Chapter 08

IP 基礎與定址

本章提要

- 8-1 IP 基礎
- 8-2 擷取封包
- 8-3 IP 封包的傳送模式
- 8-4 IP 位址表示法
- 8-5 IP 位址的等級
- 8-6 子網路（Subnet）
- 8-7 無等級的 IP 位址
- 8-8 網路位址轉譯（NAT）

IP 基礎與定址

- 網路層負責在網路系統之間傳送訊息, 亦即將訊息從來源端傳送到目的端。網路層的主要功能如下：
  - 定址（Addressing）：賦予網路裝置名稱或位址的機制。
  - 路由（Routing）：決定封包在數個網路之間的傳送路徑。
- 網路層中有不少是大家耳熟能詳的協定, 例如：TCP / IP 的 IP（Internet Protocol）, Netware 的 IPX （Internetwork Packet Exchange）等等。

8-1 IP 基礎

- Internet Protocol（IP, 網際網路協定）是整個 TCP / IP 協定組合的運作核心, 也是構成網際網路的基礎。
- IP 位於 DoD 模型的網路層
  - 對上可載送傳輸層各種協定的封包
  - 對下可將 IP 封包放到鏈結層, 透過乙太網路、記號環網路等各種技術來傳送。
- IP 所提供的服務大致可歸納為兩項：
  - IP 封包的傳送
  - IP 封包的切割與重組

8-1-1 傳送 IP 封包

- IP 是負責網路之間訊息傳送的協定, 可將 IP 封包從來源裝置傳送到目的裝置。
- 要達成這樣的目的, IP 必須依賴以下兩種機制：
  - IP 定址
  - IP 路由

IP 定址

- IP 規定網路上所有的裝置都必須有一個獨一無二的 IP 位址（IP Address）以資識別。
- 同理，每個 IP 封包都會記載目的裝置的 IP 位址，封包才能正確地送達目的地。

同一裝置可以擁有多個 IP 位址嗎？

- 所有使用 IP 的網路裝置，至少都必須有一個獨一無二的 IP 位址。
- 指派多個『獨一無二的 IP 位址』給同一個網路裝置，但是同一個 IP 位址卻不能重覆指派給兩個（或以上）網路裝置。
  - 必須有作業系統的支援
  - Windows NT / 2000 / XP / 2003、Unix / Linux 便可指派（Binding）多個 IP 位址給同一張網路卡
  - 在 Windows 95 / 98 等系統，便不支援這樣的功能

IP 定址

- 全球負責分配 IP 位址。此機構的最高單位為 ICANN（Internet Corporation for Assigned Names and Numbers），網址為 http://www.icann.org/。
- ICANN 會依地區與國家, 授權給公正的單位來執行分配 IP 位址的工作。
- 在台灣是由 TWNIC（Taiwan Network Information Center, 財團法人臺灣網路資訊中心）所負責, 網址為 http://www.twnic.net/。

IP 路由

- 網際網路可視為由許多個網路連結成的大型網路。
- 網路之間還必須有傳送的機制，才能將 IP 封包透過一個個的網路，送達目的地。此種傳送機制稱為 IP 路由（IP Routing）。

IP 路由

- 每個網路透過路由器（Router）相互連接。路由器的功能是為 IP 封包選擇傳送的路徑。

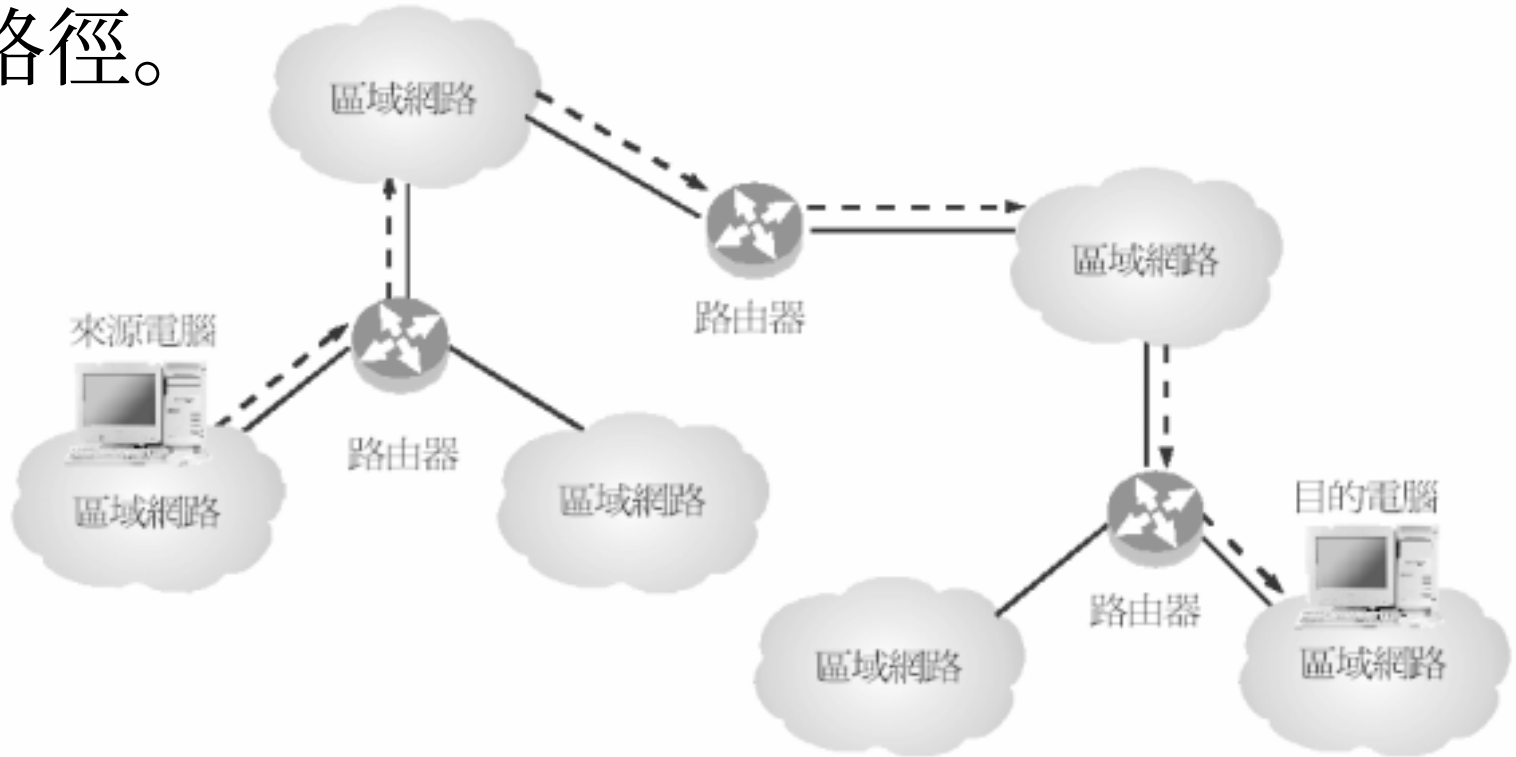


圖 8-01　在網路之間傳送 IP 封包的機制稱爲 IP 路由

非連接式的傳送特性

- 使用非連接式（Connectionless）的傳送方式。
  - IP 封包時, 來源與目的裝置雙方毋須事先建立連線, 即可將 IP 封包送達。
  - 可提高傳輸的效率。
  - 傳送方式較易在此種機制中運作。
- 相對於非連接式的傳送方式, 也有連接式（Connection-Oriented）的傳送方式

8-1-2 切割與重組 IP 封包

- 每一種鏈結層的技術都會有所謂的最大傳輸單位（Maximum Transmission Unit, MTU），亦即該種技術所能傳輸的最大承載資料（Payload）長度。

表 8-01　常見鏈結層技術的最大傳輸單位

技術	最大傳輸單位
乙太網路	1500 Bytes
FDDI	4352 Bytes
X.25	1600 Bytes
ATM	9180 Bytes

切割與重組 IP 封包

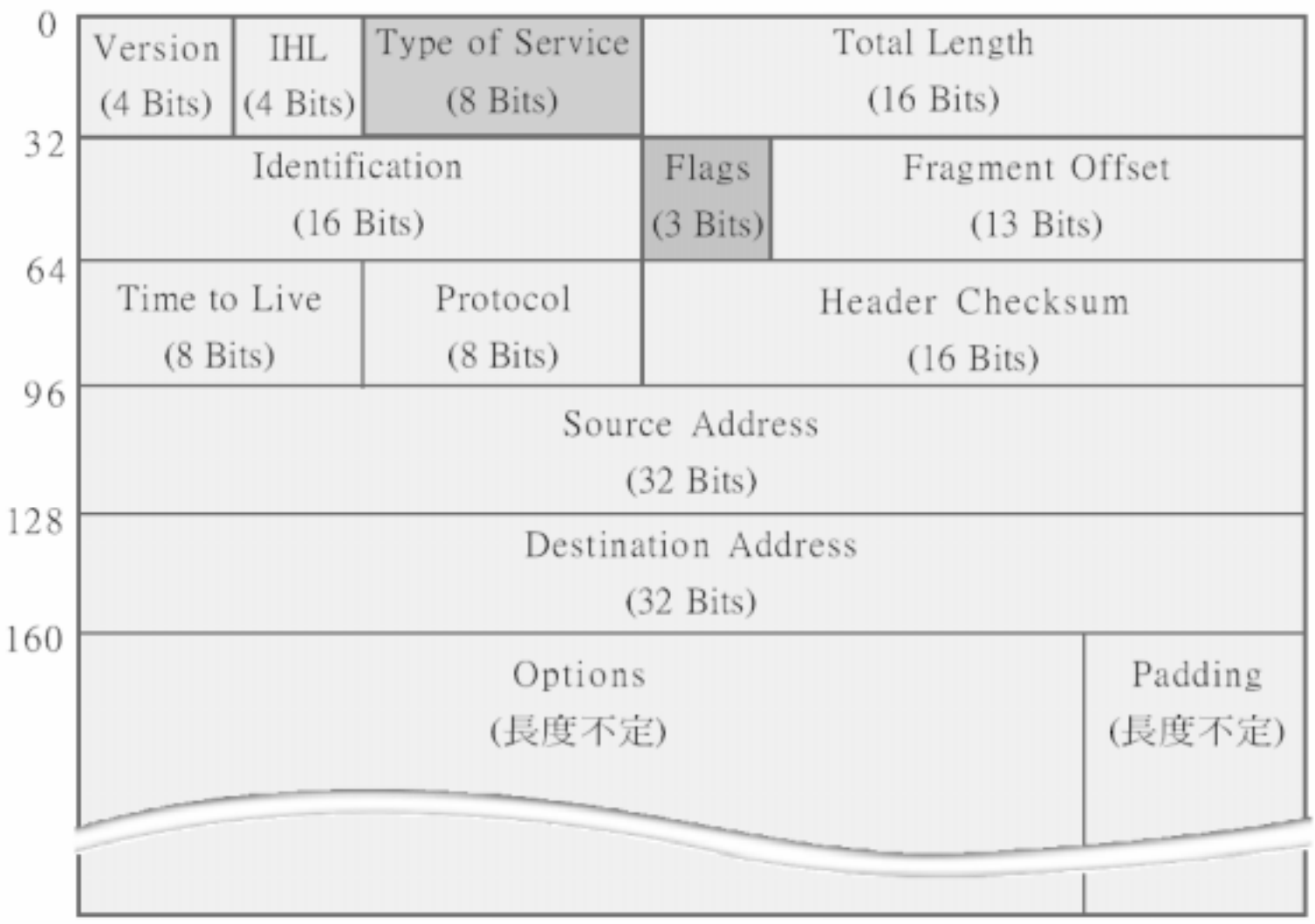
- IP 封包在傳送過程中，可能會經過許多個使用不同技術的網路。
- 路由器必須有 IP 封包切割與重組（Fragmentation & Reassembly）的機制，將過長的封包加以切割，以便能在最大傳輸單位較小的網路上傳輸。切割後的 IP 封包，會由目的裝置重組，恢復成原來 IP 封包的模樣。

