# 第十三章 TCP/IP 與 Internet 網路連結技術

包含 IP、ARP、RARP、ICMP、TCP、UDP 與 IPv6 通訊協定，並介紹 Internet 網路連結技術之 RIP、IGRP、EIGRP、BGP 等協定及其運作原理。

## 13-1 TCP/IP 網路簡介

在 1960 年代末期，**美國國防部（Department of Defense, DoD）**有鑒於機構內，不同廠商之電腦充斥，各種電腦都有自己的作業系統及網路，彼此之間溝通非常困難，甚至無法互相傳送檔案，因此決定建構一個標準的通訊協定，讓不同廠商之間的電腦能夠連結在一起，並使能互相通信及傳遞資料。於是在 1968 年接受若干大學和公司的建議，成立『**國防部尖端研究企劃署』(Defense Advanced Research Project Agency, DARPA)**負責該工作。初期 DARPA 架設一個實驗性的分封交換網路，稱之為『**ARPANET**』，作為連結一般政府機關及實驗室的電腦，效果非常良好。同一個年代 Unix 也在 Bell 實驗室被發展出來。

1970 年代初期，ARPANET 開始嘗試加入不同的傳輸介質，如移動式無線電、衛星連線等等。直到 1975 年，DARPA 制定了標準介面，使其更容易與一般區域性網路連接，例如 Ethernet 或 Token-Ring 網路等，TCP/IP 的基本雛形就因此而誕生。到了 1980 年，TCP/IP 正式問世，DARPA 為了推廣它，便以極低的價錢安裝在不同電腦上，然而當時各大型廠商都有自己的網路系統，對於 TCP/IP 的發展興趣索然，DARPA 便以提供獎學金方式，與柏克萊（Berkeley）大學合作，將 TCP/IP 植入 BSD Unix 作業系統內。隨著 Unix 作業系統漸漸普及於各大學之間，TCP/IP 也漸成為各大學和研究機構之內電腦的主要連線。1983 年美國國防部為了顧及機密要求，將 ARPANET 分割成兩個網路：MILNET 和 ARPANET。ARPANET 為非機密部分；而 MILNET 為機密部分，僅供與 DoD 簽約合作之廠商使用。在同一時期，Internet 網路開始風行於各學校與研究單位之間，當時它代表由 MILNET 和 ARPANET 所構成的整個網路。

到了 1980 年代末期，隨著 Internet 網路的普及，網路的商業化應用如雨後春筍般的被發展出來，Internet 網路漸漸深入到辦公室，Internet 的應用再也不限制於學校或研究單位。因此，TCP/IP 網路由軍方發展出來，並經歷工程界、學術界、而到達商業界。從此以後，各

電腦廠商已漸漸正視 TCP/IP 的威力，而開始在自家電腦上植入 TCP/IP 通訊協定，也使 TCP/IP 不再拘限於 Unix 作業系統，不同廠商的作業系統也都可以利用 TCP/IP 來互相通訊及傳送檔案。ISO 為了希望能整合不同廠商電腦之間的連線，以數十年光陰推展 OSI 協定標準，卻依然沒有達成目的，沒想到竟被 TCP/IP 捷足先登，目前全世界大部分網路系統都已被 TCP/IP 整合成功。

除了 Unix 作業系統以 TCP/IP 作為區域性網路連線外，在大部份人的認知中， TCP/IP 是廣域網路上的通訊協定，而區域網路連結的通訊協定仍侷限於各自開發的網路系統。例如 Microsoft 網路的 NETBEUI、Novell 網路的 IPX、以及 IBM 的 DLC 等等。但隨著區域網路之間連結性的需求日益增加，許多廠商也漸漸以 TCP/IP 通訊協定作為區域網路之間的連線使用。

## 13-2 TCP/IP 通訊協定堆疊

一般所說的 TCP/IP 是指 TCP 和 IP 兩個通訊協定，而 TCP/IP 網路是指 ARPANET 網路。目前 ARPANET 網路與『**網際網路』( Internet )** 已幾乎整合在一起，都以 Internet 網路為代名詞。圖 13-1 為 TCP/IP 通訊協定的堆疊，我們還是依照傳統 OSI 參考模式和它比較相關的功能。基本上，早期 ARPANET 所訴求的是讓各偏遠地區上的電腦彼此之間能互相連接 ( 軍事用途 )，至於應用方面則較為簡單的遠端登入、電子郵遞和檔案傳送等等。因此，ARPANET 網路早期並沒有提供較複雜的使用環境，在應用層方面也沒有再細分表現層和交談層。Internet 網路也沿用 ARPANET 架構，在通訊協定方面只區分為四個層次。但隨著 Internet 網路的應用逐漸複雜，標準化的資料表示 ( 如加密、壓縮等 ) 是否有需要 ( 表現層功能 )，或異質電腦的程序之間的對談 ( 多方通訊 ) 標準是否有需要制定 ( 交談層功能 )，也漸漸在 Internet 網路中蘊釀著。

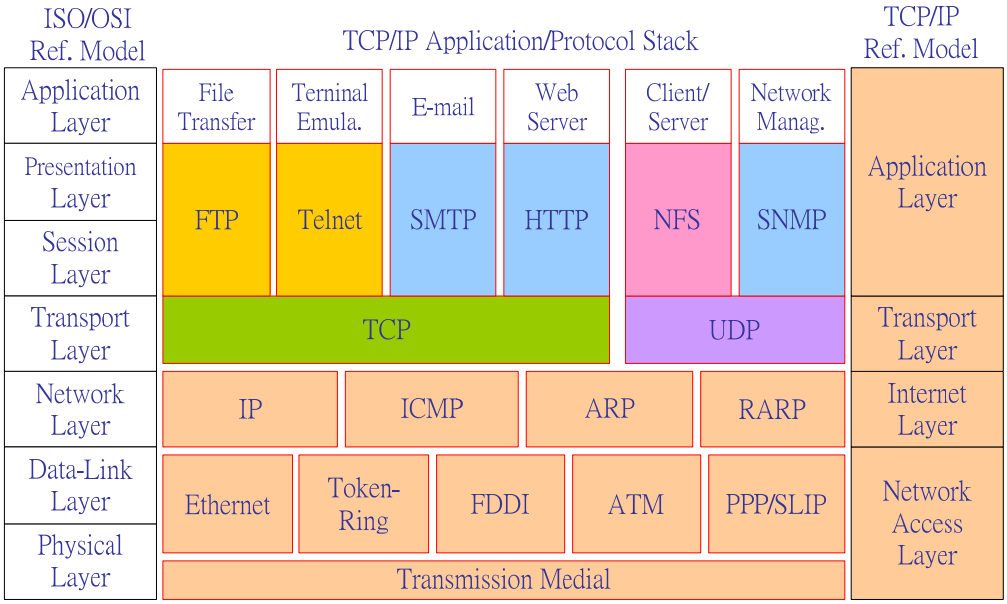



**圖 13-1 TCP/IP 通訊協定堆疊**

在 TCP/IP 通訊協定堆疊中，區分為四個層次，各個層次功能如下：

## 應用層（Application Layer）

簡單的說，應用層就是在網路上所開發的應用軟體。隨著網路的發展，應用軟體的開發愈來愈多，應用層也就愈來愈豐富，延伸出許多新的網路軟體技術。雖然 TCP/IP 網路沒有另外區分表現層和交談層，並不表示沒有提供這方面的服務，只是沒有提供這兩個層次的標準介面。儘管它減少開發軟體的方便性，但也促進新技術的發展。以下列出在 TCP/IP 網路上較常見的應用軟體：(有關應用層的相關技術請參考本書第六章)

**(1) FTP（File Transfer Protocol）:** 遠端檔案傳輸協定，透過 FTP 可和不同地區的異質電腦之間檔案互相傳送。

**(2) SMTP（Simple Mail Transfer Protocol）:** 簡易郵件傳輸協定。在各個電子郵件伺服器之間郵件傳輸的協定，使用者可透過 SMTP 傳送郵件。

**(3) HTTP（HyperText Transfer Protocol）:** 超文件傳輸協定。使用者（瀏覽器）和網頁伺服器器（Web Server）之間超文件（文字、聲音、圖片、影像等）的傳輸協定。

**(4) DNS（Domain Name Server）:** 將主機名稱和 IP 位址之間的轉換。

## 傳輸層（Transport Layer）

傳輸層如同 OSI 參考模式的第四層（請參考本書第五章）。基本上，傳輸層是提供可靠性連線服務（TCP），但也提供非連接方式（UDP）的傳輸，以作為一般網路管理或快速資料傳輸之連線使用。兩個主要通訊軟體說明如下：

**(1) TCP（Transmission Control Protocol）：**傳輸控制協定。**提供連接導向（Connection -oriented）**程序（Process）之間的可靠性（Reliable）連線服務。TCP 提供標準傳輸介面，讓不同電腦之間可以連線。

**(2) UDP（User Datagram Protocol）：**使用者電報傳輸協定。提供**非連接服務（Connectionless）**的使用者（或程序）之間連線。類似 TCP 服務但為不可靠性（Unreliable）連線。

## 網際層（Internet Layer）

網際層（Internet Layer）相當於 OSI 參考模式的網路層（請參考本書第四章）。TCP/IP 網路為提供遠距離之間的網路連結，其網際層採用變異性較高的電報傳輸（Datagram）方式，亦是『**網際協定**』（Internet Protocol, IP）。雖然網際層還有若干個通訊軟體（ICMP、IGMP 等），但都包裝在 IP 封包內，以 IP 方式傳輸（Datagram）。以下介紹幾個較重要的通訊軟體：

**(1) IP（Internet Protocol）：**提供網路之間的路徑選擇協定。遠端電腦之間可透過 IP 協定尋找出對方位址，並能互相連接在一起。

**(2) ICMP（Internet Control Message Protocol）：**網際控制訊息協定。網路之間互相傳送網路狀況的資料格式，以及回報方式的協定。使用者可利用 ICMP 查詢網路狀況（網路負載情況或斷路等等）。

**(3) ARP（Address Resolution Protocol）：**位址解析協定。某部電腦可透過 ARP 協定以對方（使用者）的網路位址（IP 位址），來查問其網路介面卡位址（Ethernet 位址）。

**(4) RARP（Reverse Address Resolution Protocol）:** 反向位址解析協定。使用者透過 RARP 協定以本身的網路介面卡位址（Ethernet 位址），向網路上其他電腦（如名稱伺服器）詢問本身的網路位址（IP 位址）

## 網路存取層（Network Access Layer）

網路存取層相當於 OSI 參考模式中的第一、二層，TCP/IP 網路並未對它提出特殊標準，因此未再細分層次。媒介存取層大多是沿用現有的網路介面存取方式，在區域網路方面以 IEEE 802 系列為主，如 Ethernet、Token-Ring、FDDI 等。廣域網路方面，早期有 PPP、SLIP 等通訊協定，目前為要求更高的傳輸速度，即有 ATM 網路中的 IP over ATM 或 ADSL、Cable Modem 等標準介面被製定出來。

## 13-2-1 協定資料單元包裝

TCP/IP 協定堆疊的特性如同 OSI 參考模式一樣，各個層次之間也具有隔離性和獨立性。上下層之間的『**協定資料單元**』( Protocol Data Unit, PDU ) 經過『**包裝**』( Encapsulation ) ( 傳送端 )和『**拆裝**』( Decapsulation ) ( 接收端 )，控制訊息( 通訊協定 )包裝在『**協定標頭**』( Protocol header ) 上。

