

網路架構大概論 3—IP 概念、分級與子網路遮罩

希望經過上篇的連續燃燒彈轟炸之後，各位讀者還有力氣接續看完這篇文章。如果讀者上篇沒有把整篇看懂，至少要知道最基礎的網路 4 層架構，從上層數下來就是應用層、傳輸層、網路層、鏈結層，從下往上數也要背得滾瓜爛熟，不僅有助理解本次內容，對於未來自行架設網路也相當有幫助。

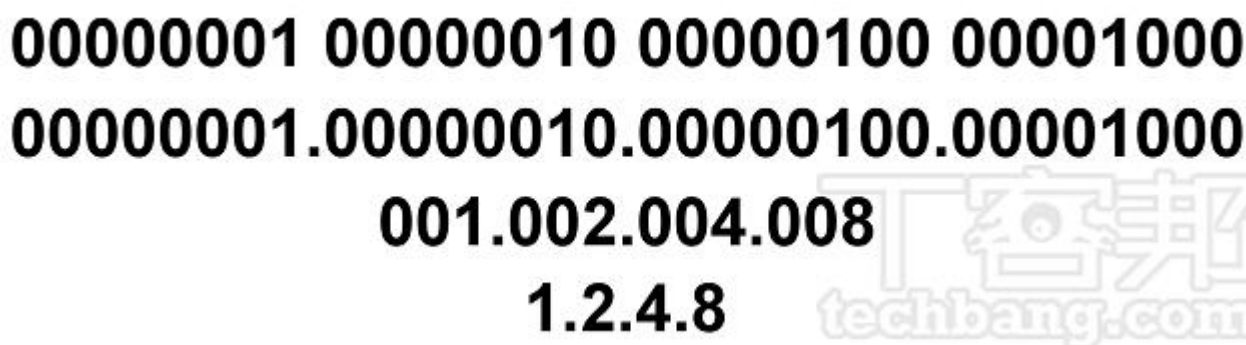
說到自行架設家庭網路，就不能不談到 IP，IP 活在網路架構第 2 層，是現今網路的主要架構。如果讀者已有自行裝設家用路由器的經驗，或曾經接觸過 192.168.0.1 這類的數字，就應該對 IP 概念略知一二；但筆者相信絕大多數人對於 IP 還是懵懵懂懂的状态，曾架設過家庭網路的讀者也可能只知道將 IP 位址設定在 192.168.0.x 就會通了，知其然不知其所以然，並不了解為什麼設定這種 IP 就會通。

IPv4 的位址

在此我們就跳過 IP 版本發展的歷史，直接進入目前世界上使用最廣泛的第四版 IP；IPv4 定義 IP 使用 32 個連續的 0 或是 1 來定址，而大家經常把 32 bit 分組，以 1 組 8 bit 轉換為 10 進位標示。例如 00000001 00000010 00000100 00001000 經常轉換成 1.2.4.8 這種表示法，所以說 32 bit 的 IP 位址，共有 0.0.0.0~255.255.255.255 這麼多的位址可以使用，為 2^{32} 個，可分配給約 43 億個網路設備相互連接，但實際上因為繞送或是其它特殊的保留位置，實際可用的位址約 42 億個，消失的位址稍後會詳細說明。除此之外 1.2.4.8 和 001.002.004.008 這 2 個指的都是同樣的位址，只不過在實務上會將 0 省略不寫。

只要裝置想連上網路，每個網路介面都需要 1 個網路 IP 位置，如果你的電腦中裝設 2 張網路介面卡，則 2 張介面卡均要取得 IP 為止才能正常運作；同理可證，如果筆電同時擁有無線和有線網路，同樣各需取得 IP 才能上網。

00000001 00000010 00000100 00001000
00000001.00000010.00000100.00001000
001.002.004.008
1.2.4.8



▲ IPv4 位址的不同表示法，圖片表示的位址都是對等的

IP 位址的組成

為了管理方便，使用上常將 32 bit 的 IP 再度拆分，由前方的「網路位址」加上後方的「主機位址」共同組成，此外 IPv4 更將位址分成 5 個等級，如以下圖片所示。

