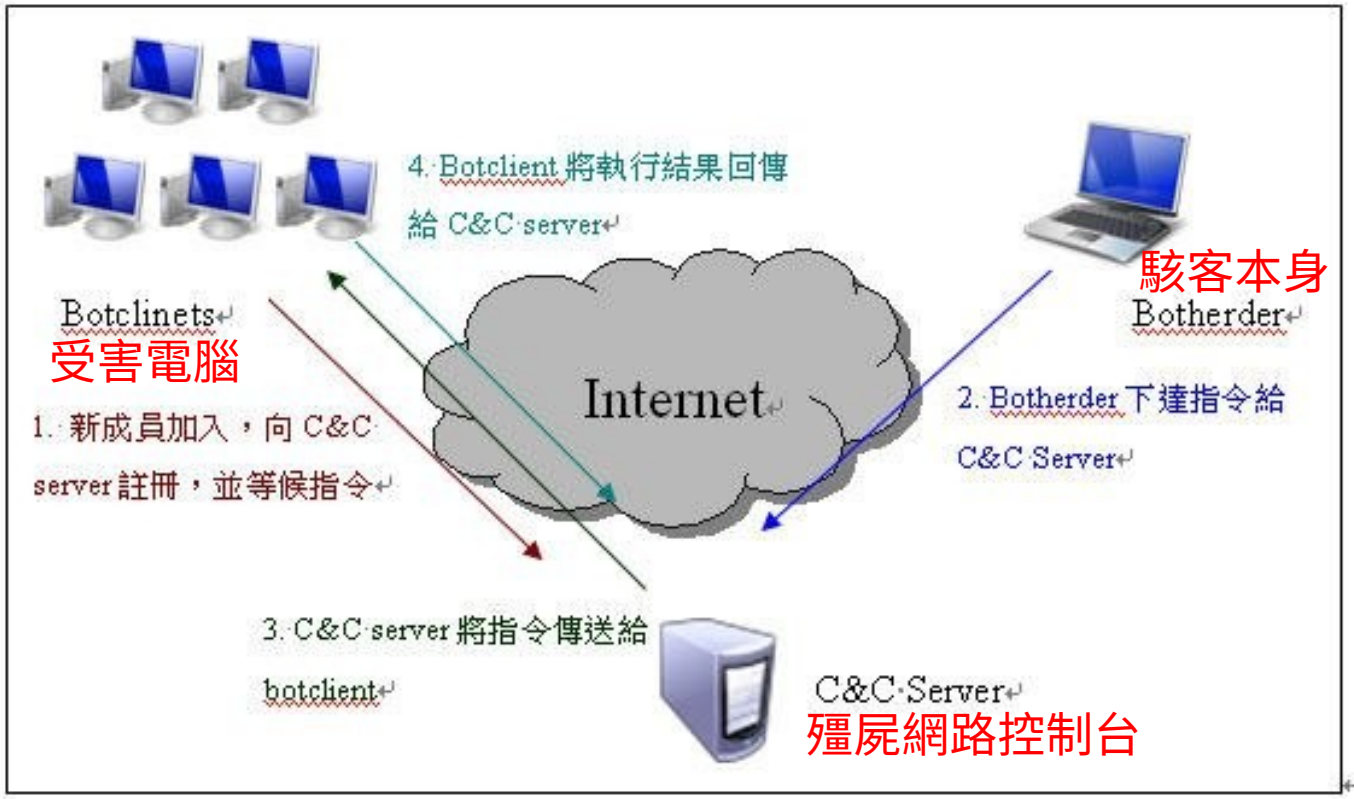
網路基礎班

大綱

- 近期常遇到的資安事件
  - 對外攻擊
    - Bonet
    - ICMP Remote Dos
- 網路層
  - IP(Internet Protocol)
  - 路由 Route
- 傳輸層
  - NAT 網路位址轉換

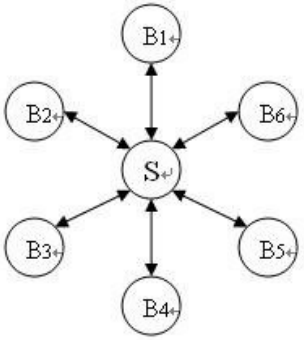
近期常遇到的資安事件

- 殭屍網路 (Bonet)

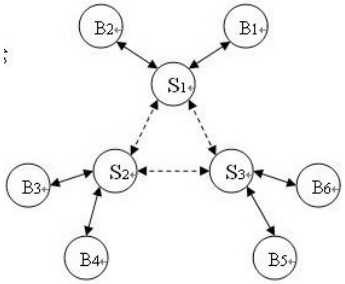


殭屍網路 (Bonet)

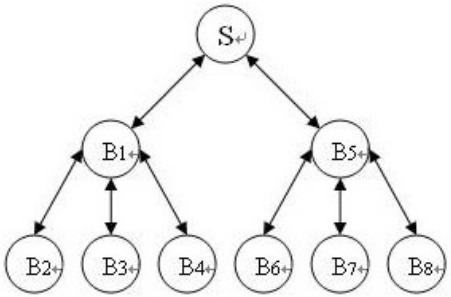
- 拓樸



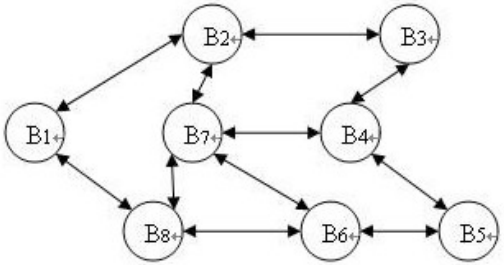
星狀



多重



階層式



隨機式

殭屍網路 (Bonet)- 範例

開始時間	結束時間	名稱	訊息	彙總的事件	攻擊者	攻擊者連接埠	攻擊者 FQ	攻擊者所在	攻擊者所在	目標位址	目標連接埠
1 六月 2011	1 六月 201	utm: HTTP	Botnet: Citadel.Botnet,	1	163.16.	56664		TW	Taiwan	95.173.179.60	80
1 六月 2011	1 六月 201	utm: HTTP	Botnet: Citadel.Botnet,	1	163.16.	56650		TW	Taiwan	95.173.179.60	80
1 六月 2011	1 六月 201	utm: HTTP	Botnet: Citadel.Botnet,	1	163.16.	56625		TW	Taiwan	95.173.179.60	80
1 六月 2011	1 六月 201	utm: HTTP	Botnet: Citadel.Botnet,	1	163.16.	56610		TW	Taiwan	95.173.179.60	80
1 六月 2011	1 六月 201	utm: HTTP	Botnet: Citadel.Botnet,	1	163.16.	56591		TW	Taiwan	95.173.179.60	80
1 六月 2011	1 六月 201	utm: HTTP	Botnet: Citadel.Botnet,	1	163.16.	56563		TW	Taiwan	95.173.179.60	80
1 六月 2011	1 六月 201	utm: HTTP	Botnet: Citadel.Botnet,	1	163.16.	56541		TW	Taiwan	95.173.179.60	80
1 六月 2011	1 六月 201	utm: HTTP	Botnet: Citadel.Botnet,	1	163.16.	56519		TW	Taiwan	95.173.179.60	80
1 六月 2011	1 六月 201	utm: HTTP	Botnet: Citadel.Botnet,	1	163.16.	56499		TW	Taiwan	95.173.179.60	80
1 六月 2011	1 六月 201	utm: HTTP	Botnet: Citadel.Botnet,	1	163.16.	56472		TW	Taiwan	95.173.179.60	80
1 六月 2011	1 六月 201	utm: HTTP	Botnet: Citadel.Botnet,	1	163.16.	56462		TW	Taiwan	95.173.179.60	80

開始時間	結束時間	名稱	訊息	彙總的事件	攻擊者	攻擊者連接埠	攻擊者 FQ	攻擊者所在	攻擊者所在	目標位址	目標連接埠
31 五月 20	31 五月 20	utm: udp	Botnet: Ma	1	163.16.	14176		TW	Taiwan	192.42.119.41	3700(
31 五月 20	31 五月 20	utm: udp	Botnet: Ma	1	163.16.	26826		TW	Taiwan	50.116.56.144	3700(
31 五月 20	31 五月 20	utm: udp	Botnet: Ma	1	163.16.	28281		TW	Taiwan	192.42.119.41	3700(
31 五月 20	31 五月 20	utm: udp	Botnet: Ma	1	163.16.	4031		TW	Taiwan	50.116.56.144	3700(
31 五月 20	31 五月 20	utm: udp	Botnet: Ma	1	163.16.	16682		TW	Taiwan	192.42.119.41	3700(
31 五月 20	31 五月 20	utm: udp	Botnet: Ma	1	163.16.	15514		TW	Taiwan	50.116.56.144	3700(
31 五月 20	31 五月 20	utm: udp	Botnet: Ma	1	163.16.	22249		TW	Taiwan	50.116.56.144	3700(
31 五月 20	31 五月 20	utm: udp	Botnet: Ma	1	163.16.	11819		TW	Taiwan	192.42.119.41	3700(
31 五月 20	31 五月 20	utm: udp	Botnet: Ma	1	163.16.	3249		TW	Taiwan	50.116.56.144	3700(
31 五月 20	31 五月 20	utm: udp	Botnet: Ma	1	163.16.	16377		TW	Taiwan	192.42.119.41	3700(
31 五月 20	31 五月 20	utm: udp	Botnet: Ma	1	163.16.	12676		TW	Taiwan	50.116.56.144	3700(

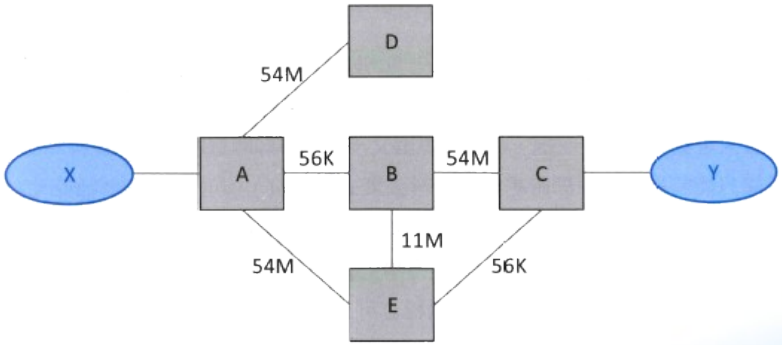
DOS- 阻斷服務攻擊

- DOS(Denial of Service Attack) 阻斷式攻擊，也稱作洪水攻擊
  - 攻擊名

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)