8-1-3 IP 封包的結構

- IP 在傳送資料的基本單位當然是 IP 封包。IP 封包主要是由兩部份所組成：
  - IP 表頭（Header）：記錄有關 IP 位址、路由、封包識別等資訊。
  - IP Payload：載送上層協定（例如：TCP、UDP 等）的封包。

圖 8-02　IP 封包的結構

IP 表頭


0
Version (4 Bits)
IHL (4 Bits)
Type of Service (8 Bits)
Total Length (16 Bits)
32
Identification (16 Bits)
Flags (3 Bits)
Fragment Offset (13 Bits)
64
Time to Live (8 Bits)
Protocol (8 Bits)
Header Checksum (16 Bits)
96
Source Address (32 Bits)
128
Destination Address (32 Bits)
160
Options (長度不定)
Padding (長度不定)

IP 表頭

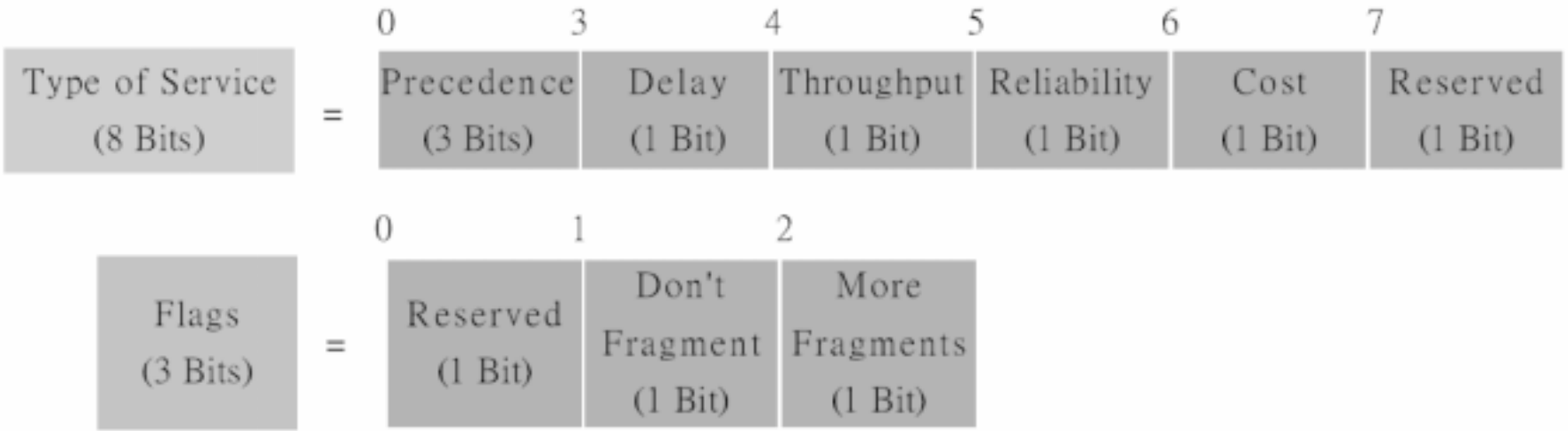


圖 8-03　IP 封包結構與表頭欄位

IP 表頭

- 以下為 IP 表頭中較為重要的資訊：
  - 目的位址（Destination Address）
  - 來源位址（Source Address）
  - 上層協定（Protocol）
  - IP 封包識別碼（Identification）
  - 切割與重組相關資訊
  - 存活時間（Time to Live, TTL）

目的位址（**Destination Address**）

- IP 表頭記錄了目的端的 IP 位址。在後續路由過程中，必須藉由此項資訊，才能將 IP 封包傳送到目的端，因此可說是 IP 表頭中最重要的資訊。

來源位址（**Source Address**）

- 記錄了來源端的 IP 位址。
- 目的端收到 IP 封包後，若必須回覆時，會用到此項資訊。

上層協定（**Protocol**）

- 用來記錄上層所使用的協定, 亦即 IP Payload 中所載送的是何種協定的資料。
- 目的端收到此 IP 封包後, 才知道要將之送到何種上層協定（例如：TCP、UDP 等）。

IP 封包識別碼（Identification）

- IP 封包識別碼是由來源端決定，並按照 IP 封包發出的順序遞增 1。
- 在 IP 路由的過程中，每個 IP 封包所走的路徑可能不一樣，因此，到達目的裝置的先後順序可能與出發時的順序略有不同。
- 目的裝置便可利用 IP 封包的識別碼，判斷 IP 封包原來的順序。
- 此外，識別碼在 IP 封包的切割與重組中，也扮演了重要的角色。

存活時間（Time to Live, TTL）

- 為了避免 IP 封包在眾多路由器之間『流浪』，因此在 IP 表頭中記錄了存活時間，限制 IP 封包在路由器之間傳送的次數。
  - 當來源裝置送出 IP 封包時，會設定存活時間初始值。
  - 例如：Windows 2000 / XP 預設為 128。當 IP 封包每經過一部路由器時，路由器便會將 IP 表頭中的存活時間減 1。
  - 當路由器收到存活時間為 1 的 IP 封包時，便直接將之丟棄，不會再傳送出去。

8-2 擷取封包

- 在本章以及後續各章中, 我們會用 NetAnalyzer 實際擷取封包, 一一剖析每個欄位的意義與內容, 驗證各章介紹的理論。
- 接下來, 就利用 NetAnalyzer 擷取 IP 封包, 看看 IP 表頭欄位的內容。

8-2-1 環境設定

- 擷取環境是由以下兩部電腦所組成：

表 8-02 擷取 IP 封包的測試環境

電腦名稱	IP 位址	備註
A	203.74.205.111	Linux FTP Server
B	203.74.205.204	Windows XP, 安裝 NetAnalyzer

- 首先從 B 電腦以 FTP 工具程式（Windows 作業系統內建）連上 A 電腦 FTP Server, 並開始傳送檔案。
- 在檔案傳送的過程中, 從 B 電腦擷取 IP 封包。

