

第七章 IP定址(IP addressing)

- 本章介紹IP位址表示法、IP位址的等級、IP位址的結構、常見的3種位址等級、特殊的IP位址、子網路切割、子網路遮罩、無等級的IP位址、網路位址轉譯(NAT)等這些都是學習網際網路的重要觀念

IP 位址表示法

- IP 位址是以 32 Bits 的二進位數字來表示

11001011010010101100110101101111

總共有 32 個 0/1

1. 以 8 Bits 為單位, 將 32 Bits 的 IP 位址分成 4 段 :

11001011 01001010 11001101 01101111

每一段是 8 Bits

2. 將各段的二進位數字轉換成十進位, 再以 . 隔開

203.74.205.111

※ IPv4 與 IPv6

- IPv4 的 IP 位址是由 32 Bits 組成, 理論上會有 $2^{32} = 4294967296$ (將近 43 億個) 種組合。
- IPv6 的 IP 位址是由 128 Bits 所組成, 2^{128} 可說是天文數字, 可提供非常充裕的 IP 位址空間。

IP 位址的等級

- IP 位址的結構
- 常見的 3 種位址等級
- 特殊的 IP 位址

IP 位址的結構

- IP 位址是由網路位址與主機位址兩部份所組成
- 網路位址用來表示網路
- 主機位址表示在該網路下的主機位址
- 主機位址的位元數表示該網路的容許的IP數量
- 網路位址+主機位址= 32 bits



圖 7-7 32 Bits 的 IP 位址是由網路位址與主機位址兩部份所組成

IP 位址的結構

- 網路位址 (Network ID)
網路位址位於 IP 位址的前段, 可用來識別所屬的網路。
- 主機位址 (Host ID)
主機位址位於 IP 位址的後段, 可用來識別網路上個別的裝置
- IP 在設計時便依據網路位址的長度, 劃分出 IP 位址等級

常見的 3 種位址等級

- Class A

- 網路位址的前導位元為 0
- 總共只有 $2^7 = 128$ 個 Class A 網址
- 每個 Class A 網址可運用的主機位址為 $2^{24} = 16777216$ 個 (一千六百多萬)

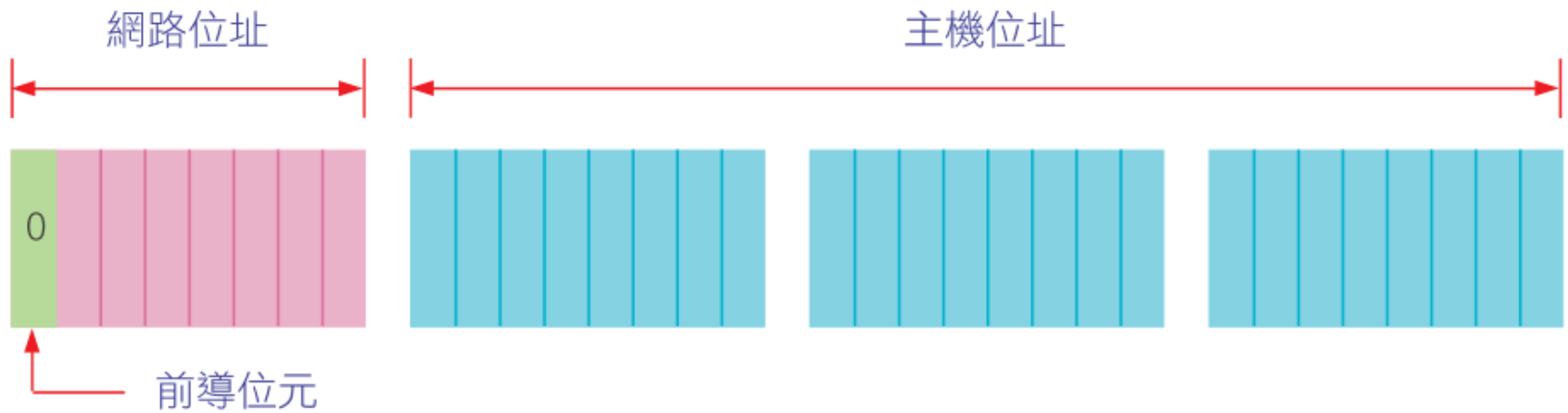


圖 7-8 Class A 的 IP 位址

常見的 3 種位址等級

- Class B :
 - 網路位址前導位元為10
 - 網路位址長度 $16-2=14$, 共有 $2^{14}=16384$ 個網路
 - Class B 網路可資運用的主機位址有 $2^{16} = 65536$ 個

