上個章節我們利用 Squid 伺服器的快取功能，減少了用戶端直接連接 Internet 的機會，因而提高了網路頻寬的使用效率。接下來要討論的是另一個 Internet 上日愈嚴重的問題－IP 不足，這在目前以 IPv 4 為主軸的網路環境中，的確困擾許多系統及網路設計人員。在 1 我們將使用 NAT 的方式來提供此一問題的解決方案，此外，利用 NAT 觀念的延伸，本書也將介紹防火牆的基本觀念，以及它對企業網路安全性的影響。

9-1 淺談 IP

因為 NAT 主要是為了解決 IP 位址不足的問題，所以在學習 NAT 之前，必須先對 IP 位址的意義及功能有基本的了解。在此小節中，我們將就 IP 的基本特性作一簡介，以幫助讀者建立正確的觀念。

IP 的定義

IP（Internet Protocol）是位於網路層（Network Layer）的通訊協定，同時也是 TCP/IP 中最重要的二個通訊協定之一，目前在 Internet 中通用的版本為 IPv 4，有關它的標準都定義在 RFC 791 中。

在 IP 中主要定義三個基本觀念：

- 在 TCP/IP 網路中定義資料傳輸的基本單位—資料包（Datagram），所以資料在網路上傳遞都具有特定的格式。
- IP 執行路由（Routing）的功能，它會選擇一條最佳路徑以供資料傳輸之用。
- 訂立封包在不可靠（Unreliable）的網路上傳遞時，應該遵守的原則。

而通常 IP 是利用以下的運作模式將資料傳送到網路上：

步驟1 來源主機 IP 階層之上的傳輸服務先將資料以 TCP 或 UDP 的格式傳送到 IP 階層

步驟2 IP 階層將來源及目的地資訊（用來在網路上路由的資料）與 IP 資料流組合

步驟3 IP 階層將資料流向下傳送到網路介面階層，在這一層中，資料連結服務會將 IP 資料流轉換成框架（Frame），以便在實體網路中的特定媒體上進行傳遞。

步驟4 因為每個 IP 資料流都包含來源及目的地 IP 位址，所以每部主機上的 IP 階層服務會檢查每個資料流的目的地位址，然後將這個位址與區域維護的路由表相比較，再判定需進一步採取的轉送動作，而在目的地主機上則執行反向處理。

IP 定址

除了路由之外，IP 的另一項重要功能為—定址（Addressing），目前 Internet 上都使用這套標準來表示主機和網路節區的邏輯位址，透過這個管理模式，我們可以確定每部主機或是網路都擁有唯一的識別方法，這可避免位址重覆的發生。

注意一點，雖然每個網路設備的硬體位址也具有唯一性，可用來精確表示網路上的主機位置，但因為無法利用其位址來建立一套管理原則，所以通常無法達到定址的功能，因此才設計出 IP 的定址方法。

在 IP v 4 中，每部主機所使用的 IP 位址都是以 32 個 2 進位的數字來表示，例如 01110101011001010010110101101111，這種表示法可以確保 Internet 上的每部主機都有唯一的位址。因為此類型的位址都需經過 InterNIC 的授權才可使用，所以若知道特定主機的 IP 位址，就可利用這個位址連接到此主機。

在以上的例子中，我們使用 32 個 2 進位數字來表示 IP 位址，當然也可以使用十六進位（75652D6F）或是十進位（1969565039）來表示，但這些表示法都很難讓一般使用者記憶。

因此，IP 位址通常使用 Dotted Decimal Notation（DDN）表示法，它是將 32 個 2 進位的位元分為四個位元組（有時也稱為 Octets），然後將每個位元組以十位進值來表示，而每個位元組之間以一個句點（.）來區隔。因此上例中的 IP 位址 DDE 表示法為 117.101.45.111，這個表示法並沒有什麼特殊的意義，只是利於識別上的方便。