如圖 13-2 中，傳送端 ( User_A ) 發送一個訊息經由應用層加入 AH 的協定前頭，再經過傳輸層加入 TH 包裝成為 TL-PDU，再傳送給網際層。接收端依反方向拆裝，網際層接收到 IL-PDU 拆解出 IH 協定標頭，得到傳送端給予有關網際層的控制訊息，再將 TL-PDU 傳送給傳輸層，依此類推，各層次之間的通訊協定就如此構成。路由器 ( Router_X 和 Router_Y ) 只負責封包路徑之尋找及轉送，因此只提供到網際層 ( Internet Layer ) 的服務，對於 PDU 的拆裝和解裝也只有到網際層。

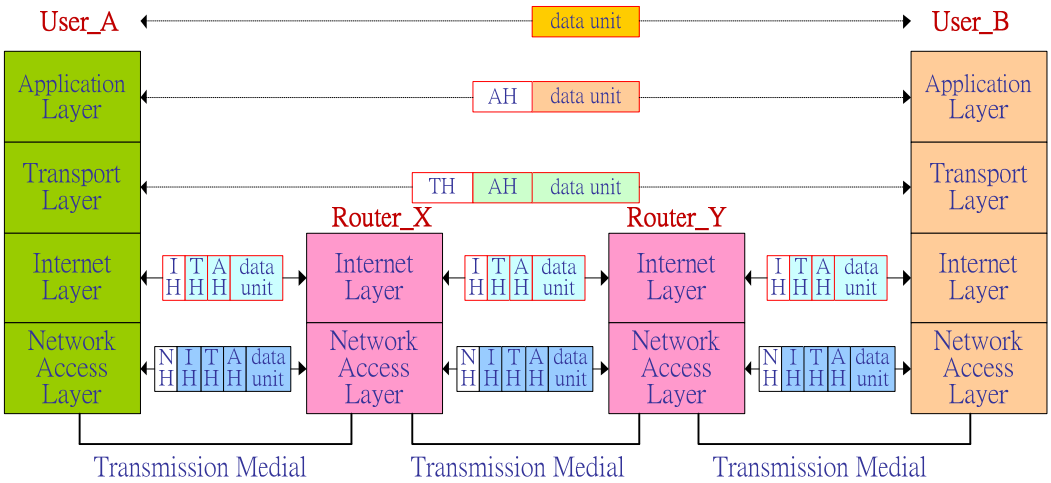



**圖 13-2 TCP/IP 之協定資料單元的包裝**

## 13-2-2 資料名稱及協定定址

在 OSI 參考模式之中各個層次的資料都稱為『**協定資料單元**』( Protocol Data Unit, PDU )，如傳輸層 ( Transport Layer ) 的資料就稱為 TL-PDU。同樣的，TCP/IP 協定堆疊的每一層資料都有其固定的結構和名稱，理論上，每一層皆可忽略其他層次的資料結構。但實際上，由於考量了傳輸效率的因素，每一層的資料結構都被設計成相容於該層的上、下兩層的資料結構。在 TCP/IP 網路底下，我們為了能突顯出每一資料單元的特性，而各訂一個特殊的名稱，這樣在程式設計時，也比較能夠區分其屬性。各層次資料單元的名稱如圖 13-3 所示，其中應用層如使用 TCP 連接時，其資料單元稱之為『**串流**』( Stream )；而使用 UDP 連線則稱之為『**訊息**』( Message )。在傳輸層方面，TCP 的協定資料單元，稱之為『資料段』( Segment )；在 UDP 中則稱為『**封包**』( Packet )。網際層的資料單元統稱為『資料片』( Datagram )；網路存取層的資料單元稱為『**訊框**』( Frame )。但在網路上傳送的資料包裝，一般還是以『**封包**』( Packet ) 稱呼較多。

在通訊協定裡，每一層次皆有多工處理的功能，每一條虛擬鏈路在各層次之間都要有一個位址，這各位址就是在 OSI 參考模式中，各層次之間的『**服務存取點**』( Service Access Point )。TCP/IP 制定一個『**協定定址方法**』( Protocol Addressing ) 來表示一個通訊連線，在各層次之間的連結位址，如圖 13-3 與 13-4 所示。各層次間的連接位址有：網路實體位址( 如 Ethernet Address )、 IP 位址 ( IP address )、協定號碼 ( Protocol Number ) 與埠口號碼 ( Port Number )。其中協定號碼比較特殊，這是因為傳輸層或許多網際層協定 ( 如 TCP、UDP、ICMP ) 都是使用 IP 封包轉送，因此，必須有協定號碼來標示目前 IP 封包上，所承載的資料是屬於哪一個通訊軟體 ( 如 TCP 或 ICMP )。

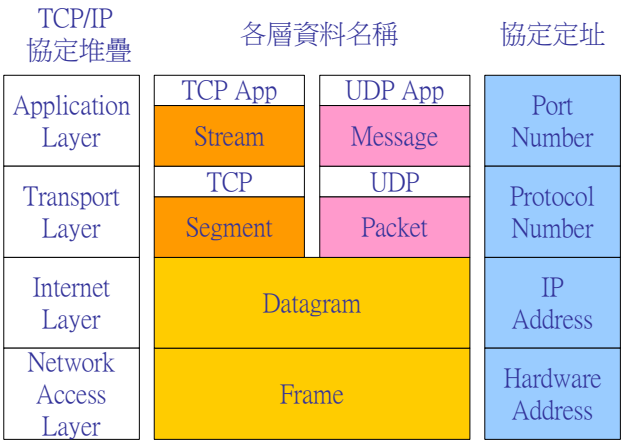



**圖 13-3 TCP/IP 協定堆疊各層的資料名稱及定址**

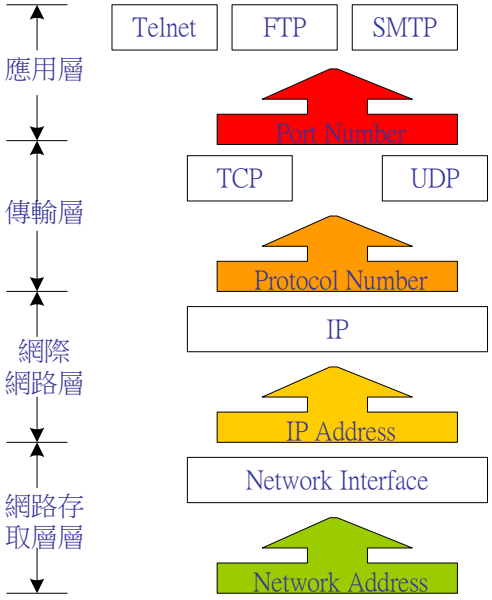



圖 13-4 TCP/IP 各層次的定址名稱

# 13-3 IP 通訊協定

IP 通訊協定是 TCP/IP 網路之中最主要的協定，用來在廣泛複雜的網路上找到所欲連接之工作站，並負責雙方的連線。IP 通訊協定所採用的連接技術是『**電報傳輸**』( Datagram )( 請參考本書第四章 )，主要工作有二：(1) 為每一部工作站定名，使成為網路唯一的識別名稱，有了這個名稱呼叫，才可以連結其它工作站，或被其它工作站連結，宛如電話號碼一般。(2) 尋找連結路徑。在廣泛複雜網路之中，尋找出可到達目的地的最佳路徑。因此，IP 通訊協定是 TCP/IP 網路中最為重要、也最為複雜的通訊軟體。目前 Internet 網路已連結全世界上億的電腦，任何地區的網路只要透過簡單的路由器就可銜接上 Internet，每一部路由器的主要功能就是實現 IP 通訊協定功能，所以 IP 必須有足夠的共通性和連結性，本節就依照這個方向介紹 IP 通訊協定。首先，我們來觀察 IP 協定的封包格式，如圖 13-5 所示，各欄位功能如下：

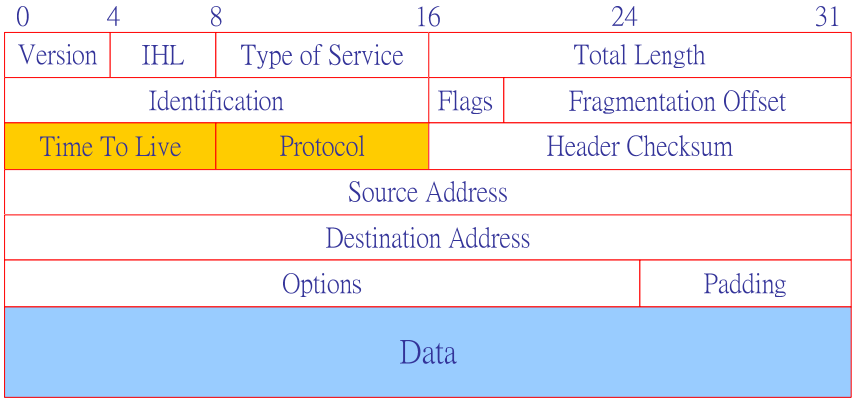


圖 13-5 IP 封包之結構

**(1) 版本（Version）：** 4 位元。表示 IP 封包的 IP 版本。

**(2) 網際標頭長度（Internet Header Length, IHL）：** 4 位元。表示本 IP 封包標頭的長度（位元組表示）。範圍為 5 ~ 15，預設值為 5。

**(3) 服務型態( Type of Service, TOS ):** 8 位元。其內容為 "PPPDTRUU"，PPP 表示本 IP 封包的優先權（Precedence）；D = 0 表示一般延遲（Delay），D = 1 表示低延遲；T = 0 為一般傳送量( Throughput )，T = 1 為高傳送量；R = 0 為一般可靠度，R = 1 為高可靠度（Reliability）；UU 保留未用。

**(4) 總長度（Total Length）：** 16 位元。是指該封包的總長度，包括封包標頭及資料的長度。範圍由 576 ~ 65535 位元組。

**(5) 辨識碼（Identification）：** 8 位元。表示資料分割（fragmentation）的識別編號。同一筆資料如被分割成若干個區段，每段給予相同的辨識碼，接收端再依辨識碼組合回原來資料封包。

**(6) 旗標（Flags）：** 3 位元。其格式為 "0DM"。D = 0 表示可以分段，D = 1 為不可分段（Don’ t fragment）；M = 0 表示最後分段，M = 1 為不是最後分段（More fragment）。

**(7) 分段偏移（Fragment Offset）：** 13 位元。表示目前的分段在原始的資料中所在的位址。原始分段允許有 8192 個分段，以每 8 個位元為一個基本偏移量，所以最大容許 65536 位元資料，此值和總長度一樣。因此範圍為 0 ~ 8191，預設值為 0。

**(8) 存活時間（Time to Live, TTL）：** 8 位元。表示該資料片在網路上的存活時間，封包每經過一個路由器( 或網路閘門 )，該值就被減一。如路由器發現某封包的 TTL = 0，便將該資料片丟棄而不轉送。範圍 0 ~ 255。