8-2-2 檢視封包內容

- 我們從擷取的封包中, 找出一個 FTP 協定封包作為範例。

檢視封包內容

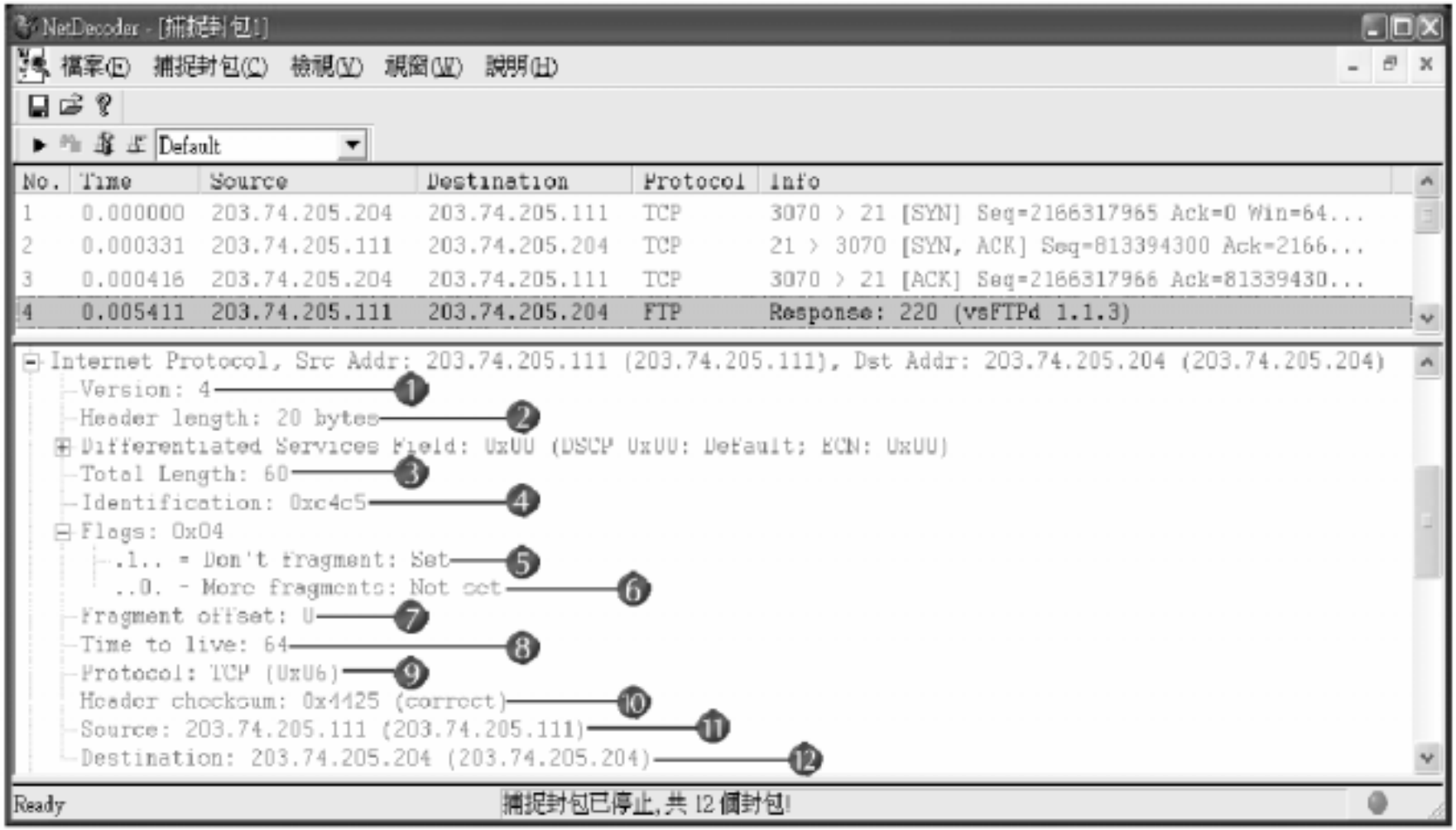


圖 8-04 IP 封包表頭內容

檢視封包內容

- 以下為 IP 封包表頭的說明。
- 請注意， NetAnalyzer 已解讀大部份欄位的資訊, 以較易閱讀的方式呈現出來。

❶Version：4 代表此 IP 封包所使用的版本為 IPv4 。

❷Header Length：IP 表頭的長度為 20 Bytes。

❸Total Length：IP 封包的總長度。

檢視封包內容

❹Identification：此 IP 封包的識別碼。

❺此為 Don‘t Fragment 欄位。1 代表傳送過程中不可切割。

❻此為 More Fragments 欄位。因為是未經切割的 IP 封包, 因此為 0。

❼因為未經切割, 所以 Fragment Offset 為 0。

❽Linux 預設的 Time to Live 為 64 。

檢視封包內容

❾記錄 Transport 層所用的協定。FTP 使用的是 TCP 協定。

❿這是錯誤檢查碼。每個 IP 封包可能會有不同的錯誤檢查碼。

⓫IP 封包來源裝置的 IP 位址, 亦即 A 電腦的 IP 位址。

⓬IP 封包目的裝置的位址, 亦即 B 電腦的 IP 位址。

8-3 IP 封包的傳送模式

- 在傳送 IP 封包時，一定會指明來源位址與目的位址。來源位址當然只有一個，但是目的位址卻可能代表單一或多部裝置。
- 依據目的位址的不同，可區分為 3 種傳送模式：
  - 單點傳送
  - 廣播傳送
  - 多點傳送

8-3-1 單點傳送（Unicast）

- 一對一的傳送模式。
- 在網際網路上傳送的封包，絕大多數都是單點傳送的 IP 封包。

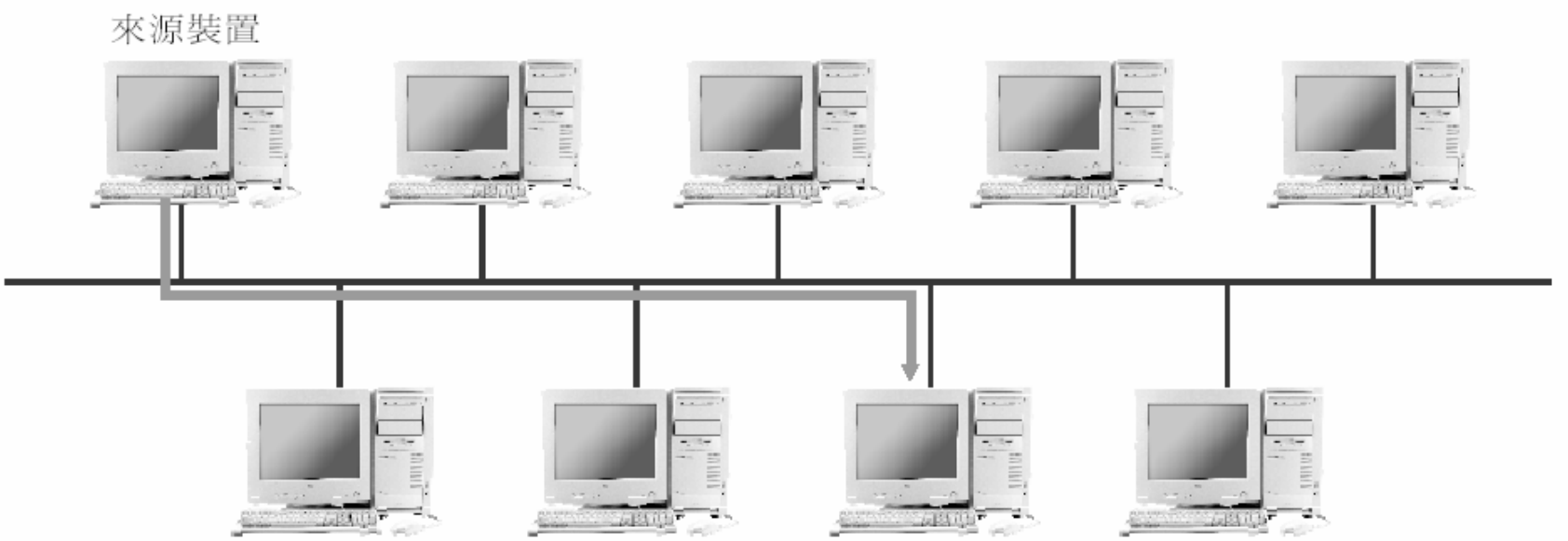


圖 8-05　單點傳送的 IP 封包只會由指定的裝置所處理

8-3-2 廣播傳送（Broadcast）

- 一對多的傳送模式。
- 由於某些協定必須透過廣播來運作，例如：ARP。

圖 8-06　廣播傳送的 IP 封包會由指定網路內的全部裝置所處理

8-3-3 多點傳送（Multicast）

- 多點傳送的 IP 封包, 其 IP 表頭中的目的位址代表的是一群裝置。凡是屬於這一群的裝置都會收到此一多點傳送封包。

圖 8-07 多點傳送的 IP 封包會送至一群指定的裝置

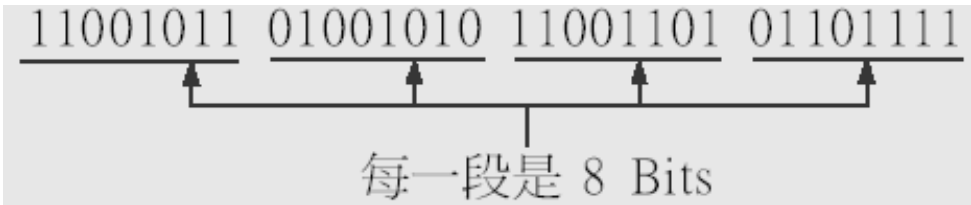
8-4 IP 位址表示法

- IP 位址本質上是一個長度為 32 Bits 的二進位數字, 看起來就是一長串的 0 或 1：

- 為了方便起見, 一般使用下列方式來轉換這一長串的 0 / 1 數字：

IP 位址表示法

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



- 2. 將各段的二進位數字轉換成十進位數字, 再以『.』隔開以利閱讀：

```
203.74.205.111
```

這種表示方式讀者應該就很熟悉了吧。通常我們在設定 IP 位址時, 都是以這種格式來輸入。

IPv4 與 IPv6

- 目前網際網路上通用的 IP 版本為第 4 版, 稱為 IPv4。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, 2128 可說是天文數字, 可提供非常充裕的 IP 位址空間

8-5 IP 位址的等級

- 當初在設計 IP 時, 著眼於路由與管理上的需求, 因此制定了 IP 位址的等級（Class）。

8-5-1 IP 位址的結構

- IP 位址必須能記載裝置所屬之網路。為了達成此目的, IP 位址是由網路位址與主機位址兩部份所組成：

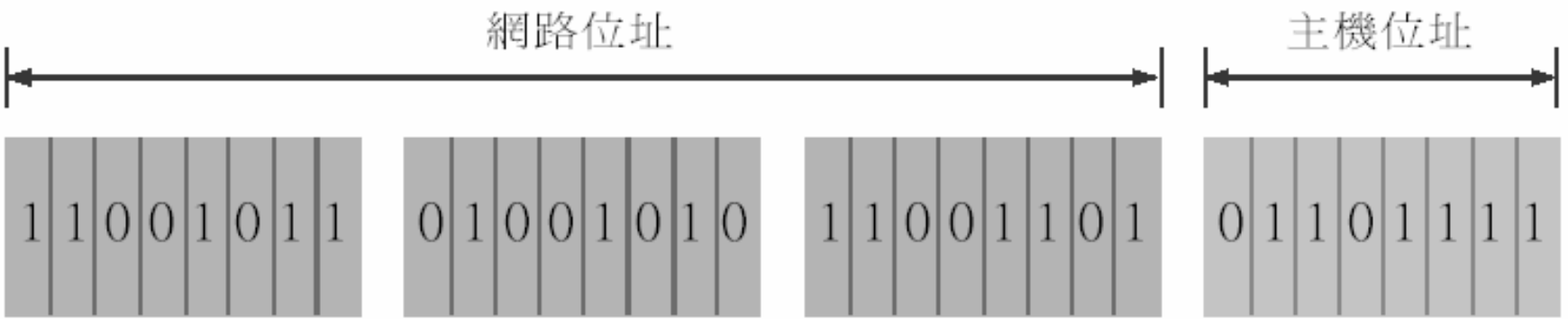


圖 8-08　32 Bits 的 IP 位址是由網路位址與主機位址兩部份所組成

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。
- 同一網路上的所有裝置，都會有相同的網路位址。IP 路由便是依據 IP 位址的網路位址，決定要將 IP 封包送至哪個網路。

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。同一網路上的裝置都會有相同的網路位址，而各裝置之間則是以主機位址來區別。