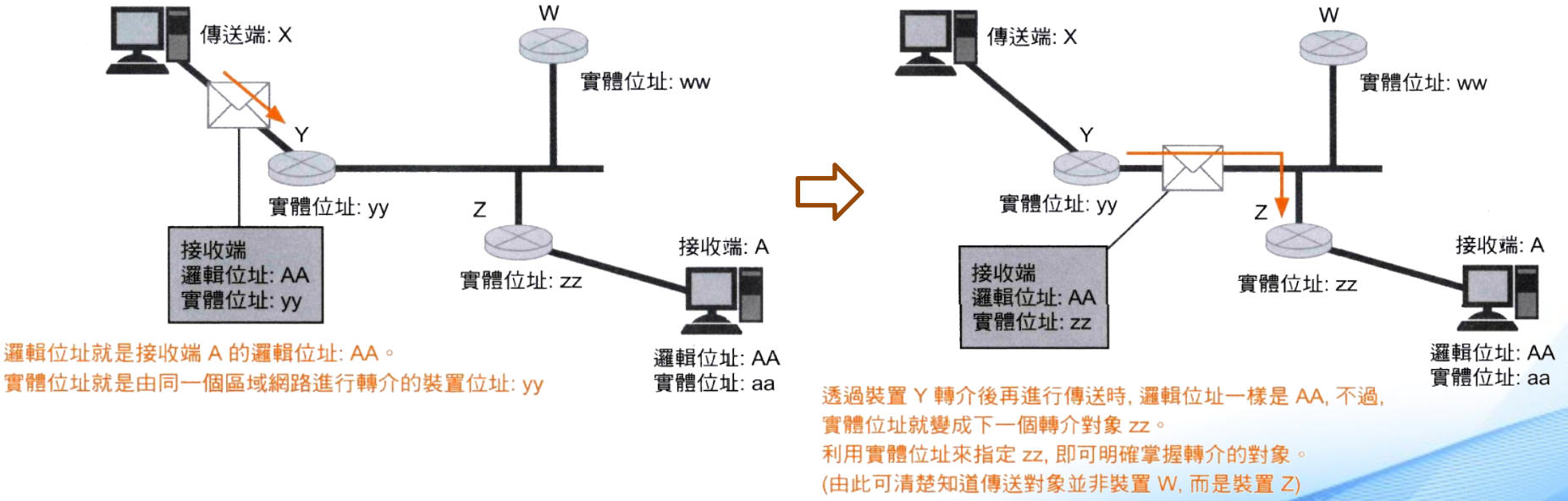
- 網路層做兩件事：
  - 定址 (Addressing) ：決定裝置在網路上的邏輯位址 (IP 位址)
  - 路由 (Routing) ：尋找封包到達目的地的路徑，包括判斷正確路徑及最佳路徑



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



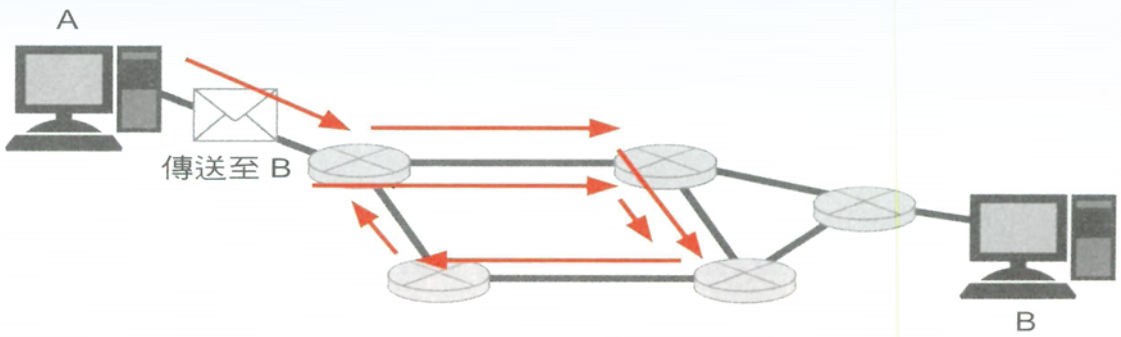
Internet Protocol 封包標頭

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。

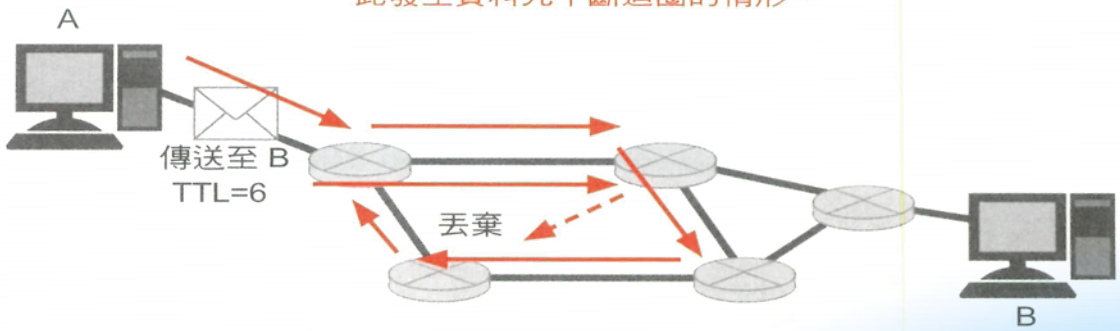
	名稱	位元	說明
1	版本	4	IP 版本
2	標頭長度	4	標頭的長度
3	服務類型	8	封包的優先度/重要度
4	資料長度	16	IP 標頭與資料承載之總長度
5	ID	16	資料元的識別編號
6	旗標 (Flag)	3	判斷是否已經將資料元分割完成
7	分割定位 (Fragment offset)	13	若希望能在分割時回復原始值即可使用本功能
8	TTL	8	封包的存活時間
9	通訊協定	8	指定上層通訊協定
10	標頭檢查碼 (Header Checksum)	16	用來進行 IP 標頭錯誤檢查的代碼
11	傳送端 IP 位址	32	傳送端邏輯位址
12	目的地 IP 位址	32	目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

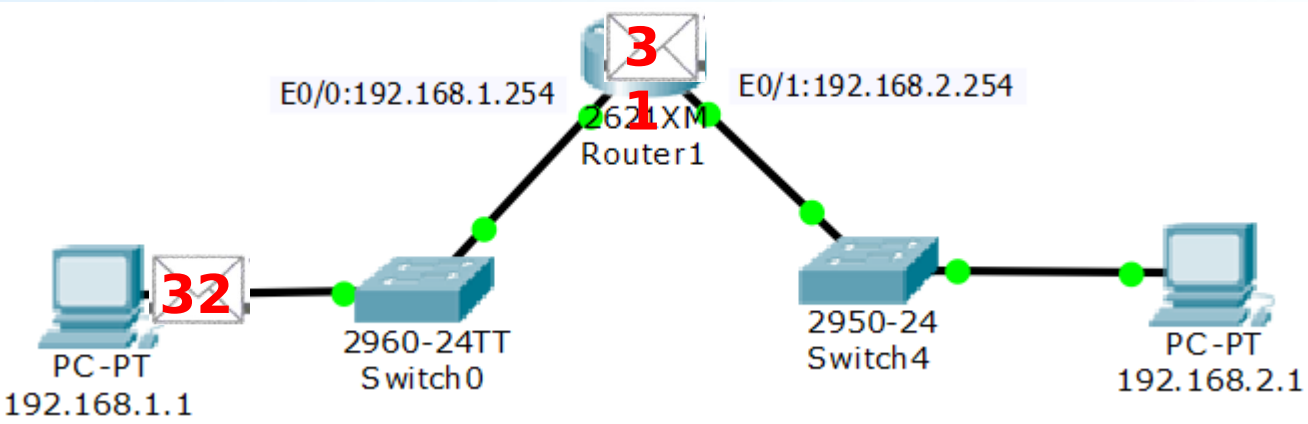


路徑選擇錯誤，而無法到達目的地，因
此發生資料元不斷迴圈的情形。



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)

LAB1-TTL & 封包查看



- Linux 系統的 TTL 值為 64 或 255
- Windows NT/2000/XP 系統的默認 TTL 值為 128
- Win7 系統的 TTL 值是 64
- Windows 98 系統的 TTL 值為 32
- UNIX 主機的 TTL 值為 255

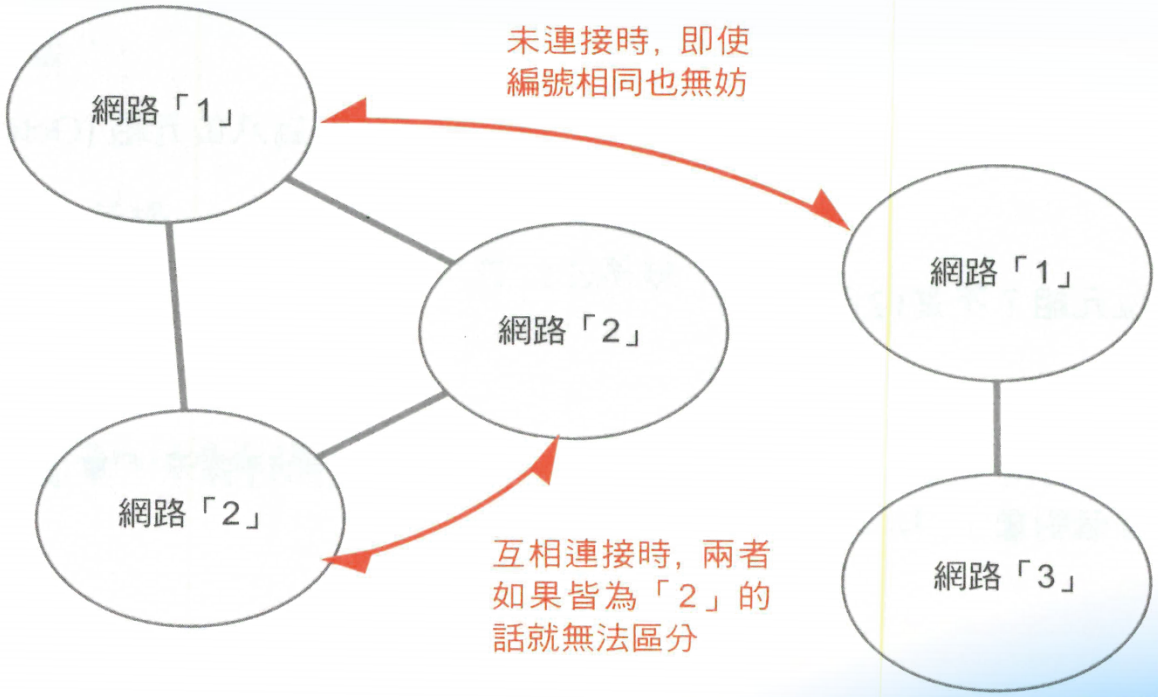
網路邏輯位置 (1/2)