**(9) 協定號碼（Protocol Number）：** 8 位元。表示該 IP 封包所承載通訊協定的協定號碼。在 TCP/IP 協定中，許多通訊協定（如 IP、ICMP、TCP、UDP 等等）都被包裝成 IP 封包，而以 IP 通訊協定發送。所以，在 IP 封包裡必須有協定號碼欄位，

來表示目前所承載之資料是屬於哪一個通訊協定（IP、ICMP、TCP 等等）。一些較常用著名（well-known）的協定號碼如表 13-1 所示。

**(10) 標頭檢查集（Header Checksum）：** 16 位元。做標頭錯誤檢查用。

**(11) 來源位址（Source Address）：** 32 位元。發送此 IP 封包的來源位址。

**(12) 目的位址（Destination Address）：** 32 位元。目的主機之位址。

**(13) 選項欄位( Options ):** 可變長度。提供多種選擇性服務。例如：來源路徑選擇( Source routing ) 用來追蹤 IP 封包所經過的路徑等等。

**(14) 填補欄位（Padding）：** IP 資料片的標頭一定是 32 位元的整數倍，當 Options 欄位不足 32 位元整數倍時由 Padding 欄位補足。

表 13-1 著名協定號碼（節錄）

| 協定名稱 | 協定號碼 | 協定全名（協定包裝在 IP 資料片內） |
|---|---|---|
| ICMP | 1 | Internet Control Message Protocol |
| IGMP | 2 | Internet Group Management Protocol |
| GGP | 3 | Gateway-to –Gateway Protocol |
| IP | 4 | IP in IP encapsulation |
| TCP | 6 | Transmission Control Protocol |
| EGP | 8 | Exterior Gateway Protocol |
| IGP | 9 | Interior Gateway Protocol |
| UDP | 17 | User Datagram Protocol |

## 13-3-1 IP 位址

## IP 位址結構

在 TCP/IP 網路中，任何一部連線的電腦或網路設備都稱為主機 ( host )。TCP/IP 被設計成適合連接全球各地不同類型、位置的網路系統，為了方便標定每部主機，TCP/IP 定義了一套通用的定址方法。當時所期望的定址格式是，必須能提供足夠的路徑選擇 ( routing ) 資訊，而且不要佔用太多記憶體空間，因此，將『**IP 位址**』( IP Address ) 的長度設定為 32 位元。為方便表達，我們將此 32 位元分割成四段，每連續 8 位元為一組，每組並以十進位值 ( 0 ~ 255 ) 表示，每組之間以點 ( dot ) 分隔。整個 IP 位主表示法就如下所示：

dec3.dec2.dec1.dec0（如 163.15.2.1）

雖然 IP 位址長為 32 為元，但其中包含兩種號碼：網路號碼（Network number）及主機號碼（Host number），因此 IP 位址也可以表示成：（如圖 13-6 所示）

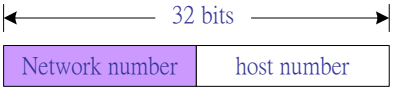



圖 13-6 IP 位址結構

實務連接的時候，並非每一部主機上都只有一個 IP 位址，一般 IP 位址都依照網路介面卡（Ethernet 網路卡）設定。如主機有特殊需要安裝多個網路介面卡（如當路由器使用），每只網路介面卡上都必須設定一個 IP 位址，因此，一部主機上就擁有多個 IP 位址，TCP/IP 網路也容許類似虛擬主機的設定，表示一只網路介面卡上可設定多個 IP 位址。

## IP 位址分級

下面我們要談，在 32 位元長度的位址中，應該用多少位址長度來表示網路位址或主機位址。TCP/IP 網路依照所能容納的主機和網路的數量多寡分成 A、B、C 、D 和 E 五種類級（class），如圖 13-7 所示，其中 Class D 目前為多點廣播（Multicast）位址，Class E 則保留未來發展之用。分級技巧是配置不同數目的網路位址，網路位址的位元數愈多，所能指定的網路數量就愈多，但相對應的主機位址就愈少。Class C 所能容納的網路位址最多，所以在國際間網路上，大多採用 Class C 定址模式。Class A 所能容納的主機位址最多，但相對應的所能容納的網路位址最少，一般使用在區域網路的定址模式。各類級的特性如下：

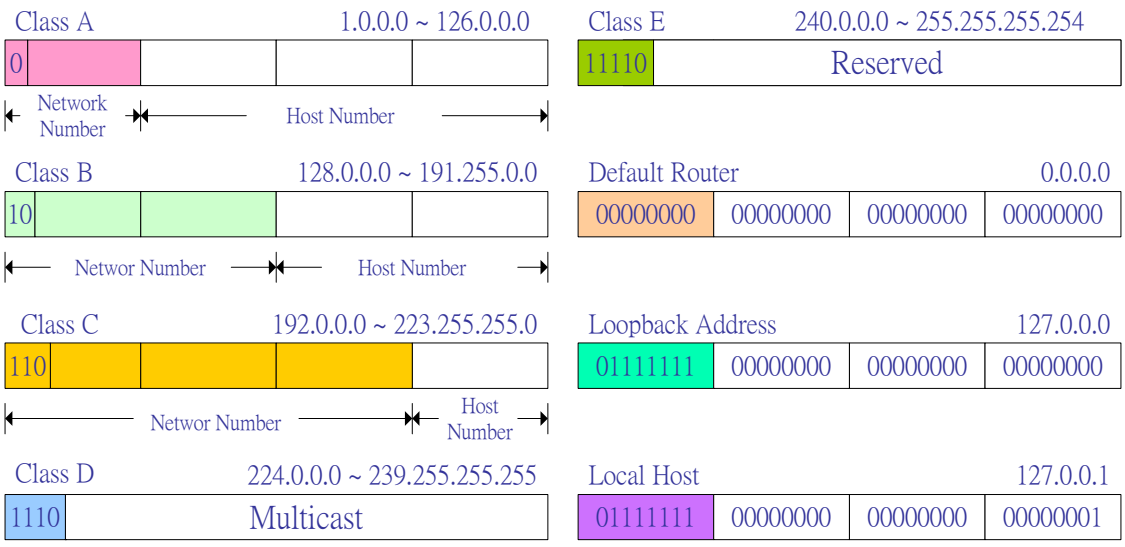


圖 13-7 各類級的 IP 位址結構

**(1) Class A**：以最高位元（第 31 位元）為 0 表示 Class A 模式。前一位元組（8 位元）表示網路位址；而後 24 位元表示主機位址。網路位址由 1.0.0.0 ~ 126.0.0.0，所能表示的主機位址是 **1.0.0.0 ~ 126.255.255.255** 的範圍之內。**Netmask = 255.0.0.0**（下小節說明）。

**(2) Class B**：以二個最高位元為 10 表示 Class B 模式。前 16 位元表示網路位址；而後 16 位元表示主機位址。網路位址由 128.0.0.0 ~ 191.255.0.0，所能表示的主機位址為 **128.0.0.0 ~ 191.255.255.255** 的範圍之內。**Netmask = 255.255.0.0**。

**(3) Class C**：以前三個最高位元為 110 表示 Class C 模式。前 24 位元是網路位址；而後 8 位元為主機位址。網路位址由 192.0.0.0 ~ 223.255.255.0，所能表示的主機位址為 **192.0.0.0 ~ 223.255.255.255** 的範圍之內。**Netmask = 255.255.255.0**。

**(4) Class D**：以前四個位元為 **1110 表示 Class D 模式**。其主要應用於多點廣播（Multicast），一些特殊應用軟體皆用此模式，來對某些定點（工作站）廣播，如隨選視訊（VOD）就用此定址模式，對若干個定點工作站廣播視訊。

**(5) Class E**：以前四個最高位元為 **1111 表示 Class E 模式**。目前保留尚未使用。

另外，網路位址 **0 和 127** 保留給特殊用途使用。網路 0 代表預設路徑位址，通常都將主機的**『預設路由器』( Default router )**位址設定為 **0.0.0.0**。網路 **127 代表回繞( Loopback )** 位址，方便主機自己定址使用，並以 **127.0.0.1 表主機本身自己**。在一般網路上，設定某一個網路位址的主機位址都為 1 時，稱之為**『廣播位址』( Broadcast Address )**，表示針對這個網路上的主機廣播，例如在 162.15.0.0 網路上的廣播位址為 162.15.255.255。又對於網路上所有主機廣播的位址為 255.255.255.255。

剛開始設計 TCP/IP 網路時，電腦還未普及，網路也非常少，TCP/IP 協定開始應用時只連結大型主機，因此 32 位元容量的 IP 位址對當時來講已足足有餘，沒有想到後來 Internet 網路竟然大為風行，導致 IP 位址不足問題的發生。理論上，任何一部電腦連結上 Internet 網路都需要一個獨一無二的 IP 位址，因此 IP 位址將會在短期內被耗盡。雖然目前已提出 IPv6 的解決方案，但要網路上使用中的路由器和主機都更新為 IPv6 的通訊協定，並非易事。目

前網路上大都是透過『**網路位址轉換器**』( Network Address Translator, NAT ) 來增加私人網路位址，以解決 IP 位址不足的問題。

## 網路遮罩（Network Mask, Netmask）

IP 位址是由網路號碼和主機號碼組成的 32 位元，為方便起見，一般都用 [network#, host#] 表示。網路號碼決定主機所屬的網路位址，因此主機在傳遞封包之前，會先過濾出網路號碼，再決定封包應該往哪一個網路傳送。

為使能由 IP 位址中過濾出網路號碼，我們使用『**網路遮罩**』( Netmask ) 來過濾。網路遮罩亦為 32 位元，在位元中 "1" 表示網路位址；而 "0" 表示主機位址，其遮罩方式如圖 13-8 所示。如 IP 分級方式，Class A 網路遮罩為 255.0.0.0；Class B 為 255.255.0.0；Class C 為 255.255.255.0。在一般網路遮罩，皆是 IP 位址的前面若干位元設定為 "1"，因此，我們以網路號碼的長度( 也是網路遮罩的長度 )來代表網路位址的範圍，以『主機號碼/網路號碼長度』來表示一個網路位址，如 163.15.2.3/16 ( 網路遮罩長度為 16 )表示該主機是在 163.15.0.0 網路中的 0.0.2.3 位址。

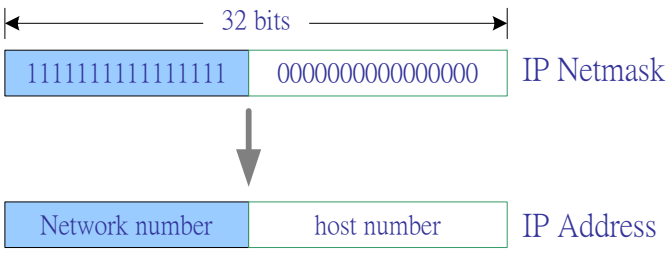



圖 13-8 IP Netmask

## 次網遮罩（Subnet Mask）

如果硬要將網路位址區分為三個類級( Class A ~ C )，也許很難滿足各種環境需求。例如，目前 TANet 網路使用 Class B 的定址模式，分配到每一個學校 2 ~ 3 個網路號碼。每一個學校裡的網路，是由多個系所的區域網路所構成。在技術上，每一個區域網路都要有一個網路號碼，因此網路號碼一定不符所需，這就是 IP 分級所衍生的問題之一。解決的方法是再劃分次網路 ( Subnet )，產生次網路的基本原理，是將原有主機號碼的幾個位元拿來當網路號碼，並不改變原來 32 位元的 IP 位址格式。

