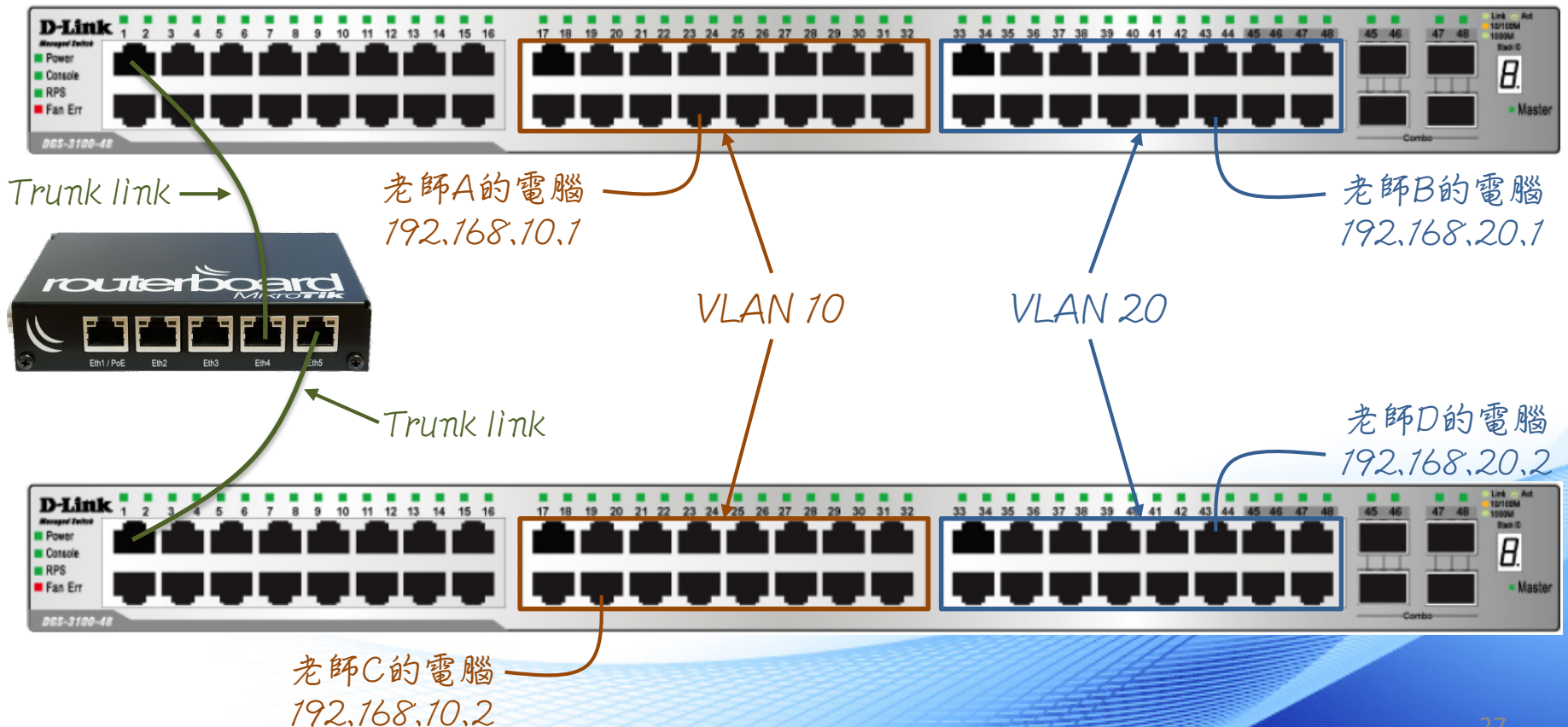



Lab6 – 利用路由器讓 VLAN 彼此互通

- 延續 Lab 5 的設定，把兩台 DGS-3100 的 trunk link 接到 RB450G 的第 4 與第 5 埠，讓 VLAN 10 與 VLAN 20 互通



Vlan、Switch、Routing、NAT 原理與實作

011100
01 011100
0 01 011100
111 00 0 01 011100
100 1 0 111 00 0 01 011100
111 00 0 01 011100
1100
1100 1 0 111 00 0 01 011100



大綱

- Route 原理
- NAT 原理
- Route LAB 模擬
 - 設定VLAN
 - 設定Trunk
 - 廣播風暴
 - 啟用STP防止接線迴圈

Route 原理

Application 應用層

- 使用者所使用的應用程式或網頁

Presentation 表現層

- 資料的壓縮、解壓縮以及加解密等

Session 會談層

- 連線的建立與結束、資料的傳輸模式(全/半雙工)

Transport 傳輸層

- 流量控制、傳輸的可靠性

Network 網路層

- 定址及路由

Data Link 資料鏈結層

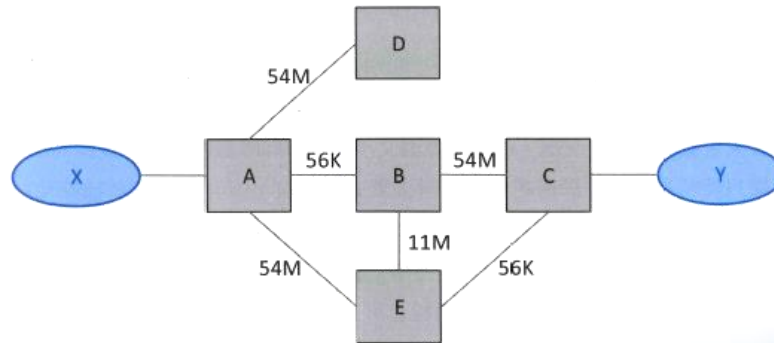
- 介質存取控制的方法以及定址

Physical 實體層

- 訊號傳送的介質規格、訊號編碼與轉換

網路層負責做啥？

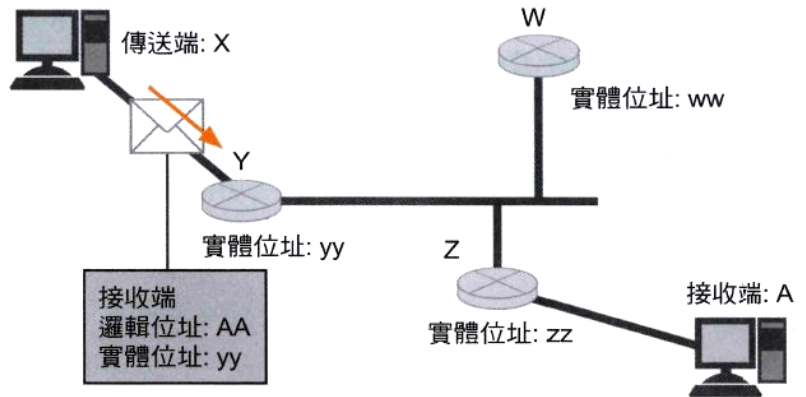
- 網路層使用的通訊協定是 Internet Protocol (IP)，為網際網路的業界標準 (De facto)
- 網路層做兩件事：
 - 定址 (Addressing)：決定裝置在網路上的邏輯位址 (IP位址)
 - 路由 (Routing)：尋找封包到達目的地的路徑，包括判斷正確路徑及最佳路徑



序號	來源	可能路徑	目的
1	X	A → B → C	Y
2		A → B → E → C	
3		A → E → B → C	
4		A → E → C	

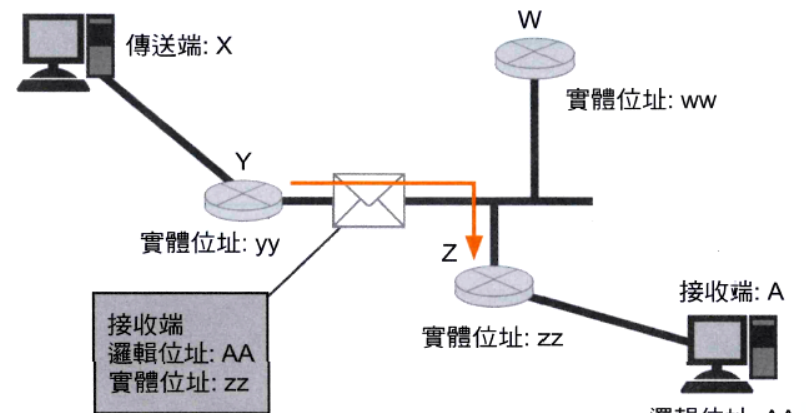
實體位址與邏輯位址

- 如下圖，若 X 欲傳輸封包至 A，整個傳輸過程中封包的目的地邏輯位址均相同，但是實體位址會因為封包經過不同的區域網路而改變



邏輯位址就是接收端 A 的邏輯位址: AA。

實體位址就是由同一個區域網路進行轉介的裝置位址: yy



透過裝置 Y 轉介後再進行傳送時，邏輯位址一樣是 AA，不過，實體位址就變成下一個轉介對象 zz。

利用實體位址來指定 zz，即可明確掌握轉介的對象。

(由此可清楚知道傳送對象並非裝置 W，而是裝置 Z)

Internet Protocol 封包標頭

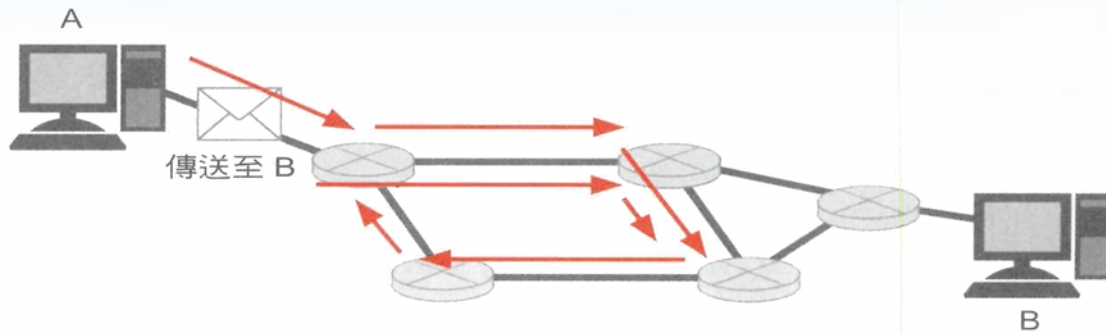
IP 封包是由含有 IP 資訊的標頭, 以及除了標頭部分外, 其他希望傳送的資料本體之資料承載 (Payload) 等兩部分所組成。