- 即使更換實體網路設備，邏輯位置仍可維持不變
- 由 所屬網路位址 (Network ID) + 主機位址 (Host ID) 所構成，以 IPv4 為例：

- 在設備所連接的整個網路中必須獨一無二
- 由網管人員為各網路節點設定並統一管理
- 所在網路變更時，邏輯位置也會改變

網路邏輯位置 (2/2)

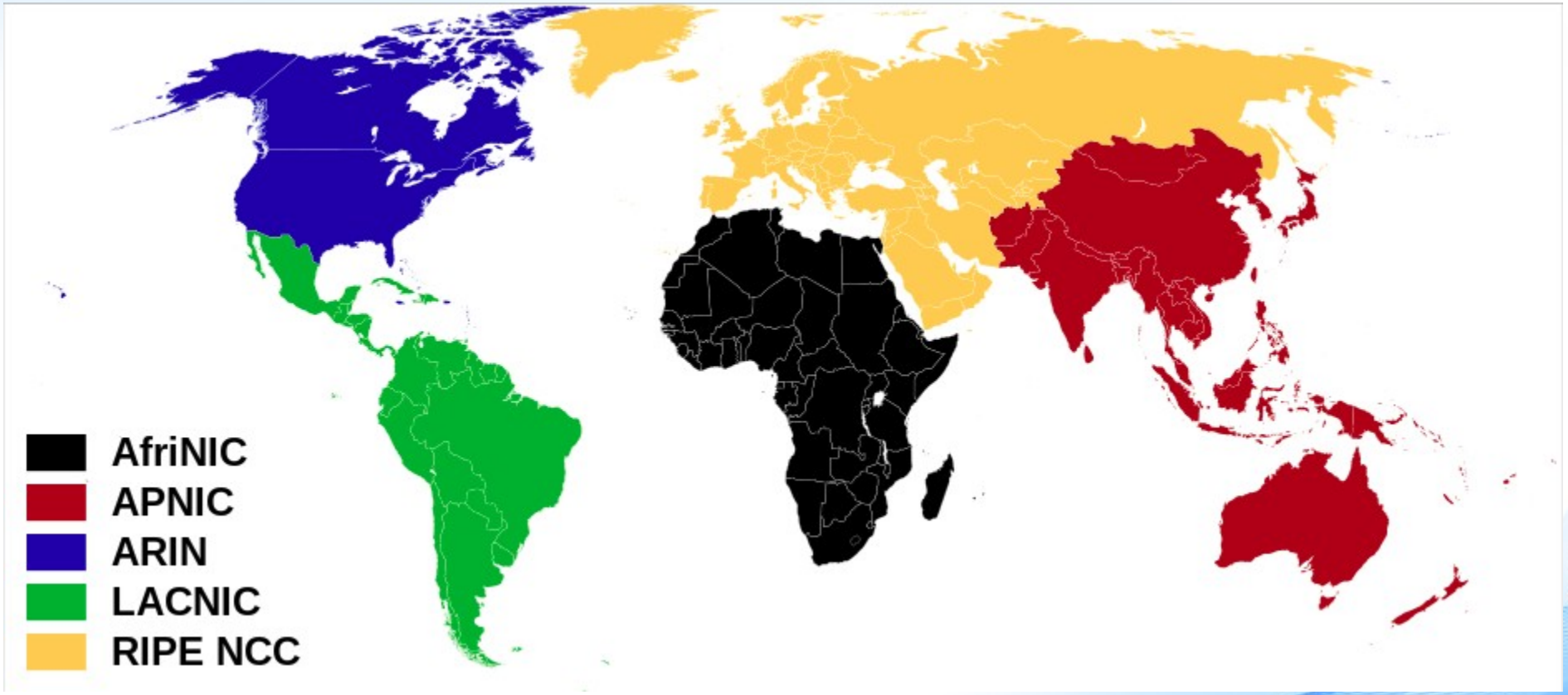
在連接的所有網路中必須是獨一無二的



IP 位址

由 Internet Assigned Numbers Authority (IANA) 分配。 IANA 下又依地域分為五個分支。其中 ARIN ：負責北美； RIPE NCC ：歐洲地區、中亞、俄國、西亞； APNIC ：亞太地區； AFRINIC ：非洲； LACNIC ：中南美洲、加勒比亞海。

- 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
- IP 過去是由 NIC （Network Information Center）負責分配、管理。


AfriNIC
APNIC
ARIN
LACNIC
RIPE NCC

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

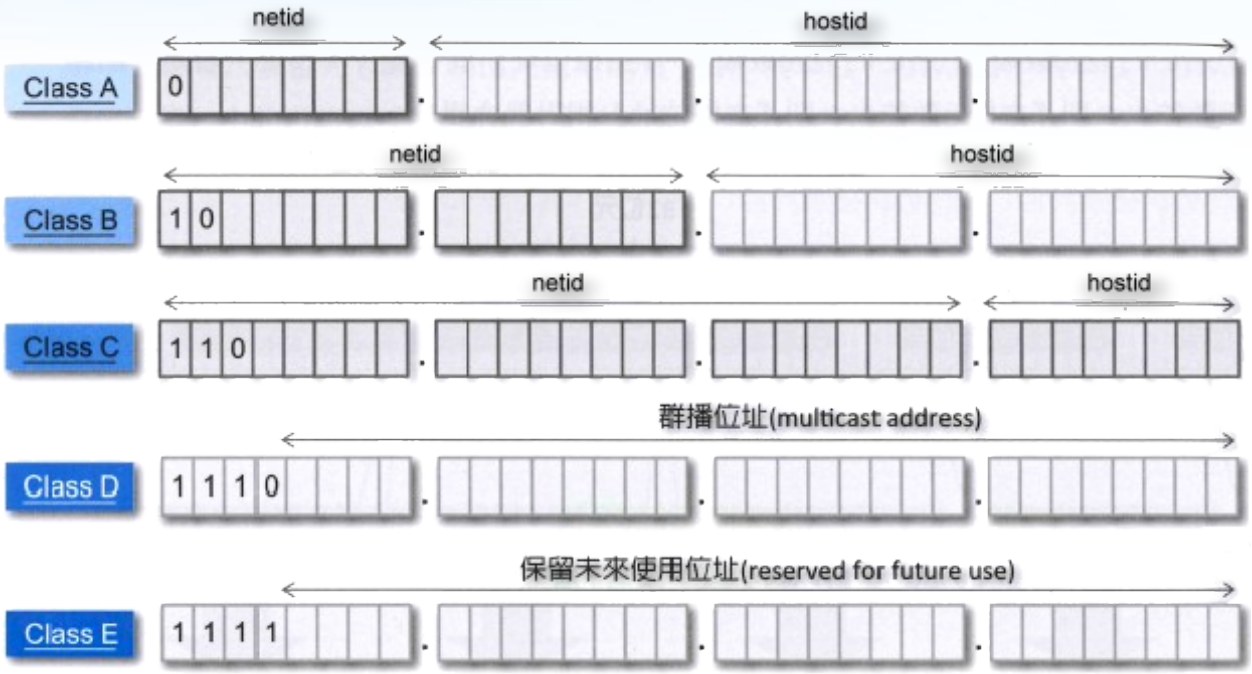
利用位元組來分割資料	11000000	10101000	00101010	00000001
將位元組轉換為 10 進制標示方式	192	168	42	1
插入點即可形成位元組的分隔	192 .	168 .	42 .	1

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)

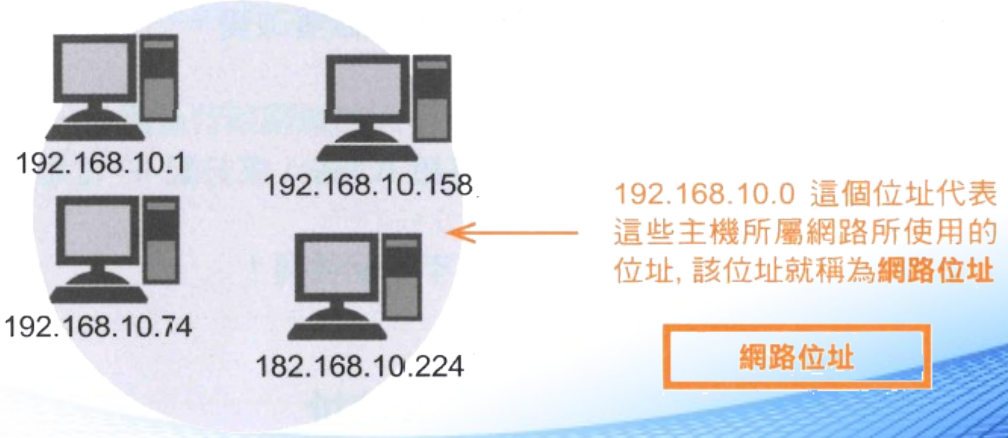
五種分級在十進位的表示：
Class A : 0.0.0.0 ~ 127.255.255.255
Class B : 128.0.0.0 ~ 191.255.255.255
Class C : 192.0.0.0 ~ 223.255.255.255
Class D : 224.0.0.0 ~ 239.255.255.255
Class E : 240.0.0.0 ~ 255.255.255.255

特殊用途的 IP 位址 (1/3)

具有特別的意義, 而且無法真正地被分配給主機的位址

當該網路為等級 C, 而且網路部分為 192.168.10 時

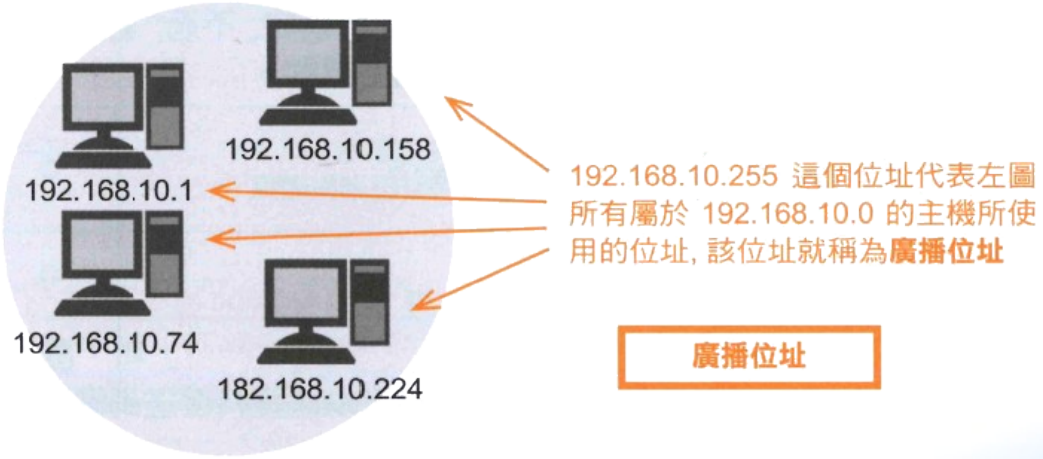
第 1 個八位元組	第 2 個八位元組	第 3 個八位元組	第 4 個八位元組
網路部分			主機部分
11000000	101010000	00001010	00000000
192	168	10	0