如欲劃分次網路，就必須有次網路的編號，原來 IP 位址所表達的是 [network#, host#] 方式，就必須更換為 [network#, subnet#, host#] 形式。而增加次網路號碼，就必須犧牲原來主機號碼的數量，次網路號碼增加愈多，主機號號碼就減少愈多，這樣做並不會改變整個位址格式，因為原來網路號碼並未改變，對外部網路而言，次網路位址也被視為主機位址，因此不影響外部網路的連結問題。我們以一個例子說明，假使希望在 163.15.0.0 的網路上增加 8 個次網路，基本上，163.15.0.0/16 網路是屬於 Class B 格式，它原來的 IP Netmask 為 255.255.0.0。我們為了增加 8 個次網路，必須將 3 個位元的主機號碼拿來當次網路號碼，因此 Netmask 為 255.255.224.0，如圖 13-9 所示。

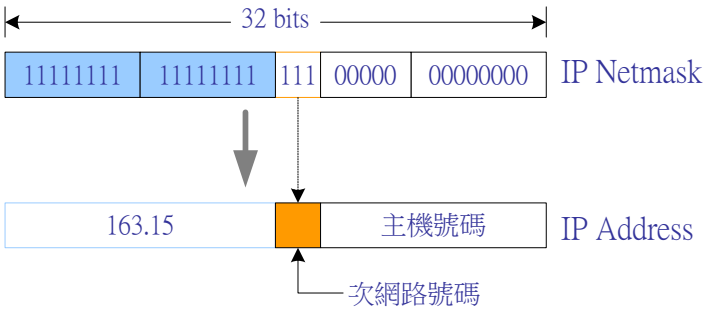



圖 13-9 次網路號碼

分割後所產生的網路位址為：( Network number = 163.15.0.0、Netmask = 255.255.224.0 )

163.15.0.0/19、163.15.32.0/19、163.15.64.0/19、163.15.96.0/19、

163.15.128.0/19、163.15.160.0/19、163.15.192.0/19、162.15.224.0/19。

主機位址和網路位址範圍為：

- 第 1 個次網路範圍：163.15.0.0 ~ 163.15.31.255。
- 第 2 個次網路範圍：163.15.32.0 ~ 163.15.63.255。
- 第 3 個次網路範圍：163.15.64.0 ~ 163.15.95.255。
- 第 4 個次網路範圍：163.15.96.0 ~ 163.15.127.255。
- 第 5 個次網路範圍：163.128.0.0 ~ 163.15.159.255。
- 第 6 個次網路範圍：163.160.0.0 ~ 163.15.191.255。
- 第 7 個次網路範圍：163.15.192.0 ~ 163.15.223.255。
- 第 8 個次網路範圍：163.15.224.0 ~ 163.15.255.255。

依照 RFC 950 規範，將網路位址為 0，保留給預設路由器使用；主機位址都是 1 時保留給廣播位址使用。因此，經過此網路分割後，子網路位址為 0 或都是 1（如 163.15.0.0 與 163.15.224.0 網路），還是必須保留，不可分配給工作站使用。

## 13-3-2 IP 協定特性

基本上，IP 的連接技術是非連接方式的『**電報傳輸**』（Datagram），因此在網路通訊的技術上，具有下列特性：

**(1) IP 是非連接（Connectionless）服務**。表示 IP 在傳送封包之前，雙方並未事先建立連線。發送端直接將封包發送到網路上，由網路上各個路由器（或網路閘門）負責轉送到達目的地。

**(2) IP 無錯誤偵測功能**。當封包進入路由器時，路由器只針對封包標頭上的目的位址轉送，並不保證該封包是否可安全無恙傳送到目的地，因此沒有針對封包內的資料作錯誤偵測。封包在傳輸當中，是否受到干擾或其他原因，而發生錯誤，這必須由委託傳送（或上層）的通訊軟體自行負責偵測。

**(3) 封包彼此之間的次序，經傳送到對方後，可能和原來的不同**。因為，每個封包都自行依當時網路情況尋找路徑（電報傳輸方式），所經過的路徑也不一定相同，到達的次序就不一定會和原來次序相同。

**(4) 封包可能被重複傳送**。重複傳送的原因可能是發送端的上一層協定在溢時後，未收到接收端的回應確認（中途遺失？），再發送另一個同樣的封包。而實際上，接收端在收到第一個封包時已作回應（對方沒收到？），結果又再收到同樣的封包。IP 本身只負責傳送封包，封包是否重複傳送，這必須由上層通訊軟體負責偵測。

**(5) IP 並不驗證目的主機是否有確實收到正確的資料**。

## 13-3-3 IP 路徑選擇

IP 路徑選擇（IP Routing）是所有 TCP/IP 網路最主要的中心樞紐。上層的應用程式若想在浩瀚的網路之中找到欲通訊的對象，就得利用 IP 路徑選擇的功能。

在傳送過程之中，也許會經過許多『**網路閘門**』(Gateway)或『**路由器**』(Router)，這些設備都必須具有路徑選擇的功能。當一筆資料由傳送端發出後，它將不知道，也不可能知道，這筆資料是否可安全到達目的地，和可能經過哪些路徑。所經過的路徑都是由封包到達某一路由器後，再由該路由器決定應該往哪一下個路徑(Next hop)傳送。因此，一筆資料可安全到達目的地，是由網路上所經過的路由器共同來完成，並非發送端事先可以控制的。

通常區域網路的範圍較小，在同一網路內，主機和主機之間無須借助路徑選擇即可通訊，一般都使用廣播方式(Broadcast)通訊。傳送主機將封包廣播到網路上，同一網路上所有主機收到該封包後，會先檢查封包標頭的目的位址是否和自己的位址相符，如果相符就收下該封包；否則忽略它。但在廣域網路上就無法利用廣播方式來傳送封包，如果每部主機都廣播，則整個網路將被廣播封包所佔滿。因此網路之間需設置一個以上的對外網路閘門或路由器，網路閘門就是負責過濾對外的通訊封包，它們卡在網路之間，只讓必要的封包通過，且阻擋不必要的封包經過。

以下說明路徑選擇的處理方式。當某一部主機或路由器(網路閘門)要發送封包時，首先檢查封包之目的 IP 位址，其處理程序如下：

**(1)** 一般路由器(或網路閘門)都安裝有兩個以上的網路卡，每個網路卡連接一個網路，也代表一個網路號碼。當它由任一個網路(或網路卡)上收到一個封包後，依照下列 )、2、3 處理。

**(2)** 若目的位址的網路號碼與本主機(或路由器)的網路號碼相同時，則表示目的主機在本網路內，不需選擇路徑，直接將封包送出，例如採用廣播方式(查詢 ARP 動作)。

**(3)** 若目的位址的網路號碼與本主機(或路由器)的網路號碼不同時，則表示目的主機不在本網路內，必須跨越路由器到其他網路。就將該封包轉送給另一路由器，由它去負責轉送。

當主機(或路由器)發現所要發送(或轉送)的封包不在本網路內，而必須將該封包轉送給其它路由器負責傳送時，如果網路上有多個路由器，應該轉送給哪一個路由器？或給哪一個路由器最為理想？這就牽涉到路徑選擇的問題。一般在路由器(或網路閘門)內部皆有維護一個『路由表』(Routing Table)，當封包進入時，依照路由表上尋找出應該傳送給哪一個路由器，才可到達目的地(或最佳路徑)。建構(或維護)這路由表有兩種方法：

**(1) 靜態路徑選擇( Static routing ):** 路由表是由人工建立而成，建立後除非再由人工修改，否則不會變更。系統維護人員會依照網路狀況或規劃網路拓樸圖架構來建立靜態路由表。

**(2) 動態路徑選擇 ( Dynamic routing ):** 路由表是由網路上路由器 ( 或網路閘門 ) 隨時交換訊息所建立而成。因此，路由器會隨時依照網路狀況自動維護路由表。至於路由表如何建立的技術，在本書第四章有詳細介紹其演算法。

當路由器欲轉送封包時，首先查閱靜態路由表，如有適合的路徑便傳送出去，否則再搜尋動態路由表，找出較適當的路徑再傳送。

我們以圖 13-10 來說明 IP 路徑選擇的運作程序。圖中有三個網路：163.15.2.0/24、163.15.3.0/24 和 163.15.4.0/24 ( Class B 位址分割子網路 )，利用兩個路由器 ( Router_A 與 Router_B ) 所連結而成。每一路由器上都有兩個連接埠口，並個別設定 IP 位址。圖 13-10 (b) 為兩個路由器的路由表，其可能是靜態路由( Static Routing )或動態路由( Dynamic Routing )。我們以下列三種情況來說明路徑選擇的運作程序：

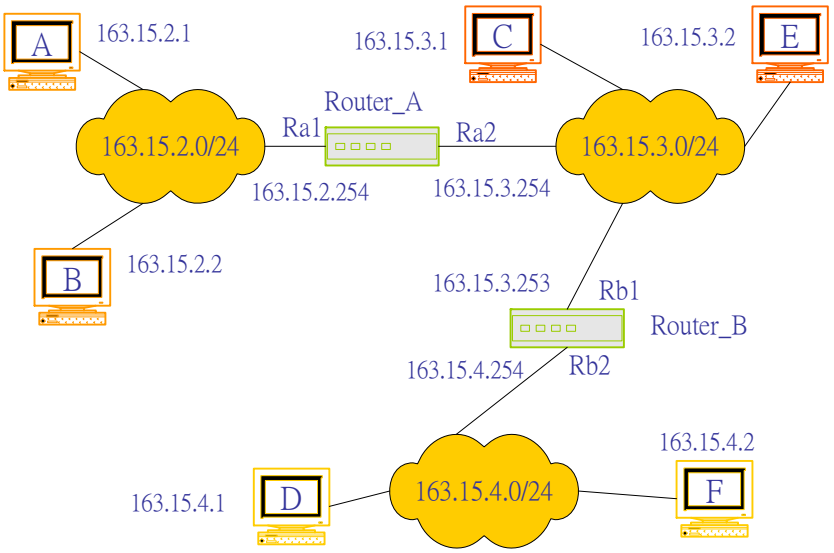



**圖 13-10 (a) IP 路徑選擇範例**

Router_A 路由表

| 目的網路位址 | 轉送位址 |
|---|---|
| 163.15.2.0/24 | 163.15.2.254 |
| 163.15.3.0/24 | 163.15.3.254 |
| 163.15.4.0/24 | 163.15.3.254 |

Router_B 路由表

| 目的網路位址 | 轉送位址 |
|---|---|
| 163.15.2.0/24 | 163.15.3.253 |
| 163.15.3.0/24 | 163.15.3.253 |
| 163.15.4.0/24 | 163.15.4.254 |

**圖 13-10 (b) Router A 和 B 的路由表**

**(1) 主機 A（163.15.2.1）欲傳送封包給主機 B（163.15.2.2）：**主機 A 發現目的網路位址和自己網路號碼相同（163.15.2.0/24），便將封包直接廣播到網路上，主機 B 由網路上收到封包。

**(2) 主機 A（163.15.2.1）欲傳送封包給主機 C（163.15.3.1）：**目的網路號碼不同，必須透過路由器轉送。主機 A 便將封包傳送給 Router_A 的 R1a（預定路由器），Router_A 由 Ra1 埠口收到封包（目的位址為 163.15.3.1）後，便由路由表上得知網路位址是 163.15.3.0/24 的封包，必須轉送到 163.15.3.254（Ra2），便將該封包由 Ra2 埠口廣播出去（163.15.3.0/24 網路）。主機 C 由網路上讀取到該封包。