Class A 0nnnnnnnn.xxxxxxxx.xxxxxxxx.xxxxxxxx

Class B 10nnnnnnnn.nnnnnnnnnn.xxxxxxxx.xxxxxxxx

Class C 110nnnnnn.nnnnnnnnnn.nnnnnnnnnn.xxxxxxxx

Class D 1110ssss.ssssssssss.ssssssssss.ssssssssss

Class E 1111ssss.ssssssssss.ssssssssss.ssssssssss

▲ Class A~E 5 種不同的 IP 位址等級

Class A~C 的分法比較常見，Class D、E 做為特殊保留用途，之後再詳加說明。大家應該會發現，在圖片中的寫法分別出現了 0、1、n、x 不同的寫法，而這是有其含意的。

Class A~C 有規定其開頭位元數值，Class A 為 02、Class B 為 102、Class C 為 1102，所以只要看到 IP 位址開頭為 0.x.x.x~127.x.x.x，都是屬於 Class A 的位址。Class B 的位址則是因為 10 開頭，所以位址 128.0.x.x~191.255.x.x 都是 Class B 的管轄範圍；那 Class C 呢？就請各位讀者自行算算看了。

各個等級的網路，旗下能夠劃分幾個網路系統也有所規定，Class A 網路除了第一個位元須以 0 開頭之外，其後 7 個位元就是網路的位址（圖中 n 的部分），之後的 24 個位元就是主機位址。也就是說，Class A 能夠擁有 128 個網路系統，而每個網路系統能夠擁有 16777216 個位址（圖中 x 的部分）。Class B 則是規定以 10 開頭，其後 14 個位元為網路位址，最後 16 個位元為主機位址，可提供 16384 個網路，每個網路擁有 65536 個位址。

至於 Class C 的網路則是以 110 開頭，後接 21 個位元網路位址，再接 8 個位元主機位址，可提供 2097152 個網路系統，每個網路系統 256 個位址。

101010^2

在一連串的數值之後，緊接著「下標的數字」，其意義為表示這串數值使用何種進位算法，例如 2 進位（2）、8 進位（8）、16 進位（16）。為避免內文雜亂，本文只在少部分數值加入此種寫法。

保留的 IP 位址

本文開頭時有說到，部分 IP 位址會保留做為其它用途，實際上無法分配給主機使用。其中有 2 種 IP 位址不可分配給主機使用，分別為主機位址全為 0、或是全為 1 的狀況。

第一種情形，就是主機位址不可全部為 0，例如 1.0.0.0（Class A）或是 192.168.0.0（Class C）這種狀況，這種位址原本是用來設計將資料封包丟給網路下所有的主機，但現今大多用於識別 IP 位址所屬網域，所以這種位址不可分配。

第二種情形就是主機位置全部為 1 的狀況，例如 1.255.255.255（Class A）或是 192.168.0.255（Class C），此種 IP 位址指的是「把資料送給此網路下的所有主機」。如果今天某主機送出的資料封包目的地為 192.168.0.255，路由器就會把這份資料封包送給 192.168.0.1~192.168.0.254 當中所有的電腦。我們把 192.168.0.255 這個 IP 位址稱作「廣播位置」，如同里長伯使用擴音喇叭公告事項般，任何想傳送到這個位址上的資料，都會被送到網路中每一台主機。

不同等級的保留位址

除了主機位址不可全為 0 或全為 1 的狀況之外，各個不同等級的網路位址，還有保留部分位址，挪作其它用途，這些 IP 有的無法指派給主機使用，有的則無法在公用的網際網路上傳送；這些無法在公用網路上傳送的位址，稱之為私有位址（private IP）。

另外還必須向讀者說明，部分保留位址是在 Class 制定時就已經預訂保留，部分則是制定 Class 之後才因實際需求而保留，詳細的保留位址範圍可參考 RFC 5735 與 RFC 6598 文件。

有時我們可以見到 192.168.0.0/16 這樣的標示法，「/」其後的數字代表從頭開始，有幾個位元為主機位址，譬如 192.168.0.0/16 就代表前 16 位元為網路位址，指的也就是 192.168.0.0~192.168.255.255 這段網域。

「/」是從 CIDR（classless inter-domain routing）開始才有的寫法，關於 CIDR 文後有較詳盡的解說。

Class A

在 Class A 之中，有 4 個網域無法使用，分別為 0.0.0.0/8、10.0.0.0/8、100.64.0.0/10、127.0.0.0/8。0.0.0.0/8 是個特殊的網路區段，這個位址表示所有、任何、預設的意思。如果在路由表的來源 IP 為只填入 0.0.0.0，代表的就是無論資料封包從哪裡過來，一律套用此路由規則。