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)

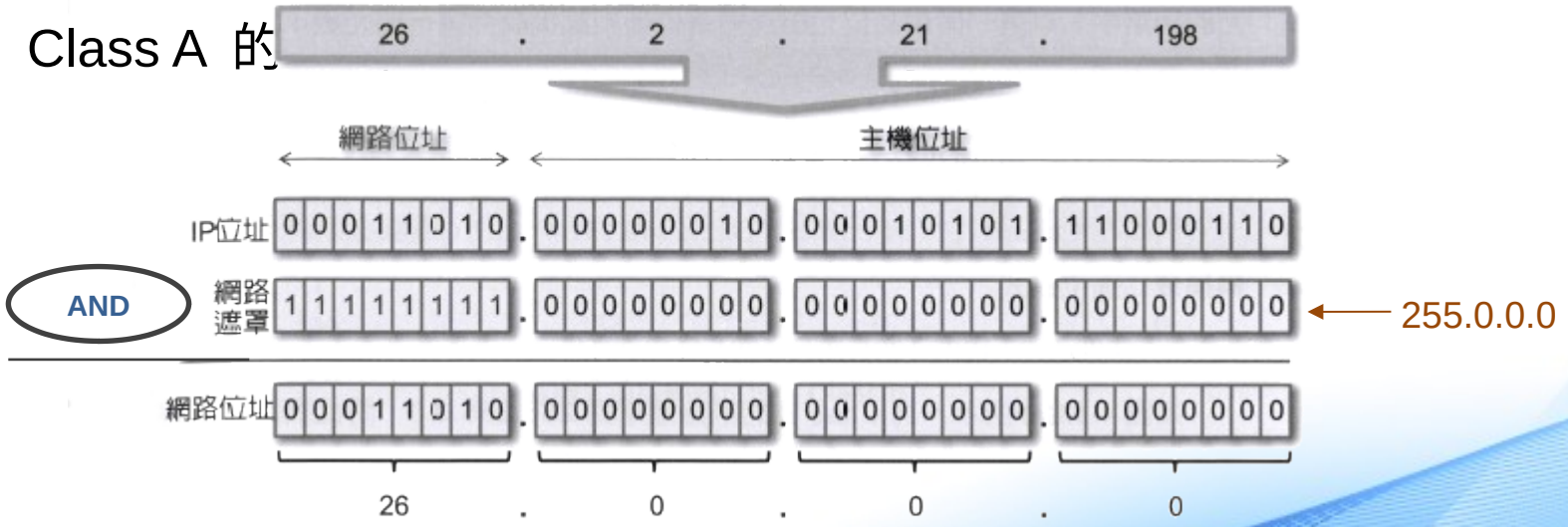
- netid 為 127 的 Class A 位址 (127.0.0.0 ~ 127.255.255.255)：
  代表本機位址 (localhost)，又稱為 loopback 位址，主要是方便使用者對本機的網路進行測試

- 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

網路遮罩 (1/2)

- 電腦不像人類可以用眼睛和大腦判斷出一個 IP 位址屬於哪一個網路，必須搭配 IP 位址與網路遮罩並經過 Bitwise AND 運算才能得到

以 Class A 的



網路遮罩 (2/2)

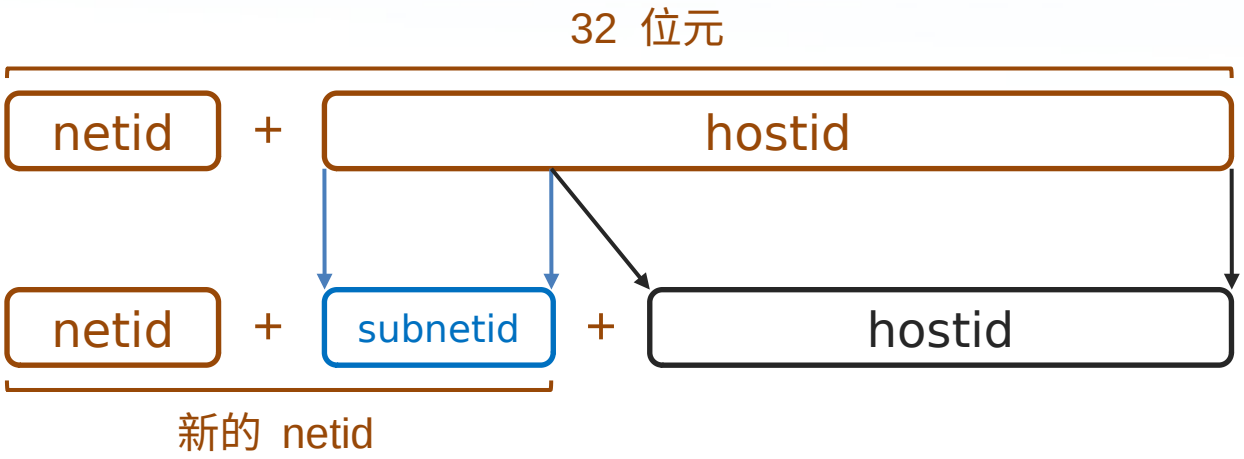
- IPv4 網路遮罩的特性：
  - 與 IPv4 位址長度相同
  - 一定是連續的 1 接連續的 0
  - 連續 1 的數量代表把 IPv4 位址前面多少個位元視為 netid
  - 兩種表示法：
    - 10 進位表示法，例如： 255.255.255.0
    - Bit counts ，例如： /24

子網路切割 (1/2)

- 當一個企業或機關單位申請到一段較大的網路時 (例如 Class A 或 B) ，如果把所有的主機都接在同一段網路中，將會造成一些問題，例如：
  - 若有其中一台主機中毒亂發封包癱瘓整個網路，想要追查到這台主機將會很困難
  - 如果同時有很多主機在發送廣播封包時會影響網路效能
  - 某些部門經常要透過網路傳輸大量資料時，會影響到其他正常使用者

子網路切割 (2/2)

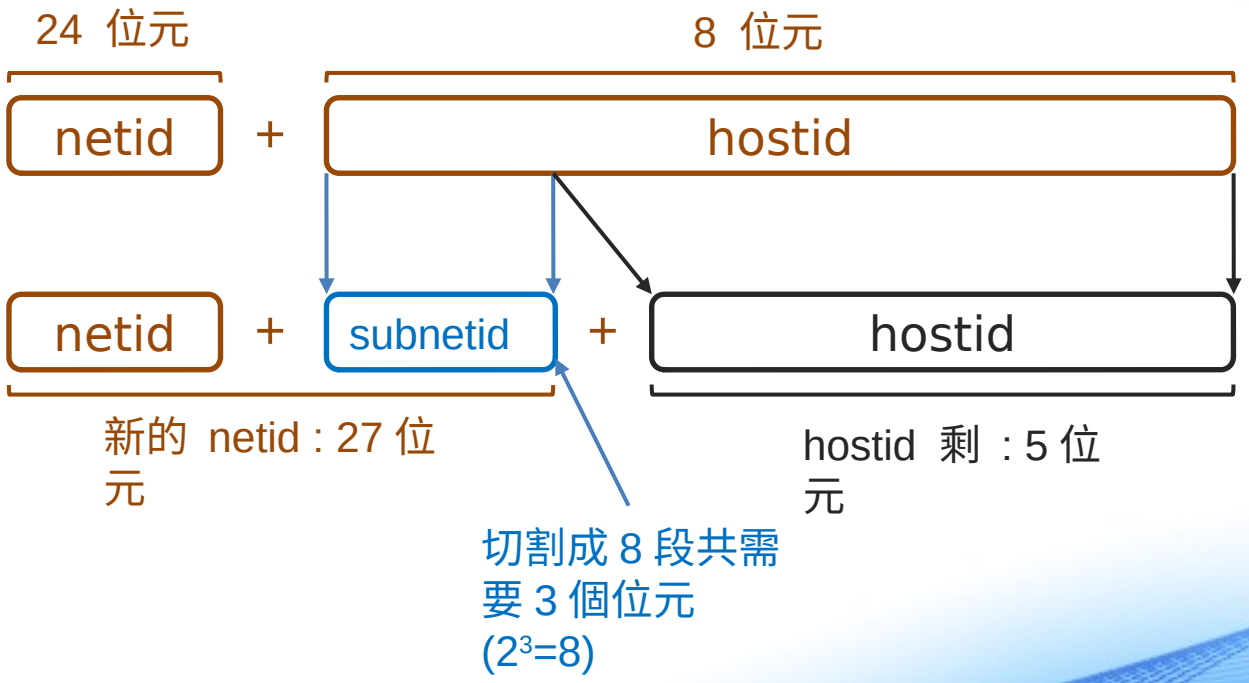
- 以 IPv4 為例，把一個較大的網路切割成數個較小的子網路：



給予 subnetid 的位元數決定了子網路的數量
而剩下 hostid 的位元數決定每個子網路的主機數量

子網路切割範例 (1/3)

- 假設某機關申請得到一段 163.32.166.0/24 的網段，網管想要把網段均勻切割成 8 個子網路給各部門使用：



子網路切割範例 (2/3)

- 假設某機關申請得到一段 163.32.166.0/24 的網段，網管想要把網段均勻切割成 8 個子網路給各部門使用：

只看最後 8 位元的狀況：

	subnetid			hostid	
Subnet 1	0	0	0		範圍：00000000 ~ 00011111 (0~31)
Subnet 2	0	0	1		範圍：00100000 ~ 00111111 (32~63)
Subnet 3	0	1	0		範圍：01000000 ~ 01011111 (64~95)
⋮					⋮
Subnet 8	1	1	1		範圍：11100000 ~ 11111111 (224~255)

子網路切割範例 (3/3)