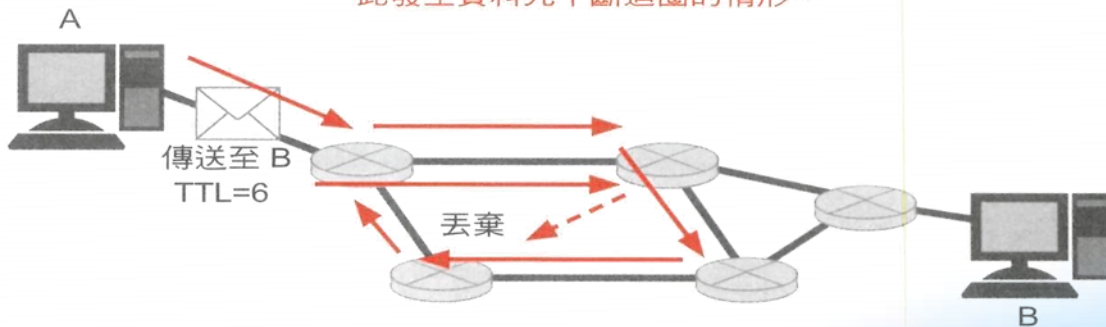
	名稱	位元	說明
1	版本	4	IP 版本
2	標頭長度	4	標頭的長度
3	服務類型	8	封包的優先度/重要度
4	資料長度	16	IP 標頭與資料承載之總長度
5	ID	16	資料元的識別編號
6	旗標 (Flag)	3	判斷是否已經將資料元分割完成
7	分割定位 (Fragment offset)	13	若希望能在分割時回復原始值即可使用本功能
8	TTL	8	封包的存活時間
9	通訊協定	8	指定上層通訊協定
10	標頭檢查碼 (Header Checksum)	16	用來進行 IP 標頭錯誤檢查的代碼
11	傳送端 IP 位址	32	傳送端邏輯位址
12	目的地 IP 位址	32	目的地邏輯位址
(13)	Option	n	選擇性欄位, 在特殊設定時才使用本功能

封包存活時間 (TTL)

當 IP 資料元持續在網間徘徊時，
TTL 可決定其必須消失的時間



路徑選擇錯誤，而無法到達目的地，因此發生資料元不斷迴圈的情形。



事先設定好 TTL，一旦資料元在固定期間內發生迴圈，就會被丟棄。
(實際上必須根據中間的路由器數量進行判斷，上例所示為連續通過路由器 6 次後就會被丟棄)

IP 位址

- 由 NIC (Network Information Center) 分配。NIC 下又依地域分為數個分支。其中 InterNIC：責負美國及其它地區； ENIC：歐洲地區； APNIC：亞太地區
- IPv4：32 bits、IPv6：128 bits
- 如何分別 netid 及 hostid
 - 分級式(Classful)：IPv4 較早的設計，目前也還有不少人口語上這麼用
 - 不分級式(Classless)：利用 網路遮罩(netmask) 來區分，IPv4 及 IPv6 均採用此法

IPv4 網路位址表示法

標示 IP 位址時, 必須先依不同的位元組別, 轉換為 10 進制

標示為 2 進制 (位元)

11000000101010000010101000000001

利用位元組
來分割資料

11000000

10101000

00101010

00000001

將位元組轉換為
10 進制標示方式

192

168

42

1

插入點即可形成
位元組的分隔

192

168

42

1

通常會利用上述標示法來敘述
(每個點皆以 10 進制來標示)

第 1 個
八位元組

第 2 個
八位元組

第 3 個
八位元組

第 4 個
八位元組

11000000

10101000

00101010

00000001

192

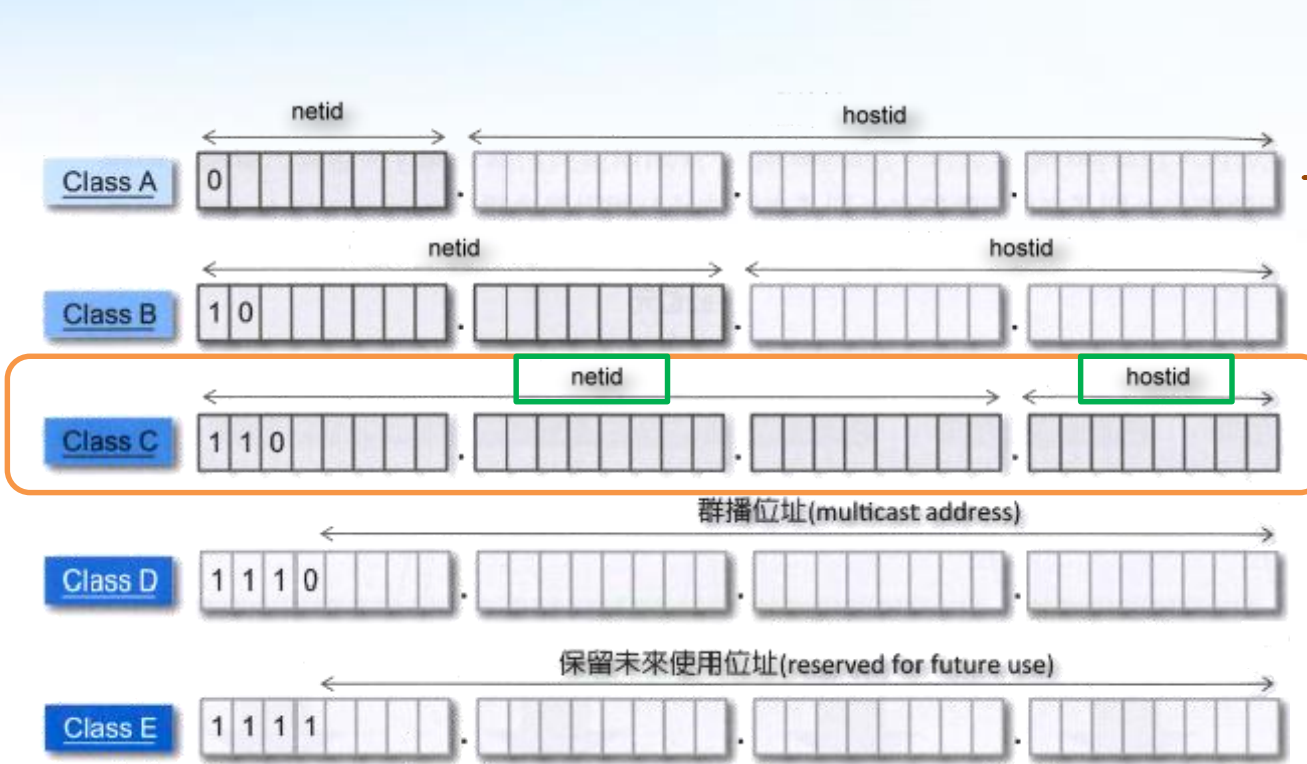
168

42

1

位元組之間的區隔就稱之為「八位元組 (Octet)」, 從頭開始
分別被稱為「第 1 個八位元組」、「第 2 個八位元組」...等

分級式 IPv4 位址



00000000.00000000.
00000000.00000000
(0.0.0.0)
⋮
01111111.11111111.
11111111.11111111
(127.255.255.255)

五種分級在十進位的表示：

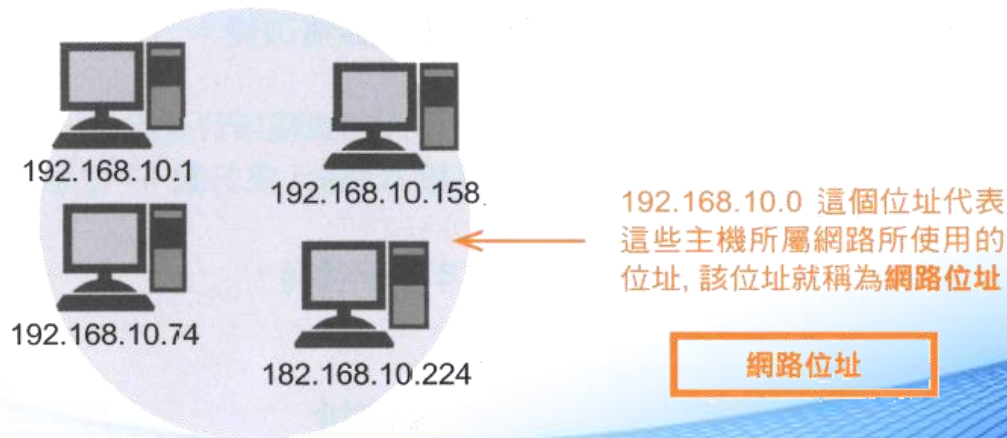
- Class A : 0.0.0.0 ~ 127.255.255.255
- Class B : 128.0.0.0 ~ 191.255.255.255
- Class C : 192.0.0.0 ~ 223.255.255.255
- Class D : 224.0.0.0 ~ 239.255.255.255
- Class E : 240.0.0.0 ~ 255.255.255.255

特殊用途的 IP 位址 (1/3)

具有特別的意義, 而且無法真正地分配給主機的位址

當該網路為等級 C, 而且網路部分為 192.168.10 時

第 1 個八位元組	第 2 個八位元組	第 3 個八位元組	第 4 個八位元組
網路部分			主機部分
11000000	101010000	00001010	00000000
192	168	10	0



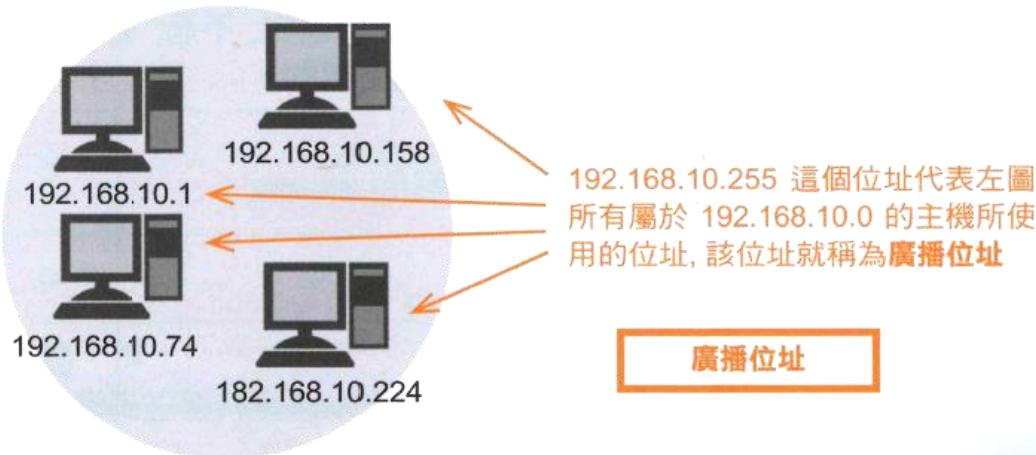
特殊用途的 IP 位址 (2/3)