**(3) 主機 A（163.15.2.1）欲傳送封包給主機 D（163.15.4.1）：**Router_A 是網路（163.15.2.0/24）的唯一出口，主機（163.15.2.1）勢必將封包傳送給 Router_A（與網路號碼無關）。Router_A 由路由表上查詢後，便由 Ra2（163.15.3.254）廣播出去（也可直接傳給 163.15.3.253）。Router_B 由 Rb1 收到封包，再由路由表上查出，應轉送到 Rb2（163.15.4.254），便由 Rb2 埠口將封包廣播出去。主機 D 由網路上（163.15.4.1/24）收到該封包。

上述中，我們都假設直接將封包廣播到網路上，其實它必須經過查詢網路實體位址（Ethernet 位址）後，再傳送給對方，這方面將在下一節中說明。

## 13-4 ARP 與 RARP 通訊協定

在 TCP/IP 網路下，每一部主機都有一個 IP 位址。理論上，欲傳送封包給任何一部主機只要知道它的 IP 位址，便可依照此 IP 位址傳送給該主機。但事實上，IP 封包在網路上傳遞時，還是必須透過實際網路位址，才能送達目的位址。例如，IP 網路架設在 Ethernet 上（IP over Ethernet），Ethernet 網路上所有工作站依照 Ethernet 位址傳送資料，接收端收到訊框後也依照 Ethernet 位址判斷是否傳送給自己，由此可見，在實體網路上，並沒有使用到 IP 位址。因此，某一部主機欲依照 IP 位址傳送給另一部主機，首先必須知道該主機的實體網路位址（一般稱為 MAC 位址），再依 MAC 位址傳送，亦即，必須擁有該主機的 IP/MAC 對照表，同樣的，任何一部主機也必須知道自己的 IP/MAC 對照關係。問題是當某部主機欲依照 IP 位址發送資料給另一主機時，它該如何得知對方的 MAC 位址（如 Ethernet 位址）？一般主機知道自己的 MAC 位址，又該如何去得到自己的 IP 位址？

在 TCP/IP 通訊協定裡有兩個協定來解決上述的問題，一為『**位址解析協定**』( Address Resolution Protocol, ARP )；另一為『反向位址解析協定』( Reverse Address Resolution Protocol, RARP )。ARP 是用來查問欲傳送之目地主機的 MAC 位址，也就是說，由已知的 IP 位址查問其相對應的網路實體位址；而 RARP 是由已知的網路實體位址 ( MAC 位址 ) 查詢其相對應的 IP 位址。

## 13-4-1 ARP 通訊協定

『**位址解析協定**』( ARP ) 是被用來以 IP 位址查詢其相對應的網路實體位址 ( MAC 位址 )，其運作方式如圖 13-11 所示。首先主機 A ( 163.15.2.1 ) 的網際層 ( Internet Layer ) 發送出 ARP Request ( 查問 163.15.2.4 ) 訊息給網路存取層 ( Network Access Layer )，網路存取層之 MAC 層 ( Ethernet 層 ) 再將 ARP Request 訊息包裝在 Ethernet 訊框內，並廣播在網路上。網路上 ( 區域網路內 ) 所有主機接收到廣播訊框再拆解訊框。主機 C ( 163.15.2.4 ) 的網際層收到 ARP Request 後，並由其中瞭解是詢問自己，便回應 ARP Reply ( 包含 Ethernet 位址 ) 給網路存取層，網路存取層再發送訊框給主機 A ( 163.15.2.1 )。當然，其它主機也會收到 ARP Request 訊號，但皆判斷不是詢問自己而不予理會。

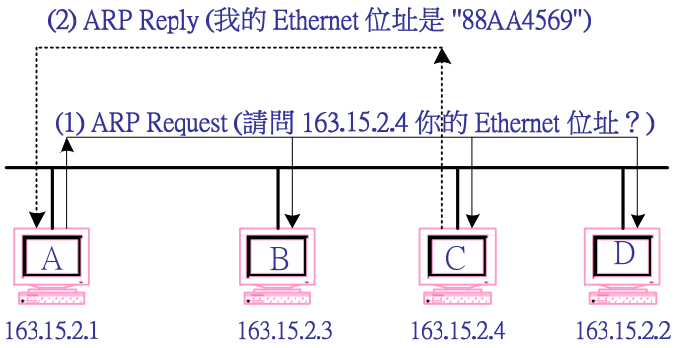



圖 13-11 ARP 運作方式

| 0 | 8 | 16 | 24 | 31 |
|---|---|---|---|---|
| Hardware Type | | Protocol Type | | |
| HLEN | PLEN | Operation Type | | |
| Sender HA (Byte 0 ~ 3) | | | | |
| Sender HA (Byte 4 ~ 5) | | Sender IP (Byte 0 ~ 1) | | |
| Sender IP (Byte 2 ~ 3) | | Target HA (Byte 0 ~ 1) | | |
| Target HA (Byte 2 ~ 5) | | | | |
| Target IP (Byte 0 ~ 3) | | | | |

圖 13-12 ARP 封包格式

不論 ARP 的 Request 和 Reply，或 RARP 之 Request 和 Reply 都使用 ARP 封包格式。ARP 封包格式如圖 13-12 所示，各欄位功能如下：( 值得注意的是 ARP 封包並沒有經過 IP 封包包裝 )

**(1) Hardware Type**：表示發送主機使用之網路實體介面種類，如 1 表示 Ethernet 網路介面。

**(2) Protocol Type**：表示所使用的通訊協定，如 0x0800 表示 IP 協定，其它通訊協定模式如表 13-1 所示。

**(3) Operation Type**：表示此封包的工作模式：

- 1 → ARP 要求（ARP Request）
- 2 → ARP 回應（ARP Reply）
- 3 → RARP 要求（RARP Request）
- 4 → RARP 回應（RARP Reply）

**(4) HLEN**：網路介面卡硬體位址長度。若 Ethernet 位址的長度為 6。

**(5) PLEN**：網路協定位址長度。因為 IP 位址長 4 個位元組，此值為 4。

**(6) Sender HW**：發送端的硬體位址。如果是 Ethernet 網路的話，此為 6 個位元組長的地址，如 0x8823AA112233。

**(7) Target HW**：目的地的硬體位址。

**(8) Sender IP**：發送端的 IP 位址，如 163.15.2.1。

**(9) Target IP**：目的地主機的 IP 位址，如 163.15.2.4。

並非主機每次欲發送封包之前，都要詢問對方的網路硬體位址。一般主機的快取記憶體（Cache memory）上，都有維護一只『**ARP 索引表**』( 由 ARP 協定建立，又稱為 ARP caching )。當主機電腦欲依照 IP 位址發送封包時，首先到快取記憶體上的 ARP 索引表查詢是否有相對應之硬體位址，如果沒有再發送 ARP Request 到網路上詢問。詢問後將相關的 IP 和硬體位址登錄在索引表上，下次可以再使用。相對應的，網路上任何一部電腦接收到 ARP Request 封包時，不管該封包是否詢問自己，在 ARP 封包內都有紀錄傳送者的 IP 位址和硬體位址（MAC），便將其 IP 位址和硬體位址紀錄在本身的索引表內。

又在 TCP/IP 網路上的任何主機啟動時，都會公佈（announce）ARP 訊息告訴網路上所有工作站自己的 IP 和硬體位址。快取記憶體上的索引表必須隨時更新，否則所紀錄的資料也許會失去時效性（也許是主機更換 IP 位址），這必須由系統維護人員去設定自動更替時間。

## 13-4-2 RARP 通訊協定

一般主機電腦上的 IP 位址設定有靜態設定和動態設定兩種方法。靜態設定是於主機電腦上直接用人工設定 IP 位址，設定後如沒有再用人工修改，則 IP 位址永遠不變；動態設定並未設定 IP 位址，每當主機啟動時，再由網路上某部伺服器給予 IP 位址，因此，每次啟動時得到的 IP 位址不一定相同。如果主機電腦採用動態指定 IP 位址模式，啟動就必須利用『**反向位址解析協定**』（Reverse Address Resolution Protocol, RARP），向網路上的伺服器（如 DHCP Server）要求給于一個 IP 位址。

RARP 的動作是，主機電腦用自己硬體位址（MAC 位址）向伺服器詢問自己的 IP 位址，如圖 13-13 所示。圖中假設各主機皆以動態設定 IP 位址，主機 A 為『**動態主機組態伺服器**』（Dynamic Host Configuration Protocol, DHCP），負責分配 IP 位址給網路上主機。電腦主機啟動時便要求 DHCP 伺服器分配一個 IP 位址，電腦主機關機時便釋放該 IP 位址，下次開機時再要求重新分配。例如主機 C 啟動時立即在網路廣播（或傳送給 DHCP 伺服器）RARP Request（要求 IP 位址），主機 A 收到 RARP Request 並驗證其 Ethernet 位址是否可以給予 IP 位址，再回應 RARP Reply 給主機 C，其中攜帶對方的 IP 和 MAC 位址。RARP 封包格式和 ARP 一樣，不再另述。

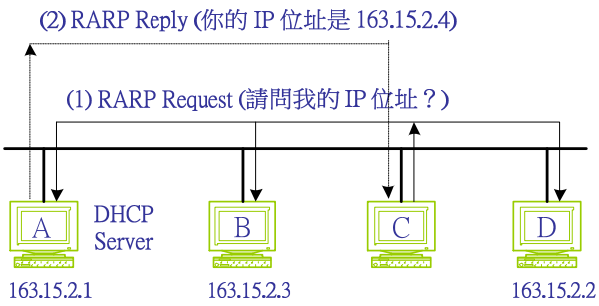



圖 13-13 RARP 運作方式

# 13-5 ICMP 通訊協定

根據我們的瞭解，IP 網路是一種不可靠的傳輸方式，傳送中的封包必須經過多層路由器的轉送才能到達目的地。因此，在發送封包之前，我們很難預測該封包是否可以安全到達目的地。我們也很迫切的想知道目前網路的狀況，尤其在傳送失敗時，更想瞭解問題出在什麼地方。TCP/IP 網路中提供一種稱之為『**網際控制訊息協定**』( Internet Control Message Protocol, ICMP ) 的通訊軟體，用來偵測網路的狀況。在 IP 網路上，任何一部主機或路由器皆設置有 ICMP 協定，它們就可以利用 ICMP 來互相交換網路目前的狀況訊息，例如，主機不存在、網路斷線等等狀況。

ICMP 封包無法直接傳送到網路上，必須如同 TCP 封包一樣被嵌入 IP 封包內，以 IP 方式傳送 ( 如表 13-1 )，包裝在 IP 內的封包格式，如圖 13-14 所示。