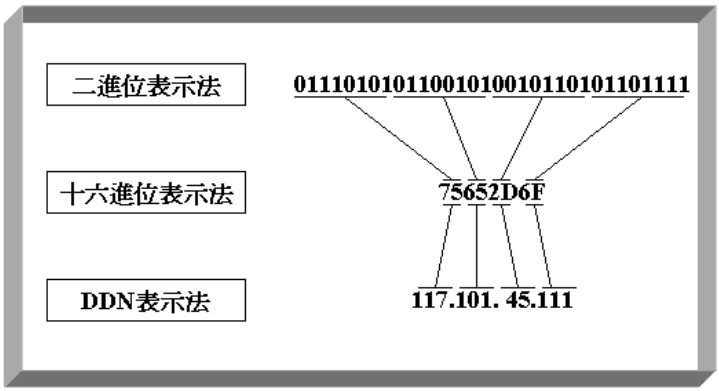

圖 9-1　不同的 IP 位址表示法

根據 IP 的定義，每個 IP 位址都是由二個部份所組成：網路識別碼（Network ID）及主機識別碼（Host ID），例如網路識別碼包含 8 個位元，則主機識別碼就有 32 – 8 = 24 個位元。若要判斷網路識別碼和主機識別碼包含的位元數，則必須使用「子網路遮罩」（Subnet Mask）和 IP 位址來運算。舉例來說，在一般的情形下，IP 位址為 150.23.51.36 的網路識別碼是「150.23」而主機識別碼為「51.36」。

圖 9-2　IP 位址是由網路識別碼及主機識別碼所組成

網路識別碼在網路中是相當重要的觀念，因為它可用來識別 TCP/IP 網路中的網路節區，所有位於同一個網路節區中的主機，都擁有相同的網路識別碼。

換句話說，如果二部主機 IP 位址包含相同的網路識別碼，則它們可互相傳遞訊息，而不需透過路由器或閘道器的轉送。反之，若二部主機 IP 位址經過子網路遮罩運算後的網路識別碼不同，則它們必須透過路由器或閘道器的轉送才可彼此通訊。所以在規劃區域網路時須特別注意這點，否則隨意的指定 IP 位址，可能會產生無法通訊的問題

而主機識別碼是用來辨識 TCP/IP 網路中的節點（可能是工作站、伺服器、路由器或其他 TCP/IP 裝置），每部裝置的主機識別碼在本地的網路節區都必須是唯一，若是同一網路節區中的二部主機具有相同的主機識別碼，則它們會發生無法連接網路的問題，但是在不同網路節區中的二部主機可以使用相同的主機識別碼。

舉例來說，150.128.3.11 和 150.128.3.11 不能同時存在網路中，因為它們的網路識別碼和主機識別碼都相同，但是 150.128.3.11 和 145.200.3.11 可以同時存在不同的網路中，因為它們的主機識別碼雖然相同，但是網路識別碼卻不同。

IP 位址類別

因為每個 IP 位址都是是由 32 個 2 進位的數字所組成，所以理論上應該會存在 2 的 32 次方個外部 IP 位址（2^{32} = 4294967296），但是事實上並沒有這個多 IP 位址。目前 InterNIC 利用控制 IP 位址中的第一個位元組（前 8 個位元）來區分為五個 IP 類別，我們稱它們為 Class A、Class B、Class C、Class D 和 Class E。

IP 位址類別定義出每個位址的網路及主機識別碼使用那些位元，以及每個網路支援的網路及主機數目，而一般 Internet 上的主機 IP 位址都

屬於 Class A、Class B 和 Class C 三類，它們的內容如下表所示（X 表示可為 0 或 1 的二進位值）：

IP 位址類別				
類別	1st 位元組	1st 位元組數值	網路數	每個網路主機數
A	0XXXXXX	1 到 126	126	16777214
B	10XXXXXX	128 到 191	16384	65534
C	110XXXXX	192 到 223	2097152	254
D	1110XXXX	224 到 239	—	—
E	11110XXX	240 到 254	—	—

❖ **Class A**

在 Class A 網路中，每個網路都是利用前 8 個位元來定義，因此有時也稱為「/8 網路」。因為第一個位元已被事先定義為二進位的 0，所以 Class A 的第 1 個位元組是由 00000001 到 01111111，也就是十進位的 1 到 127，但因為 127 是特殊的網路識別碼（Loopback Address），所以目前 Internet 上具有 126 個 Class A 網路。