當該網路為等級 C, 而且網路部分為 192.168.10 時

第 1 個八位元組	第 2 個八位元組	第 3 個八位元組	第 4 個八位元組
網路部分			主機部分
11000000	101010000	00001010	11111111
192	168	10	255

小測驗：

若163.32.250.119為分級式IPv4位址，請列出其網路位址和廣播位址，及實際可用IP的範圍



特殊用途的 IP 位址 (3/3)

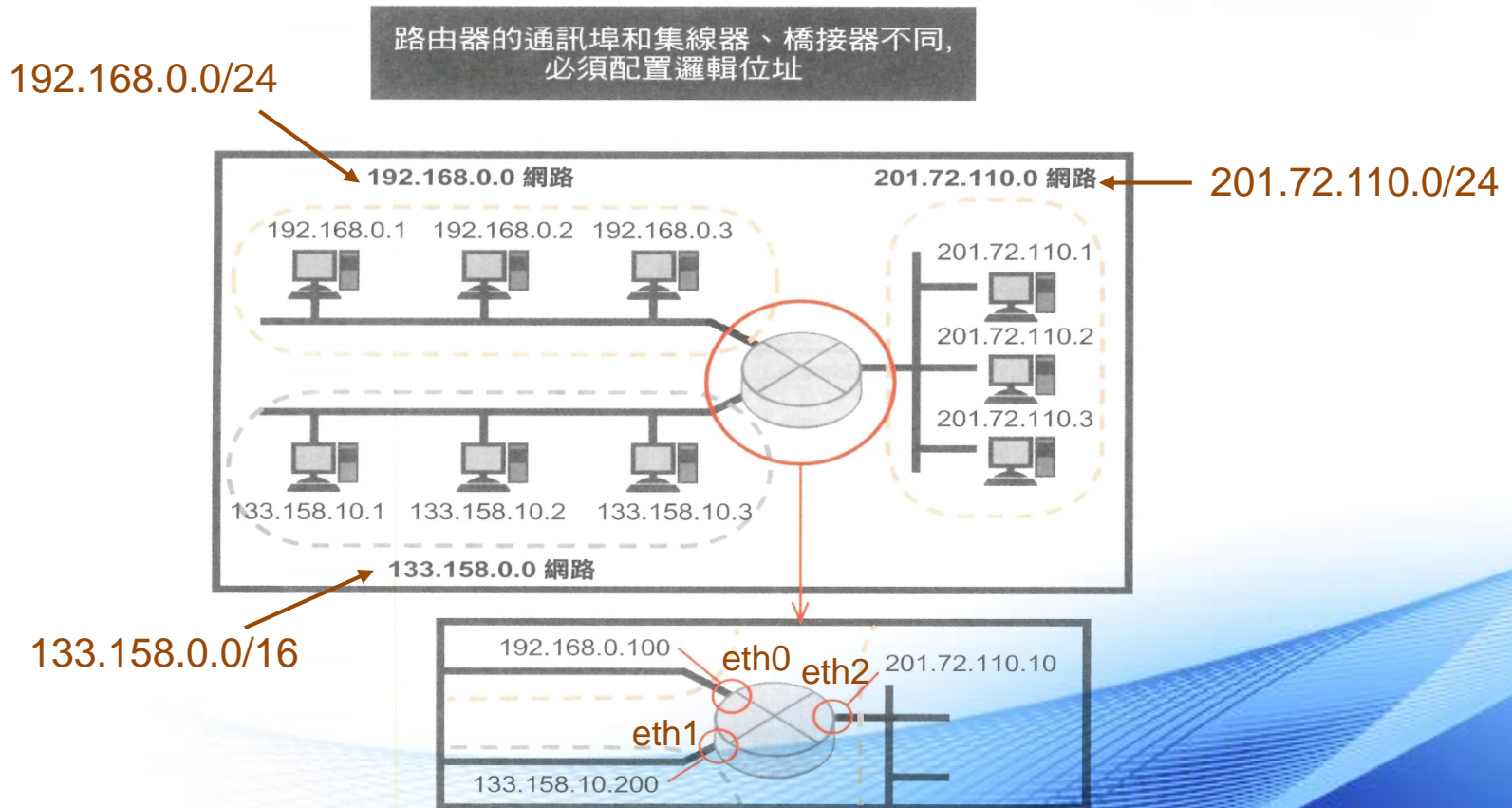
- netid 為 127 的 Class A 位址 (127.0.0.0 ~ 127.255.255.255) :
代表本機位址(localhost)，又稱為 loopback 位址，主要是方便使用者對本機的網路進行測試
- 私有IP位址 (Private IP address) :
無須經過向上游申請的手續即可使用，但是這些 IP 除非透過網路位址轉換(Network Address Translation, NAT)，否則無法與網際網路進行通訊
 - Class A : 10.0.0.0 ~ 10.255.255.255
 - Class B : 172.16.0.0 ~ 172.31.255.255
 - Class C : 192.168.0.0 ~ 192.168.255.255

路由器 – Router (1/2)

- 負責執行路徑選擇的工作
- 利用路由表 (routing table) 來判斷封包傳送的路徑，而路由表依賴網路位址來區分不同的網路
- 依據路由表維護的方式可分為：
 - 靜態路由 (static routing)：
透過人工方式，將網路的相關資訊輸入路由表，此方法不適合經常變動的網路環境或較大型的網路環境
 - 動態路由 (dynamic routing)：
藉由網路設備彼此之間交換路由表學習到整體網路的相關資訊

路由器 – Router (2/2)

- 路由器上面的每個網路介面都**必須屬於不同的邏輯網路** (不同的 netid)，並且各邏輯網路會自成一個**廣播域 (Broadcast Domain)**



路由表

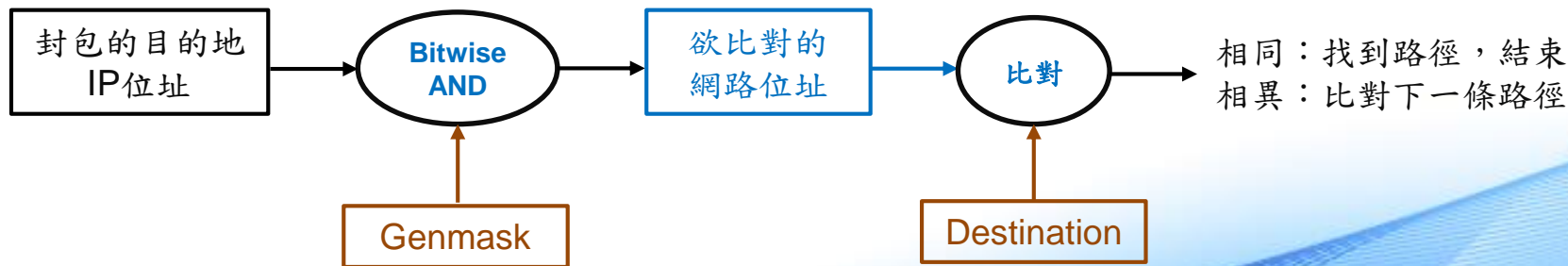
- 路由表的每一筆路徑基本上會包括以下五個項目：
 - 目的地網路 (Network Destination)：
目的地網路的網路位址
 - 網路遮罩 (Genmask)：
用於計算目的位址屬於哪個網路
 - 閘道 (Gateway)：
表示要到達的目的地網路是透過哪個「閘門」過去，如果此項目有顯示IP的話，表示該路由需要經過路由器的幫忙才能夠傳送出去，如果顯示 * 或 0.0.0.0 表示該路由是直接由本機傳送
 - 介面 (Interface)：
代表要到達的目的地網路是經由本機的哪個實體介面出去
 - 計量 (Metric)：
代表到達目的地網路成本的量測值，通常值越小表示該路徑到達目的地網路越佳或越快

路由表的運作

- 以前兩頁的網路架構為例，其中路由器的路由表應存在以下三筆路徑：

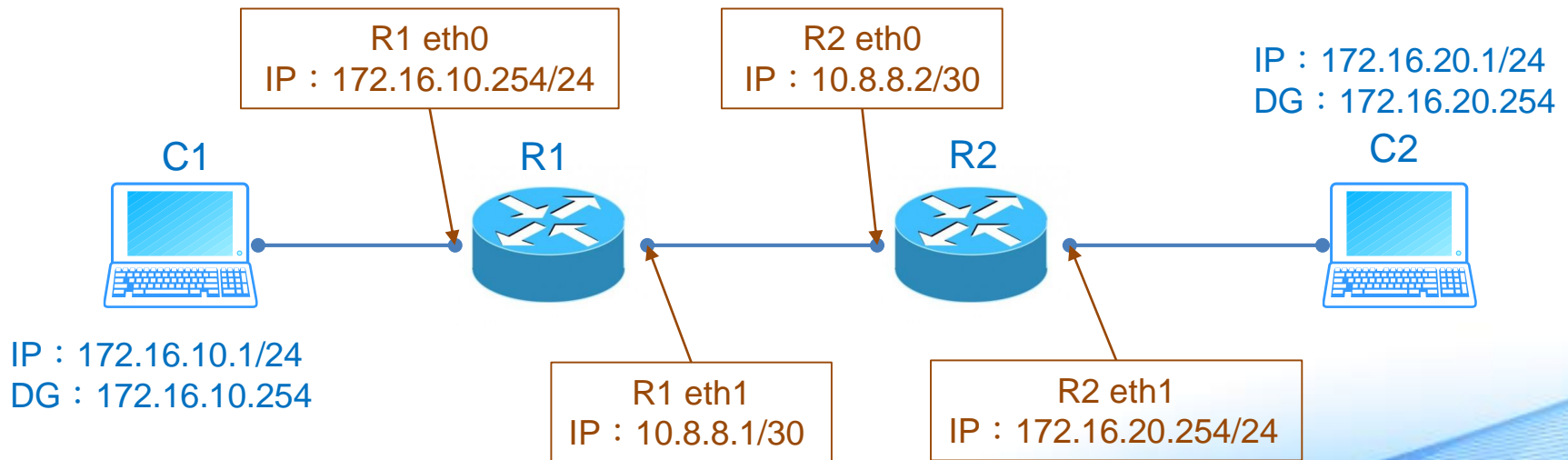
Destination	Gateway	Genmask	Iface
192.168.0.0	0.0.0.0	255.255.255.0	eth0
133.158.0.0	0.0.0.0	255.255.0.0	eth1
201.72.110.0	0.0.0.0	255.255.255.0	eth2