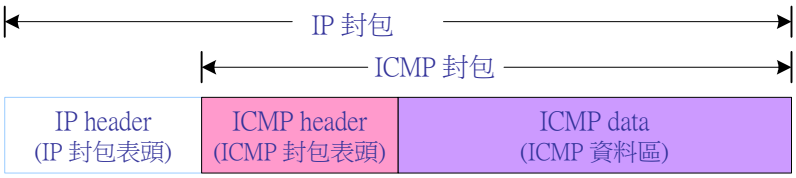



**圖 13-14 ICMP 封包嵌入 IP 封包內傳送**

圖 13-15 為 ICMP 封包格式，其各欄位功能如下：

**(1) 訊息型態 ( Message Type ):** 表示該 ICMP 所欲控制之訊息型態，共有 13 種型態，訊息型態之型態代表值如表 13-2 所示。

**(2) 編碼 ( Code ):** 對各種訊息型態進一步說明工作內容。

**(3) 檢查集檢查碼 ( Checksum ):** 對該封包檢查集錯誤偵測。

**(4) 訊息說明 ( Message description ):** 依照不同的控制訊息，而有不同的說明方式。

**(5) 訊息資料 ( Message Data ):** 依照不同的控制訊息，而有不同的資料表示。

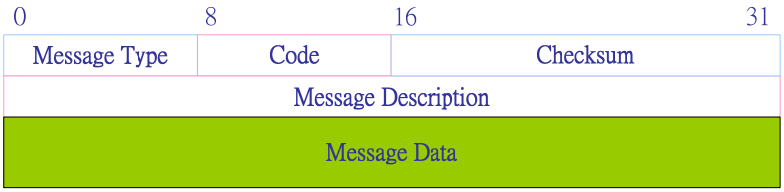



**圖 15-15 ICMP 封包格式**

**表 13-2 ICMP 訊息型態**

| Message Type | ICMP 訊息功能 |
|---|---|
| 0 | Echo Reply（回應答覆） |
| 3 | Destination Unreachable（目的地無法到達） |
| 4 | Source Quench（來源抑制） |
| 5 | Redirect（改變傳輸路徑） |
| 8 | Echo Request（回應要求） |
| 11 | Time Exceeded for a Datagram（溢時傳輸） |
| 12 | Parameter Problem on a Datagram（參數問題） |
| 13 | Timestamp Request（時間標籤要求） |
| 14 | Timestamp Reply（時間標籤回覆） |
| 15 | Information Request（資訊要求）（停用） |
| 16 | Information Reply（資訊回覆）（停用） |
| 17 | Address Mask Request（位址遮罩要求） |
| 18 | Address Mask Reply（位址遮罩回覆） |

各種不同的控制訊息型態，以下分別說明之：

## 13-5-1 回聲要求/回聲回應

**『回聲要求』(Echo Request)(Type 8)**是用來要求對方回聲，如有**『回聲回應』(Echo Replay)**(Type 0)表示對方主機或路由器工作正常。也可以用來測試網路路徑是否確實可以到達，被測試端用 ICMP Echo Reply 封包答覆對方的回聲要求。TCP/IP 的主機電腦（或路由器等設備）上皆有提供 "ping" 指令，其用來實現 Echo Request 命令。例如，在主機電腦上執行 ping 163.15.2.1 指令，當 163.15.2.1 之網路設備接收到該訊號時，必須立即回應 Echo Reply，而在主機電腦上會顯示經歷時間，或主機電腦在溢時之候，未收到 Echo Reply 訊號，則會顯示 Request timed out 訊息。被測試端和測試端之間也許經過多個路由器(或網路閘門)，但如果收到 Echo Reply 訊號，則表示該路徑是可到達的。

圖 13-16 為 Echo Request 及 Echo Reply 的封包格式，其中 Identifier（識別碼）和 Sequence Number（順序號碼）是用檢查回聲回應封包是針對哪一個回聲要求所產生的。

一般我們可以連續發送多個 Echo Request 給被測試端，每個回聲要求都給予一個順序編號放置在 Identifier 內，被測試端發送 Echo Reply 時將 Echo Request 內之 Identifier 的值放置於

Sequence Number 欄位內，告訴發送端是針對哪一個 Echo Request 的回聲回覆。另外，封包內之 Option Data 可有可無，如 Echo Request 有放置資料，回覆 Echo Replay 就依照該資料送回。

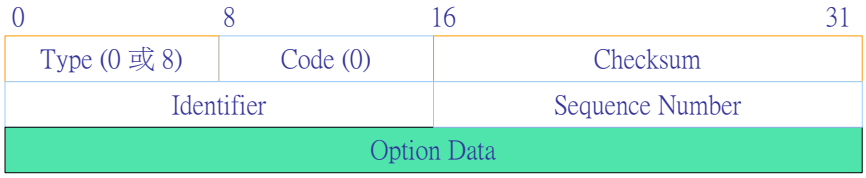



**圖 13-16 Echo Request/Reply 封包格式**

## 13-5-2 目的地無法到達

當路由器（或網路閘門）發現，某一個 IP 封包無法往下一個路徑傳送時，便發送 **ICMP Destination Unreachable（目的地無法到達，Type 3）**封包給原始發送該封包者，並將封包丟棄。因此，在回應封包之 Message Data 欄位內必須註明是哪一個 IP 封包被丟棄，如圖 13-17 所示。而另封包內之 Code 欄位是用來註明無法到達目的地的原因，原因分類如下：

- 0: Network Unreachable（無法到達目的網路）
- 1: Host Unreachable（無法到達目的主機）
- 2: Protocol Unreachable（通訊協定不存在）
- 3: Port Unreachable（無法到達連接埠）
- 4: Fragmentation Needed and DF set（資料需分割並設定不可分割位元）
- 5: Source Route Failed（來源路徑選擇失敗）
- 6: Destination Network Unknown（無法識別目的地網路）
- 7: Destination Host Unknown（無法識別目的地主機）
- 8: Source Host Isolated（來源主機被隔離）
- 9: Communication with Destination Network Administratively Prohibited(管理上禁止和目的地網路通訊）

- 10: Communication with Destination Host Administratively Prohibited（管理上禁止和目的地主機通訊）
- 11: Network Unreachable for Type of Service（無法到達此型態的網路服務）
- 12: Host Unreachable for Type of Service（無法到達此型態的主機服務）

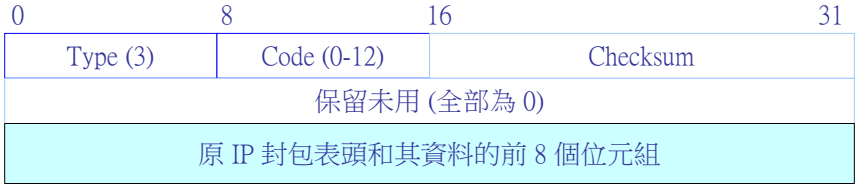



**圖 13-17 Destination Unreachable 封包格式**

## 13-5-3 來源抑制

當網路上路由器（或網路閘門）因為進入的封包速度過快，而來不及處理的時候（本身的緩衝器已溢滿），會將再進入的封包丟棄，並發送一個 **ICMP Source Quench（來源抑制，Type 4）**封包給該 IP 封包的來源主機。原發送主機接收到 Source Quench 封包後會暫停或降低發出封包的速度，一直到沒有接收到路由器所發送的 Source Quench 後，再恢復原來的發送速度。Source Quench 的封包格式如圖 13-18 所示。

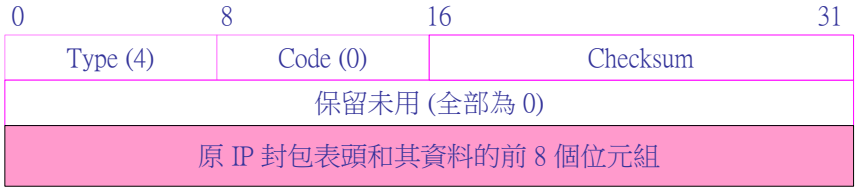



**圖 13-18 Source Quench 封包格式**

## 13-5-4 改變傳輸路徑

在某些情況下（如網路拓樸圖改變或網路斷線），路由器發現原來由它轉送的目的位址，經由別的路由器轉送會比較快速，則該路由器便利**用 ICMP Redirect （改變傳輸路徑，Type 5）**訊息通知原發送端，請它改變傳輸路徑，傳送到另一個路由器上。圖 13-19 為 Redirect 的封包格式，其中 "Gateway IP Address" 表示新轉向傳輸路徑的路由器之位址，Code 欄位表示轉向的原因：

- 0: Redirect Datagram for the Net（網路變更而轉向）
- 1: Redirect Datagram for the Host（主機變更而轉向）
- 2: Redirect Datagram for the Type of Service and Net(網路和服務型態變更而轉向）
- 3: Redirect Datagram for the Type of Service and Host（主機和服務型態變更而轉向）

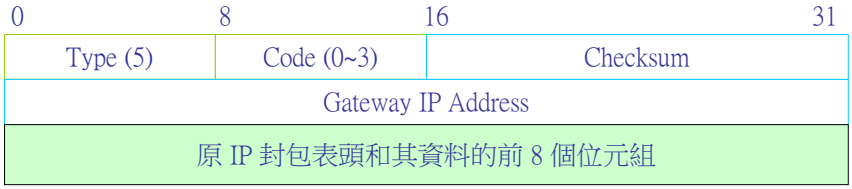



**圖 13-19 Redirect 封包格式**

## 13-5-5 溢時傳輸

當路由器（或網路閘門）發現某一個 IP 封包內之 TTL（Time to Live）為 0 時，會發送一個 **ICMP Time Exceeded(溢時傳輸，Type 11)**封包給原發送封包者，並將該封包丟棄。為了避免封包在網路上不停的環繞，封包發送之前會在 TTL 欄位設定一個值，表示該封包的存活時間。封包在傳送後，每經過一個路由器，就將 TTL 內的值減一。如果路由器發現某個封包內的 TTL 值為 0，便判斷該封包已在網路上環繞，找不到適當路徑到達目的地，而將其丟棄。另外一種情況，接收端也會發送 ICMP Time Exceeded 訊息給來源端，此情況是資料片重組（Fragment reassembly）發生問題。當 IP 封包被分為若干個資料片段傳送時，接收端收到一筆資料片段時會設定一個計時時間，如在溢時（timeout）後未收到下一筆資料片段，則將發送 ICMP Time Exceeded 給原傳送端。圖 13-20 為 Time Exceeded 之封包格式，其中 Code = 0 表示 TTL = 0 時發送該封包；而 Code = 1 表示資料片段重組失敗所以要重新發送封包。

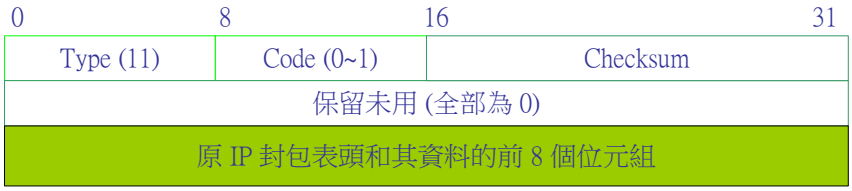



**圖 13-20 Time Exceeded 封包格式**

## 13-5-6 參數問題

當路由器（或網路閘門）發現 IP 封包內的某些欄位的值（參數）不正確，而無法處理該封包時，便發送 **ICMP Parameter Problem（參數問題，Type 12）**封包給原發送者。封包格式如圖 13-21 所示，其中 Pointer 欄位表示錯誤參數之位址。