Class A 使用最後 3 個位元組（24 個位元）來表示主機識別碼，因此每個 Class A 網路可以包含的主機數目為 2 的 24 次方，也就是 16777216 部主機。但是主機識別碼全為 1 和 0 表示廣播及網路位址，因此每個 Class A 網路實際的主機數目為 16777214，由此可知，所有 Class A 的主機數目是 126 * 16777214 = 2113928964。

❖ **Class B**

在 Class B 網路中，每個網路都是利用前 16 個位元來定義，因此有時也稱為「/16 網路」。因為前 2 個位元已被事先定義為二進位的 10，所以 Class B 的第一個位元組是由 10000001 到 10111111，也就是十進位的 128 到 191，而第二個位元組也是網

路識別碼，所以 Internet 上具有 64 * 2^8 = 16384 個 Class B 網路。

Class B 使用最後 2 個位元組(16 個位元)來表示主機識別碼，因此每個 Class B 網路可以包含的主機數目為 2 的 16 次方，也就是 65536 部主機。但是主機識別碼全為 1 和 0 表示廣播及網路位址，因此實際的主機數目為 65534，由此可知，所有 Class B 的主機數目是 16384 * 65534 = 1073709056。

❖ **Class C**

在 Class C 網路中，每個網路都是利用前 24 個位元來定義，因此有時也稱為「/24 網路」。因為前 3 個位元已被事先定義為二進位的 110，所以 Class C 的第一個位元組是由 11000001 到 11011111，也就是十進位的 192 到 223，而第 2 和第 3 個位元組也是網路識別碼，所以目前 Internet 上具有 32 * 2^{16}= 2097152 個 Class C 網路。

Class C 使用最後 1 個位元組(8 個位元)來表示主機識別碼，因此每個 Class C 網路可以包含的主機數目為 2 的 8 次方，也就是 256 部主機。但是主機識別碼全為 1 和 0 表示廣播及網路位址，因此實際的主機數目為 254，而所有 Class C 的主機數目是 254 * 2097152 = 532676608。

❖ **Class D**

Class D 的 IP 位址只供多點傳送(Multicast)的群組電腦使用，也就是說，以這些位址傳送的訊息可以同時傳送到多部主機，它是用在某些特殊的群組軟體或服務。

Class D 網路的前 4 個位元已被事先定義為二進位的 1110，所以 Class D 的第一個位元組是由 11100001 到 11101111，也就是十進位的 224 到 239，所以目前有 16 個 Class D 網路，但這些位址並不提供一般 Internet 主機使用，而且它可不具有子網路遮罩。

❖ **Class E**

Class E 是屬於實驗用的位址，這些位址並不提供一般 Internet 主機使用，它的前 5 個位元已被事先定義為二進位的 11110，所以 Class D 的第一個位元組是由 11110001 到 11110111，也就是十進位的 240 到 254，所以目前有 15 個 Class E 網路。

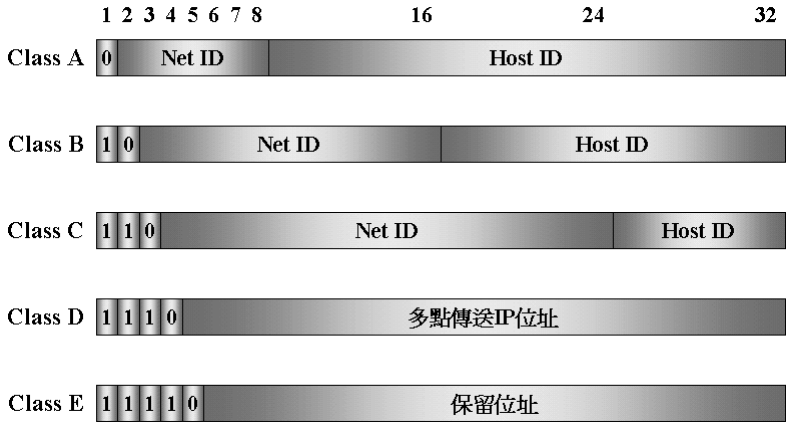

圖 9-3　IP 位址類別

❖ **私有 IP 位址**

若是網路並不連接 Internet，則不需為了使用 TCP/IP 通訊協定而向 InterNIC 或 ISP 取得已登錄的 IP 位址使用權，在此情形下，IANA 建議使用「私有 IP 位址」(Private IP Address)。