任何要被送出的封包都必須經過以下程序比對路徑：



路由表範例 (1/2)

- 假設有一網路架構如下，兩台電腦 C1 及 C2 分別接在路由器 R1 及 R2 上，若要使 C1 與 C2 互相 ping 得到 (第三層連通)，則 R1 與 R2 的路由表應如何設定？



路由表範例 (2/2)

- R1 路由表中已經存在的項目：

Destination	Gateway	Genmask	Iface
172.16.10.0	0.0.0.0	255.255.255.0	eth0
10.8.8.0	0.0.0.0	255.255.255.252	eth1

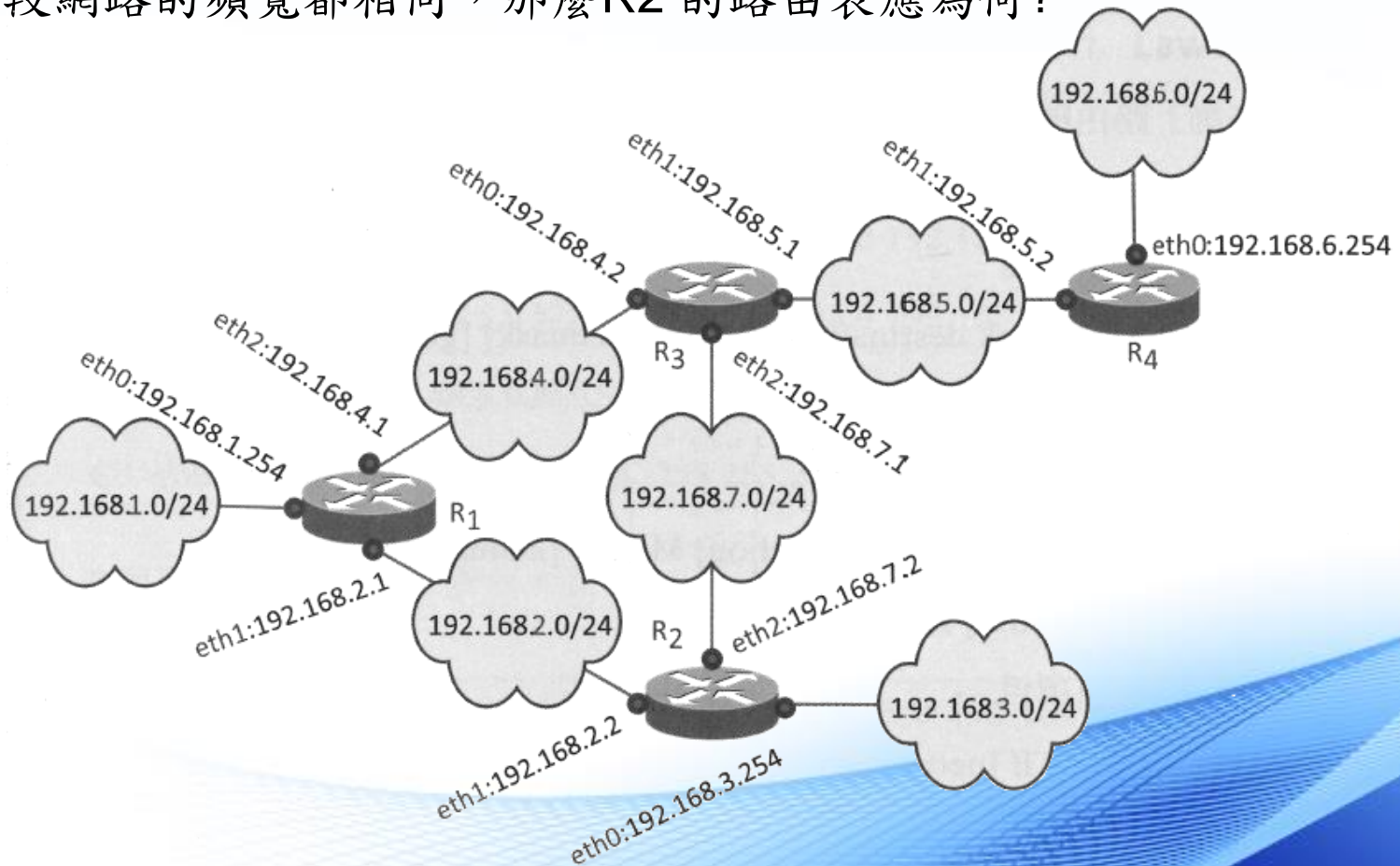
- R2 路由表中已經存在的項目：

Destination	Gateway	Genmask	Iface
172.16.20.0	0.0.0.0	255.255.255.0	eth1
10.8.8.0	0.0.0.0	255.255.255.252	eth0

請完成路由表，使C1 與 C2 可互相 ping 通

路由表練習 (1/2)

- 假設有一網路架構如下，若所有網路彼此之間都可以互相連通，且每段網路的頻寬都相同，那麼R2 的路由表應為何？



路由表練習 (2/2)

- 請完成 R2 的路由表：

Destination	Gateway	Genmask	Iface
192.168.3.0	0.0.0.0	255.255.255.0	eth0
192.168.7.0	0.0.0.0	255.255.255.0	eth2
192.168.2.0	0.0.0.0	255.255.255.0	eth1

用戶端路由表 (1/2)

- 並不是只有路由器會維護路由表，用戶端裝置也會維護路由表用來決定封包該往哪裡送
- Linux系統：
在 shell 中輸入 `route -n`

```
root@unknown:/tmp/home/root# route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
10.8.8.1         0.0.0.0         255.255.255.255 UH    0     0     0     vlan2
10.8.8.0         0.0.0.0         255.255.255.252 U     0     0     0     vlan2
192.168.2.0     0.0.0.0         255.255.255.0   U     0     0     0     br0
127.0.0.0       0.0.0.0         255.0.0.0       U     0     0     0     lo
0.0.0.0         10.8.8.1       0.0.0.0         UG    0     0     0     vlan2
root@unknown:/tmp/home/root#
```

用戶端路由表 (2/2)