127.0.0.0/8，保留做為網路主機的內部迴圈之用，任何發送到 127.0.0.1 的資料封包，都將原封不動的傳回發送主機上，可用以偵測網路環境是否架設妥當。

10.0.0.0/8 網路區段做為內部網路私有 IP 使用，這個範圍的 IP 不可在網際網路上使用，如果任何獲得此 IP 的主機，想要和網際網路上的電腦相互通訊時，則必須通過網路位址轉換（NAT、network address translation）機制，將私有 IP 轉換為合法的網際網路 IP。由於 10.0.0.0/8 的私有 IP 不會在網際網路上出現，就可以在不同的網路下重複使用而不相互影響。

100.64.0.0/10 這個網路範圍在 2012 年 4 月所公布的 RFC 6598 文件之中，才將它劃為內部私有 IP 使用，而且是專門給各地區 ISP 供應商所使用的 CGN（carrier-grade NAT）技術，在 IPv4/IPv6 轉換期間提供過度解決方案。一般來說，NAT 主要是家庭、學校、機關、公司自行所架設的私有網路與外界溝通的轉換機制，但是因為 IPv4 位址接近配發完畢，而 IPv6 又遲遲無法全面上線，加上老舊的網路設備不支援 IPv6 網路，所以產生了由 ISP 業者主導的大型 NAT 網路，在不同地區重複配發相同的 IP 區段位址，解決位址不夠用的燃眉之急。

Class A 扣除掉這些無法被使用的位址，實際上可提供 125（128-3）個網路系統，每個網路系統可提供 16777214（16777216-2）個主機位址。其中 100.0.0.0/8 這個位址範圍中，因為少掉了 100.64.0.0/10 這個部分，所以可提供 12582910（16777216-2-4194304）個主機位址。

產品頁面：DIR-600		Hardware Version：Bx 韌體版本：2.11			
					
DIR-600 //	設定	進階	工具	狀態	支援
網路網路	網路設定 使用此功能表選單以調整您路由器的內部網路設定，並且也可設定內建的 DHCP 伺服器以指派 IP 位址到您網路上的電腦。在此所設定的 IP 位址是您用來使用網頁式管理介面的 IP 位址。如果您在這個功能表選單變更 IP 位址，您可能需要調整您個人電腦的網路設定以再次使用此網路。 請注意這個功能表選單不是必要的，且您不需要變更任何這裡的設定以讓您的網路設定好並執行。 <input type="button" value="儲存設定"/> <input type="button" value="不要儲存設定"/>				有幫助的提示... <ul style="list-style-type: none"> • 如果在您的網路上已經有一台 DHCP 伺服器或是在您網路上的所有裝置均使用靜態 IP 位址，取消勾選「啟用 DHCP 伺服器」以取消這項功能。 • 如果在您的網路上有裝置需要固定的 IP 位址，請為每一個這類裝置新增一個 DHCP 保留。
無線網路設定					
網路設定					
IPv6					
		路由器設定 使用這個功能表選單以組態設定您路由器的組態設定。在此所設定的 IP 位址是您用來使用網頁式管理介面的 IP 位址。如果您變更了這裡的 IP 位址，您可能需要調整您個人電腦的網路設定以再次使用此網路。 路由器 IP 位址： <input type="text" value="192.168.0.1"/> 預設的子網域遮罩： <input type="text" value="255.255.255.0"/> 主機名稱： <input type="text" value="DIR-600"/> 本機的網域名稱： <input type="text"/> (選填的) 啟用 DNS 中繼 (Relay)： <input type="checkbox"/>			
		DHCP 伺服器設定 使用這個功能表選單以組態設定內建的 DHCP 伺服器以對您網路上的電腦分派 IP 位址。 啟用 DHCP 伺服器： <input checked="" type="checkbox"/> DHCP IP 位址範圍： <input type="text" value="100"/> to <input type="text" value="128"/> (在區域網路 (LAN) 子網路內的位址) DHCP 租用時間： <input type="text" value="10080"/> (分鐘)			