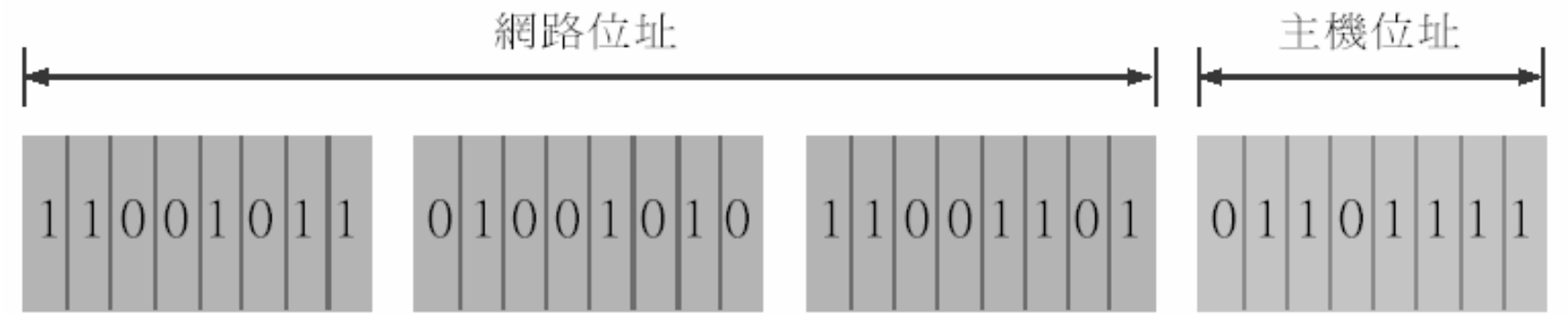


圖 8-08　32 Bits 的 IP 位址是由網路位址與主機位址兩部份所組成

主機位址（**Host ID**）

- 那麼網路位址與主機位址的長度該如何分配呢？
  - 例如：24 Bits, 那麼主機位址便只有 8 Bits, 亦即此一網路位址下共有 $2^8 = 256$ 個主機位址可資運用
  - 又例：16 Bits, 那麼主機位址便有 16 Bits, 亦即此一網路位址下共有 $2^{16} = 65536$ 個主機位址可資運用
- 為了符合不同網路規模的需求, IP 在設計時便依據網路位址的長度, 劃分出 IP 位址等級。

8-5-2 3 種常見的位址等級

- 制定了 5 種 IP 位址的等級（Class）。不過，一般最常用到的便是 Class A、B、C 這三種等級的 IP 位址。這三種等級分別使用不同長度的網路位址，因此適用於大、中、小型網路。
- IP 位址的管理機構可根據申請者的網路規模，決定要賦予何種等級。

Class A

- 網路位址的長度為 8 Bits, 最左邊的 Bit（稱為前導位元）必須為 0。Class A 的網路位址可從 00000000（二進位）至 01111111（二進位），總共有 $2^7 = 128$ 個。

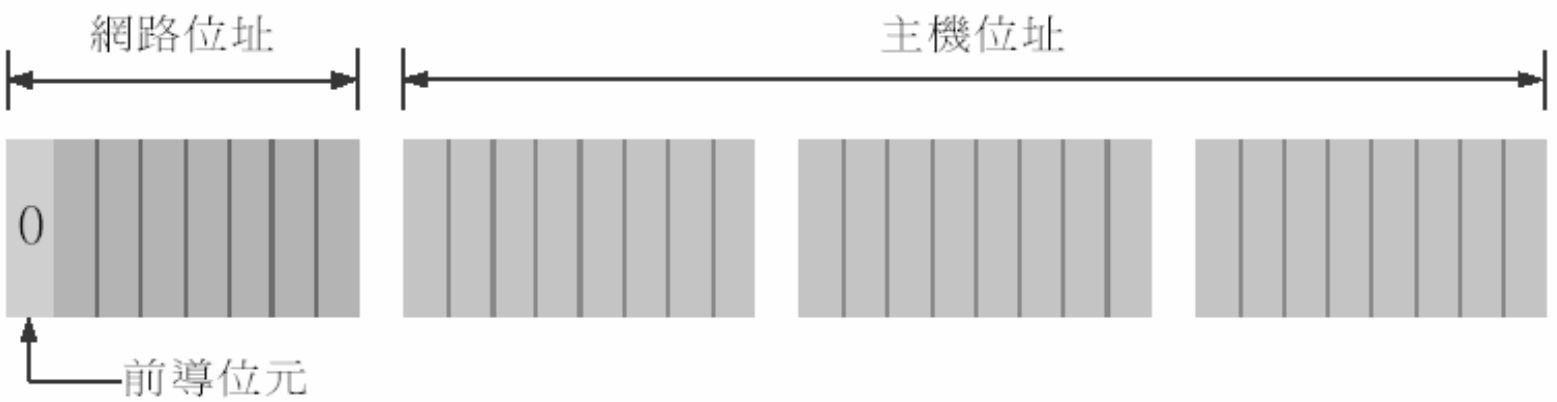


圖 8-09　Class A 的 IP 位址

Class B

- 網路位址的長度為 16 Bits, 最左邊的 2 Bits 為前導位元, 必須為 10, 因此 Class B 的 IP 位址必然介於 128.0.0.0 與 191.255.255.255 之間。
- 每個 Class B 網路可資運用的主機位址有 $2^{16} = 65536$ 個, 通常用來分配給一些大企業或 ISP 使用。

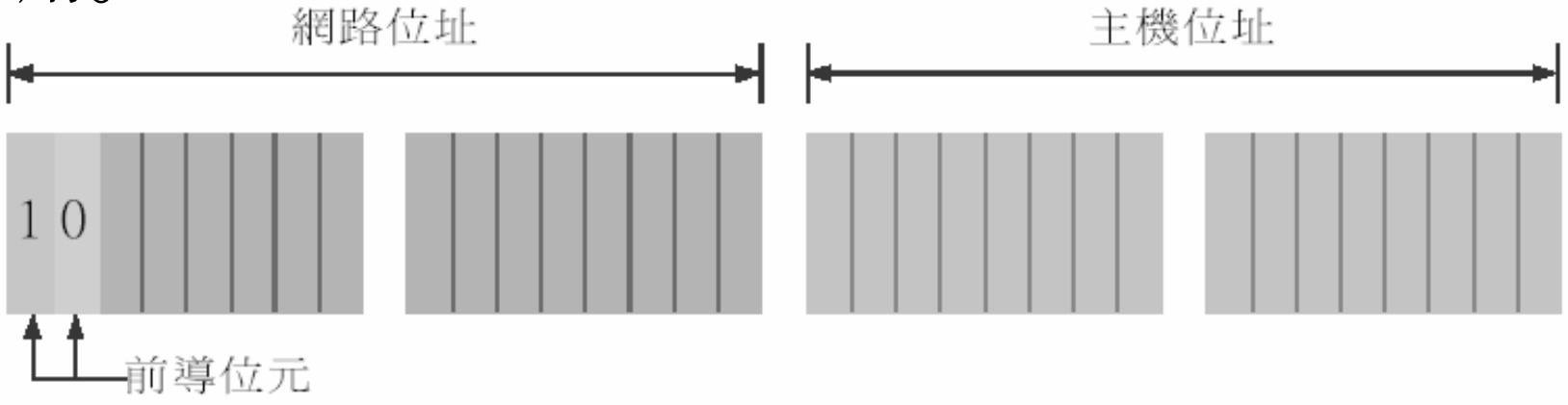


圖 8-10　Class B 的 IP 位址

Class C

- 網路位址的長度為 24 Bits, 最左邊的 3 Bits 為前導位元, 必須為 110, 因此 Class C 的 IP 位址必然介於 192.0.0.0 與 223.255.255.255 之間。
- 每個 Class C 網路可資運用的主機位址有2^8 = 256 個, 通常用來分配給一些小型企業。

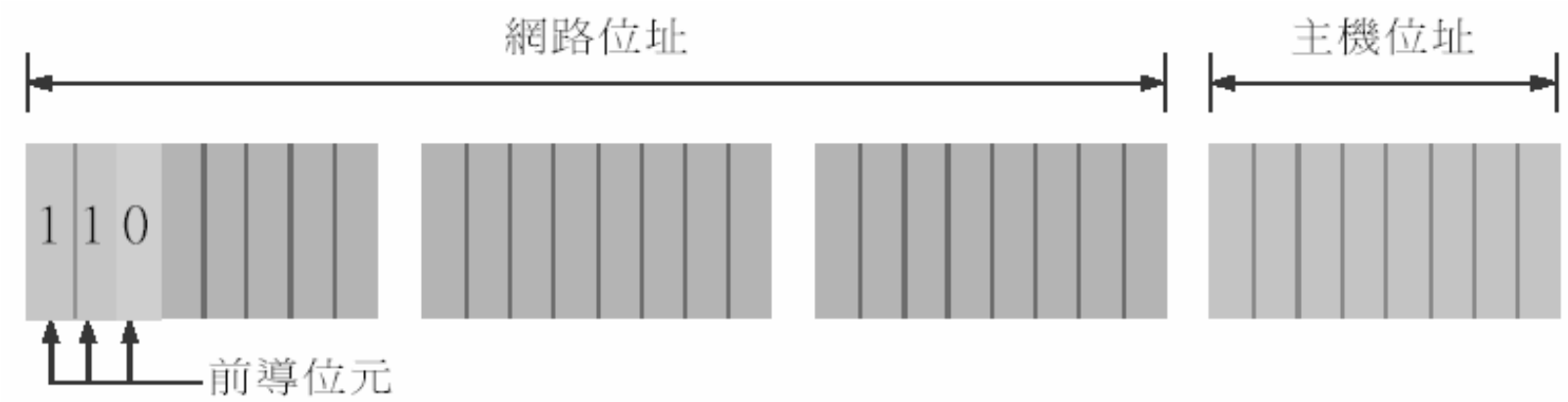


圖 8-11　Class C 的 IP 位址

小結

- 下圖將 Class A、B、C 並列, 方便讀者比較：

圖 8-12　Class A 、B 、C 的比較

小結

- 上述 Class A、B、C 的規劃，主要是針對路由與管理上的需求，可歸納出如下的優點：
  - 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。

8-5-3 特殊的 IP 位址

- 主機位址全為 0 用來代表『這個網路』（This network）, 以 Class C 為例, 203.74.205.0 用來代表該 Class C 的網路。
- 主機位址全為 1 代表網路中的全部裝置, 因此也就是『廣播』的意思。
- 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。
- Class A 的最後 1 個網路位址（也就是除了前導位元外, 其餘的網路位址位元皆設為 1）代表『Loopback』位址。其中以 127.0.0.1 最常被使用。