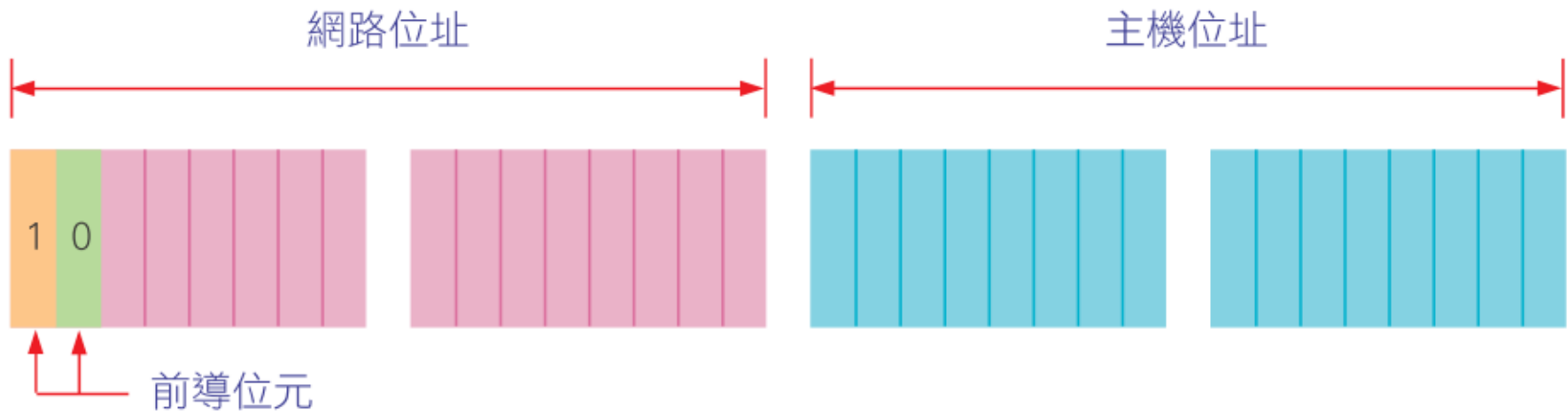


圖 7-9 Class B 的 IP 位址

常見的 3 種位址等級

- Class C :
 - 網路位址前導位元為 110
 - 網路位址長度 $24 - 3 = 21$, 共有 $2^{21} = 2097152$ 個網路
 - 每個 Class C 網路可資運用的主機位址有 $2^8 = 256$ 個

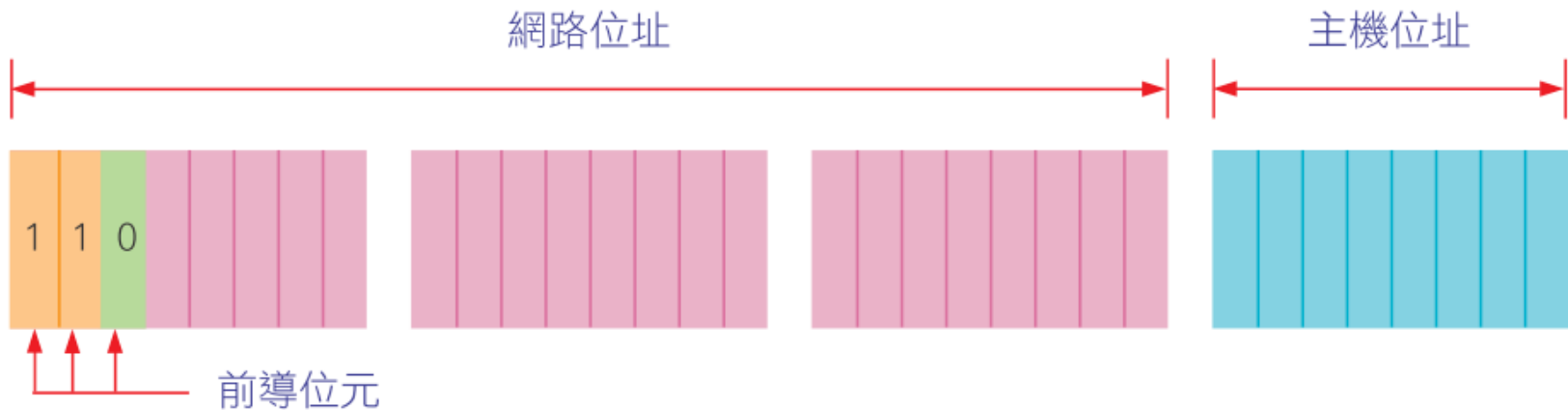


圖 7-10 Class C 的 IP 位址

常見的 3 種位址等級比較



圖 7-11 Class A、B、C 的比較

常見的 3 種位址等級

- 從 IP 位址的前導位元, 便可判斷出所屬網路的等級, 進而得知網路位址與主機位址為何。
- 依據企業或單位的實際需求, 可分配 Class A、B、C 三種等級的網路位址, 讓 IP 位址的分配更有效率。

特殊的 IP 位址

- 主機位址全為 0：用來代表該網路
- 主機位址全為 1：代表網路中的全部裝置，也就是『廣播』
- 若網路位址與主機位址皆為 1：亦即 255.255.255.255，稱為『Limited』或『Local』廣播封包。只有同一網路位址上的裝置可收到此種廣播。
- Class A 的最後 1 個網路位址：代表『Loopback』位址，主要用來測試本機電腦上的 TCP/IP 之用