▲ D-Link 的家用路由器預設私有 IP 位址為 192.168.0.0/24

Class B

Class B 將 172.16.0.0/12 切為內部網路私有 IP 之用，另外一方面，169.254.0.0/16 這個網路範圍也座落在 Class B 之內，當新加入的電腦主機無法藉由 DHCP (dynamic host configuration protocol) 獲取相對應的 IP 設定時，會拿此範圍的 IP 自動套用。所以扣除以上部分之後，Class B 網路可提供 16367 (16384-16-1) 個網路，每個網路可提供 65534 (65536-2) 個主機位址。

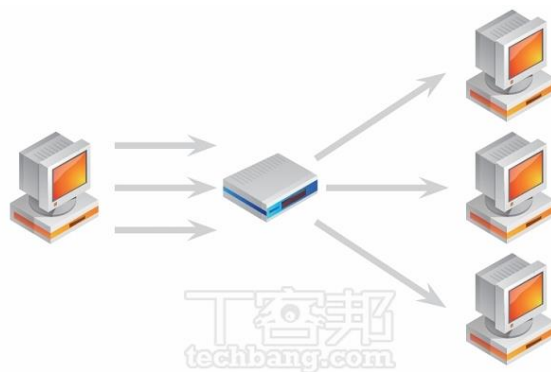
Class C

在 Class C 中，被保留的位址範圍稍微多了一點，分別有 192.0.0.0/24、192.0.2.0/24、192.88.99.0/24、192.168.0.0/16、198.18.0.0/15、198.51.100.0/24、203.0.113.0/24。

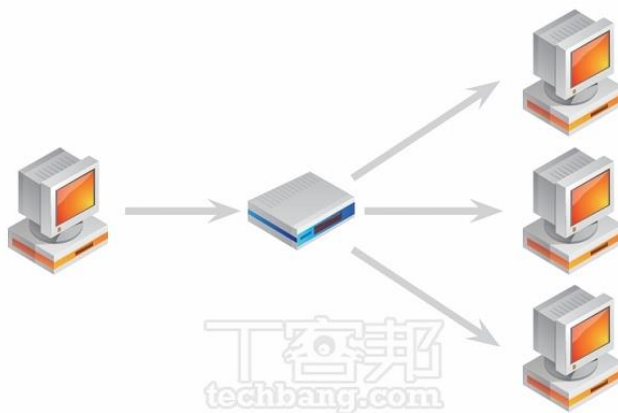
192.168.0.0/16 這個位址範圍相信大家都不陌生，在 Class C 位址之中做為私有 IP 使用，曾經買過家用路由器的讀者都會接觸到，從早期呆呆地只會拿 192.168.0.0/24 或是 192.168.1.0/24 範圍來使用，到現在逐漸延伸到 192.168.10.0/24、192.168.50.0/24 等比較高的位址範圍，避免區域網路中又有 1 個區域網路，造成 IP 打架的問題。如果讀者家中有多個相同品牌的路由器，請將 IP 位址區段分開，避免 IP 位衝突。

192.0.0.0/24 特別保留給 IETF（Internet engineering task force）組織使用，其中 192.0.0.0/29 範圍給 DS-Lite（一種 IPv4/IPv6 的轉換技術）使用。192.88.99.0/24 給 IPv6 轉 IPv4 中繼使用、198.18.0.0/15 則保留做為網路測試之用，192.0.2.0/24、198.51.100.0/24、203.0.113.0/24 則是分別做為教學測試之用。以上除了 192.88.99.0/24 可在公用網際網路出現之外，其餘的位址皆不可在網際網路上流通，Class A 和 Class B 的保留位址也是如此。

Class C 的可用位址東扣西扣下來，只剩下 206379（2097152-1-1-1-256-512-1-1）個網路可使用（不包含 IPv6 to IPv4 relay 位址），每個網路可提供 254（256-2）個主機位址。



▲發送端將同份資料複製之後傳送



▲發送端只發送 1 份資料，到達目的地之前才將檔案複製傳送

Class D、E

在最初的位址分類上，Class D 和 Class E 就不是用來分配網路或主機的位址，而是拿來當作「用途」的 IP 位址，Class D 被用作多點傳播（Multicast），而 Class E 目前未被指配為特定用途，還處於保留未知狀態。