特殊的 IP 位址

- 在 Class A、B、C 中都保留了一些私人 IP 位址（Private IP Address）

```
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
```

若 IP 封包的目的位址為私人 IP 位址時，在 ISP 的路由器不會放行此種封包，因此無法在網際網路上流通。

8-6 子網路（Subnet）

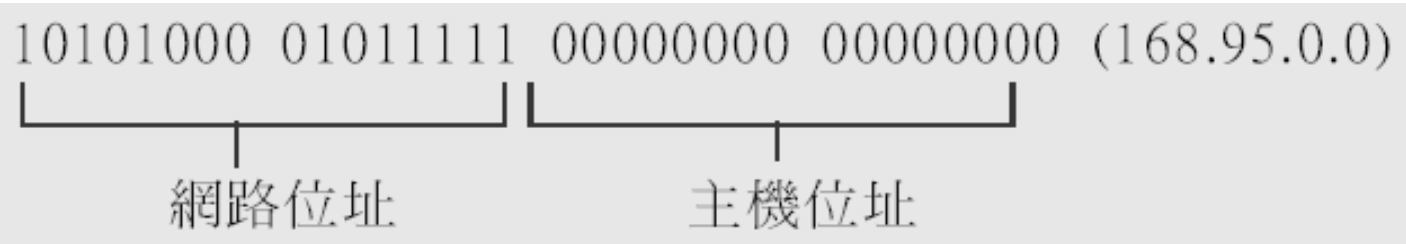
- IP 位址等級的設計雖然有許多好處，但有一個缺點，便是彈性不足。
- 解決這個問題的方法，便是讓企業能自行在內部將網路切割為子網路（Subnet）。

8-6-1 切割為子網路的原理

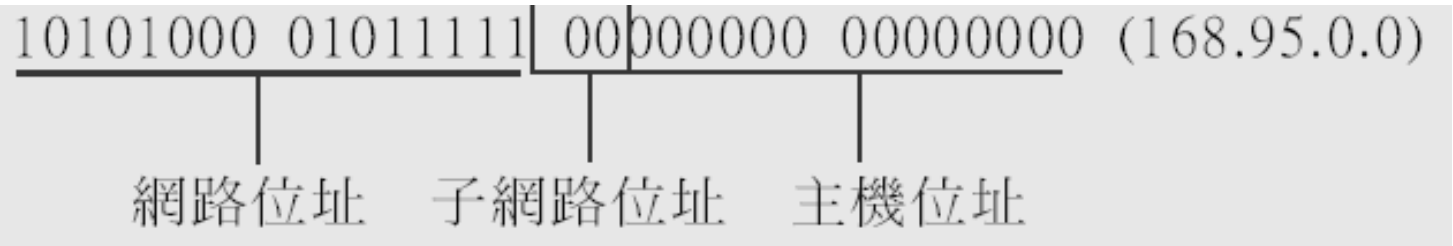
- 切割子網路的重點便是讓每個子網路擁有一個獨一無二的子網路位址（Subnet Address），以資識別子網路。
- 要切割子網路的話，必須從主機位址『借用』前面幾個 Bit，作為子網路位址。原先的網路位址加上子網路位址便可用來識別特定的子網路。

切割為子網路的原理

- 假設 A 企業申請到 Class B 的 IP 位址如下：

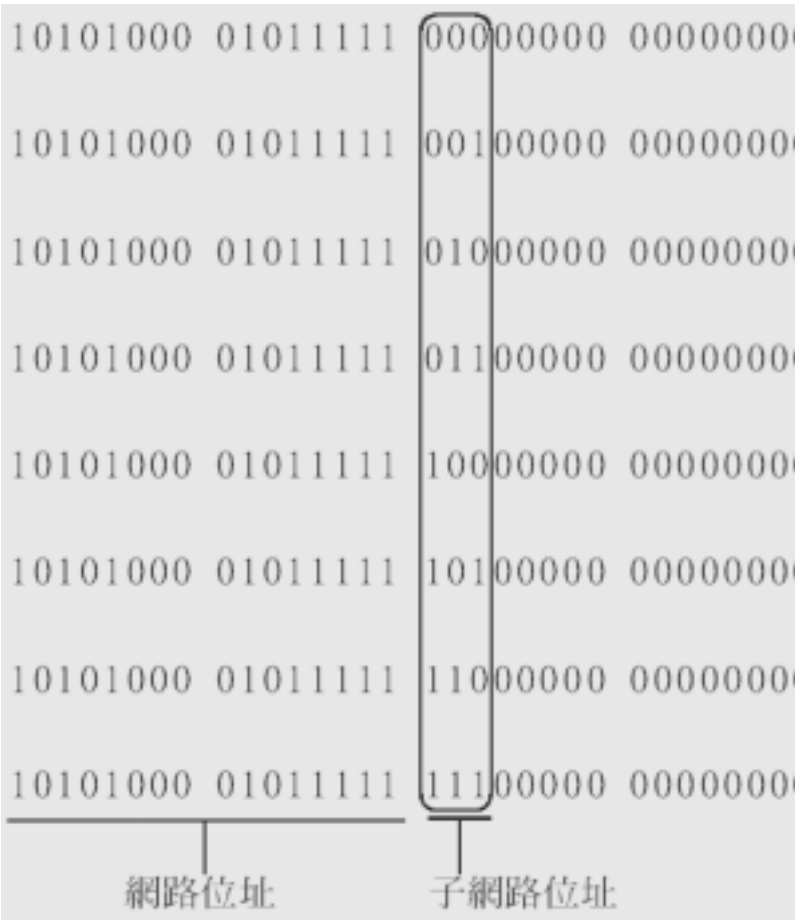


- 前面 16 Bits 是網路位址, 後面 16 Bits 則是主機位址。現在使用主機位址的前 3 Bits 作為子網路位址：



切割為子網路的原理

- 新的網路位址共 19 Bits, 可視為是, 用來識別該子網路。原先 16 Bits 的網路位址當然不可更動, 但是子網路位址卻是可以自行分配。
- 若子網路位址使用了 3 Bits, 則產生了 $2^3 = 8$ 個子網路：
- 每『借用』 n 個主機位址的位元, 便會產生 2^n 個子網路。



切割為子網路的原理

- 下表列出 Class B 網路可能切割子網路的方式：

表 8-03　Class B 可能切割的子網路

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

- 下表列出 Class C 網路可能切割子網路的方式：

表 8-04　Class C 可能切割的子網路

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

切割為子網路的原理

- 但在實際應用上, 必須記得子網路位址與主機位址不得全為 0 或 1 的原則。
- 有幾個項目實際上是不可行的：
  - 不可能使用 1 Bit 作為子網路位址。
  - 不能使主機位址只剩下 1 Bit。

8-6-2 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，也就是在路由過程中仍然能識別這些子網路。
- 此時，便產生了一個問題：無法再利用 IP 位址的前導位元，來判斷網路位址與主機位址有多少個位元。

子網路遮罩

- 子網路遮罩（Subnet Mask）正是為了此目的因應而生。以下說明子網路遮罩的特性：
  - 子網路遮罩長度為 32 Bits。
  - 子網路遮罩必須是由一串連續的 1, 再跟上一串連續的 0 所組成。

子網路遮罩

- 但不可以是如下的數字：

```
11111111 00011111 11111000 00000000
                  |
                  不連續的 1
```

- 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：

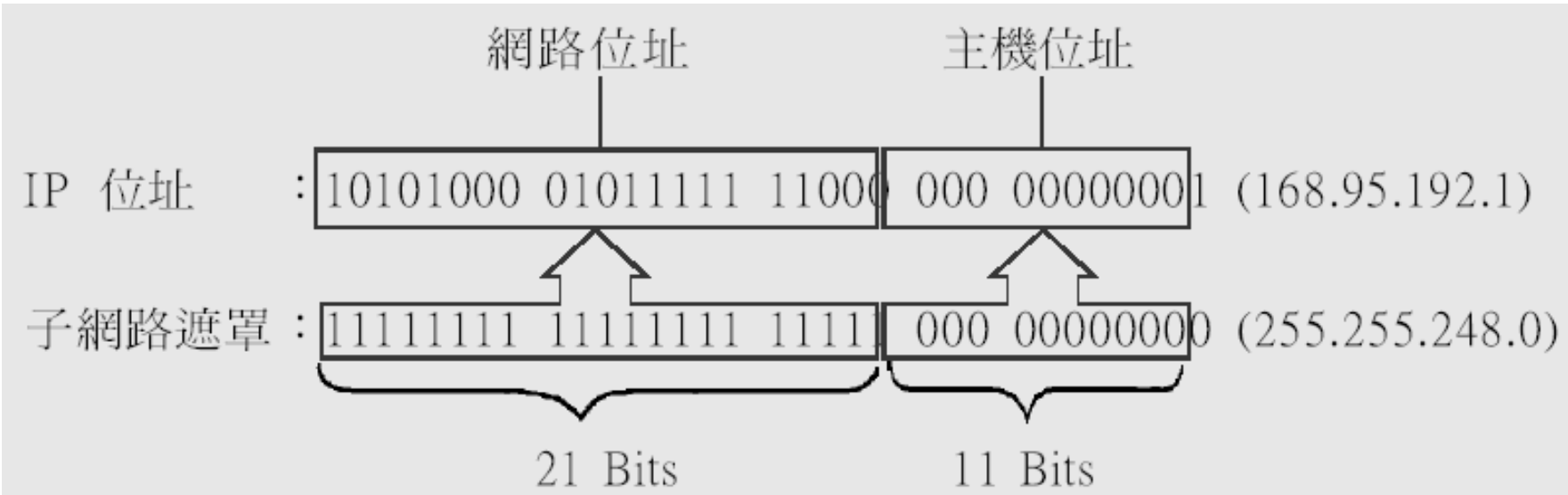
```
11111111 11111111 11111111 00000000
```

通常寫作：

```
255.255.255.0
```

子網路遮罩

- 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：



子網路遮罩

- 請注意，上述 IP 位址與子網路遮罩的組合亦可寫成： `168.95.192.1/21`
- 『/』前面是正常的 IP 表示法，『/』後面的數字 21 則代表子網路遮罩中 1 的數目。

