信祥事業群　　Network 常識-NAT(Issue 01)

等級	網路組數	網路範圍
A	7bits = 2^7 = 128 組	0-127.xx.xx.xx
B	14bits = 2^14 = 16384 組	128-191.0-254.xx.xx
C	21bits = 2^21 = 2097152 組	192-223.0-254.0-254.xx

在 RFC1918 中網際網路上負責分配 IP 位址的 IANA (Internet Assigned Number Authority) 將下面三段 IP 位址空間保留給私有網路使用

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

以上三段私有 IP 位址空間只允許用於內部私有網路中，故對外不必註冊。

較常用的解決方案是使用 NAT (Network Address Translation) Router 來動態分配正式的 IP 位址。當電腦連線到外面的網際網路時才將內部私有 IP 位址轉換成正式的 IP 位址。因爲同一時間連上網際網路的電腦個數將會低於所有內部網路的電腦總數，將正式的 IP 位址動態的分配給需要用到的電腦結束後再收回，可達到節省位址空間的目的。使用 NAT Router 幾乎與應用程式無關，因爲它只在第三層(IP 協定層)運作處理。

NAT Router 是如何來完成 IP 位址轉換的功能？

一般說來有靜態和動態二種方式，說明如下：

先定義 m 及 n 二個參數
m: 需要被轉換的 IP 位址個數 （私有的 IP 位址或舊的 IP 位址）
n: 能夠被分配的 IP 位址個數 （正式的 IP 位址或新的 IP 位址）

- **靜態 NAT 的定義爲**
  m:n-Translation， m，n≧1 and m = n (m，n is N)
  也就是說私有的 IP 位址個數與正式的 IP 位址個數相同

  靜態 NAT 的實作很簡單，只要一行邏輯轉換公式即可完成
  new-ip-addr = new-network-id OR (old-ip-addr AND (NOT netmask))

例如，NAT Router 要將網路 192.168.1 上所有的 IP 位址轉換成網路 140.109.5 上所有相對應的 IP 位址，netmask 皆爲 255.255.255.0，現在私有的 IP 位址 192.168.1.3 要轉換成正式的 IP 位址 140.109.5.3。

```
old-ip-addr     = 192.168.1.3
                = old-network-id + old-host-id
                = 1100 0000 1010 1000 0000 0001 + 0000 0011 = 192 168 1 + 3
NOT netmask     = 0000 0000 0000 0000 0000 0000   1111 1111
-------------------------------------------------------------
                AND
                = 0000 0000 0000 0000 0000 0000   0000 0011
new-network-id = 1000 1100 0110 1101 0000 0101   0000 0000 = 140 109 5
-------------------------------------------------------------
                OR
                = 1000 1100 0110 1101 0000 0101 + 0000 0011 = 140 109 5 + 3
                = new-ip-addr = 140.109.5.3
```

- **動態 NAT 的定義爲**

  m:n-Translation， m，n≧1 and m≧n (m，n is N)
  也就是說私有的 IP 位址個數大於正式的 IP 位址個數；或是雖然二者個數相同但是基於安全理由不希望使用靜態的對應方式。

  在動態 NAT 的環境中能夠連通外界網路的機器個數受限於正式的 IP 位址個數。當所有正式的 IP 位址分配完畢之後，任何的 IP 位址轉換要求將會被 NAT Router 拒絕，並回傳 host unreachable 之 ICMP 封包。動態 NAT 之實作較靜態 NAT 複雜，因爲它必需維護一個動態表格以便記錄私有 IP 位址與正式 IP 位址之對應關係。

  例如，NAT Router 要將 B 等級網路 172.16 上所有的 IP 位址動態轉換成 C 等級網路 140.109.5 上的 IP 位址範圍。每次內部網路有機器要連通外部網路時 NAT Router 會從 140.109.5 上的 IP 位址範圍內動態取得尚未分配出去的 IP 位址並記錄在動態表格中直到斷線。若是內部網路機器的資料已經存在動態表格中就使用該筆資料作轉換。只要動態表格中存在某內部網路機器的資料，外部網路的人就可以利用其所對應之正式 IP 位址與該內部網路機器連線。請參考下面的示意圖。

  ```
  src 172.16.2.100 --> NAT Router -->  src 140.109.5.20
  dst 172.16.2.100 <-- NAT Router <--  dst 140.109.5.20
  ```

動態表格

私有 IP 位址	正式 IP 位址
172.16.2.100	140.109.5.20
...	...