- Windows 系統：
在命令提示字元下輸入 `route print`

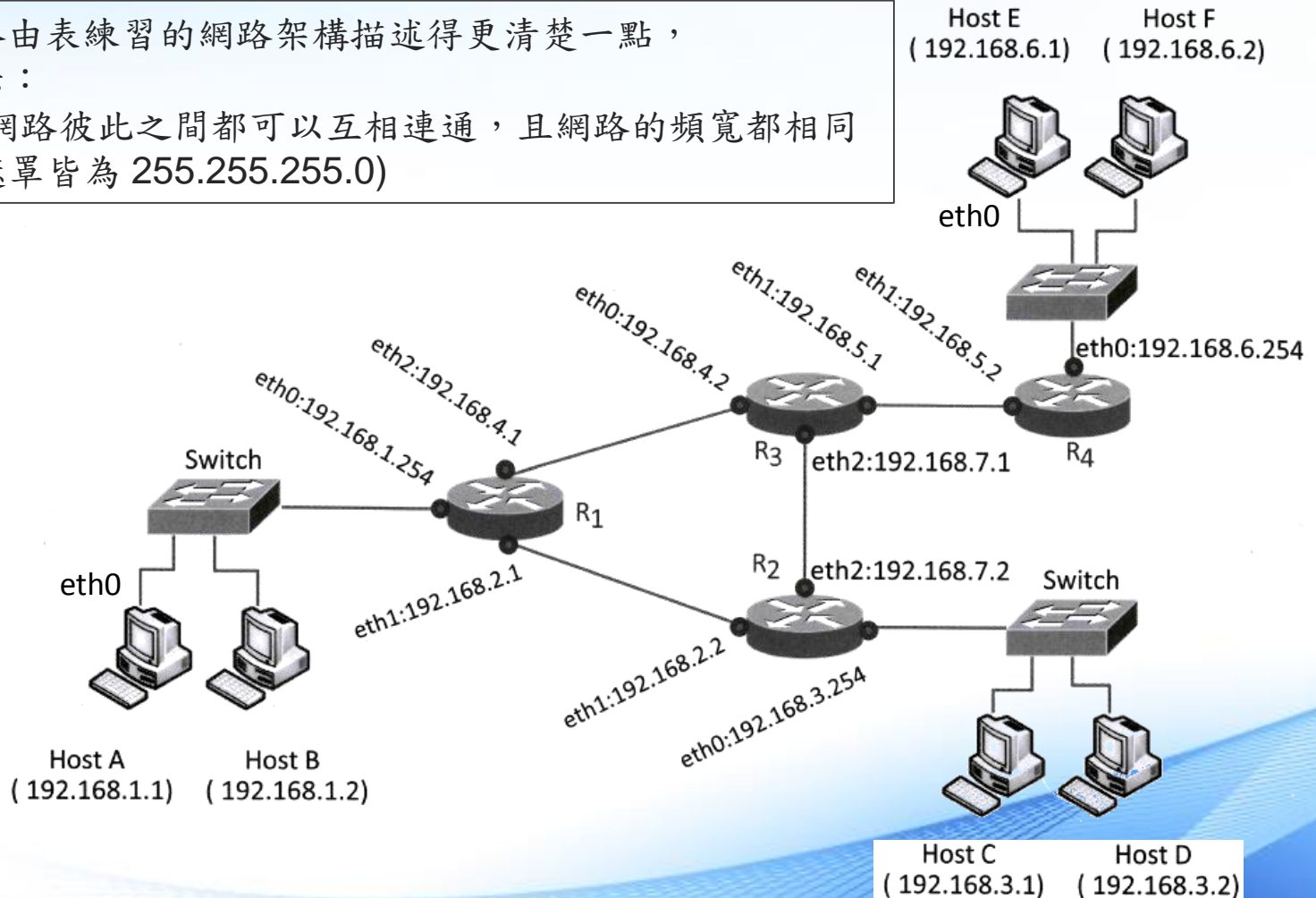
```
C:\Users\kiecuser>route print

=====
介面清單
11...00 50 56 25 01 32 .....Intel(R) PRO/1000 MT Network Connection
 1.....Software Loopback Interface 1
12...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
13...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
=====

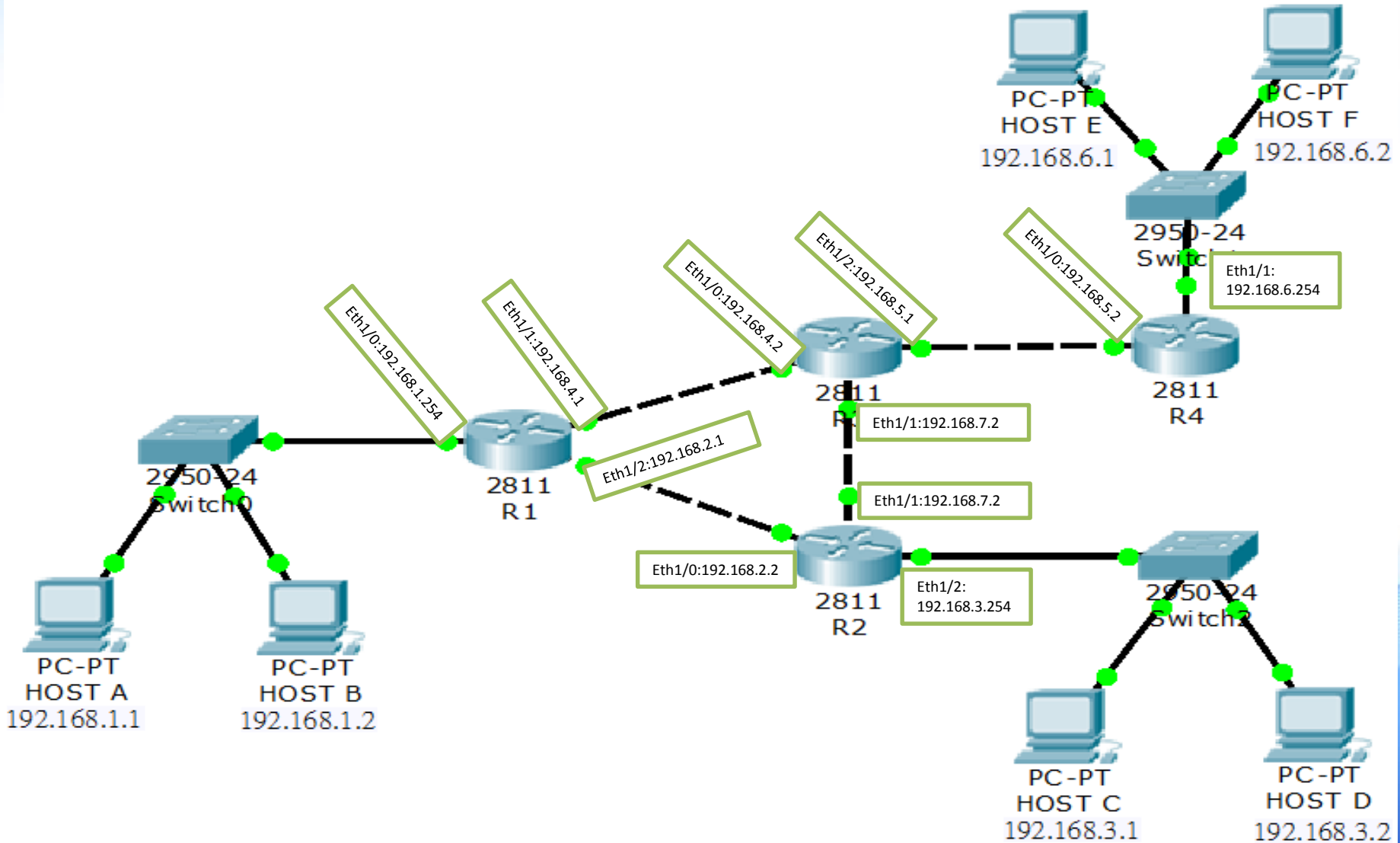
IPv4 路由表
=====
使用中的路由:
網路目的地          網路遮罩          閘道          介面          計量
0.0.0.0              0.0.0.0           163.16.5.254  163.16.5.132  266
127.0.0.0            255.0.0.0         在連結上      127.0.0.1     306
127.0.0.1            255.255.255.255  在連結上      127.0.0.1     306
127.255.255.255     255.255.255.255  在連結上      127.0.0.1     306
163.16.5.0          255.255.255.0    在連結上      163.16.5.132  266
163.16.5.132        255.255.255.255  在連結上      163.16.5.132  266
163.16.5.255        255.255.255.255  在連結上      163.16.5.132  266
224.0.0.0            240.0.0.0         在連結上      127.0.0.1     306
224.0.0.0            240.0.0.0         在連結上      163.16.5.132  266
255.255.255.255     255.255.255.255  在連結上      127.0.0.1     306
255.255.255.255     255.255.255.255  在連結上      163.16.5.132  266
=====
```


用戶端路由表練習 (1/3)

若把之前路由表練習的網路架構描述得更清楚一點，
如下圖所示：
(假設所有網路彼此之間都可以互相連通，且網路的頻寬都相同，
子網路遮罩皆為 255.255.255.0)



用戶端路由表練習 (2/3)



用戶端路由表練習 (3/3)

- 請完成 R1 的路由表：

Destination	Gateway	Genmask	Iface
-------------	---------	---------	-------

- 請完成 HOST A 的路由表：

Destination	Gateway	Genmask	Iface
-------------	---------	---------	-------

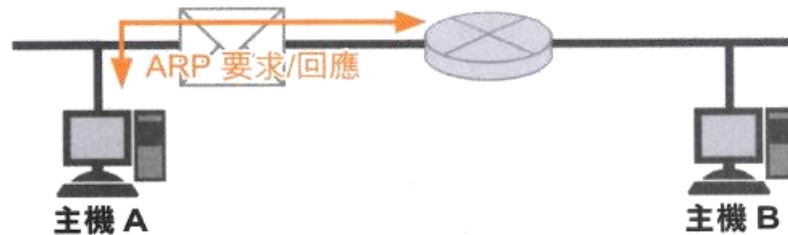
預設閘道 (Default Gateway)

- 若封包目的地 IP 的網路位址與路由表比對的結果均不符合 (沒有可用的路徑)，則該封包送往預設閘道，由預設閘道來處理
- 預設閘道在路由表裡面由一組 Network Destination 與 Genmask 皆為 0.0.0.0 的路徑表示
- 由於無論封包目的地 IP 及其網路位址為何，都會符合這筆路徑，所以在路由表的比對順序上應該放在最後面

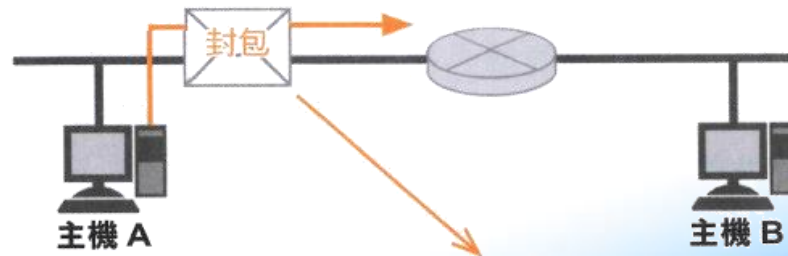
透過預設閘道的封包傳輸 (1/2)

預設閘道就是一種位於和其他網路之間連接點的裝置

- ① 要將資料傳送到其他網路時，主機會將 ARP 傳送到預設閘道上要求，以便取得預設閘道的 MAC 位址



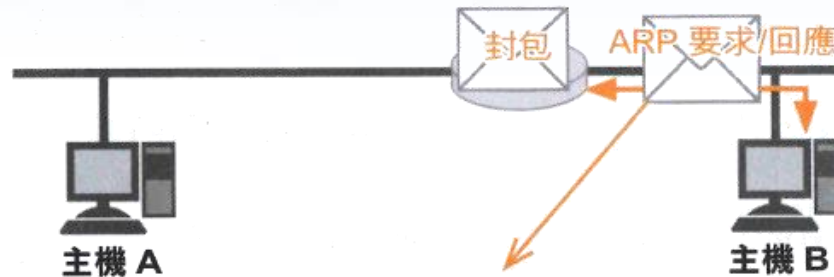
- ② 主機會將目的地 MAC 位址傳送到預設閘道，並且將目的地 IP 位址當作目的地主機來傳送封包



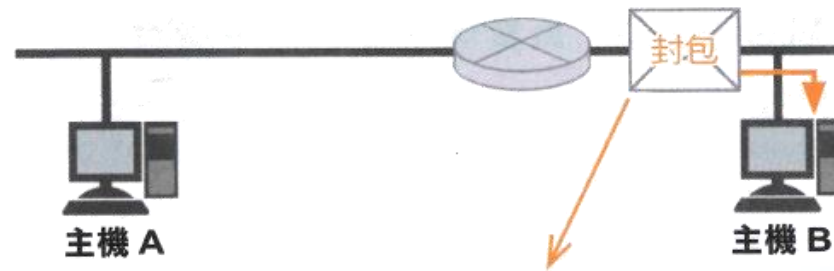
目的地MAC	傳送端MAC	傳送端IP	目的地IP	承載資料 (Payload)
路由器	主機A	主機A	主機B	

透過預設閘道的封包傳輸 (2/2)

③ 收到封包的預設閘道會開始執行路由工作，並且決定負責中繼的路由器及傳送通訊埠，接著再針對接收端 (負責中繼的路由器或目的地) 執行 ARP



④ 利用 ARP 將收到的 MAC 位址當作是目的地 MAC 位址，然後將本身的 MAC 位址改為傳送端 MAC 位址後再進行傳送，此時 IP 位址不變



目的地MAC	傳送端MAC	傳送端IP	目的地IP	承載資料 (Payload)
主機B	路由器	主機A	主機B	

動態路由 (1/2)