- 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
```

子網路遮罩

- 原先使用 A 、B、C 三種等級的網路仍然可繼續使用, 只是必須額外設定對應的子網路遮罩。Class A、B、C 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)
```

8-6-3 子網路切割實例（一）

- 假設 A 企業費了一番功夫終於申請到如下的 Class C IP 位址：

```
IP 位址     ：11001011 01001010 11001101 00000000 (203.74.205.0)

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

子網路切割實例（一）

- A 企業由於業務需求，內部必須分成 A1、A2、A3、A4 等 4 個獨立的網路。
- 首先要決定的是子網路位址的長度為 3 Bits
- 網路位址變成 24 + 3 = 27 Bits。因此，新的子網路遮罩為：

```
11111111 11111111 11111111 11100000 (255.255.255.224)
```

- 主機位址只能使用剩下的 5 Bits。因此，每個子網路可以有 $2^5 = 32$ 個可用的主機位址。

子網路切割實例（一）

- A 企業的網管人員接著便必須決定子網路分配的方式。下表將子網路依序分配給 A1 - A4 等 4 個網路：

表 8-05　A 企業可用的子網路

網路	可設定的 IP 位址	子網路遮罩
A1	203.74.205.33 - 203.74.205.62	255.255.255.224
A2	203.74.205.65 - 203.74.205.94	255.255.255.224
A3	203.74.205.97 - 203.74.205.126	255.255.255.224
A4	203.74.205.129 - 203.74.205.158	255.255.255.224
未分配	203.74.205.161 - 203.74.205.190	255.255.255.224
未分配	203.74.205.193 - 203.74.205.222	255.255.255.224

子網路切割實例（一）

- 有兩項要請讀者注意：
  - 子網路可再進一步切割成更小的子網路。
  - 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。

8-6-4 子網路切割實例（二）

- 1. 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, 我們將最後一個數字改寫為 2 進位：

```
IP 位址：   192      .168       .1          .10000110
子網路遮罩：11111111.11111111 .11111111  .11111000
                                                子網路位址
```

  - 原 IP 位址第 4 個數字的前 5 個 Bits 用來分割子網路, 故 192.168.1.134 位於 10000 這個子網路, 此子網路的網路位址為 192.168.1.128（2 進位的 10000000 相當於 10 進位的 128）。

子網路切割實例（二）

- 2. 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？
  - 我們將主機位址與 255.255.255.224 子網路遮罩改寫為 2 進位：

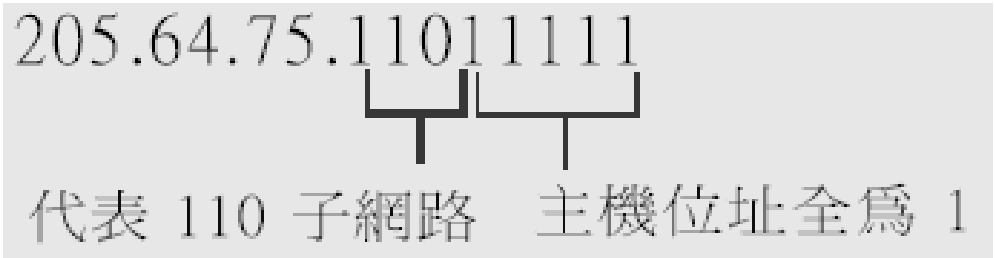
IP 位址： 205 .64 .75 .11011111

子網路遮罩：11111111.11111111 .11111111 .11100000

子網路位址

子網路切割實例（二）

- 由子網路遮罩可知, 主機位址的前 3 個 Bits 代表子網路位址：



- 由於主機位址不得全為 1, 所以 205.64.75.223 不是 110 子網路裡網路設備可用的 IP 位址。

子網路切割實例（二）

- 3. 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 $2^6 - 2 = 62$ 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（二）

- 4. 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？
  - 由於全 0 與全 1 的子網路不能使用, 所以子網路遮罩至少須能分割出 13 + 2 = 15 個子網路, $2^4 = 16 > 15$ 而 $2^3 = 8 < 15$, 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）。

8-7 無等級的 IP 位址

- 當初在設計 IP 位址的等級時, 網路環境主要是由大型主機所組成, 主機與網路的總數都相當有限。
- 對於 IP 位址的需求迅速增加。3 種等級的 IP 位址分配方式, 很快便產生了一些問題。
- 這其中最嚴重的便是 Class B 的 IP 位址面臨缺貨的危機；但是相對地, Class C 使用的數量則僅是緩慢成長。

無等級的 **IP** 位址

- 為了解決這個問題, 便產生了 Classless Inter-Domain Routing（CIDR）, 亦即無等級（Classless）的 IP 位址劃分方式。

8-7-1 CIDR 原理

- Class B 那麼快被耗盡, 有很多位址空間是浪費掉了。。
  - 是否可以將數個 Class C 的 IP 位址『合併』起來, 分配給原先要求申請 Class B 的企業。
  - 使用子網路遮罩來定義較具彈性的網路位址。
- CIDR 又稱為超網路（Supernet）

子網路 與 超網路

- 子網路（Subnet）
  - 利用子網路遮罩重新定義較長的網路位址，以便將現有的網路加以切割成 2、4、8、16 等 2 冪方數的子網路。
- 超網路（Supernet）
  - 利用子網路遮罩重新定義較短的網路位址，以便將現有 2、4、8、16 等 2 冪方數的網路，『合併』成為一個網路。

8-7-2 CIDR 實例

- 回到 B 企業的例子, 由於 B 企業所須的 1500 個 IP 位址。藉由 CIDR 的方式, 我們可以分配一個長度為 21 Bits 的網路位址給 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, 與 B 企業所需的 1500 個 IP 位址相近。
- 與直接分配 Class B 相比, 節省下許多 IP 位址空間。

CIDR 實例

- 由於合併是透過變更網路位址長度來進行, 因此會有以下的限制：
  - 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。
- 因此, 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：

CIDR 實例

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)

CIDR 實例

- 這 8 個連續的 Class C 位址可以利用下列方式來表示：

```
IP 位址     ：203.74.200.0  (11001011 01001010 11001000 00000000)
                                          代表 8 個要合併
Subnet Mask：255.255.248.0 (11111111 11111111 11111000 00000000)
```

- 表示由 203.74.200.0 開始到 203.74.207.0 共 8 個 Class C 位址空間要合併。或是使用更簡潔的方式來表示：

```
203.74.200.0 /21
```

CIDR 實例

- 雖然 CIDR 原先是為了合併 Class C 位址所設計, 但在實作上可適用於任何的 IP 位址範圍, 例如：ISP 可分配長度為 30 Bits 的網路位址給一些只有兩部電腦的個人公司。