- 假設某機關申請得到一段 163.32.166.0/24 的網段，網管想要把網段均勻切割成 8 個子網路給各部門使用：

表示 8 個子網路：

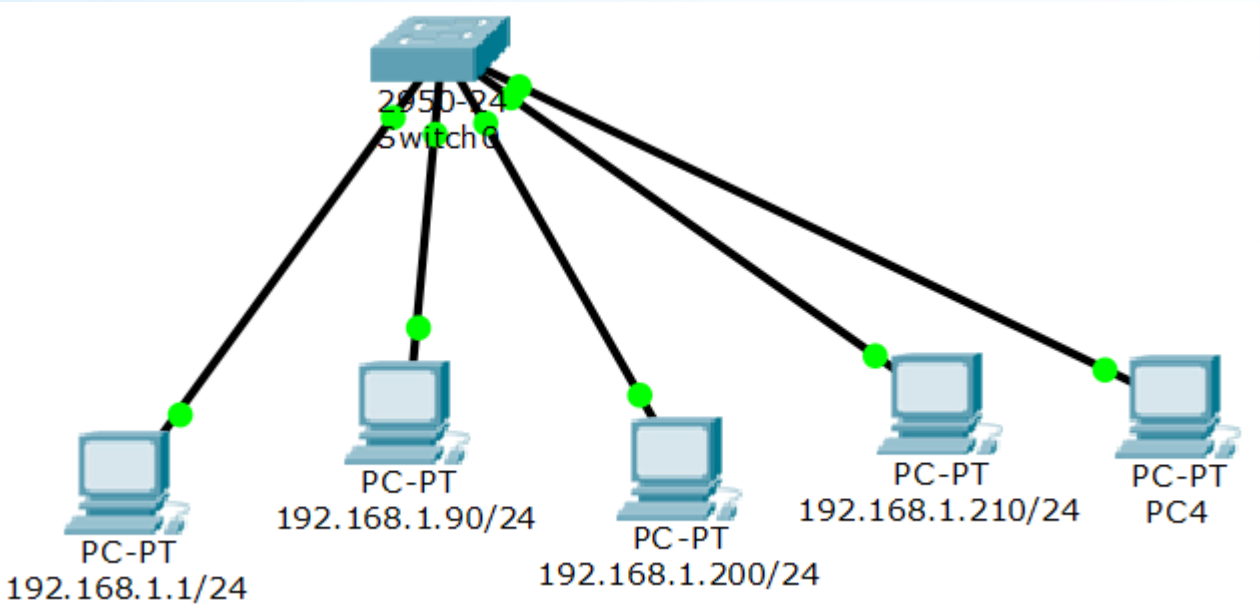
子網路編號	表示法	IP 位址範圍	可用 IP 數量
1	163.32.166.0/27	163.32.166.0 ~ 31	30
2	163.32.166.32/27	163.32.166.32 ~ 63	30
3	163.32.166.64/27	163.32.166.64 ~ 95	30
4			
⋮			
8	163.32.166.224/27	163.32.166.224~255	30

子網路切割練習

- 假設某機關申請得到一段 163.16.100.0/24 的網段，各部門至少有 30 台主機，也就是每個部門至少要給 32 個可用 IP ，若使用均勻切割的方式，該網段可以分給幾個部門使用？列出你的子網路規劃

子網路編號	表示法	IP 位址範圍	可用 IP 數量

LAB 2 – 子網路分割



- 利用 Ping 來試看看子網路在切割後的狀況 (EX:192.168.1.1 Ping -> 192.168.1.90 or 192.168.1.200)

- 如果將 PC4 設定為 192.168.1.220/25 會有哪些狀況？

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

查看 PC 中的路由表

- Windows 10
  - Cmd 中

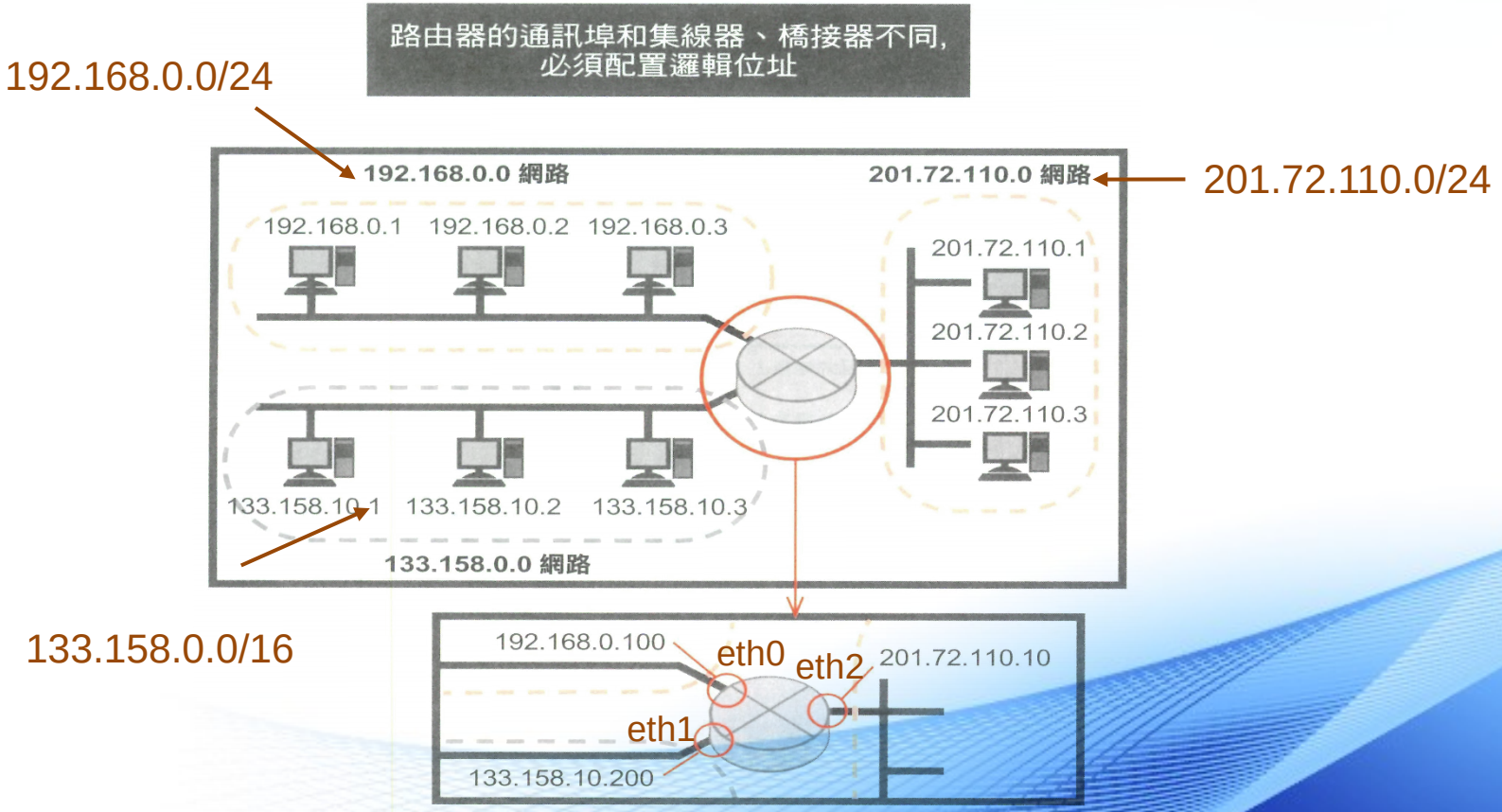
    >route print
  - Power Shell

    >get-netroute -addressfamily IPv4
- Linux

  $ ip -6 route show

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

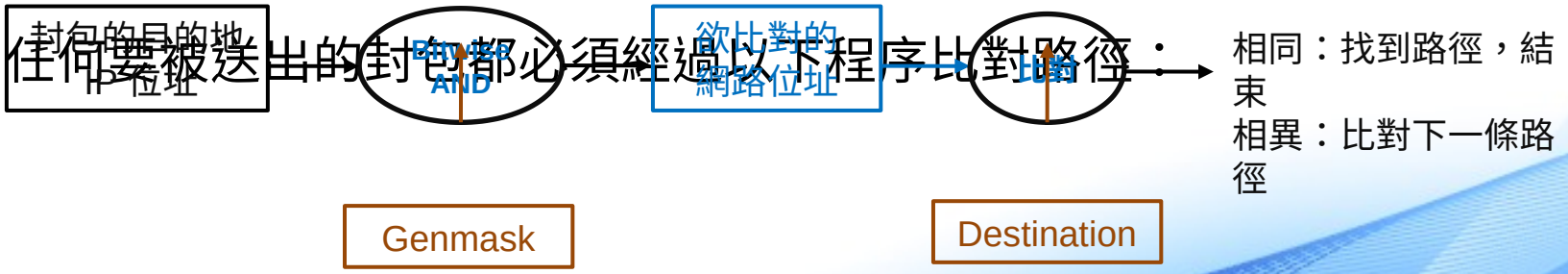
- 路由表的每一筆路徑基本上會包括以下五個項目：
  - 目的地網路 (Network Destination)：
    目的地網路的網路位址
  - 網路遮罩 (Genmask)：
    用於計算目的位址屬於哪個網路
  - 閘道 (Gateway)：
    表示要到達的目的地網路是透過哪個「閘門」過去，如果此項目有顯示 IP 的話，表示該路由需要經過路由器的幫忙才能夠傳送出去，如果顯示 * 或 0.0.0.0 表示該路由是直接由本機傳送
  - 介面 (Interface)：
    代表要到達的目的地網路是經由本機的哪個實體介面出去
  - 計量 (Metric)：
    代表到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

