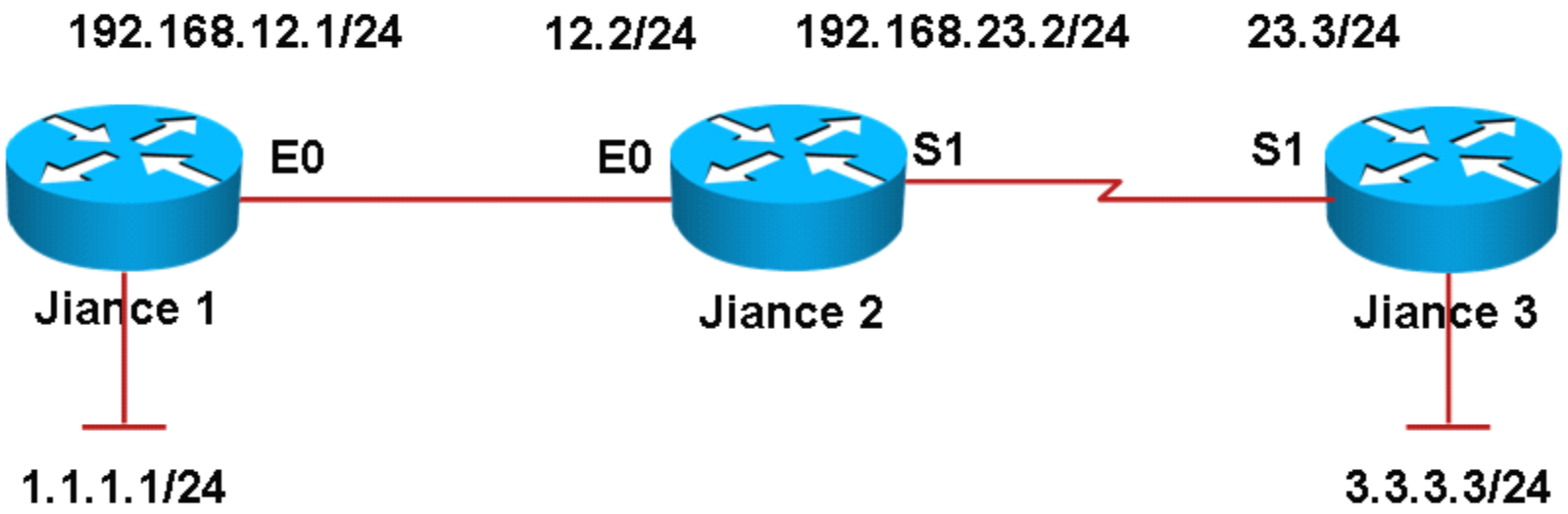
RIP動態路由


192.168.12.1/24
12.2/24
192.168.23.2/24
23.3/24
S0
S0
S1
S1
Jiance 1
Jiance 2
Jiance 3