```
128.211.176.212 /30
```

CIDR 實例

- 由於 CIDR 讓 IP 位址在分配時更具彈性與效率, 因此, 目前皆是以 CIDR 的方式來劃分 IP 位址範圍。
- 多年前, 許多專家都預測 IPv4 的 32 Bits 位址空間將於西元 2000 年用盡。所幸新的技術不斷誕生, 為 IPv4 爭取更長的壽命。除了子網路、CIDR 等方案外, 接著要介紹的『網路位址轉譯』也是一項節省 IP 位址空間的重要技術。

8-8 網路位址轉譯（NAT）

- 近年來由於網際網路的日漸普及，IP 位址也逐漸不敷使用。一般公司行號所能申請到的 IP 位址數量有限，經常有不夠用的情況發生。
- 為此『網路位址轉譯』（Network Address Translation, NAT）機制應運而生，它可以解決 IP 位址不足的頭痛問題，讓許多台電腦可以共用一個合法的 IP 位址。

8-8-1 網路位址轉譯的原理

- 網路位址轉譯的運作方式如下圖所示：

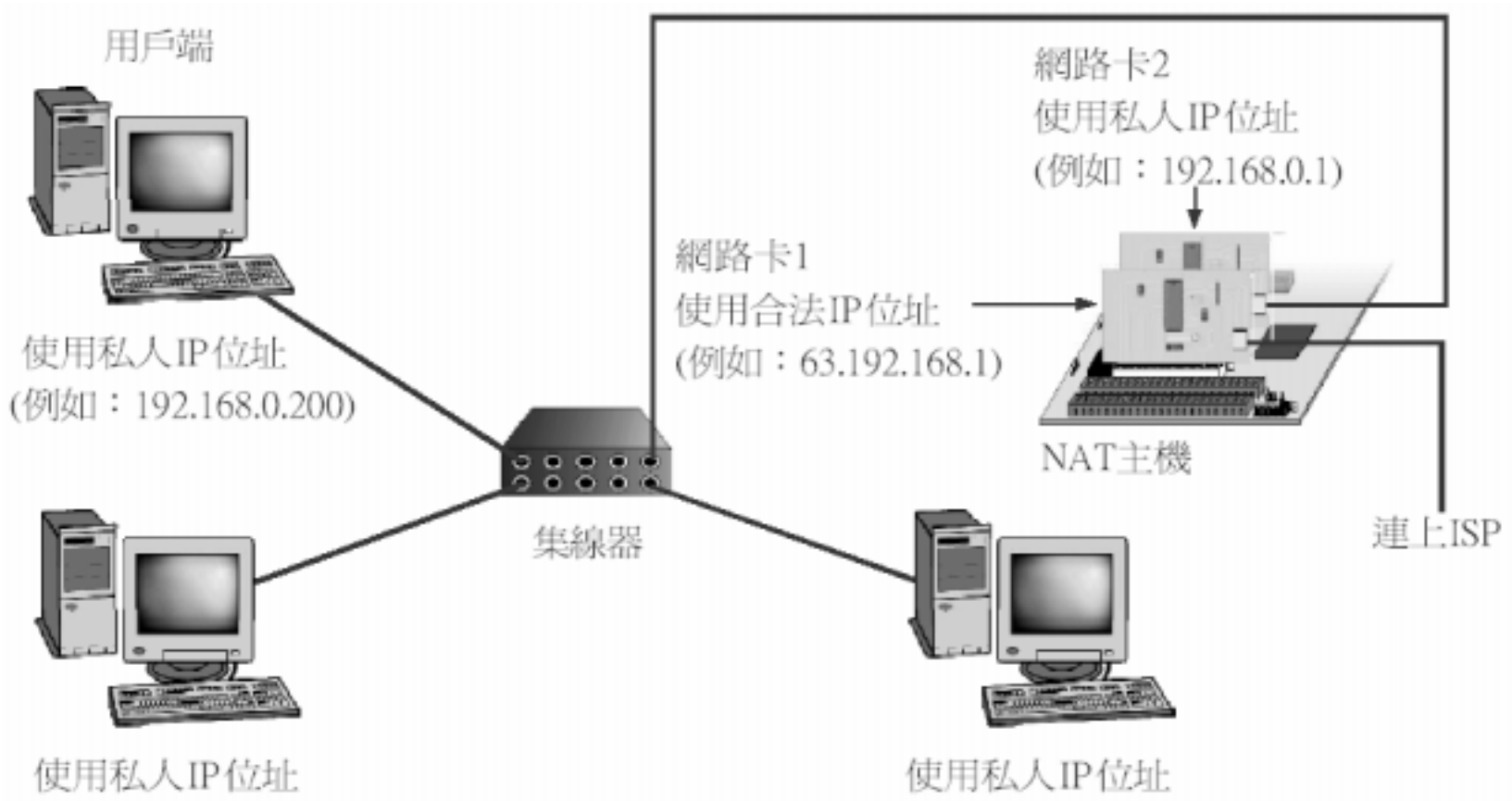


圖 8-13　網路位址轉譯的運作架構(專線或固定制 ADSL)

網路位址轉譯的原理

- 整個區域網路內的電腦（或稱用戶端）皆使用私人 IP 位址，並透過一個合法的 IP 位址與外界連線。
- 這個合法的 IP 位址可以是透過專線或固定制 ADSL 連接的固定式 IP 位址，或是透過撥接由 ISP 分配的動態 IP 位址：

網路位址轉譯的原理

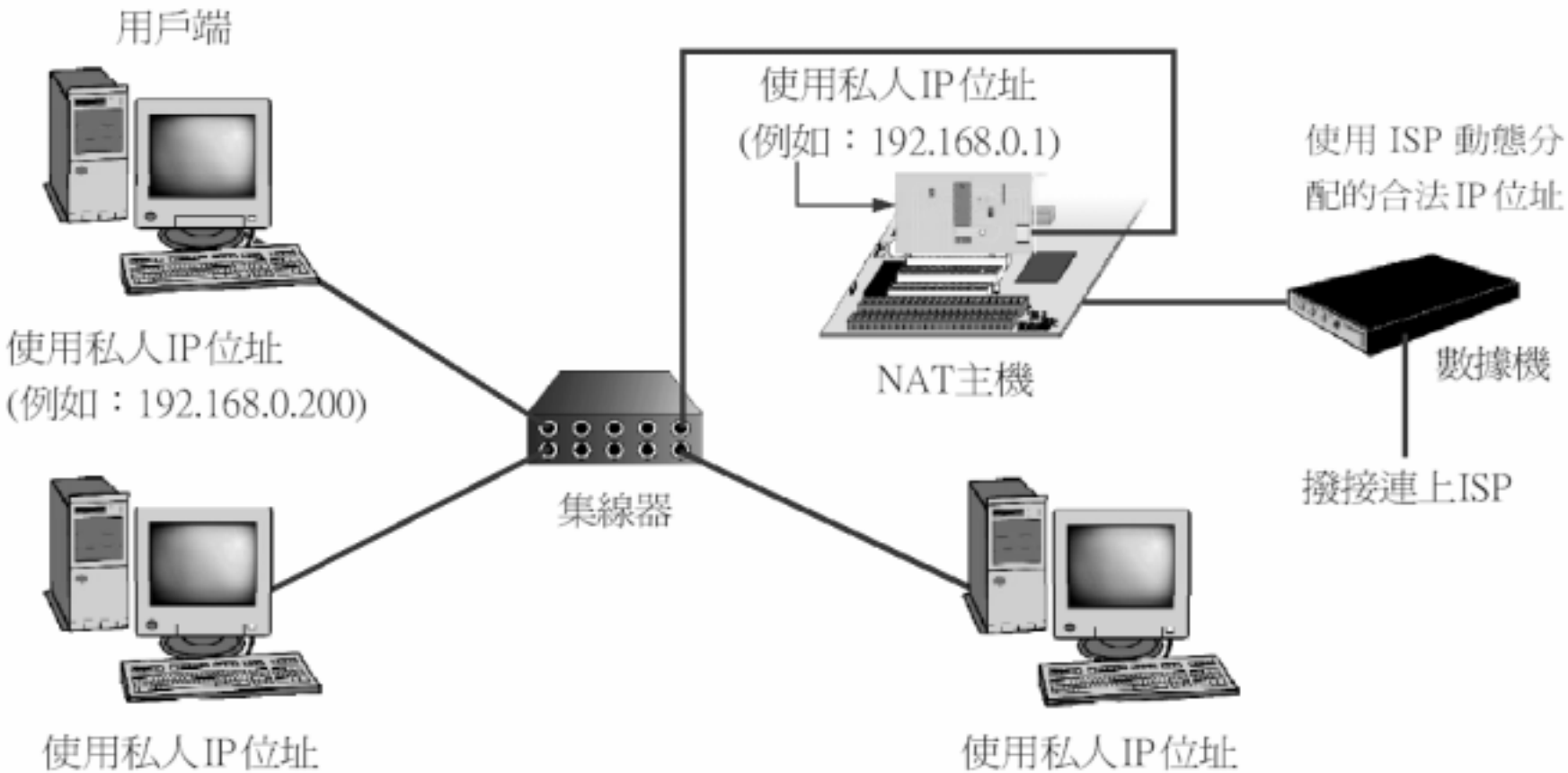


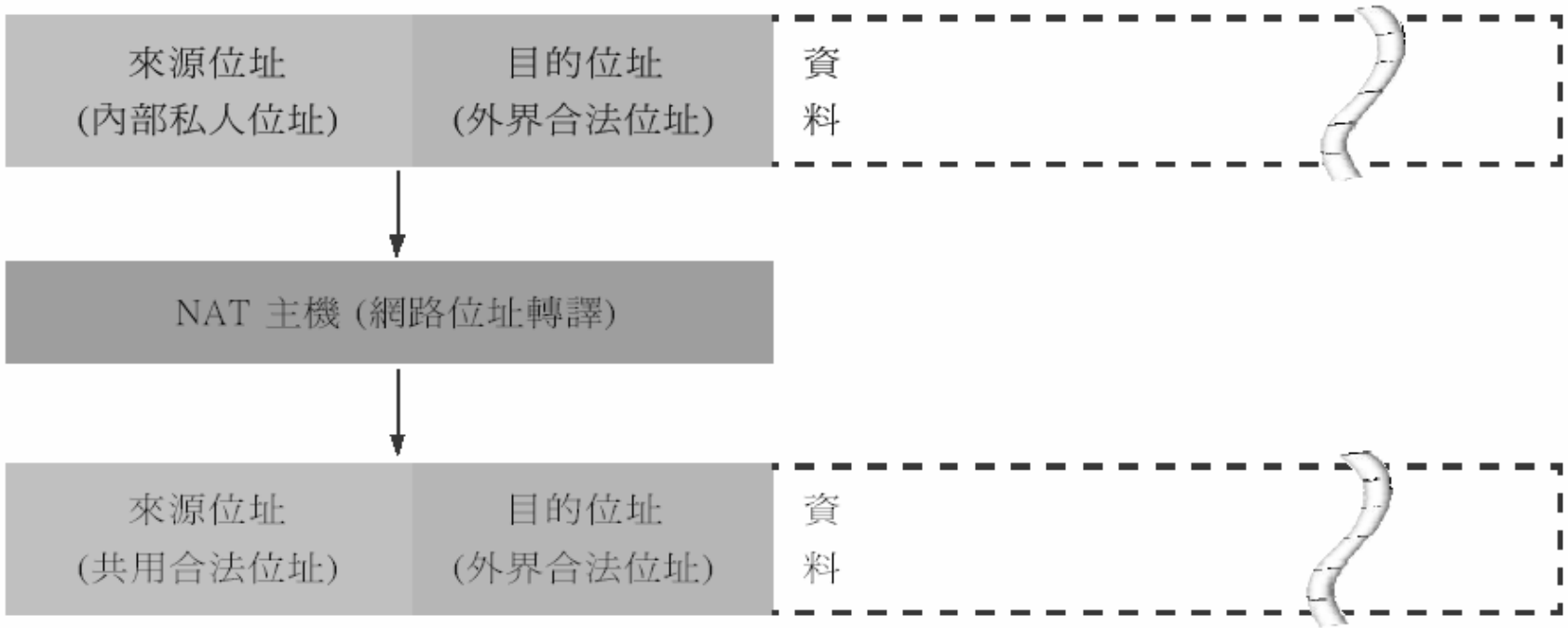
圖 8-14　網路位址轉譯的運作架構 (撥接)

網路位址轉譯的原理

- 網路位址轉譯的原理
  - 對外傳送 IP 封包, 首先會送至 NAT 主機, 並在此將 IP 封包的來源位址, 從私人位址轉為合法的 IP 位址後, 再送到外界。
  - IP 封包從外界送入時, NAT 主機會先判斷封包目的地, 然後將目的位址從合法的 IP 位址轉為私人位址, 再送到區域網路內。

網路位址轉譯的原理

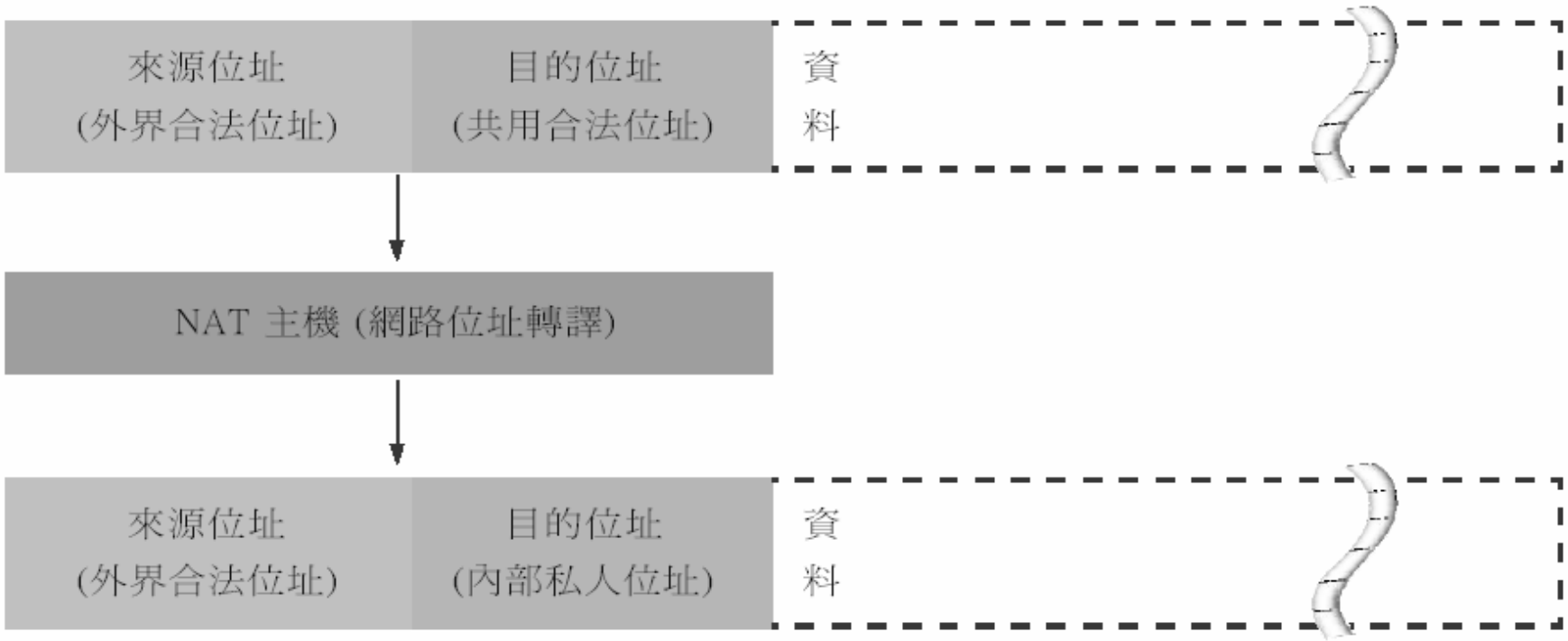
※送出封包時



NAT 主機向外送出的資料封包

網路位址轉譯的原理

※接收封包時



廣域網路傳入 NAT 主機的資料封包