絕大多數網路上的訊息傳遞，都是單點傳播（Unicast），在資料封包內填入來源位址與目的位址，相關資料只在 2 點之間傳遞。假設今天某 A 主機想要傳送 1 份相同的檔案（演唱會實況、里長廣播、網路電台、視訊會議、老師的螢幕廣播……）給其它數台電腦，便需要將此份檔案複製成許多份傳送，如圖所示。

不過既然這些資料為「一式多份」，為何不要在到達目的地時再進行複製工作，這樣不就可以減少部分的網路流量負荷嗎？沒錯！多點傳播就是在做這些事情，Class D 位址保留做為多點傳播用途，每個不同的位址有其自身所代表的群體或意義。

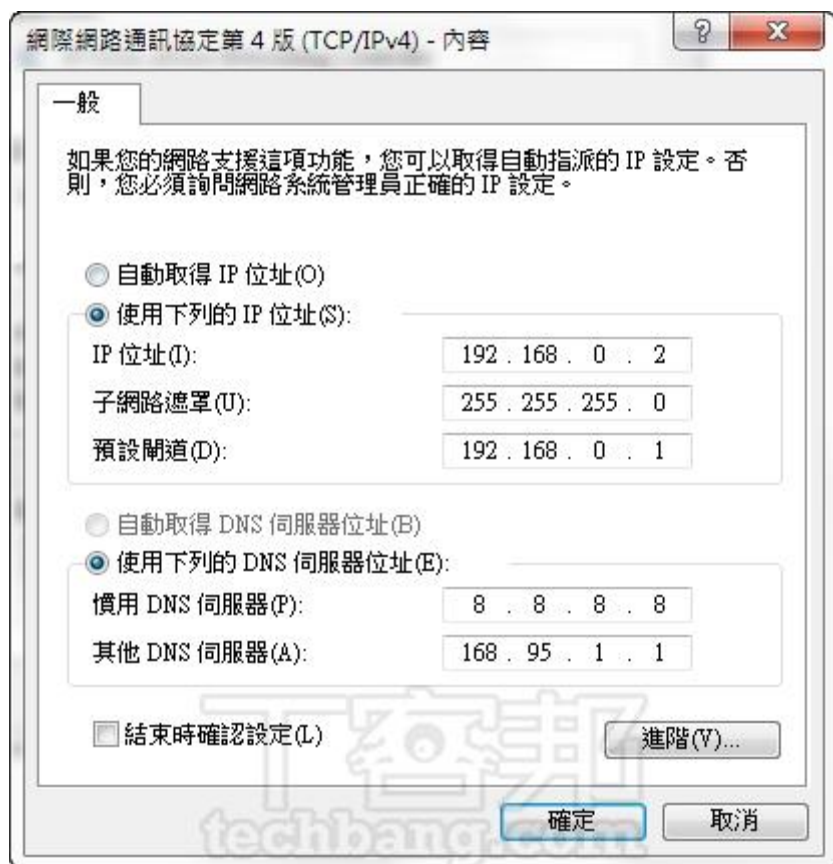
多點傳播協定也是活在第 2 層的網路層，但已經與 IP 協定略有不同，是個獨立的協定，在此不多加詳述，如果讀者有興趣，可由 IGMP 開始入門。

CIDR 無類別網域間路由

進入新的單元之前，請各位先想想自己是否了解了 Class 的分類，不用精確到記住各個 Class 有哪些保留位置，但要記得每個 Class 的網路和主機分別占了多少位元的網路位址，Class A 網路位址為前 8 位元、Class B 為前 16 位元、Class C 為前 24 位元，雖不是相當精準的分法，但有助於了解下一階段的子網路分割。

Class A 可提供 125 個網路，每個網路 16777214 個主機位址；16777214！沒錯！就是這麼多，單一網路就將近有 1700 萬台主機，哪家公司規模這麼龐大，塞得下這麼多台電腦，就算員工是章魚還是蜈蚣也是筆龐大的數目。

在分類網路發明出來後，很快地就發現到了這個問題，Class A 網路太龐大、Class C 網路又有點小，在實際使用上其實並不方便。回過頭來想想，分類網路將位址分成網路位址加主機位址的形式，但是網路位址和主機位址所占用的位元數是固定的，如果我們能彈性指派位元占用數目，不就可以任意的切割網路了嗎！