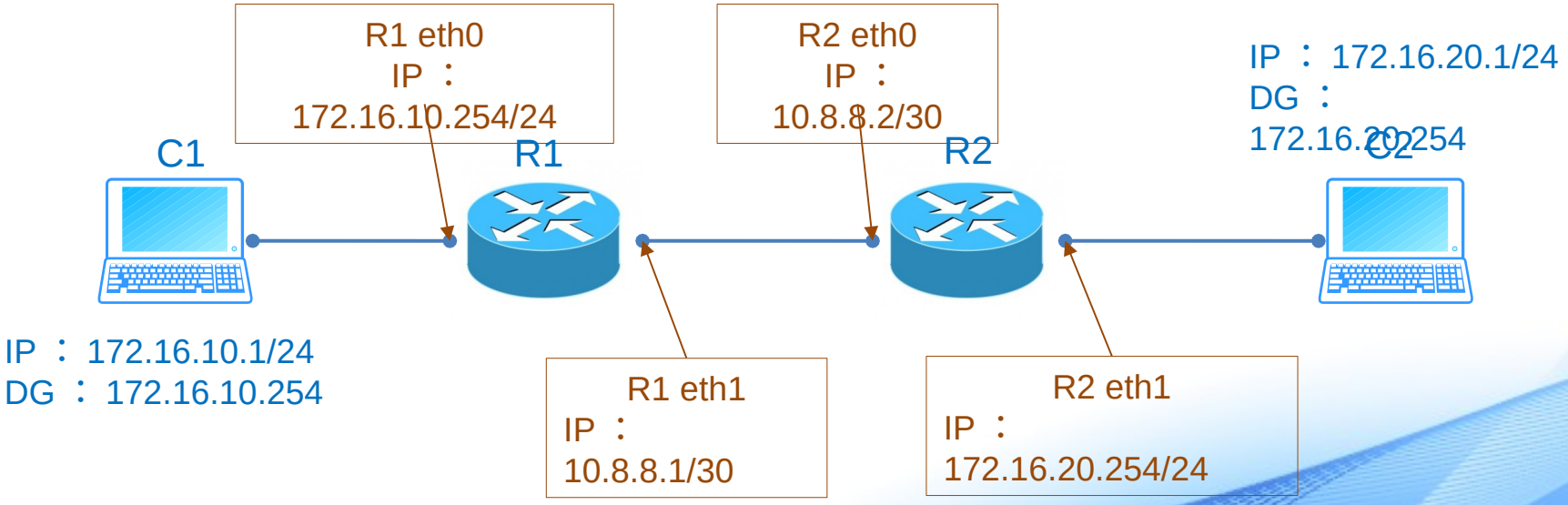
Destination	Gateway	Genmask	Iface
192.168.0.0	0.0.0.0	255.255.255.0	eth0
133.158.0.0	0.0.0.0	255.255.0.0	eth1
201.72.110.0	0.0.0.0	255.255.255.0	eth2

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：

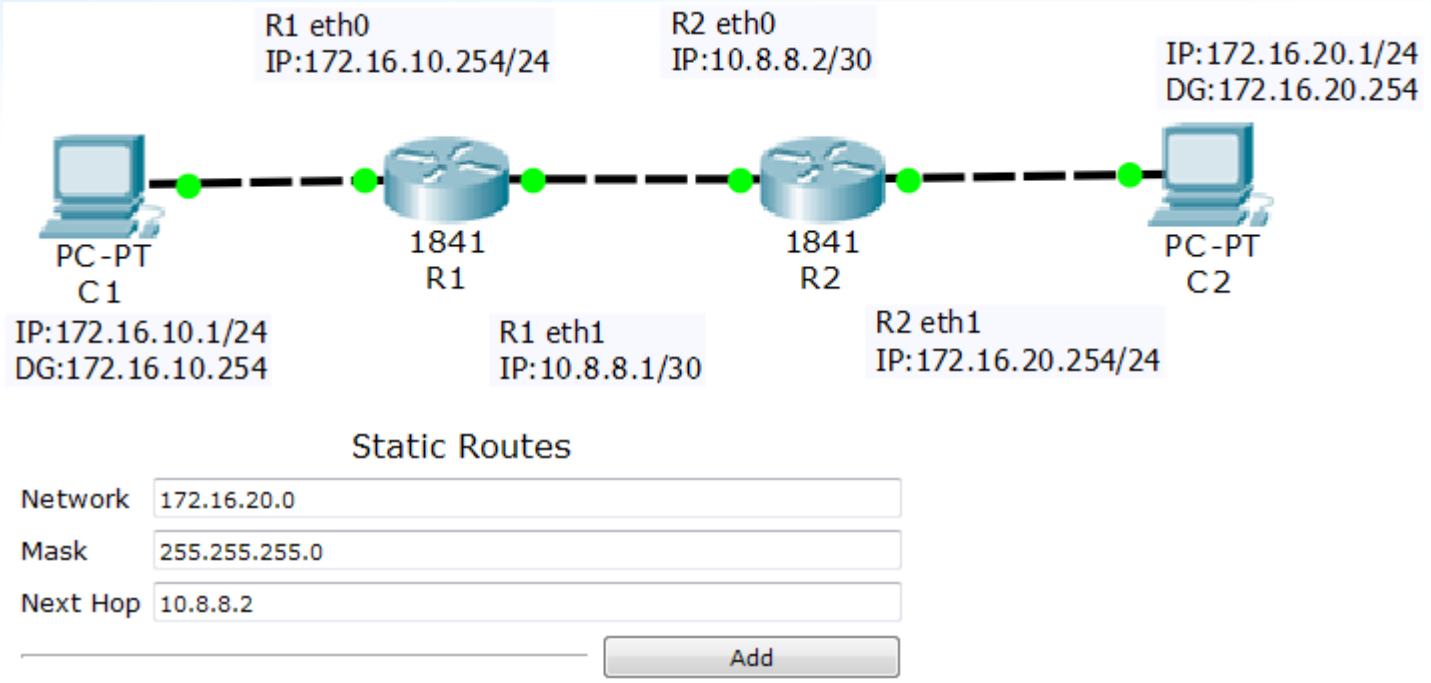
Destination	Gateway	Genmask	Iface
172.16.10.0	0.0.0.0	255.255.255.0	eth0
10.8.8.0	0.0.0.0	255.255.255.252	eth1

- 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

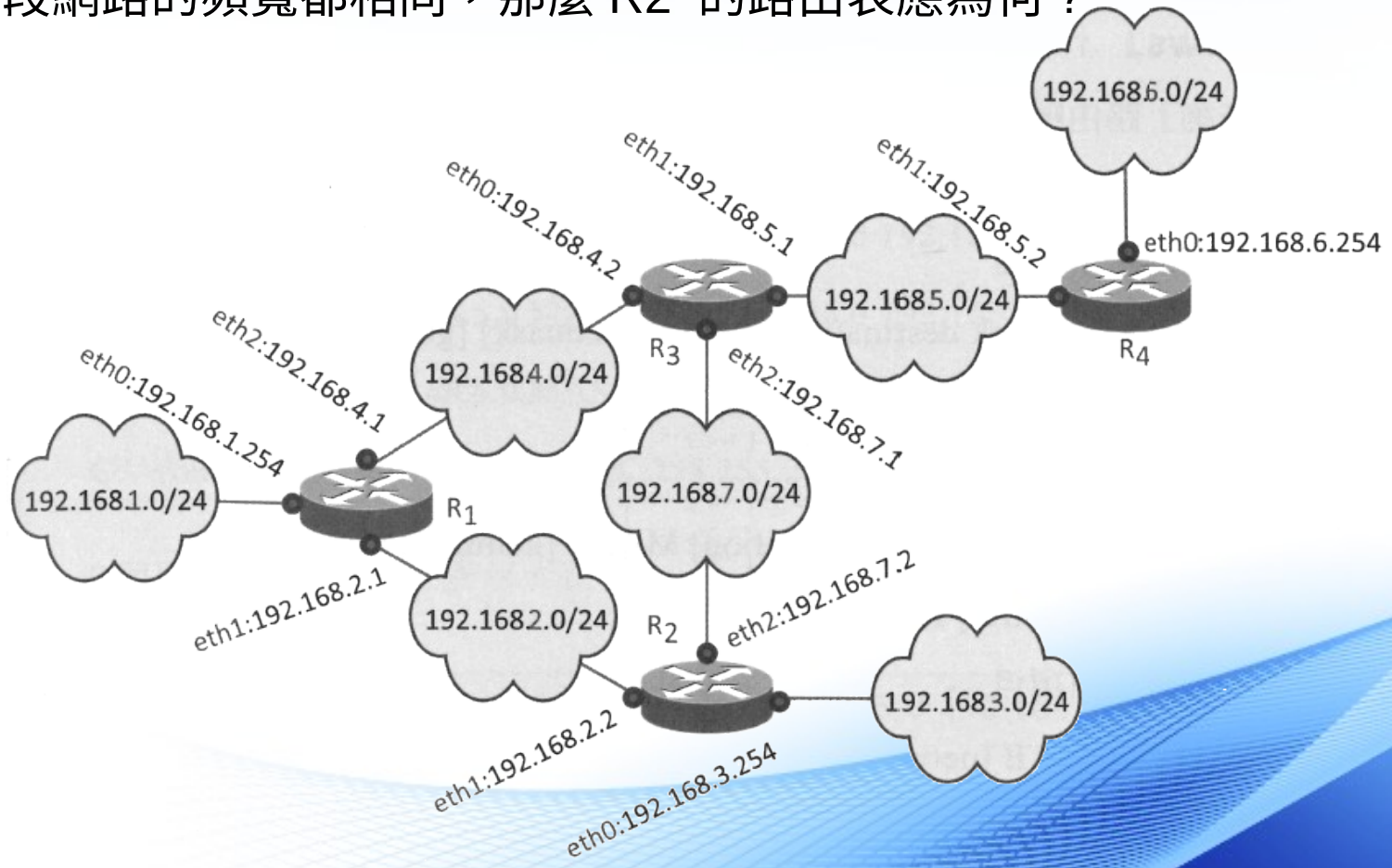
LAB 3- 路由表範例練習



- 在未設定路由表前，利用 C1 Ping 到 C2 會有甚麼訊息呢？
- 如果在設定後是否真的如我們所說的可以 Ping 的到呢？

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

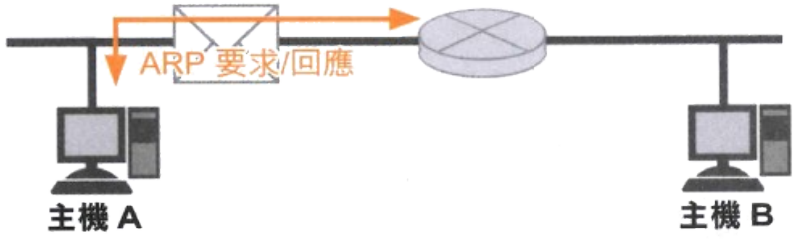
預設閘道 (Default Gateway)

- 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

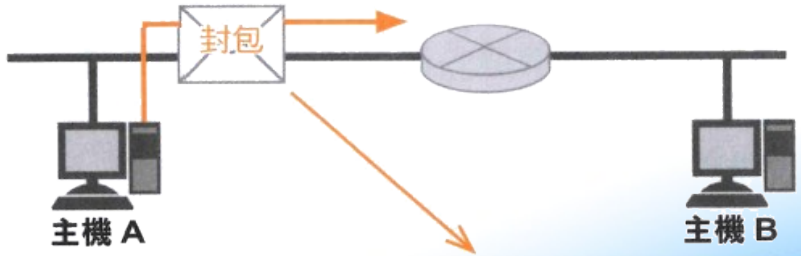
透過預設閘道的封包傳輸 (1/2)