這些位址都是由 IANA 所保留，主要提供 TCP/IP 網路上的私人使用，Internet 上的主機也不可以使用這些位址，而這些私有 IP 位址常提供 NAT 運作上使用。這些私有 IP 位址的範圍如下表所示：

私人網路識別碼	子網路遮罩	IP 位址範圍
10.0.0.0	255.255.255.0	192.168.0.1 到 10.255.255.254
172.16.0.0	255.240.0.0	172.16.0.1 到 172.31.255.254
192.168.0.0	255.255.0.0	192.168.0.1 到 192.168.255.254

有些人習慣將 IANA 所保留 IP 位址，稱為「虛擬 IP」，而在 Internet 上的位址則稱為「實體 IP」，但筆者認為這些名稱並不適當。因為保留的 IP 位址也是由 RFC 正式定義的 IP 位址，何來「虛擬」之說呢？所以本書將以「內部 IP」來表示由 IANA 所保留 IP 位址，而在 Internet 上使用的 IP 位址則以「外部 IP」來表示。

子網路遮罩

「子網路遮罩」（Subnet Mask）和一般 IP 位址相同，都是由 32 個二進位數字所組成，它唯一功能就是辨別 IP 位址中，網路識別碼和主機識別碼的部份為何，這在網路傳輸上相當重要，因為具有相同網路識別碼的主機可以直接通訊，而不同網路識別碼的主機則需要透過閘道器來轉送訊息。

在利用子網路遮罩判斷 IP 位址中的網路識別碼和主機識別碼部份時，您需依照以下的步驟來運算，本書在此以一個 Class B 的 IP 位址—150.23.56.25 和 Class B 預設的子網路遮罩—255.255.0.0 為例：

步驟 1 將 IP 位址轉換為二進位表示法

在子網路遮罩和子網路切割運算中，所有的 IP 位址及子網路遮罩都必須先轉換為二進位表示法。在本例中 150.23.56.25 的二進位表示法為 10010110000101110011100000011001。

在轉換為二進位表示法時須注意一點，若是不足 8 位時需以 0 補足，例如 56 的二進位表示法應寫成「00111000」，而不是「111000」。

步驟 2 將子網路遮罩轉換為二進位表示法

在本例中，子網路遮罩 255.255.0.0 的二進位表示法為 11111111111111110000000000000000，而各種類型網路預設的子網路遮罩如下表所示：

位址類型	子網路遮罩的位元	子網路遮罩
Class A	11111111 00000000 00000000 00000000	255.255.255.0
Class B	11111111 11111111 00000000 00000000	255.255.0.0
Class C	11111111 11111111 11111111 00000000	255.255.255.0

步驟 3 將以二進位表示法的 IP 位址和子網路遮罩利用「AND」運算

所謂「AND」運算是指真值表中「且」的運算，只要二者其中有一個是 0，則運算後的值就為 0，只有在二者都為 1 的情形下才會為 1，因此所有 AND 運算的結果為：1 AND 1 = 1、1 AND 0 = 0、0 AND 1 = 0 以及 0 AND 0 = 0 等。

在了解 AND 運算後，您就可以將以二進位表示法的 IP 位址和子網路遮罩利用「AND」來運算，下圖是運算的過程及結果：

IP 位址：	10010110000101110011100000011001
子網路遮罩：	11111111111111110000000000000000
AND 運算結果：	10010110000101110000000000000000
運算結果十位進值：	150.23.0.0

步驟 4 運算結果中非 0 的部份為網路識別碼

在 IP 位址和子網路遮罩利用「AND」運算後，它的結果中非 0 的部份即為網路識別碼，在本例中為「150.23」，但是通常我們習慣用 0 來將它寫成類以 IP 位址的形態，例如「150.23.0.0」。

而封包在進行傳送前，IP 即是以這個方法來判斷目的地主機是否存在本地網路，若是目的地主機位於遠端網路，IP 就會將此訊息傳送到路由器或預設閘道器。

若要防止定址及路由問題，應該確保在網路區段中的所有 TCP/IP 主機都使用相同的子網路遮罩。