▲子網路遮罩控制了網路區段的大小

子網路切割

一旦我們有了「網路和主機位址不必佔據固定的位元數量」的觀念後，我們就可以來任意切割網路區段。假設現在分配到 192.168.0.0~192.168.0.255 的位址，我們可以將它直接劃作 1 個網路，若網路位址為前方 24 個位元，可塞入 254 台主機；或者是分割成 2 個網路，網路位址為前方 25 個位元，各可塞入 126 台主機。而在網路中，該如何確定網路位址的長度，就要靠子網路遮罩的設定了。

要進行子網路切割，將 IP 位址全部轉換為 0 或 1 比較容易理解，例如 255.255.255.0 的子網路遮罩，轉換為 2 進位制就是 11111111 11111111 11111111 00000000。再利用子網路遮罩將和目前主機的 IP 做運算，便可得出目前的網路位址為何，最大可容納多少的主機數量。

以 192.168.0.1 位址和子網路遮罩 255.255.255.0 做為例子，轉換為 2 進位後便是 11000000 10101000 00000000 00000001 和 11111111 11111111 11111111 00000000，將

兩者進行布林運算 AND 之後，會得到 11000000 10101000 00000000 00000000，轉換回十進位為 192.168.0.0，所以 192.168.0.0 就是 192.168.0.1 的網路位置。

由此範例可知，子網路遮罩位元數為 1 的部分，就是對應到 IP 位址的網路部分；反過來說，可利用子網路遮罩控制 IP 位址中網路位元占用的多寡，控制子網路的大小（網路位元占得越多，主機位元就更少，單一網路可容納的主機數也越小）。藉由規則反推，Class A 的子網路遮罩就是 255.0.0.0、Class B 為 255.255.0.0、Class C 就是 255.255.255.0。

子網路遮罩位元為 0 的部分就是主機位址，掐頭去尾的去掉網路位址和廣播位址之後，192.168.0.0/24 就有 254 個主機位址可供分配。

2 進位轉 10 進位速算法

請先由右至左，依序在紙上寫下 2 從 0 開始的指數數值（1、2、4、8、16……），你想換算的位數有多少、就寫多少個。之後將 2 進位數值一一寫在 2 的指數數值下方，若 2 的指數下方的 2 進為數值為 1，就將這些數值全部加起來，出來的數字就是這串 2 進位數字轉換為 10 進位的數值。

$$\begin{array}{r} 2^N \quad 8 \ 4 \ 2 \ 1 \\ \quad 1 \ 1 \ 0 \ 1 \\ \quad \quad 8 \\ \quad \quad 4 \\ \quad + \quad 1 \\ \hline \quad \quad 13 \end{array}$$

利用子網路遮罩長度

上面所示範的網路切割方式，還是固定在 Class C 的範疇裡，接下來示範向 Class C 位址的主機位元借 1 位，讓網路位元變成 25 位、主機位元占 7 位，子網路遮罩就變成 11111111 11111111 11111111 10000000（255.255.255.128）。與 192.168.0.1 計算後，得到網路位址 192.168.0.0，這種藉由改變子網路遮罩的做法，稱為可變長度子網路遮蓋（variable length subnet masking）。

前述例子的 IP 位址 192.168.0.1，無論是子網路遮罩 255.255.255.0 或是 255.255.255.128，計算出來的網路都是 192.168.0.0，讀者可能感受不出差異。若是今天主機位址為 192.168.0.200，計算出來的網路位址將不同；當子網路遮罩為 255.255.255.0，網路位址為

192.168.0.0，當子網路遮罩為 255.255.255.128 時，網路位址則是 192.168.0.128，分屬不同網路。

超網合併

除了大網路分割成小網路之外，利用 VLSM 也可將小網路合併成大網路，也就是將原本劃歸為網路位址的位元，變成主機位元使用。

再使用 192.168.0.1 做為例子，如果現在子網路遮罩設定成 11111111 11111111 11111110 00000000（255.255.254.0），那麼 192.168.0.1 的網路位址就是 192.168.0.0；在此同時，192.168.1.1 的網路位址也會變成 192.168.0.0，所以 192.168.0.1 和 192.168.1.1 原本在 Class C 下分屬 2 個不同的網路，藉由擴大主機位址範圍，讓這 2 個位址在不需經由 NAT 的情況下連線。