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



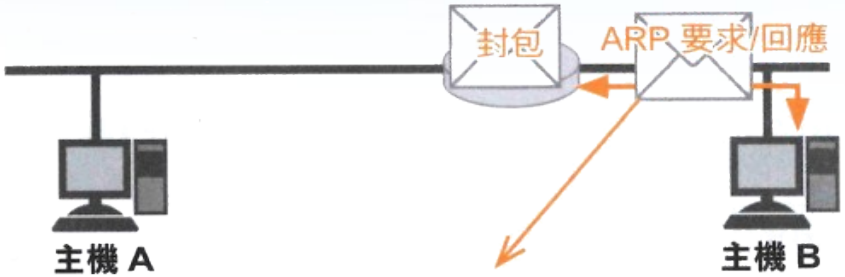
② 主機會將目的地 MAC 位址傳送到預設閘道，並且將目的地 IP 位址當作目的地主機來傳送封包



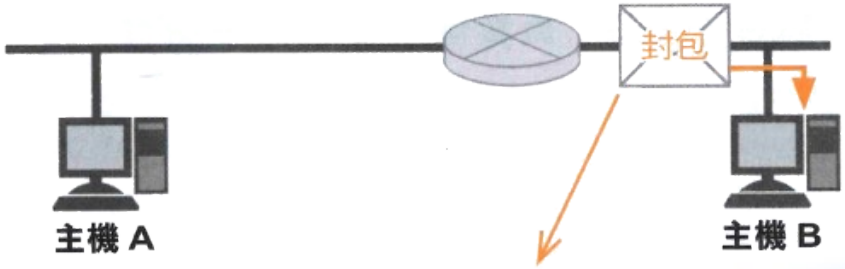
目的地MAC	傳送端MAC	傳送端IP	目的地IP	承載資料 (Payload)
路由器	主機A	主機A	主機B	

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)

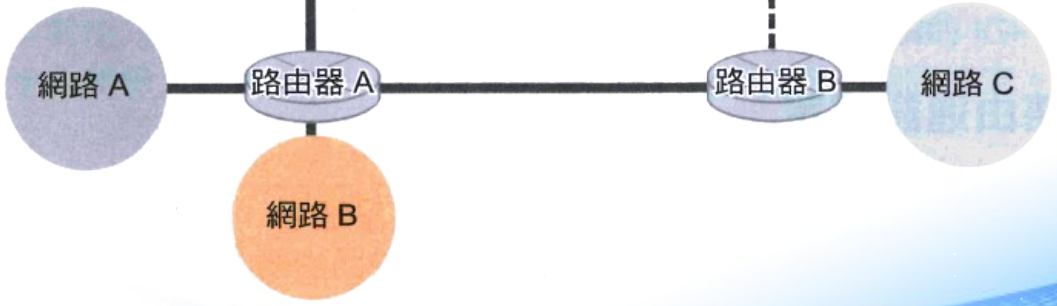
- 透過路由通訊協定 (Routing Protocol) 與相鄰路由器交換網路資訊，並更新自己的路由表，藉此學習到整個網路的路徑資訊，常見的路由通訊協定： RIP 、 OSPF

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

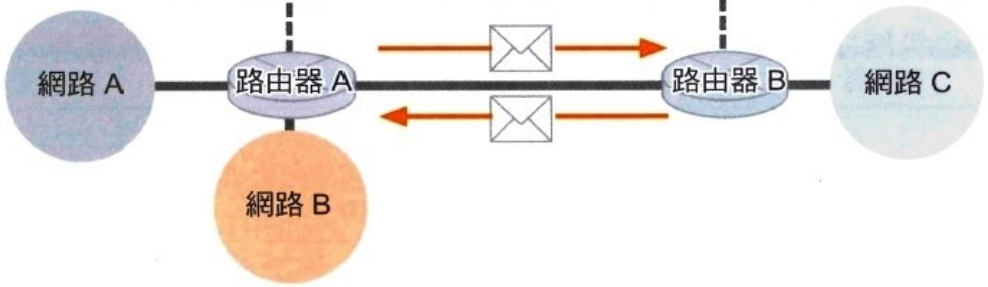


動態路由 (2/2)

② 使用路由通訊協定, 以互相交換所擁有的網路資訊

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



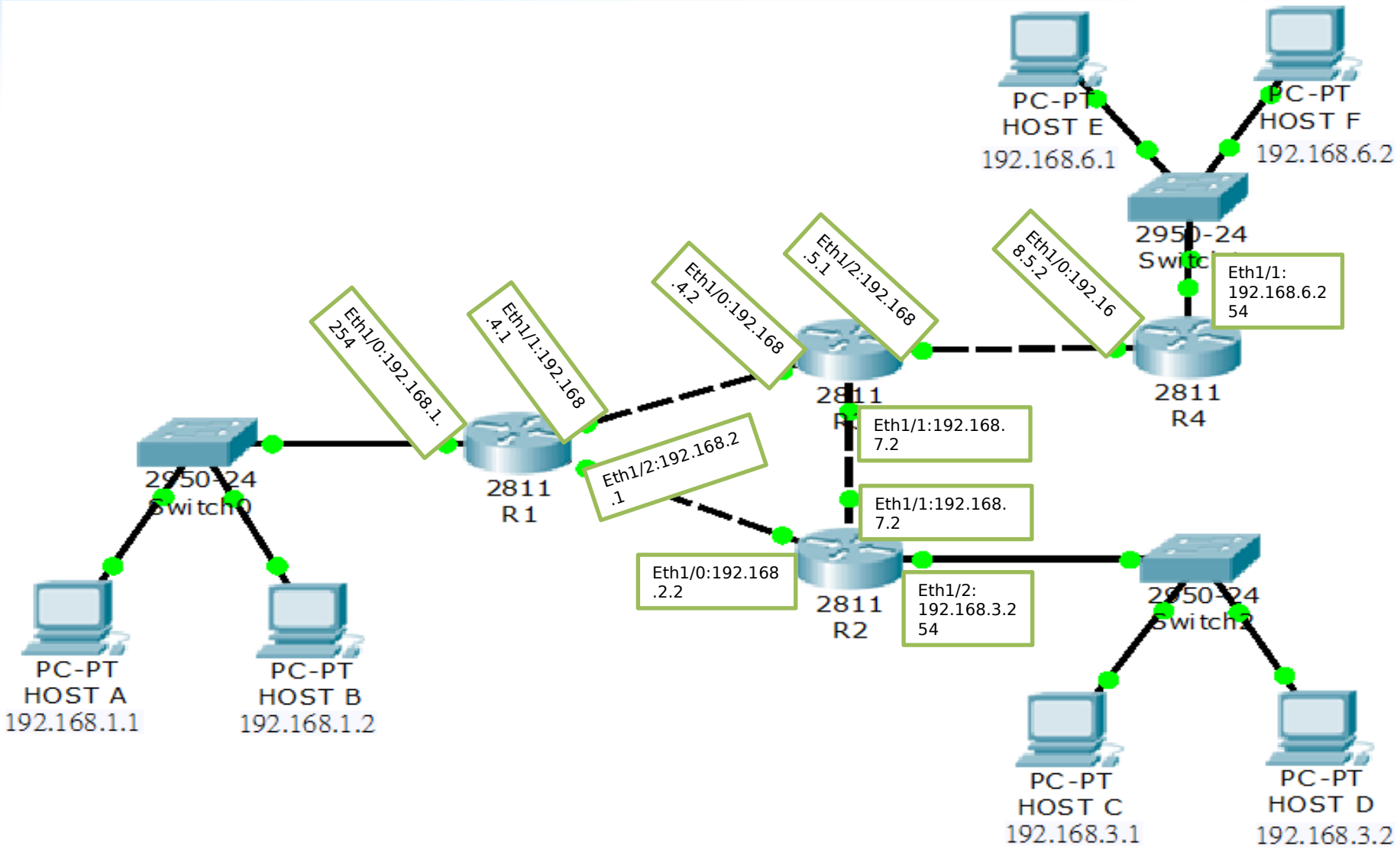
③ 使用交換後的資訊來更新路由資料表

網路	下一個路由器	距離
A	-	0
B	-	0
C	路由器B	1

網路	下一個路由器	距離
A	路由器A	1
B	路由器A	1
C	-	0

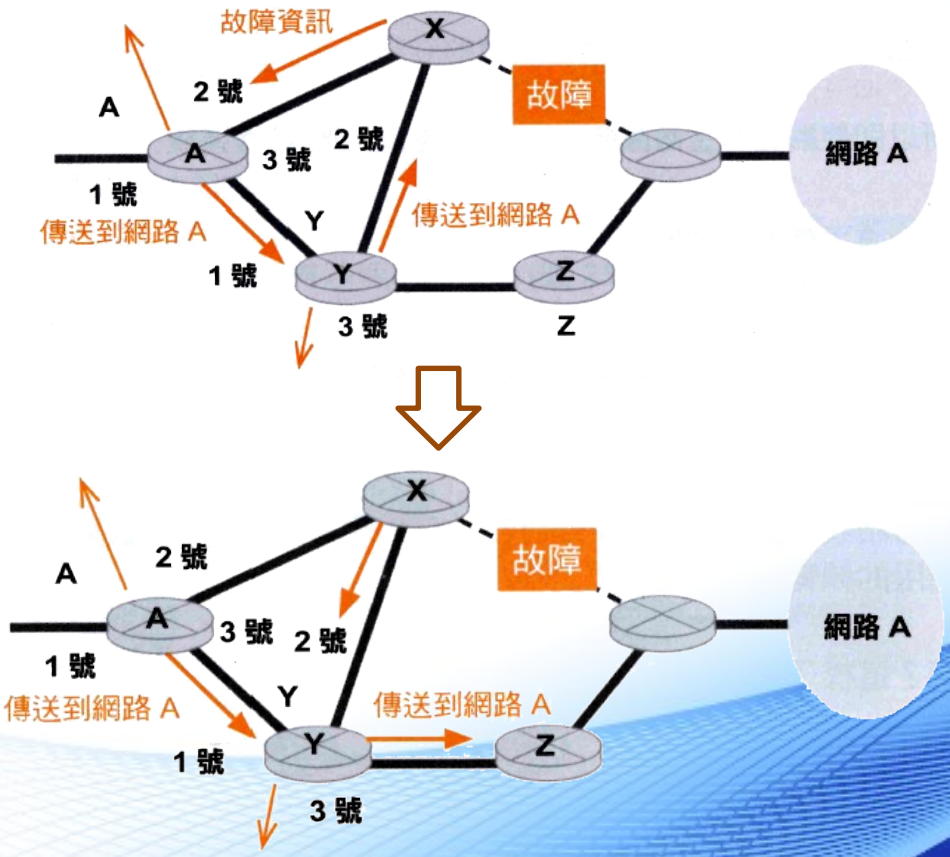
傳送對象是誰(哪一台路由器)？
傳送時間點為何？ → 路由通訊協定
傳送資訊的內容為何？
是否已經決定好接收資訊的最佳路徑了呢？