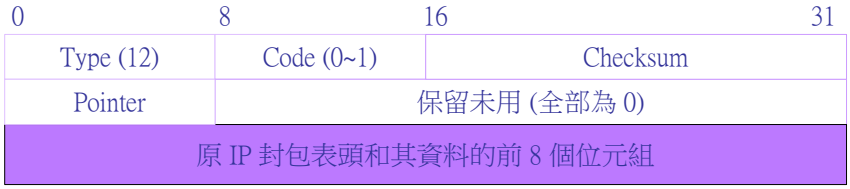



**圖 13-21 Parameter Problem 封包格式**

## 13-5-7 時間訊息要求及回覆

**ICMP Timestamp Request（時間訊息要求，Type 13）**封包是用來詢問某部主機的系統時間；而 **ICMP Timestamp Reply（時間訊息回覆，Type 14）則用來回應系統時間**，這兩個封包是用來使網路上各設備的時間達到同步。圖 13-22 為 Timestamp 的封包格式，其中 Originate Timestamp 表示詢問者自己的時間、Receive Timestamp 表示被詢問者接收到 ICMP timestamp request 封包的時間、Transmit Timestamp 為被詢問者發送回應的時間。前一項為詢問者的時間基準；後二項為被詢問者的時間基準。時間單位都是 millisecond，並以格林威治時間為基準。

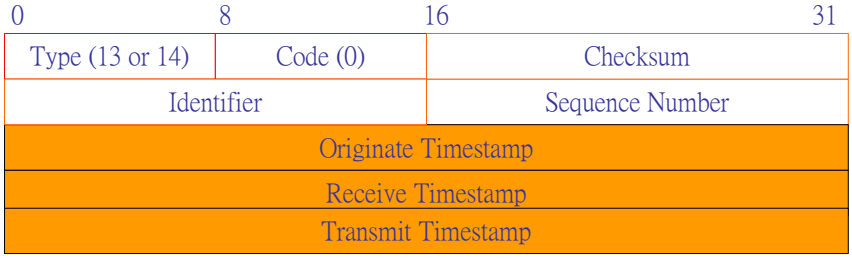



**圖 13-22 Timestamp Request/Reply 封包格式**

## 13-5-8 遮罩位址要求及回覆

**ICMP Address Mask Request/Reply （Type 17/18）**是被用來要求獲得或回應某一個次網路（Subnet）的位址遮罩（mask）時所使用，圖 13-23 為其封包格式。

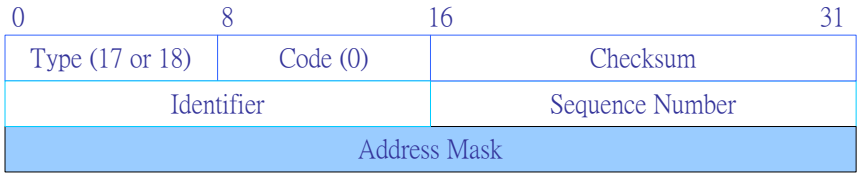



圖 15-23 Address Mask Request/Reply 封包格式

# 13-6 TCP 通訊協定

**『傳輸控制協定』( Transmission Control Protocol, TCP )** 和 IP 兩者似乎是連結在一起的同一名稱 ( TCP/IP )，兩者的功能確實是相輔相成。IP 的功能是無論兩部工作站距離多遠，都能透過 IP 技術連結在一起。TCP 提供網路的服務接點讓應用程式使用，也就是說，提供端點對端點 ( host-to-host ) 的連線。主機電腦上可能有多個應用程式需要透過網路服務，TCP 就提供多點服務的連線( 虛擬鏈路的多工功能 )讓各種應用程式可同時連結到網路上。TCP 和 IP 的關係宛如電話系統中的電話號碼和分機號碼。當我們撥接電話時，將依照電話號碼的位址在廣泛的電話大海之中找到對方，並和其連接完成 ( IP 功能，各地區的交換機就如網路閘門 )。這並不能表示我們已連絡上受話的對方，但最起碼我們也連線到對方的電話機上 ( IP 已連結到主機上 )。欲找到受話的人也許可用人工呼叫，或是再撥分機號碼( TCP 的埠口號碼 )，就像是在主機號碼上再加入分機號碼來表示通訊的個人 ( TCP 的點對點連線 )。而人與人之間的對話就像網路上應用程式之間的通訊。( 傳輸層技術請參考本書第五章 )

TCP 和 IP 另一個相輔相成的功能是由 IP 提供非連接的不可靠傳輸，至於有關可靠傳輸的處理程序就必須仰賴 TCP 來完成。換言之，IP 傳送當中，也許會發生封包損壞、封包遺失、封包重複或次序錯亂等現象，這些情況都必須由 TCP 來負責檢測出，並要求對方重送、重整封包順序等工作。因此，TCP 必須提供連接導向的連線，才能使整個網路通訊達到可靠性的傳輸。本節將依此介紹 TCP 之特性，首先介紹 TCP 的封包格式，如圖 13-24 所示，各欄位功能如下：

**(1) 來源埠口 ( Source Port ) :** 來源之 TCP 埠口。

**(2) 目的地埠口 ( Destination Port ) :** 目的地之 TCP 埠口。

**(3) 順序編號 ( Sequence Number ) :** 該封包的順序編號。( 滑動視窗法中的 N(S) )

**(4) 確認號碼（Acknowledge Number）：**回應傳送封包的確認號碼，也是期望傳送端下次發送封包的序號，其表示該確認號碼以前的封包都以正常接收。（滑動視窗法中的 N(R)）

**(5) 資料偏移量（Data Offset）：**因為 TCP 的 Option 欄位長度並非固定，Data Offset 用來表示傳輸資料（Data）是在整個封包之區段起始位址。

**(6) 位元碼（Code bits）：**（6 位元）（URG, ACK, PSH, TST, SYN, FIN）此欄位作控制訊息傳遞之用。而且目前有關 TCP/IP 網路上的特殊處理工作（如防火牆等等）都是利用這些控制碼來運作。其中：

- **URG（Urgent）：**表示該封包為緊急資料，並使 Urgent Point 欄位有效。
- **ACK（Acknowledge）：**本封包有回應確認功能，其確認 Acknowledge Number 欄位中所指定的順序號碼。
- **PSH（Push）：**請求對方立即傳送 Send Buffer 中的封包。
- **RST（Reset）：**要求對方立即結束連線（強迫性）。發送者已斷線。
- **SYN（Synchronous）：**通知對方要求建立連線（TCP 連線）。
- **FIN（Finish）：**通知對方，資料以傳輸完畢，是否同意斷線。發送者還在連線中等待對方回應。

**(7) 視窗（Window）：**此欄位是用來控制封包流量，告訴對方目前本身還有多少緩衝器（Receive Buffer）可以接收封包（滑動視窗法之特性）。如果 Window = 0 表示緩衝器已滿暫停傳送資料。Window 大小的單位是位元組（Byte）。

**(8) 檢查集（Checksum）：**對整個封包（資料和表頭）作檢查集檢查的檢查碼。

**(9) 緊急指標（Urgent Point）：**如 URG = 1 時，其代表緊急資料是在資料區的什麼位址。

**(10) 任選欄（Option）：**目前此欄位只應用於表示接收端能夠接收最大資料區段的大小。如果不使用此欄位，則可以使用任意的資料區段大小。

**(11) 填補欄位（Padding）：**將 Option 欄位補足 32 位元的整數倍。

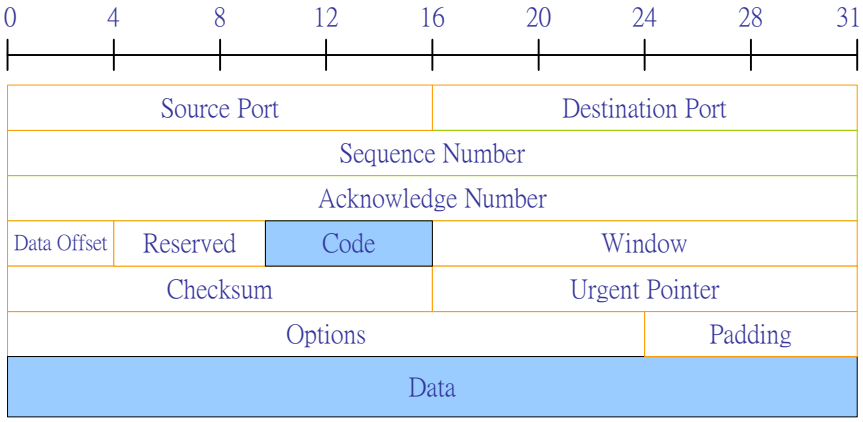



圖 13-24 TCP 封包格式

## 13-6-1 TCP 埠口

**『TCP 埠口』( TCP Port )** 是 TCP 連線中虛擬鏈路的邏輯編號，讓應用層的應用軟體可透過埠口位置銜接上網路。TCP 埠口是利用 16 位元表示，理論上可以提供 65536( = 216 ) 個連接埠。TCP 埠口和 IP 之連線是多工處理的關係 ( 如圖 13-25 所示 )，至於虛擬鏈路之間如何選擇處理次序，可依照作業系統的程序排程 ( Scheduling ) 管理，例如，分時系統 ( Time sharing system ) 以時間分割或循環點名法 ( Round-robin ) 來輪流處理，或即時系統 ( Real-time system ) 以優先權較高的連線優先處理。對於每一個連接埠口都給予唯一的編號 ( 如 2020 )，如圖 13-25 裡程式 A 連接之位址為 163.15.2.1:2020，表示在 IP 位址為 163.15.2.1 ( 宛如電話號碼 ) 的主機之第 2020 連接埠 ( 宛如分機號碼 )。程式 1 的連結位址為 163.15.4.5:8080，程式設計者或網路使用者只要記住這個位址，就可以連絡到程式 1，而不必知道 ( 也很難知道 ) 連線之間所經過何種網路，或它在全世界的哪一個角落。

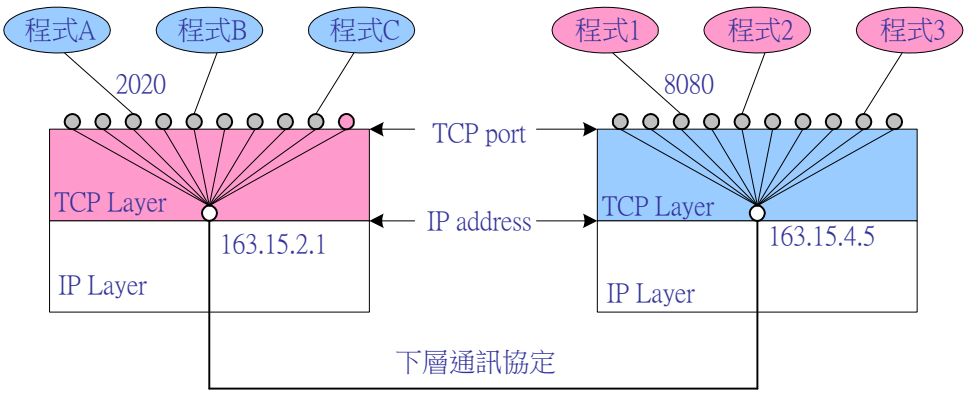



圖 13-25 TCP 與 IP 之連線關係

TCP port 的編號範圍為 0 ~ 65535（216），我們採用兩種配置方式：『**固定配置埠**』（Static Allocated Port）和『**動態配置埠**』（Dynamically Allocated Port）。將 0 ~ 1023 之位置配置給固定的應用程式（或常用伺服器）使用，使一般用戶連接時不必特別去記憶連接埠的位置，稱之為固定配置埠。例如，當使用者連接到某一主機（163.15.2.1）上的 Web Server（80），只要連接上 http://163.15.2.1，便自動連結到 Web Server，而不用輸入 http://163.15.2.1:80。我們節錄一些較常用的著名埠（Well-known）位置如表 13-3。動態配置埠是當應用程式需要連線時，才由系統動態地配置出，其埠號碼範圍為 1024 ~ 65535，但某些位置如被特別指定連線使用（如 8080），就不可以再重複配置。