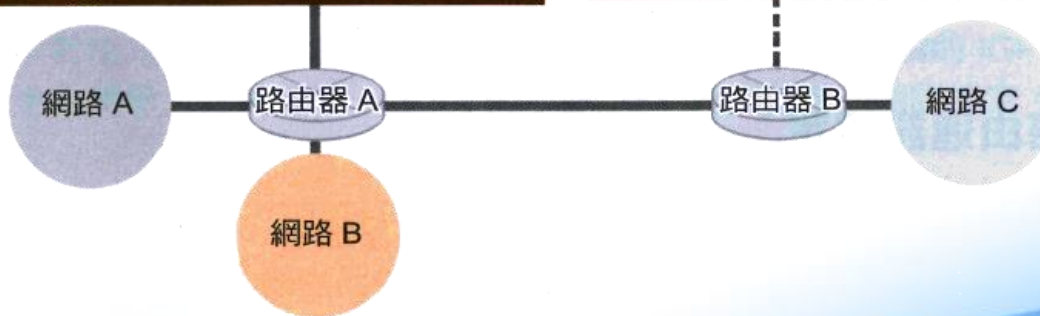
- 透過路由通訊協定(Routing Protocol) 與相鄰路由器交換網路資訊，並更新自己的路由表，藉此學習到整個網路的路徑資訊，常見的路由通訊協定：RIP、OSPF

根據路由通訊協定所決定的方式來交換資訊，並且達到路由收斂的目標。

① 路由器會將相鄰的網路資訊寫入路由資訊表

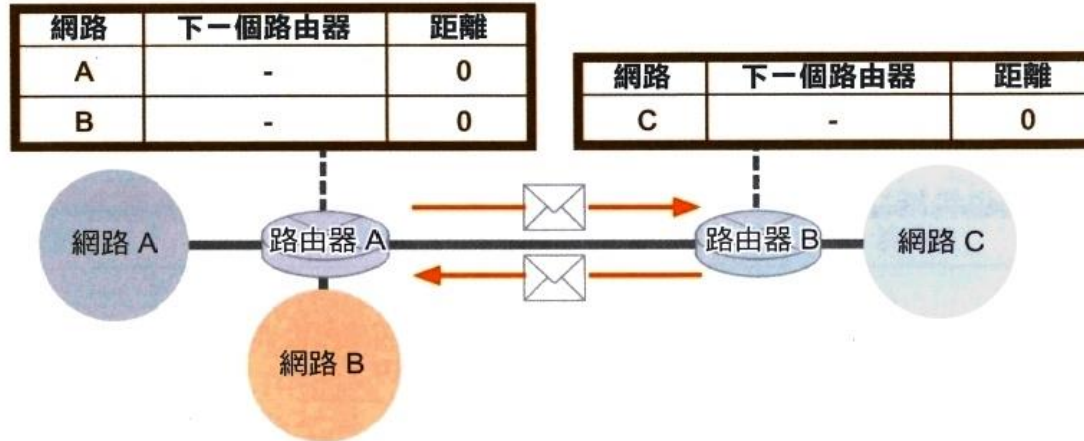
網路	下一個路由器	距離
A	-	0
B	-	0

網路	下一個路由器	距離
C	-	0

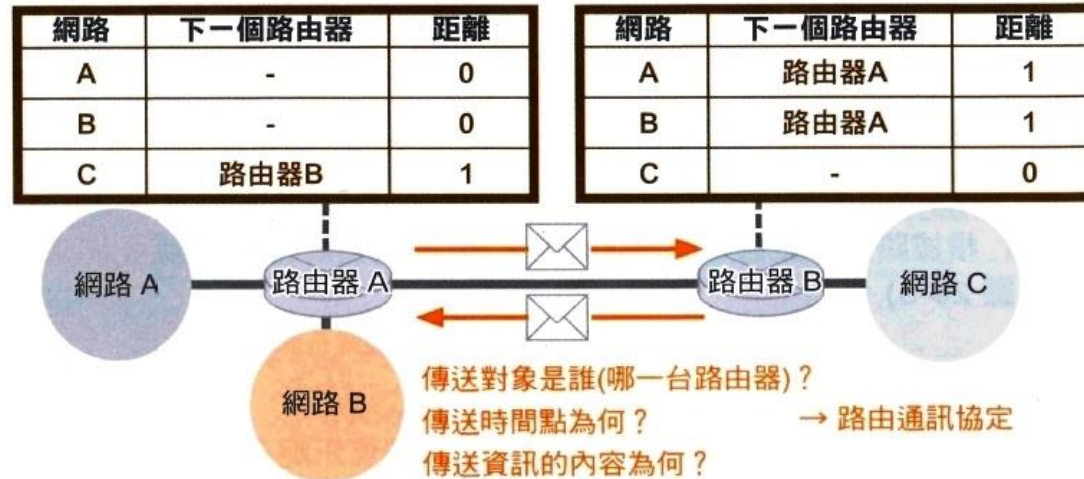


動態路由 (2/2)