特殊的 IP 位址

- 在 Class A、B、C 中都保留了一些私人 IP 位址，這些位址只能在私人網路使用，無法直接對外：

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

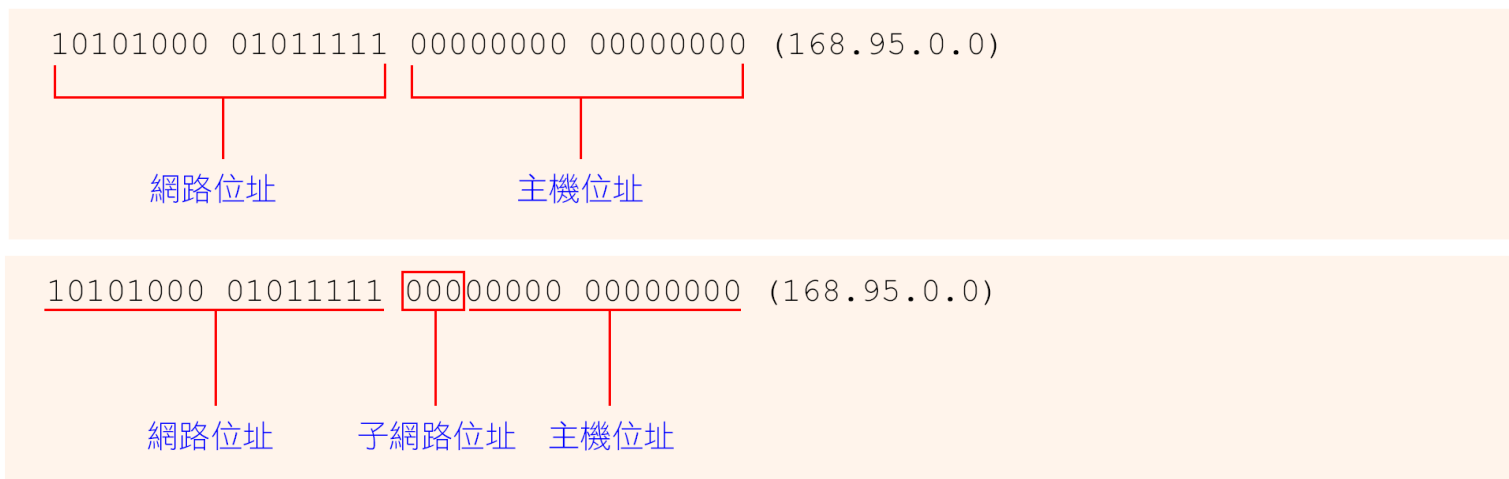
- 特殊等級：Class D (前導位元為 1110), 專用於多點傳送 (Multicast)；Class E (前導位元為 1111), 保留未用。

子網路 (Subnet)

- 切割為子網路的原理
- 子網路遮罩
- 子網路切割實例 (一)
- 子網路切割實例 (二)

切割為子網路的原理

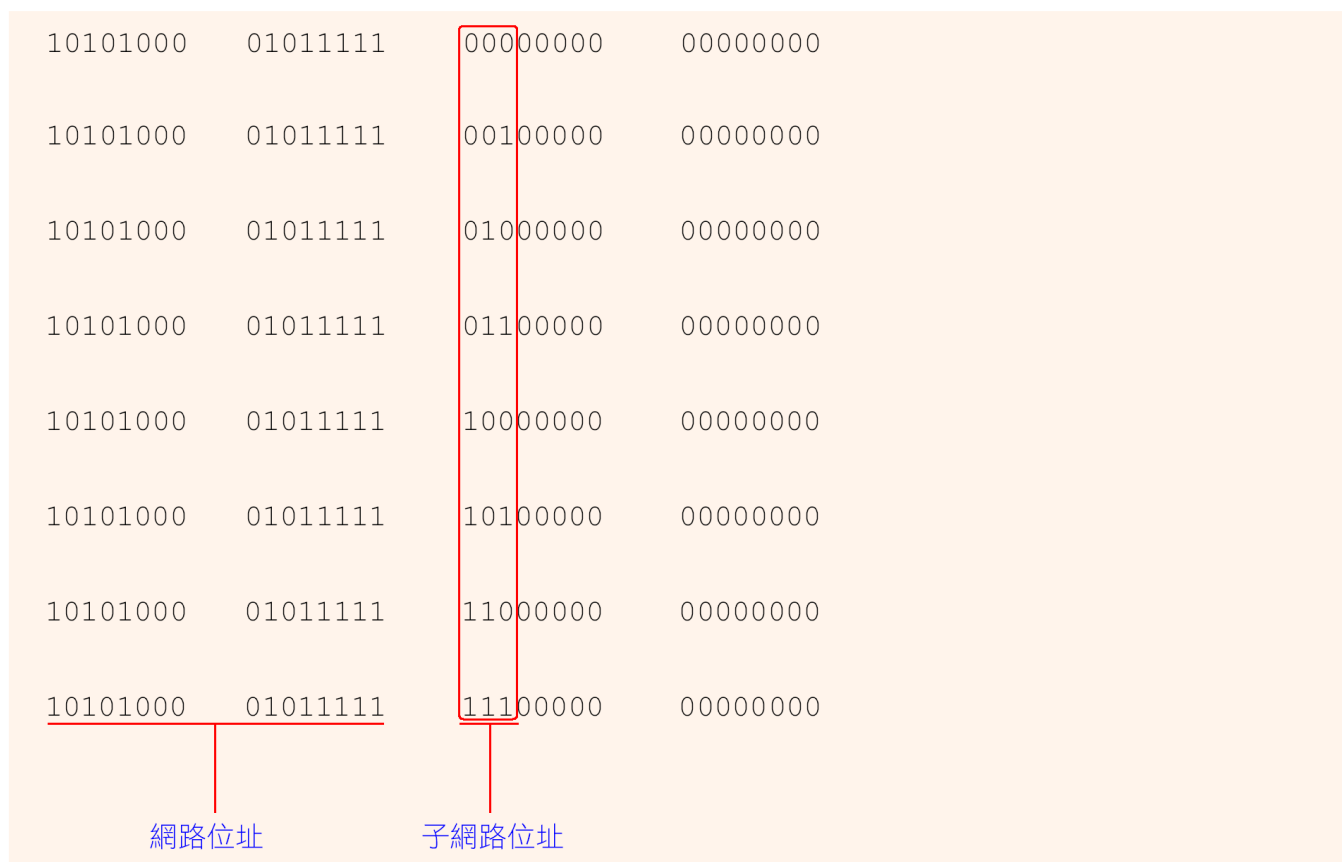
- IP位址等級的設計雖然有許多好處，但彈性不足
- 切割為子網路的重點便是讓每個子網路擁有一個獨一無二的子網路位址