這種網路合併的情況除了在公司內部網路會發生之外，還常見於一連串的固定 IP 分配。由於現今 IPv4 位址短少，不太可能 1 次配發整個 Class C 網段，可能改發較小的 /22 或是 /24，或是更小的 /28。

不過網路合併也有個但書，就是合併的網路區段位址必須是連續的，因此 192.168.0.0/24 和 192.168.1.0/24 可以直接合併，但是 192.168.0.0/24 和 192.168.2.0/24 無法跳過 192.168.1.0/24 合併，因為無法算出同時適合 192.168.0.0/24 和 192.168.2.0/24，卻不適合 192.168.1.0/24 的子網路遮罩。

使用 /31 或是 /32 會發生什麼事？

首先 /32 的網路是沒有意義的，因為只有 1 個位址，跟拔掉網路線的意思差不多，/31 就是個有趣的議題，容筆者娓娓道來。

/30 一般是切割子網路的極限，內含 4 個位址，去掉頭尾的網路位址和廣播位址，只剩下 2 個可分配給主機的位址，因此將資料傳送給另 1 台主機和將資料傳送至廣播位址的意義是一樣的。/31 內部只有 2 個位址，IP 末碼不是 0 就是 1，末碼 0 已經被拿去當作網路位址，無法分配，剩下末碼 1 的位址可以當作主機位址，廣播位址就消失了。若是想要廣播功能，可將資料丟向末碼為 0 的網路位址，這個功能是早期所定義出來的，部分路由器依然支援這種廣播方式。

/31 只使用在點對點，且 2 端分屬於不同網路的連結上，有興趣的讀者可以搜尋「RFC 3021」。

CIDR 的限制以及其它改變

了解利用 VLSM 的改變控制網路大小，現在也要來看一下其中的限制。第一，網路只能以 2 的指數做為網路大小，例如把網路分割為 1、2、4、8、16、32……個位址數量，其它的數字 19、21、37……都無法分配。這是由於網路位址本來就是 0 與 1 2 進位的組合，所以除了 2 的指數之外，無法分割為其它的數量。子網路遮罩也必須是連續 1 加上連續 0 的組合，不能出現 11111111 11111110 11111111 00000000 或是 11111111 11111111 00001000 00000000 的狀況。

其它還有網路廣播位置的改變，若是以分類網路的標準，網路位址的結尾 8 位元一定是 00000000，廣播位址的末 8 碼一定是 11111111。但是導入 CIDR 之後，位址末碼為 00000000 的 IP 位址也可分配給主機使用，而廣播位址的末 8 碼也不一定是 11111111。

舉個例子，現在有個 192.168.0.0/23 的網路區段，IP 位址為 192.168.0.0~192.168.1.255，此時的網路位址為 192.168.0.0，廣播位址為 192.168.1.255，不知大家看出端倪了嗎？在 CIDR 無類別網域間路由的規則中，第一個位址就是此網段的識別位址，最後的 IP 位址就是此網段的廣播位址。在此例中 192.168.0.255 和 192.168.1.0 都可以正常的分配給主機使用。事實上主機位址全為 0 或是全為 1 的位址可不可以分配給主機使用，取決於路由器的全域設定，Cisco IOS 的預設值是允許的。

再舉 1 個 192.168.0.0/25 的例子，IP 位址為 192.168.0.0~192.168.0.127，第一個位址 192.168.0.0 為網路位址，最後 1 個 192.168.0.127 位址就是此網段的廣播位置。所以說在 CIDR 的世界中，IP 位置要配合子網路遮罩使用，才能知道此 IP 被劃分在哪個網路之中，廣播位址是多少。

練習切割網路

前面的教導大家如何從子網路遮罩推算回網路的大小，但在現實生活中網管的任務經常是拿到 1 段 IP 位址區段，使用這些位址配出需要的網路大小。例如將 192.168.0.0/24 均分成 3 等分（事實上不可能），或是切出 1 個至少可容納 50 個人的子網路，其它部分自成 1 個子網，這些都是在網路設計時需要應對的地方。當然一般使用者只需要將自己家中設定成/24 的網路環境即可，並不需要去擔心外面網際網路的 IP 路由世界，但期許看完本章後有基本的認知，設定家用路由器更得心應手。