② 使用路由通訊協定, 以互相交換所擁有的網路資訊

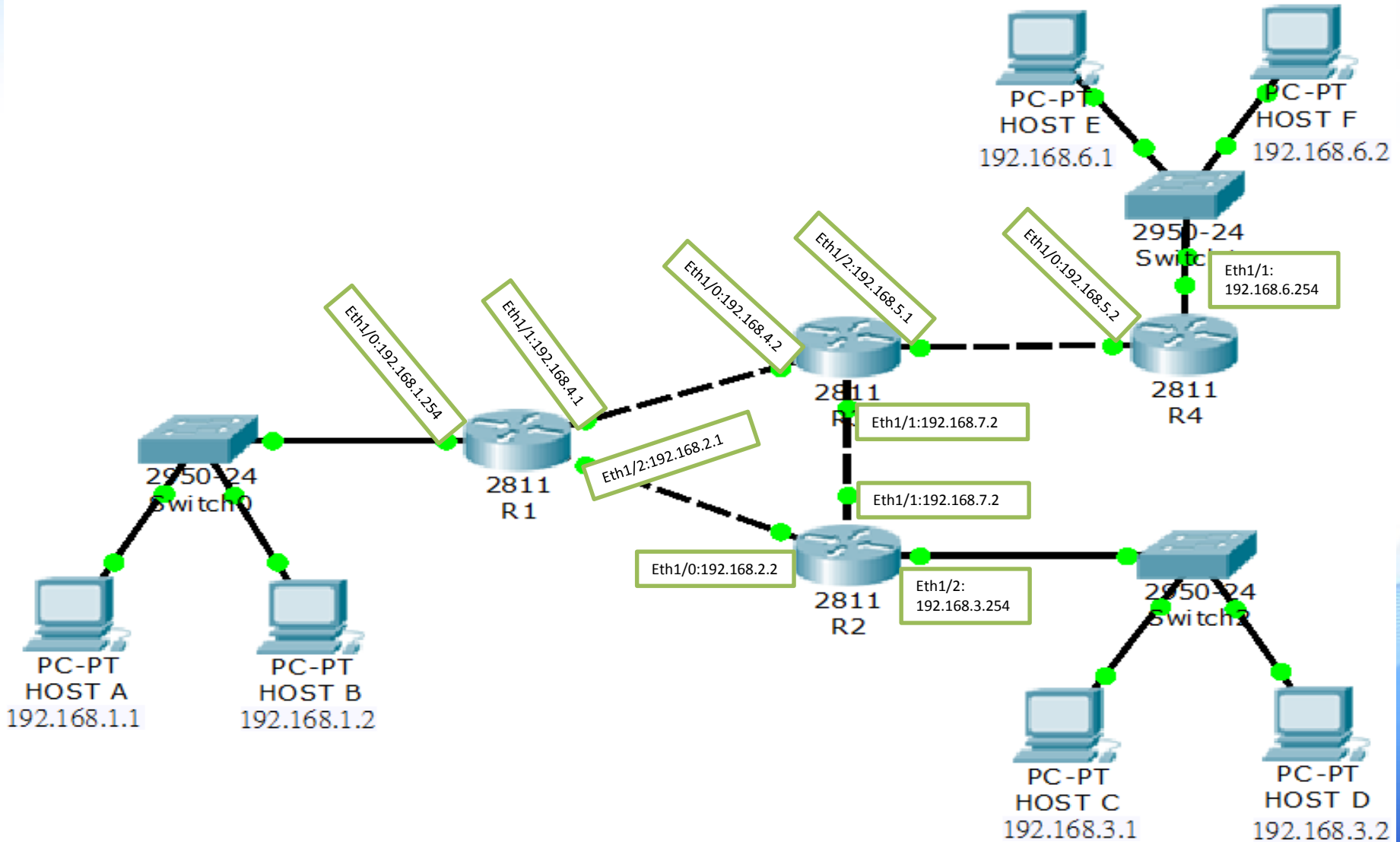


③ 使用交換後的資訊來更新路由資料表



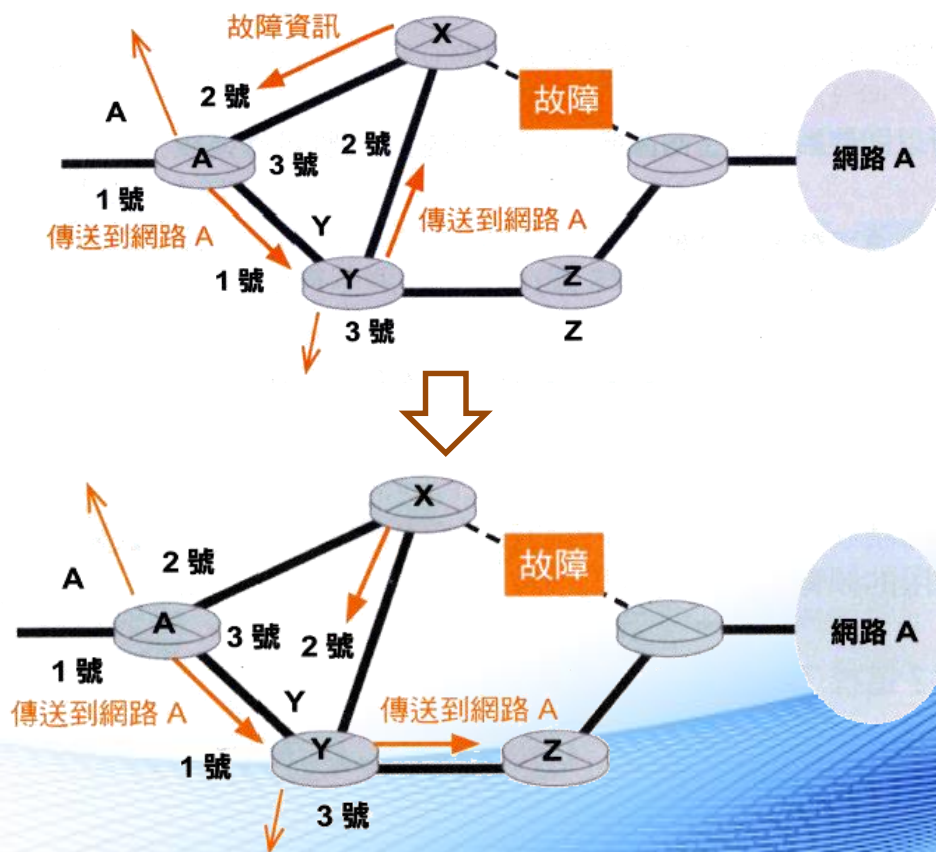
傳送對象是誰(哪一台路由器)?
 傳送時間點為何? → 路由通訊協定
 傳送資訊的內容為何?
 是否已經決定好接收資訊的最佳路徑了呢?

動態路由(RIP)實作

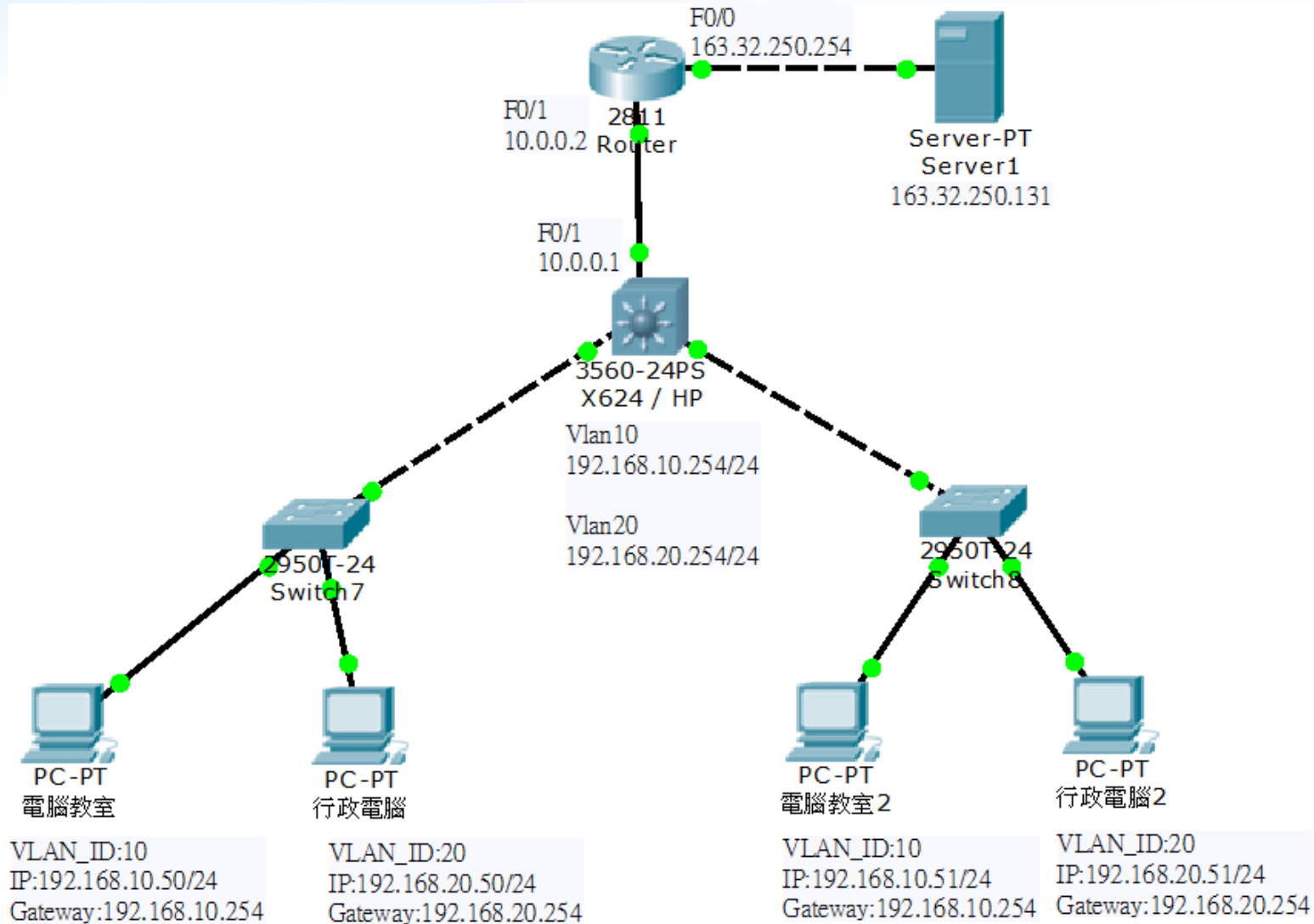


路由收斂

- 當網路連接狀況發生變更時，動態路由必須把這些變更通知其他路由器，直到所有路由器的路由表都維持在最新狀態，這個動作稱為路由收斂



學校環境模擬



NAT

原理與實作

011100
01 011100
0 01 011100
111 00 0 01 011100
100 1 0 111 00 0 01 011100
111 00 0 01 011100
1100
1100 1 0 111 00 0 01 011100

NAT 原理

Application 應用層

- 使用者所使用的應用程式或網頁

Presentation 表現層

- 資料的壓縮、解壓縮以及加解密等

Session 會談層

- 連線的建立與結束、資料的傳輸模式(全/半雙工)

Transport 傳輸層

- 流量控制、傳輸的可靠性

Network 網路層

- 定址及路由

Data Link 資料鏈結層

- 介質存取控制的方法以及定址

Physical 實體層

- 訊號傳送的介質規格、訊號編碼與轉換

什麼是NAT

- NAT(Network Address Translation)
 - 網路位置轉換
- NAPT(Network Address Port Translation)
 - 網路位址埠轉換
 - IP偽裝(Masquerade)
 - NAT最大的特色就是讓多台主機可以連到同一個外部IP位置