- 子網路位址與原先的網路位址合起來共 19 Bits, 可視為新的網路位址, 用來識別該子網路。

切割為子網路的原理

- 若子網路位址使用 3 Bits, 則產生了 $2^3 = 8$ 個子網路



切割為子網路的原理

表 7-3 Class B 可能切割的子網路

2^n

2^{16-n}

子網路位址位元數	形成的子網路數目	每個子網路可用的主機位址
1	2	32768
2	4	16384
3	8	8192
4	16	4096
5	32	2048
6	64	1024
7	128	512
8	256	256
9	512	128
10	1024	64
11	2048	32
12	4096	16
13	8192	8
14	16384	4
15	32768	2

切割為子網路的原理

表 7-4 Class C 可能切割的子網路

2^n

2^{8-n}

子網路位址位元數	形成的子網路數目	每個子網路可用的主機位址
1	2	128
2	4	64
3	8	32
4	16	16
5	32	8
6	64	4
7	128	2

子網路遮罩

- 子網路不僅是單純的將 IP 位址加以切割, 其關鍵在於切割後的子網路必須能夠**正常地**與其他網路相互連接
- 子網路遮罩是用來判斷切割後的子網路 IP 位址中, 哪幾個位元為網路位址, 哪幾個位元為主機位址

子網路遮罩的特性

- 子網路遮罩長度為 32 Bits, 與 IP 位址的長度相同
- 子網路遮罩是由一串連續的 1, 再跟上一串連續的 0 所組成。因此, 可以是以下的 32 位數字：

11111111 11111111 11111000 00000000

連續的 1

連續的 0

11111111 11111111 11111111 11100000

連續的 1

連續的 0

但不可是如下的數字：

11111111 00011111 11111000 00000000

不連續的 1

子網路遮罩的特性

- 為了方便閱讀, 子網路遮罩通常也用與 IP 位址相同的十進位來表示。例如：

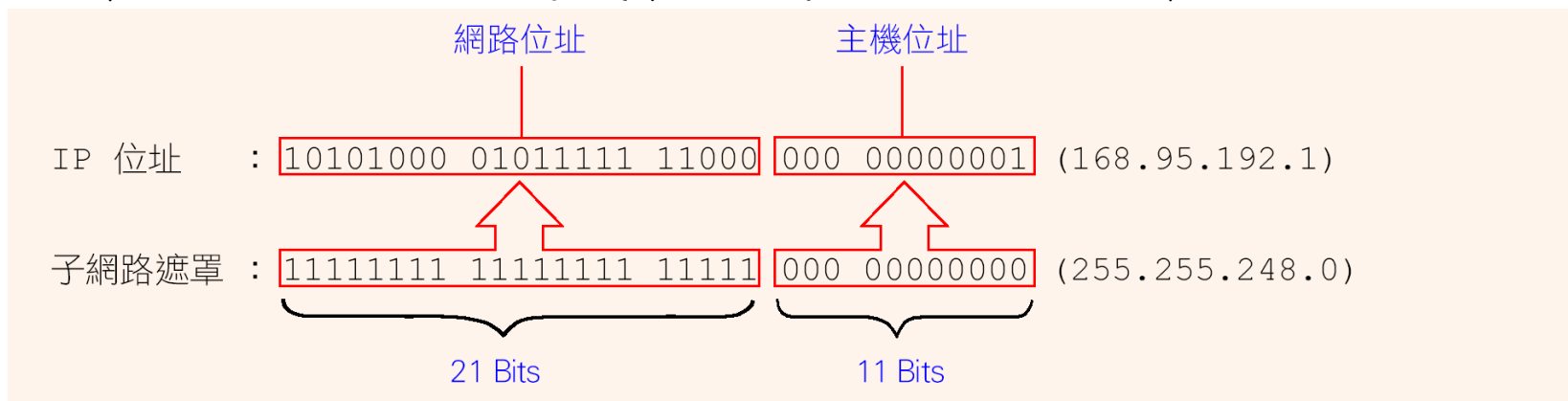
```
11111111 11111111 11111111 00000000
```

通常寫作：

```
255.255.255.0
```

子網路遮罩的特性

- 子網路遮罩必須與 IP 位址配對使用才有意義。單獨的子網路遮罩不具任何意義。當子網路遮罩與 IP 位址一起時，子網路遮罩的 1 對映至 IP 位址便是代表網路位址位元，0 對映至 IP 位址便是代表主機位址位元。例如：



亦可寫作：

168.95.192.1/21

子網路遮罩的特性

- 原有等級式的網路位址仍然可繼續使用。以 Class C 的 IP 為例：

IP 位址 : 11001011 01001010 11001101 01101111

若不執行子網路切割, 則其子網路遮罩為：

子網路遮罩 : 11111111 11111111 11111111 00000000

Class A、B、C 固定對應的子網路遮罩如下：

Class A : 11111111 00000000 00000000 00000000 (255.0.0.0)

Class B : 11111111 11111111 00000000 00000000 (255.255.0.0)

Class C : 11111111 11111111 11111111 00000000 (255.255.255.0)

子網路切割實例 (一)

- A 企業為 Class C IP 位址, 內部要分成 4 個獨立的網路 :

IP 位址 : 11001011 01001010 11001101 00000000 (203.74.205.0)

子網路遮罩 : 11111111 11111111 11111111 00000000 (255.255.255.0)

- 子網路需使用 2Bits, 所以網路位址變成 $24+2 = 26$ Bits。新的子網路遮罩為 :

11111111 11111111 11111111 11000000 (255.255.255.192)

- 原先的主機位址有 8 Bits, 但是子網路位址借用了 2 Bits, 主機位址只能使用剩下的 6 Bits。每個子網路可以有 $2^6 = 64$ 個可用的主機位址。
- 主機位址不得全為 0 或 1, 所以實際上每個子網路可分配的 IP 位址為 $2^6 - 2 = 62$ 個。