如前所述，當 m = n 時有些人基於安全上的考量使用動態 NAT。因爲使用動態 NAT 之後位於外部網路的人無法正確取得內部網路機器的 IP 位址，因爲它每次與外部網路連通的 IP 位址可能都不一樣。

由以上的介紹我們瞭解到 NAT 被提出來的目的，是爲了解決網際網路 IP 位址不足的問題。而在新舊 IP 位址區段的移轉過程中，剛好就可以利用動態 NAT 的特性來達到平順轉移的目的。另一方面由於靜態 NAT 實作容易，而且目前有現成免費的模擬程式可用，所以是一個便宜的解決方案。

案例說明

某企業決定更換 ISP 廠商，由於 IP 位址區段歸屬權的問題，必須將舊有的 IP 位址區段歸還原 ISP 廠商。但是舊有的 IP 位址區段已經分配給網路上所有的節點，況且目前都正在運作使用中，要如何收回再轉移至新的 IP 位址區段呢？而且企業主的基本要求是新舊 ISP (IP 位址區段) 的移轉期間，對網路 Availability 的影響必須降至最低。

解決的方法是，首先保留舊 ISP 先不要斷線，以備移轉失敗時可馬上恢復原來的狀態。這個期間我們會利用靜態 NAT Router，來做新舊 IP 位址區段一對一的靜態轉換工作，此時企業網路上面所有機器的網路相關設定值都不需要變動。

在新舊 IP 位址區段共同運轉的期間，網路封包流通的路由，分成二個部分來說明，請參考

- 若同是舊 IP 位址區段上二部機器互連，則路由不會經過靜態 NAT Router，網路封包只會在舊 IP 位址區段上流通。

- 若是舊 IP 位址區段上的一部機器與企業外面的機器互連，則路由會經過靜態 NAT Router。當企業內部封包通過 NAT Router 時，Source IP 位址會由舊的區段轉換至新的區段；當企業外面封包通過 NAT Router 時 Destination IP 位址會由新的區段轉換至舊的區段。

在新舊 IP 位址區段共同運轉的期間，網域名稱的查詢動作較爲複雜，這也要分成二個部分來說明， 舊 IP 位址區段必需有一個 DNS 伺服器供企業內部使用，inner-DNS 所對應的內容是舊的 IP 位址區段；新 IP 位址區段必需有一個 DNS 伺服器供企業外面使 outter-DNS 所對應的內容是新的 IP 位址區段。outter-DNS 的部分要求新 ISP 廠商協助維護。

- 對企業內部而言，由於網路上面所有機器仍然使用舊的 IP 位址區段，所以必需要有一部 DNS 伺服器，保留住網域名稱與舊 IP 位址區段的對應資料。這部 DNS 伺服器應該放置在企業內部，並只提供企業內部使用。

- 對企業外面而言，在新 IP 位址區段啓用的同時，就必需要有一部 DNS 伺服器，提供網域名稱與新 IP 位址區段的對應資料。這部 DNS 伺服器應該放置在企業外面，可以要求新 ISP 廠商協助維護，並只提供企業外面使用。

注意事項：

在新 IP 位址區段啓用之前，應該先將舊 DNS 資料記錄的 TTL (Time To Live) 值設小，因爲此值決定了該 DNS 資料記錄在其他 DNS 伺服器上存活的時間，如果此值設得很小，則其他 DNS 伺服器就不會將前一次所查詢到的資料記錄 cache 太久。當新的 IP 位址區段與 DNS 伺服器啓用之後，企業外面的人就不會因爲仍然使用舊的 DNS 資料記錄，而造成網路不通的情況。

結論

本文在 IP 轉換程序中所定義的 m 及 n 二參數,其相對比例必須依企業網路進出網際網路的通信率而調整， 此相對比例需以滿足企業網路品質所定義的阻塞率 (Blocking Probability) 爲原則。同時對於常置性服務系統 (如 WWW, Email 等) 與動態系統的分佈亦有重要的影響。

IP 轉移的維運需求已隨著網際網路的普及而日漸擴大。此處所設計的維運方式可作爲一個轉換 IP 位址區段的參考模式。 若企業主想繼續在企?
~網路上使用 相關技術，下一次再度變更 ISP 廠商時，只要導入相同的維運模式即可。如此可保障企業網路維持高度的可用度。發揮網路應有效益， 進而提升整體企業的產能與產值。