NAPT

- 轉換IP與埠號，並記錄於NAT表中

傳送端IP位址	傳送端通訊埠	目的端IP位址	目的端通訊埠	資料
192.168.0.1	1001	124.108.105.150	80	

傳送端IP位址	傳送端通訊埠	目的端IP位址	目的端通訊埠	資料
200.100.10.5	7001	124.108.105.150	80	

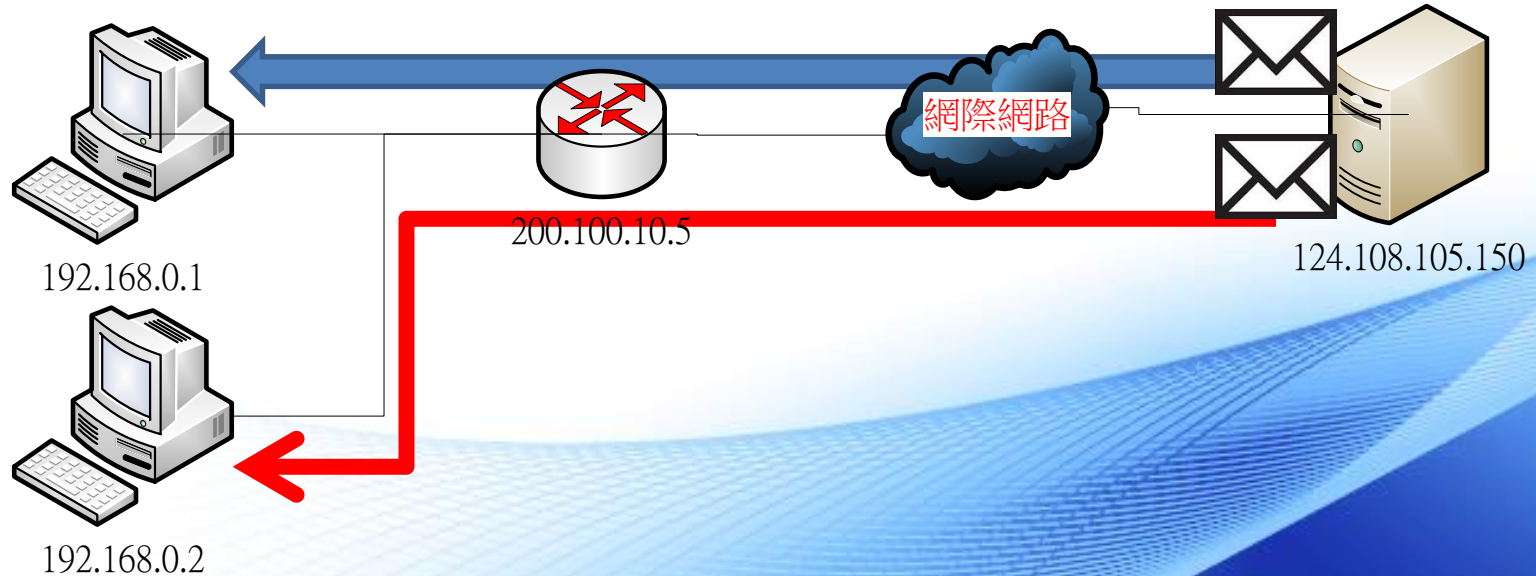


NAPT

- 封包回送時，依據NAT表中的紀錄進行轉換

傳送端IP位址	傳送端通訊埠	目的端IP位址	目的端通訊埠	資料
124.108.105.150	80	200.100.10.5	7001	

傳送端IP位址	傳送端通訊埠	目的端IP位址	目的端通訊埠	資料
200.100.10.5	80	192.168.0.1	1001	

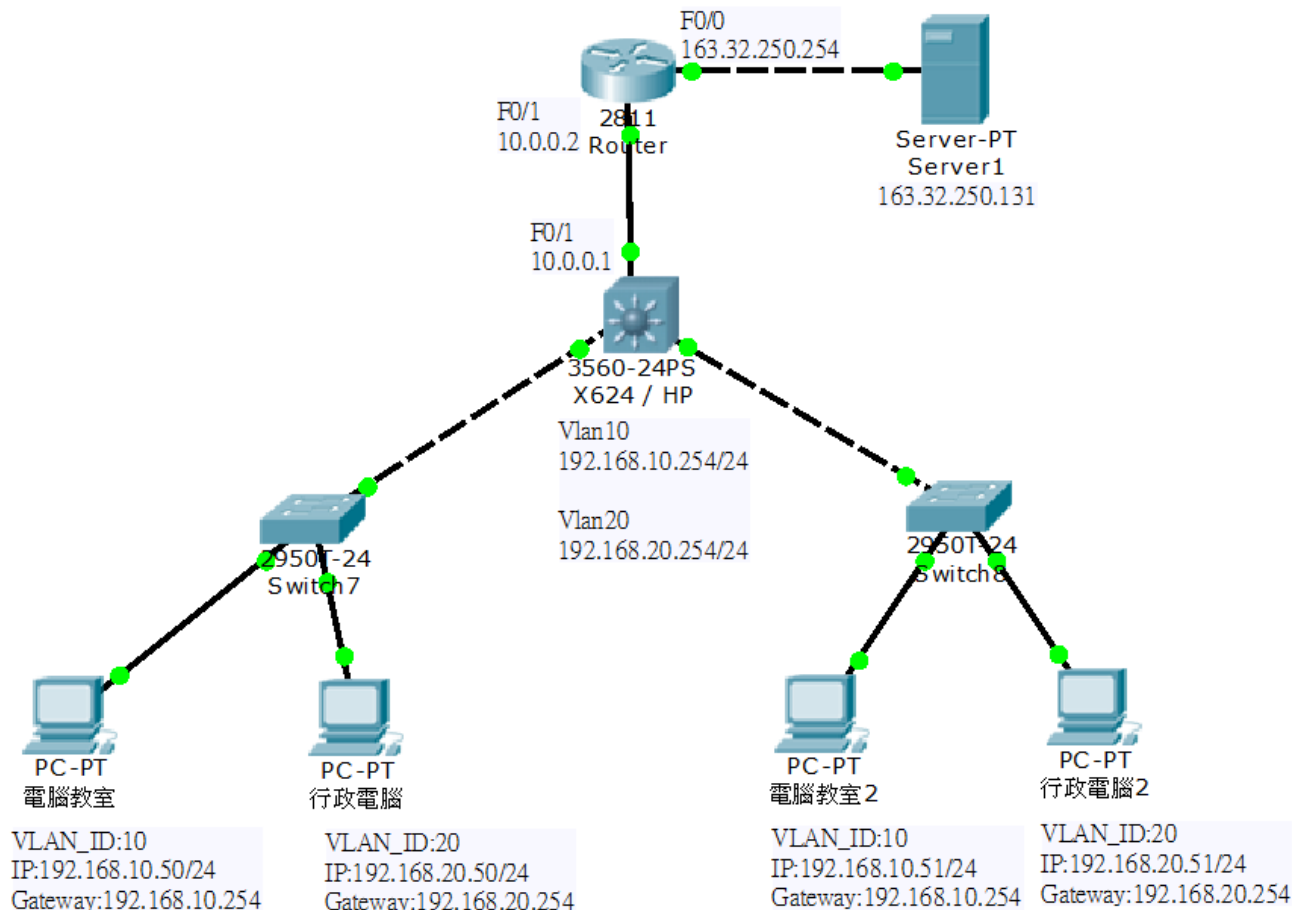


SNAT 與 DNAT

- SNAT (source network address translation)
 - 多台電腦使用一個公用IP上網(例如:電腦教室)
 - 電腦教室電腦訪問外部網站時，會將封包的表頭來源位址替換成要對外的公用IP位址。
- DNAT(destination network address translation)
 - 當有網頁服務需要放置內部網路時，外部使用者想訪問該網站的方法。

SNAT(多對多)

目的:讓192.168.10.0(Vlan10)的電腦，各自帶有163.32.250.10~19範圍內的Public IP連上網路。



SNAT(多對多)

- 指令

- ip nat pool pc1 163.32.250.10 163.32.250.19 netmask 255.255.255.0

- ※指定外部IP pool 的名稱pc1，pool的範圍是 163.32.250.10~163.32.250.19 /24

- access-list 1 permit 192.168.10.0 0.0.0.255

- ※指定內部IP範圍，使用Access-list 1來指定 192.168.10.0/24為內部IP範圍(指令是反向遮罩)

- ip nat inside source list 1 pool pc1

- ※將來源Access-list 1 轉換為Pool pc1

- int fastEthernet 0/1

- ip nat inside

- exit

- Int fastEthernet 0/0

- ip nat inside

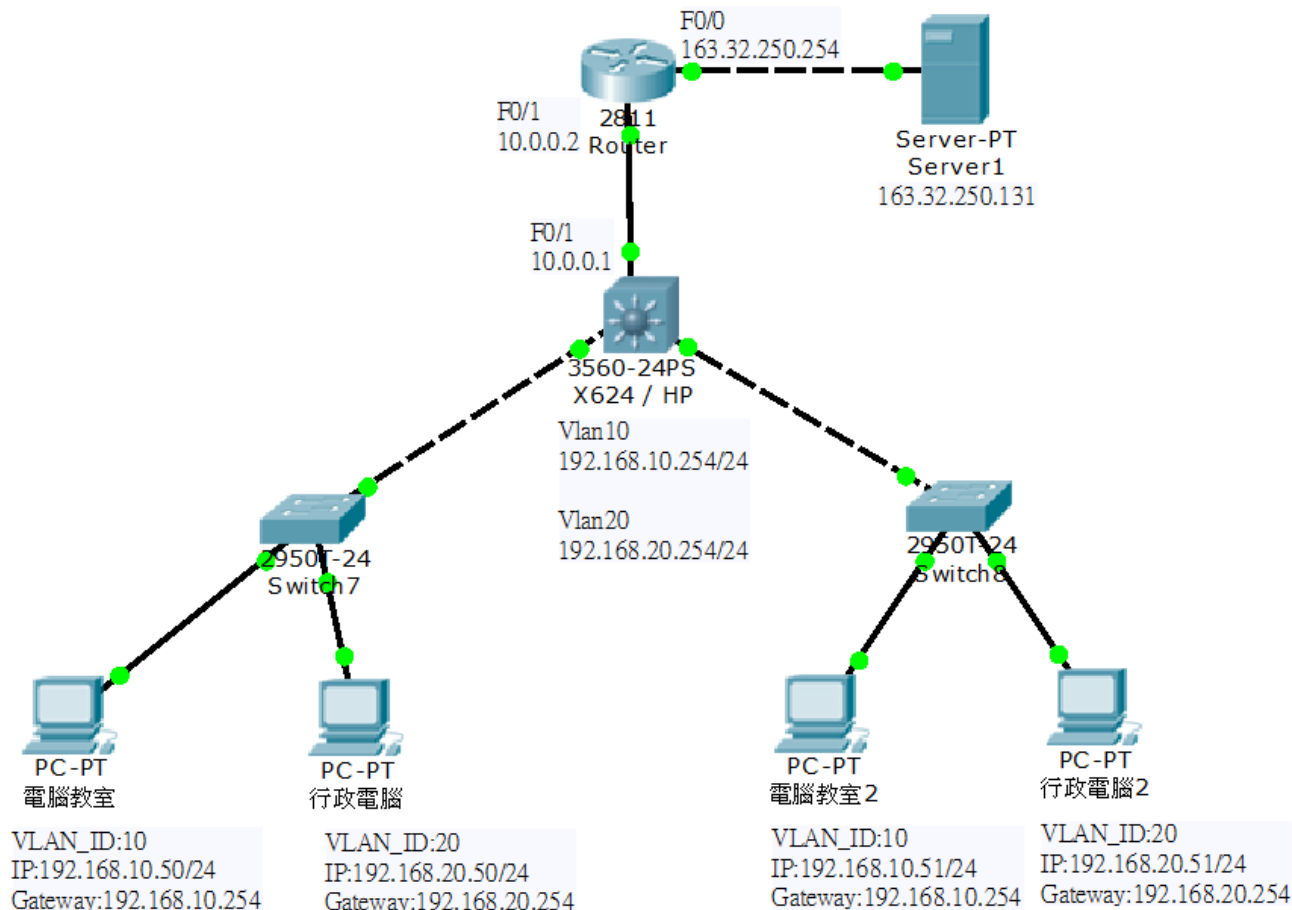
- ※宣告inside與outside範圍

SNAT(多對多)

- 完成上述指令後，可利用VLAN10端的電腦，開啟Web Browser連線至Server後，再開啟Server的Command來打入netstat查看是否如我們目的所進行連線呢？
- 如果想要讓VLAN20端的設備帶有另一段IP上網，可以怎麼做呢？

SNAT(多對一)

目的:讓192.168.10.0(Vlan10)的電腦，帶163.32.250.10的Public IP連上網路。



SNAT(多對一)

- 指令

- ip nat pool pc2 163.32.250.10 163.32.250.10 netmask 255.255.255.0

- ※指定外部IP pool 的名稱pc2，pool的範圍是 163.32.250.10 /24

- Access-list 2 permit 192.168.10.0 0.0.0.255

- ※指定內部IP範圍，使用Access-list 2來指定 192.168.10.0/24為內部IP範圍(指令是反向遮罩)

- Ip nat inside source list 2 pool pc2 **overload**

- ※將來源Access-list 2 轉換為Pool pc2

- int fastEthernet 0/1

- ip nat inside

- exit

- Int fastEthernet 0/0

- ip nat inside

- ※宣告inside與outside範圍

SNAT(多對一)

- 完成上述指令後，可利用VLAN10端的電腦，開啟Web Browser連線至Server後，再開啟Server的Command來打入netstat查看是否如我們目的所進行連線呢？
- 如果想要讓VLAN20端的設備帶有另一個IP上網，可以怎麼做呢？