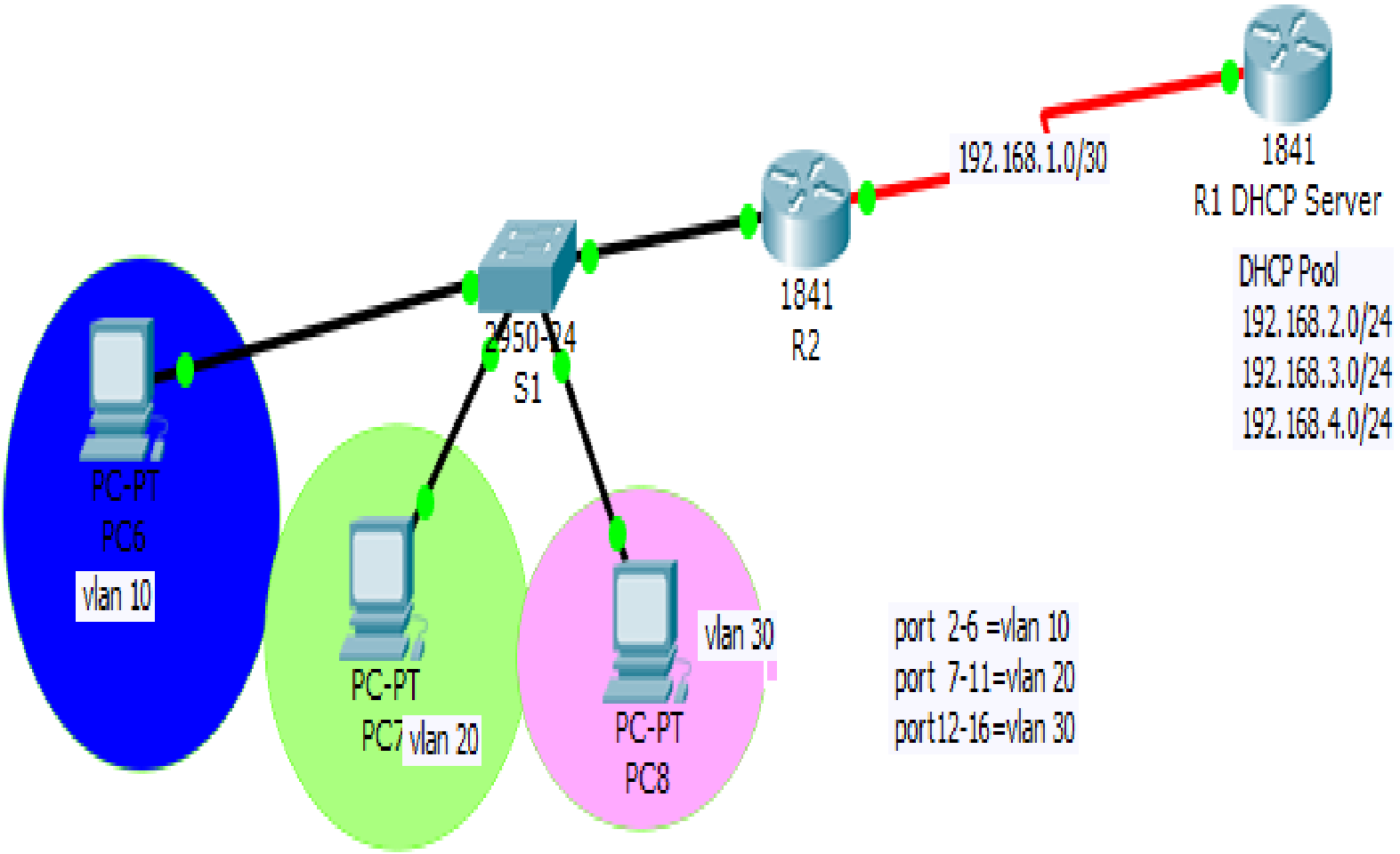
EIGRP動態路由


192.168.12.1/24
12.2/24
192.168.23.2/24
23.3/24
S0
S0
S1
S1
Jiance 1
Jiance 2
Jiance 3
172.16.0.0/24
172.16.1.0/24
172.16.2.0/24
172.16.3.0/24
10.1.1.0/24

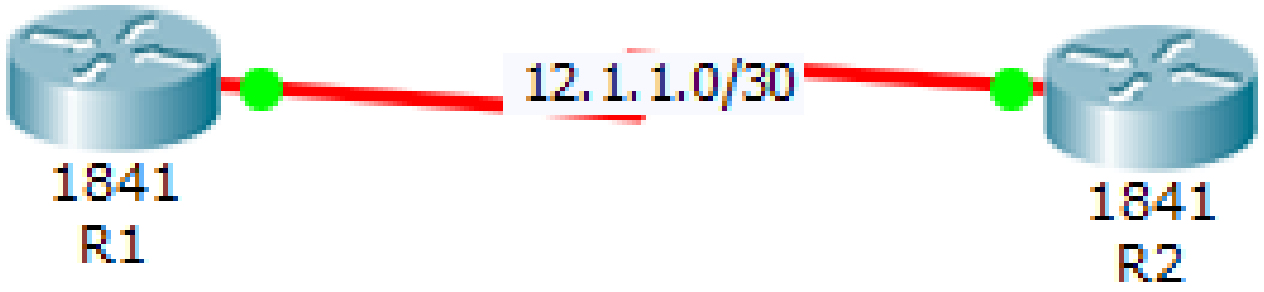
OSPF動態路由


192.168.12.1/24
12.2/24
192.168.23.2/24
23.3/24
E0
E0
S1
S1
Jiance 1
Jiance 2
Jiance 3
1.1.1.1/24
3.3.3.3/24

設定DHCP Server of Route



WAN 設定 HDLC PPP(PAP)



1.HDLC
2.PPP(PAP)

NAT網路地址轉換

192.168.12.3/24（辅助地址）

192.168.12.2/24（辅助地址）