圖 8-15　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, 網路位址轉譯機制如何判斷那個 IP 封包該送給那一台電腦呢？
  - 這主要是藉由用戶端 TCP / UDP 連接埠號碼來判斷。
- 我們以向 Internet 上的 Web 伺服器要求網頁資料為例（各作業系統實作 NAT 方式不盡相同, 以下以 Windows 為例）, 說明連接埠在 NAT 中扮演的腳色：

網路位址轉譯的原理

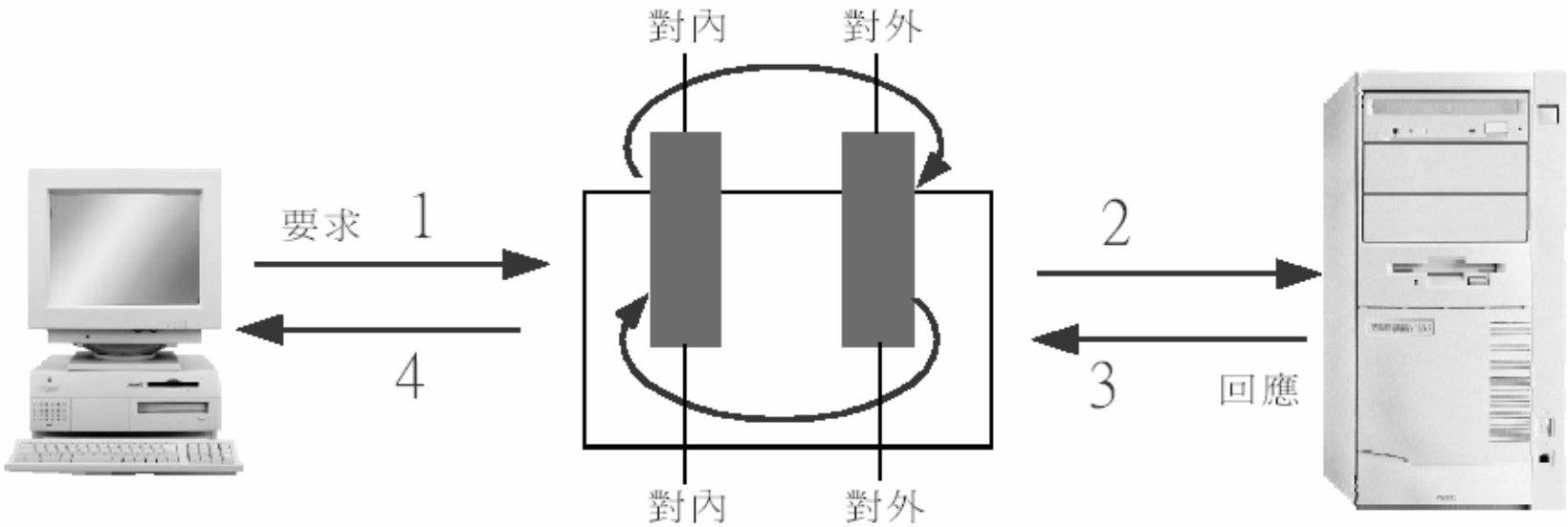


圖 8-16　透過 NAT 存取 Web 伺服器的運作方式

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）

  經由 IP 路由機制（詳見第 10 章）此封包會傳送到 NAT 主機。

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（本例為 6000，對應到 192.168.0.200：5000）。然後根據這個連接埠，產生如下的新封包：
  - 目的地 IP 位址 = 203.74.253.1（Web 伺服器）
  - 來源 IP 位址 = 63.192.168.1（NAT 主機）
  - 目的地連接埠 = 80
  - 來源連接埠 = 6000（由 NAT 主機自行產生，用來對應用戶端的 IP 位址）

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（NAT 用戶端）
  - 來源 IP 位址 = 203.74.253.1（Web 伺服器）
  - 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

8-8-2 網路位址轉譯的注意事項

- 網路位址轉譯雖然解決了 IP 位址不足的問題, 但在使用上仍有其限制：
  - 無法使用某些加密協定
  - 增加伺服器的運算負擔
  - 外界主動存取時, 設定較為複雜

外界主動存取時, 設定較為複雜

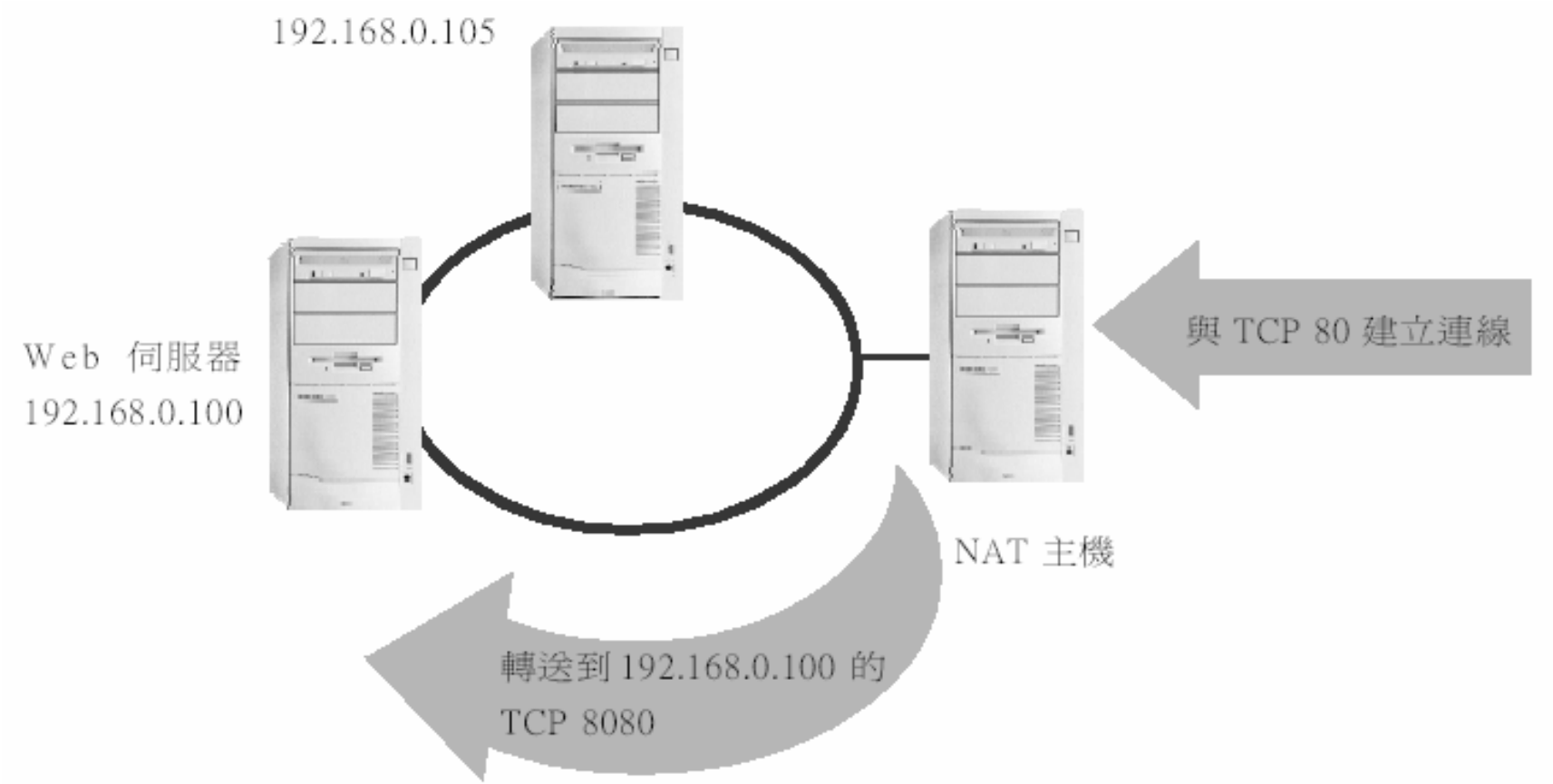


圖 8-17 在 NAT 環境架設 Web 伺服器之示意圖

外界主動存取時, 設定較為複雜

- 基本上, 上述的原理適用於所有的 NAT 環境, 然而在實際的設定方式上, 會因為各家產品的限制條件而有差異。