LAB 4- 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



Layer 4

傳輸層

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

傳輸層負責做啥？(1/3)

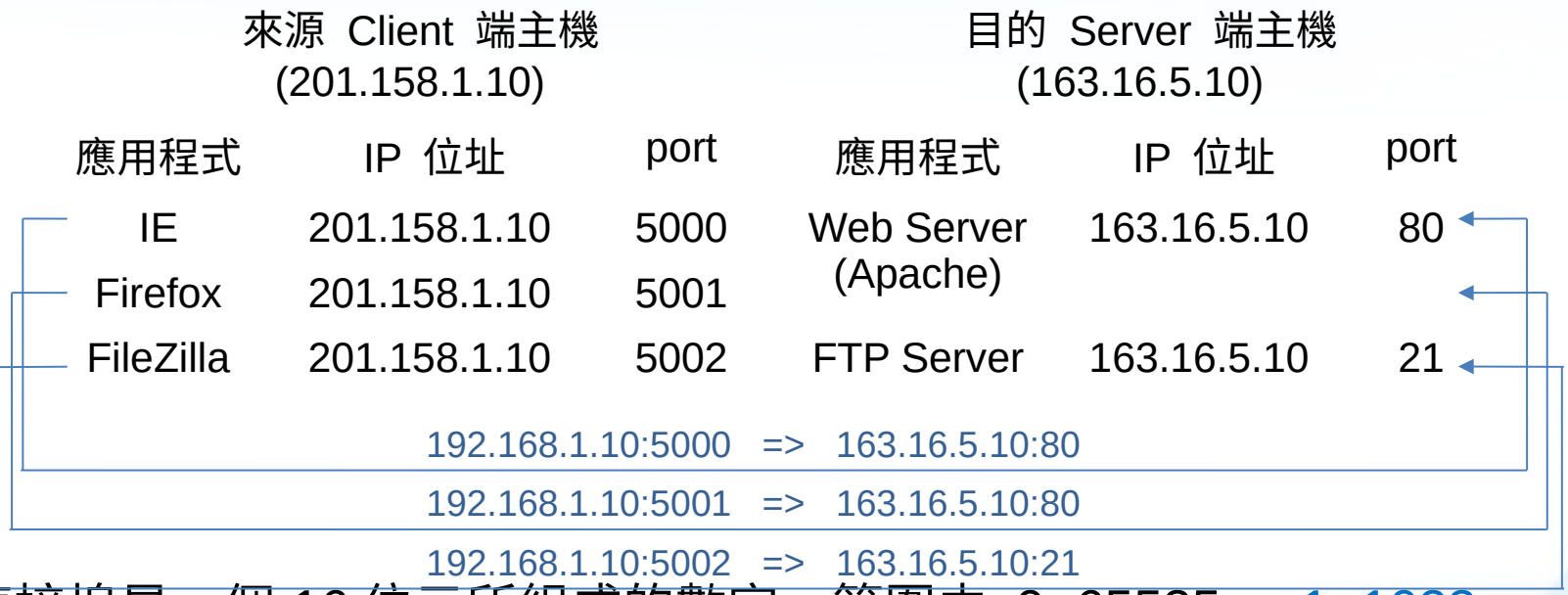
- 資料鏈結層 (Layer 2)：讓相同區域網路中的點對點互相連接
  網路層 (Layer 3)：讓不同邏輯網路彼此互相連接
  傳輸層 (Layer 4)：讓不同主機的程序彼此互相連接

- 傳輸層使用了連接埠 (port) 的概念來區別一台主機之中的網路服務，並達到網路連線的多工處理
  - 如果沒有傳輸層的網路通訊情形：

來源 Client 端主機 (201.158.1.10)		目的 Server 端主機 (163.16.5.10)	
應用程式	IP 位址	應用程式	IP 位址
IE	201.158.1.10	Web Server (Apache)	163.16.5.10
Firefox	?		
FileZilla	?	FTP Server	?

傳輸層負責做啥？(2/3)

– 具備傳輸層的網路通訊情形：



- 連接埠是一個 16 位元所組成的數字，範圍由 0~65535，1~1023 被稱為公認埠 (Well-known Port)，Client 端可隨機使用 1024 以後的埠號

傳輸層負責做啥？(3/3)

- 傳輸層使用 TCP (Transmission Control Protocol) 與 UDP (User Datagram Protocol) 兩大主要協定，提供對網路傳輸的可靠與效率上的取捨
- TCP 是一個可靠的通訊協定，傳送端送出封包後會等待接收端確認是否正確收到，也因此傳輸上較沒效率
- TCP 具有流量控制的能力，能夠協調雙方的封包傳送速度，以避免因大量封包湧入造成主機無法及時處理的狀況下丟棄封包
- UDP 不具上述 TCP 的功能，它是個不可靠的通訊協定，但是相對傳輸上較有效率

常見的公認埠

服務名稱	連接埠號	傳輸協定
FTP (File Transfer Protocol) Data	20	TCP
FTP Control	21	TCP
SSH (Secure Shell)	22	TCP
Telnet (Telecommunication network)	23	TCP
SMTP (Simple Mail Transfer Protocol)	25	TCP
DNS (Domain Name System)	53	UDP
HTTP (HyperText Transfer Protocol)	80	TCP
POP3 (Post Office Protocol – Ver. 3)	110	TCP
SNMP (Simple Network Management Protocol)	161	UDP
HTTPs (Hypertext Transfer Protocol Secure)	443	TCP

網路位址轉換 (NAT)

- 為了暫時解決全球 IPv4 位址枯竭的問題，讓私有 IP 位址透過轉換能夠與網際網路進行通訊的技術

- 目前最廣泛使用的是 NAT 技術的其中一種，稱為網路位址埠轉換 (Network Address Port Translation, NAPT) ，也就是俗稱的 IP 分享器所使用的技術

- NAPT 使用 IP 偽裝 (IP Masquerade) 的方法來達到 IP 轉換的目的，並且由於 NAPT 伺服器會連接兩個以上的邏輯網路，因此也會兼具路由器的功能

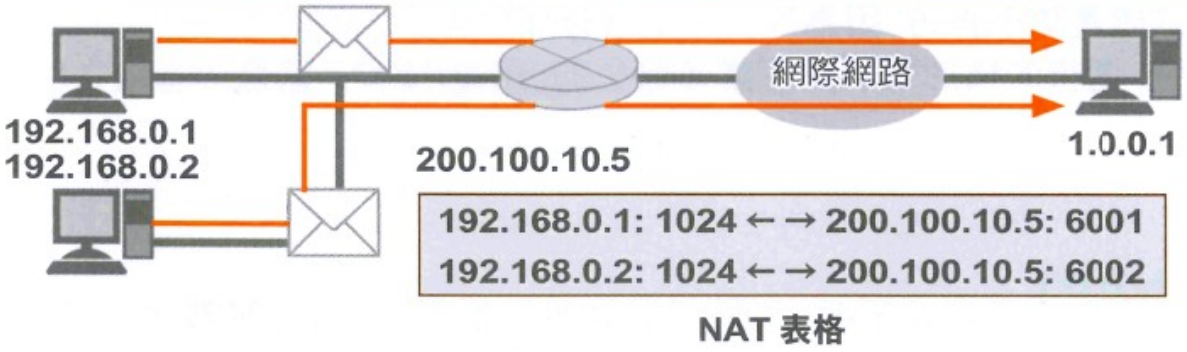
網路位址埠轉換 (1/2)

讓多台主機可以連接到同一個全球 IP 位址

① NAPT 和 NAT 一樣具有轉換 IP 位址的功能, 不過除了轉換 IP 位址外, 還能同時轉換通訊埠編號, 並且將對應關係記錄於 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	1024	1.0.0.1	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	1024	1.0.0.1	80	



192.168.0.1: 1024 ← → 200.100.10.5: 6001
192.168.0.2: 1024 ← → 200.100.10.5: 6002

NAT 表格

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
192.168.0.2	1024	1.0.0.1	80	

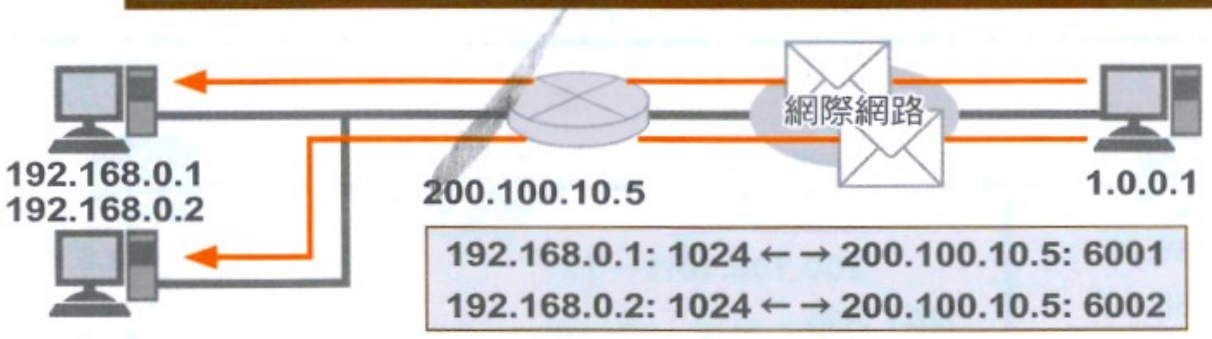
傳送端IP位址	傳送端通訊埠	目的端IP位址	目的端通訊埠	資料
200.100.10.5	6002	1.0.0.1	80	

網路位址埠轉換 (2/2)

② 答覆時，必須利用 NAT 表格來確認 IP 位址和通訊埠編號，以進行 IP 位址和通訊埠編號的轉換

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
1.0.0.1	80	200.100.10.5	6001	

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	1024	



192.168.0.1: 1024 ← → 200.100.10.5: 6001
192.168.0.2: 1024 ← → 200.100.10.5: 6002

NAT 表格

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
1.0.0.1	80	200.100.10.5	6002	

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
1.0.0.1	80	192.168.0.2	1024	

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.	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
2 00.10. 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

來源IP	NAT 來源IP	來源Port	來源IP名稱解析	來源區域	目的IP	目的Po
10.0.0.6	163. [redacted] 180	64089			209.95.41.41	3800
10.0.0.158	163. [redacted] 180	55431			168.95.192.1	53
10.0.0.158	163. [redacted] 180	40574			168.95.192.1	53

SNAT(多對一)

目的 : 讓 192.168.1.0 的電腦，帶 10.1.1.253 的 IP 連上 Server