子網路切割實例 (一)

表 7-5 A 企業可用的子網路

網路	可設定的 IP 位址	子網路遮罩
A1	203.74.205.1 - 203.74.205.62	255.255.255.192
A2	203.74.205.65 - 203.74.205.126	255.255.255.192
A3	203.74.205.129 - 203.74.205.190	255.255.255.192
A4	203.74.205.193 - 203.74.205.254	255.255.255.192

- 接著必須在 A 企業所有的路由器上設定 A1、A2、A3、A4 等子網路的路由紀錄, 以便在路由器能將 IP 封包正確地傳送到切割後的子網路。

子網路切割實例 (一)

- 子網路可再進一步切割成更小的子網路。承上例, 例如: 網管人員可以再將 A1 網路切割成更小的子網路。方法仍舊是從主機位址借用幾個位元來作為子網路位址。
- 子網路切割時所作的設定, 都是在企業內部。換言之, 遠端的網路或路由器並不須知道 A 企業內部是如何切割子網路。如此, 可保持網際網路上路由架構的簡單性。
- 子網路的切割對於子網路的外部而言沒有影響

子網路切割實例 (二)

- 某台主機的 IP 位址為 192.168.1.134, 子網路遮罩為 255.255.255.248, 則該主機所在的子網路的『網路位址』為何?
- 由網路位址第一個數字 192 得知此主機位於 Class C 等級, 我們將 IP 位址最後一個數字 134 及子網路遮罩改寫為 2 進位:

IP 位址: 192 .168 .1 .10000110

子網路遮罩: 11111111.11111111 .11111111 .11111000

子網路位址

192.168.1.128

子網路切割實例 (三)

- 假設某個子網路的子網路遮罩為 255.255.255.224, 請判斷 205.64.75.223 是否屬於此子網路裡網路設備可用的 IP 位址?

IP 位址： 205 .64 .75 .11011111

子網路遮罩： 11111111.11111111 .11111111 .11100000

子網路位址

- 由子網路遮罩可知, 主機位址的前 3 個 Bits 代表子網路位址：

205.64.75.11011111

代表 110 子網路主機位址全為 1

子網路切割實例 (四)

- 255.255.252.0 這個子網路遮罩最多可將132.114.0.0 這個網路分割為幾個有效的子網路？每個子網路中最多可以有幾台主機？

IP 位址： 132 .114 .0 .0

子網路遮罩：11111111 .11111111 .11111100 .00000000 (255.255.252.0)

- 由 IP 位址第 1 個數字 132 得知此網路是 Class B 等級，子網路遮罩藉由第 3 個數字的前 6 個 Bits 用來分割子網路，所以最多可分割出 $2^6 = 64$ 個子網路；主機位址以 $8 + 2 = 10$ 個 Bits 來表示，所以每個子網路可以有 $2^{10} - 2 = 1022$ 台主機。

子網路切割實例 (五)

- 在 Class C 等級網路中若至少要分割出 13 個子網路, 則子網路遮罩為何?
- 由於 $2^4 = 16 > 13$ 而 $2^3 = 8 < 13$, 表示至少須借用 IP 位址最後一個數字的前 4 個 Bits 來分割子網路, 故子網路遮罩為
11111111.11111111.11111111.11110000
(255.255.255.240)。

無等級的 IP 位址

目前 Class B 網址嚴重不足, 但其實 Class C 仍有餘裕, 因此產生 CIDR (Classless Inter-Domain Routing) 的劃分方式

- CIDR 原理
- CIDR 實例

CIDR 原理

- 使用 子網路遮罩 來定義較具彈性的網路位址, 可合併數個Class C 的 IP 位址
- CIDR 又稱為超網路 (Supernet), 與子網路可算是一體的兩面, 其差異如下:
 - 子網路 (Subnet): 利用子網路遮罩重新定義較長的網路位址, 將現有的網路加以切割
 - 超網路 (Supernet): 利用子網路遮罩重新定義較短的網路位址, 將現有網路『合併』成為一個網路。

CIDR 實例

- 藉由CIDR的方式, 我們可以分配一個長度為 21 Bits 的網路位址 (稱為 /21 位址) 給 B 企業, 那麼 B 企業可供運用的主機位址將會有 $32-21 = 11$ Bits, 總共可產生 $2^{11} = 2048$ 個 IP 位址
- 合併網路的限制：
 - 用來合併的 Class C 的網路位址必然是連續的。
 - 用來合併的 Class C 的網路位址數目必然是 2 的冪方數。

16/16 21/11

CIDR 實例

- B 企業實際上分配到的可能是如下的 8 個連續 Class C 位址空間：

203.74.200.0	(11001011	01001010	11001000	00000000)
203.74.201.0	(11001011	01001010	11001001	00000000)
203.74.202.0	(11001011	01001010	11001010	00000000)
203.74.203.0	(11001011	01001010	11001011	00000000)
203.74.204.0	(11001011	01001010	11001100	00000000)
203.74.205.0	(11001011	01001010	11001101	00000000)
203.74.206.0	(11001011	01001010	11001110	00000000)
203.74.207.0	(11001011	01001010	11001111	00000000)

- 可以利用下列方式表示：

IP 位址：203.74.200.0 (11001011 01001010 11001000 00000000)

Subnet Mask：255.255.248.0 (11111111 11111111 11111000 00000000)

代表要合併 8 個位址空間

網路位址轉譯 (NAT)

- 由於網際網路的日漸普及, IP 位址也已經不敷使用。在 1994 年正式發表的 NAT 技術有效改善此問題。
- NAT 分成 3 類：
 - 靜態 NAT (Static NAT)
一個私人 IP 位址對應一個固定的合法 IP 位址
 - 動態 NAT (Dynamic NAT)
一個私人 IP 位址對應一個不固定的合法 IP 位址
 - NAT (Network Address Port Translation)
利用記錄連接埠 (Port) 的編號, 讓多個私人 IP 位址共用一個合法 IP 位址

網路位址轉譯 (NAT)

- 網路位址轉譯的原理
- 網路位址轉譯的注意事項

網路位址轉譯的原理

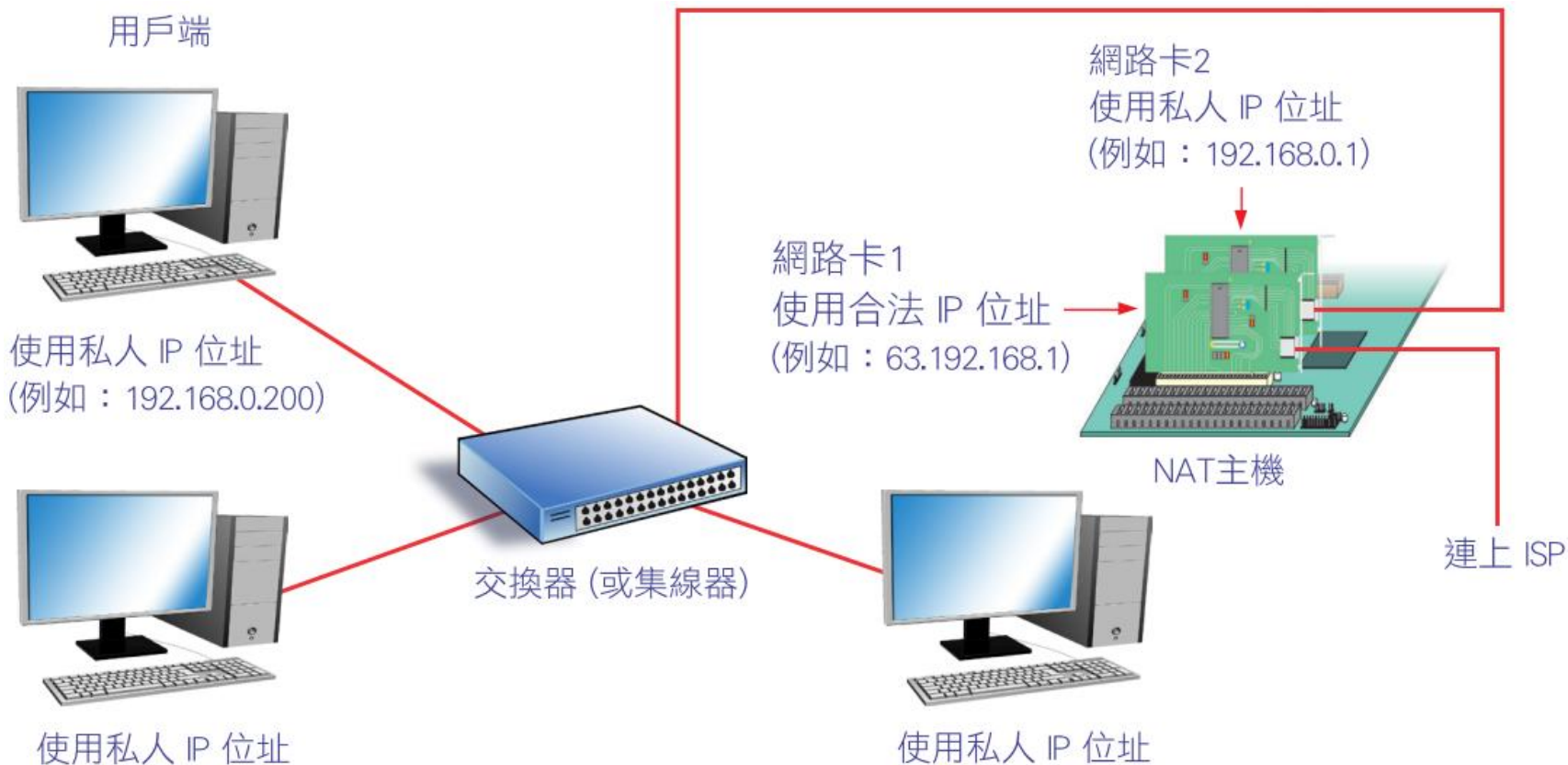


圖 7-12 網路位址轉譯的運作架構

目前一般家庭上網所用的『寬頻分享器』或『無線分享器』，就相當於圖中 NAT 主機與交換器的結合

網路位址轉譯的原理



圖 7-13 寬頻分享器或無線分享器的網路連線示意圖

網路位址轉譯的原理

The screenshot shows the web interface of a Buffalo WCR-G300 wireless access point. The browser address bar shows the IP address 192.168.100.254. The page title is "AirStation Settings" and the device name is "WCR-G300". The navigation menu includes "設定", "網際網路/LAN", "無線組態", "安全性", "LAN組態", "管理組態", and "狀態". The "網際網路/LAN" menu is expanded, showing sub-menus: "網際網路", "PPPoE", "DDNS", "LAN", "DHCP租用", "NAT", and "路由". The "NAT" sub-menu is selected, and the "網路位址轉址設定" (NAT Settings) page is displayed. The "位址轉址" (NAT) option is checked and labeled "啟用". The "已刪除封包的輸出記錄" (Output log for deleted packets) option is unchecked and labeled "啟用". A "套用" (Apply) button is visible. The right side of the page contains detailed information about NAT, including a description: "架構位址轉譯，將網際網路端連接到網際網路。" (Structure address translation, connecting the Internet side to the Internet.), a section for "位址轉址" (NAT) with instructions: "您可以選取要 [啟用] 或 [停用] 位址轉譯。預設為啟用。" (You can select to [enable] or [disable] address translation. Default is enable.), a "註:" (Note) section: "連線到網際網路時，正常情況下應該 [啟用] 位址轉譯。" (When connecting to the Internet, normally you should [enable] address translation.), and a section for "記錄刪除的封包" (Log deleted packets) with instructions: "指定是否要以日誌記錄由於 [位址轉譯] 錯誤而刪除的封包。預設值是 [停用]。" (Specify whether to log deleted packets due to [address translation] errors. The default value is [disable].)

圖 7-14 無線分享器都會提供網路轉址 (NAT) 功能

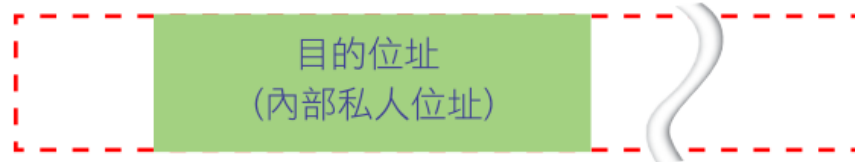
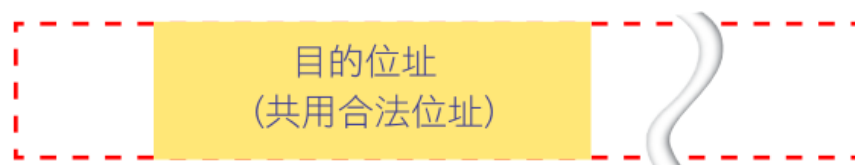
網路位址轉譯的原理

※送出封包時



NAT 主機向外部送出的資料封包

※接收封包時



NAT 主機向內部送出的資料封包

圖 7-15 網路位址轉譯的運作方式

網路位址轉譯的原理

- 當區域網路內許多部電腦的私人位址都對應到同一個合法 IP 位址時,藉由用戶端 TCP/UDP 連接埠號碼來判斷封包要送到哪一台電腦

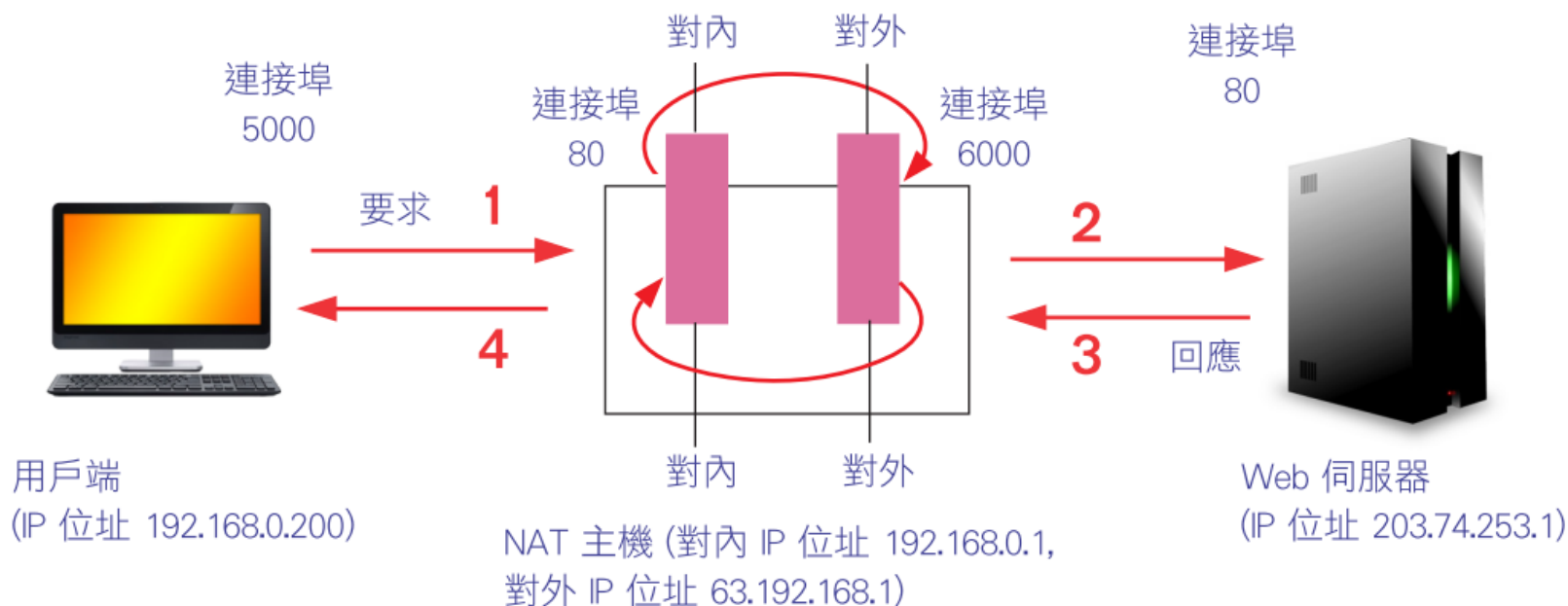


圖 7-16 透過 NAT 存取 Web 伺服器的運作方式

網路位址轉譯的原理

1. 用戶端要向 Web 伺服器要求網頁資料, 其 IP 封包會包含以下的資訊:

- 目的地 IP 位址 = 203.74.253.1 (Web 伺服器)
- 來源 IP 位址 = 192.168.0.200 (NAT 用戶端)
- 目的地連接埠 = 80 (Web 伺服器預設使用的連接埠)
- 來源連接埠 = 5000 (由用戶端應用程式自行決定使用的連接埠)

網路位址轉譯的原理

2. NAT 主機收到用戶端的要求後，會使用本機的一個連接埠 (稱為 NAT 連接埠)，來對應用戶端的 IP 位址與來源連接埠：

- 目的地 IP 位址 = 203.74.253.1 (沒變)
- 來源 IP 位址 = 63.192.168.1 (從 NAT 用戶端變為 NAT 主機)
- 目的地連接埠 = 80 (沒變)
- 來源連接埠 = 6000 (由 NAT 主機自行產生，用來對應用戶端原始的 IP 位址與連接埠)

網路位址轉譯的原理

3. Web 伺服器傳回網頁資料, 其封包會包含以下的資訊：

- 目的地 IP 位址= 63.192.168.1 (NAT 主機)
- 來源 IP 位址= 203.74.253.1 (Web 伺服器)
- 目的地連接埠= 6000
- 來源連接埠= 80

網路位址轉譯的原理

4. NAT 主機收到傳回的資料後,發現目的地連接埠 6000 對應到 192.168.0.200 這個 IP 位址與 5000 這個連接埠,於是產生如下的新封包,傳送到 NAT 用戶端:

- 目的地 IP 位址= 192.168.0.200 (從 NAT 主機變成 NAT 用戶端)
- 來源 IP 位址= 203.74.253.1 (沒變)
- 目的地連接埠= 5000 (用戶端應用程式使用的連接埠編號)
- 來源連接埠= 80 (沒變)

網路位址轉譯的注意事項

- 無法使用某些加密協定
- 增加 NAT 主機的運算負擔
- 外界主動存取時, 設定較為複雜

網路位址轉譯的注意事項

- 若要在內部網路架設對外服務的伺服器，就必須在 NAT 主機手動設定轉譯機制

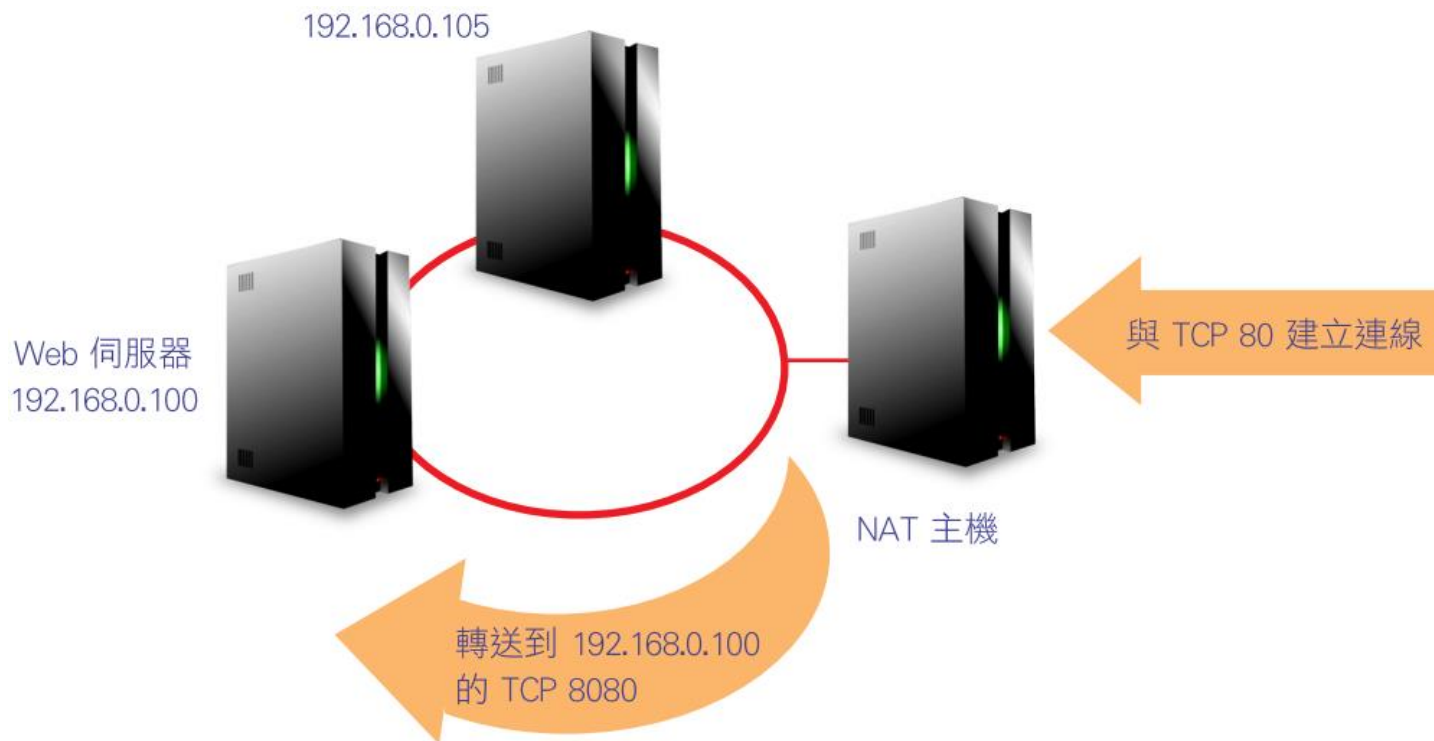


圖 7-17 在 NAT 環境架設 Web 伺服器之示意圖

本章完結