表 13-3 著名服務的埠號碼（節錄）

| 埠號碼 | 服務名稱 | 傳輸協定 | 應用服務說明 |
|---|---|---|---|
| 0 | 保留 | | |
| 1 | tcpmux | TCP | TCP port 服務多處理 |
| 7 | Echo | TCP/UDP | 回應測試 |
| 11 | systat | TCP | 系統狀態顯示 |
| 15 | netstat | TCP | 網路狀態顯示 |
| 20 | ftp-data | TCP | FTP 資料傳輸埠 |
| 21 | ftp | TCP | FTP 控制埠 |
| 23 | telnet | TCP | Telnet 遠端登入埠 |
| 25 | smtp | TCP | Simple Mail Transfer Protocol |
| 37 | time | TCP/UDP | Time Server |
| 42 | name | UDP | Name Server |
| 43 | whois | TCP | 是誰、nickname（別名） |
| 53 | domain | TCP/UDP | Domain Name Server（DNS） |
| 79 | finger | TCP | 尋找使用者 |
| 80 | http | TCP | Web Server |
| 109 | pop-2 | TCP | Post Office Protocol |
| 119 | nntp | TCP | Network News Transfer Protocol |
| 123 | ntp | TCP | Network Time Protocol |

## 13-6-2 TCP 連線管理

TCP 是連接導向的傳輸方式，對於連線管理來說，顯得特別重要。TCP 採用『**三向握手式連絡法**』（Three-way handshake）來實現連線處理方式，其中會用到封包內二個序號：

**Sequence Number( seq )**及 **Acknowledge Number( ack )**，以及 Code 欄位中四個旗標：ACK、SYN、FIN 和 RST。以下分別介紹各種連線情況的處理方式：( 基本原理請參考第五章 )

建立連線

圖 13-26 為三向握手式連絡法的連線建立圖，所謂三向握手式是表示有三個訊號來建立連線：(1) SYN ( A→B ) 表示 A 向 B 要求連線；(2) SYN&ACK ( B→A ) 為 B 回應給 A，表示同意或不同意連線要求；(3) ACK ( A→B ) 表示 A 確認收到 B 的回應。另外， seq 表示要求連線的封包號碼；ack = seq +1 表示確認 seq 封包，並要求傳遞下一個封包序號 ( 滑動視窗法確認方式 )。

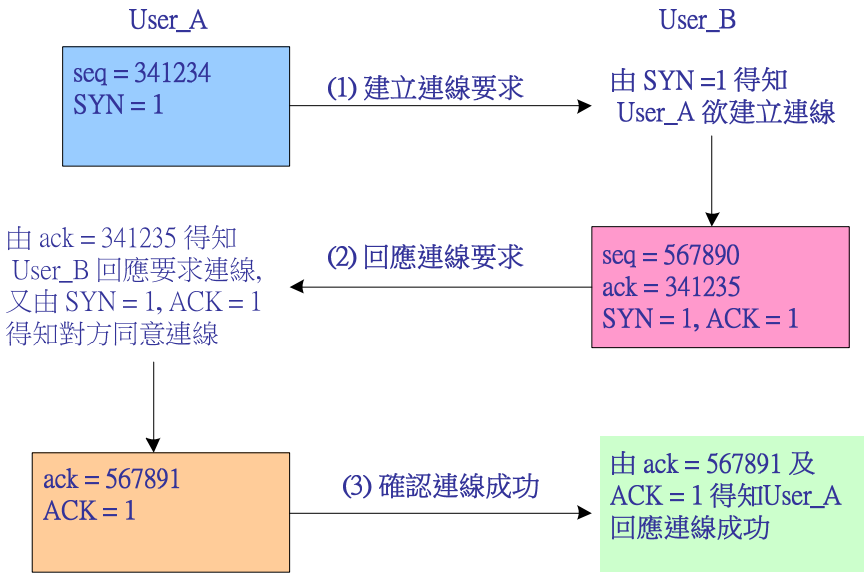



**圖 13-26 TCP 建立連線運作程序**

## (A) 資料傳送

TCP 連線中的資料流量控制也是採用滑動視窗法 ( Sliding Window )( 請參閱 3-4-2 節說明 )，錯誤偵測技巧是採用檢查集 ( Checksum ) 的方法 ( 請參閱 3-5-2 節說明 )。Sequence Number( seq ) 表示該封包的順序號碼 ( 滑動視窗法中的 N(S) )、Acknowledge Number( ack ) 為期望對方發送的封包順序號碼 ( N(R) )，也確認該序號以前的封包都已正常接收。

傳送開始的 Sequence Number 是由亂數 ( Random Number )產生。圖 13-27 為 User_A 傳送資料給 User_B 的資料流動控制程序。其中 data_length 表示每次封包內所傳送的資料位

元組數量。我們要特別強調封包序號的計算是以資料位元組（byte）為單位，而不是以傳送次數為單位。因此，回應確認序號是 ack = seq + data_length。

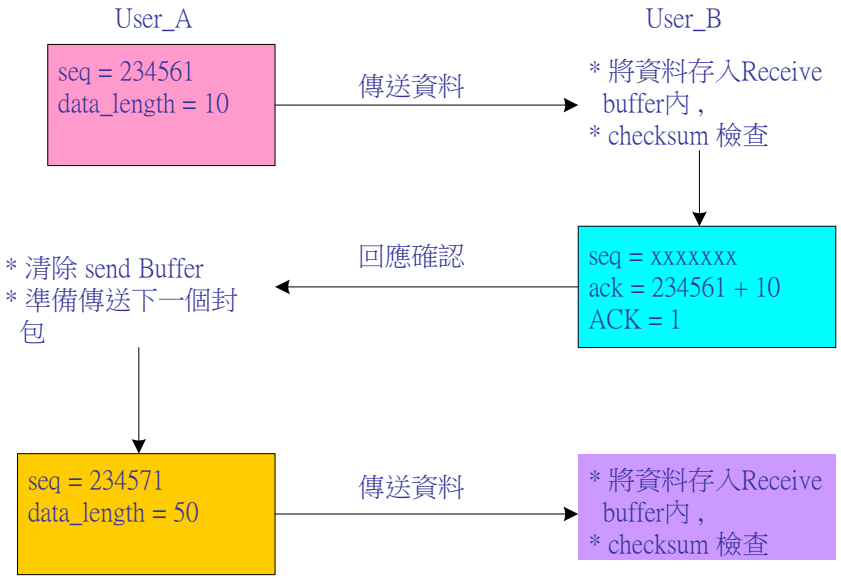



**圖 13-27 TCP 資料傳送運作方式**

## (B) 連線終止

TCP 連線使用連接導向與雙向傳輸模式，遇到要處理連線終止的問題就會變得比較麻煩。可能出現一端已經傳輸完畢，而另一端卻還要傳送資料的問題，因此雙方必須協議好才可以終止連線。圖 13-28 為連線終止的運作程序，首先 User_A 傳送完資料並告訴 User_B 工作已完成，且準備終止連線（FIN = 1）。User_B 必須詢問上層通訊軟體是否還要繼續通訊，如上層回應同意終止連線，User_B 再告訴 User_A 確實可以終止連線。為了防止封包遺失或溢時傳送，雙方請求或回應封包都以封包序號（N(S) 及 N(R)）作為確認基準。

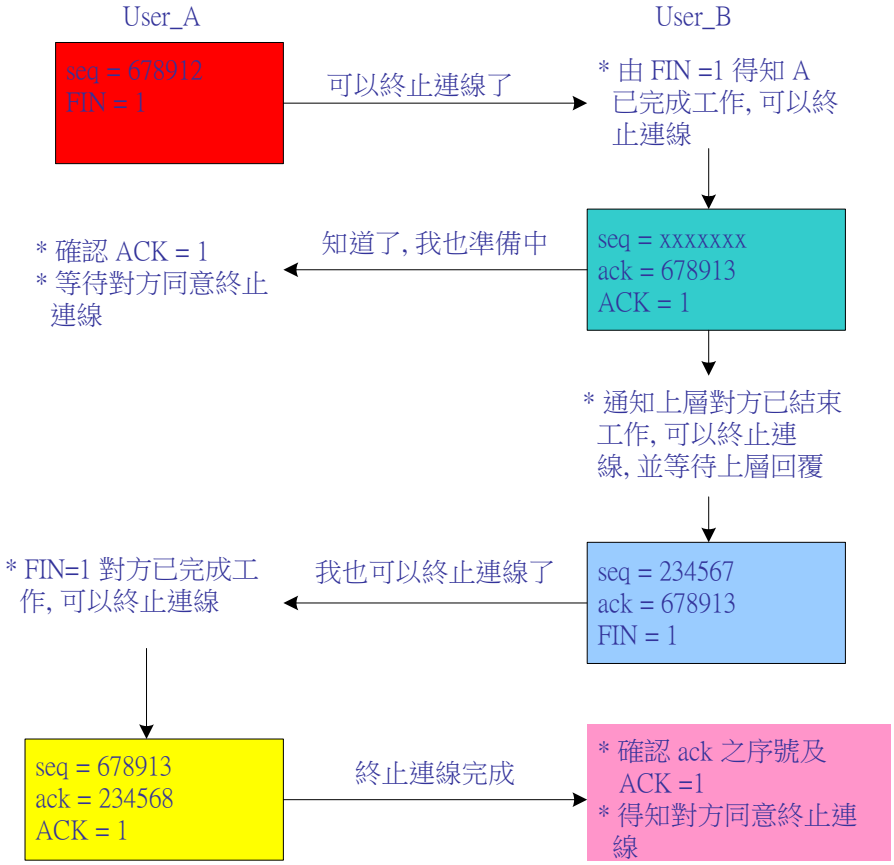



**圖 13-28 TCP 終止連線運作程序**

# 13-7 UDP 通訊協定

TCP/IP 網路除了提供可靠性服務的 TCP 連接外，也提供非連接方式傳輸，稱之為**『使用者電報傳輸協定』( User Datagram Protocol, UDP )**。UDP 傳輸協定比 TCP 簡單，沒有連線要求、連線終止、以及流量控制的管理程序。它的優點是傳輸速率較快，主要應用於較少量與即時性傳輸，但對資料正確性的要求較不高 ( 如語音或視訊 )。而其缺點則是無法提供正確性較高的資料傳輸。採用 UDP 傳輸可能會有資料重覆、資料未依序到達、資料遺失等等問題，必須由使用者自行解決。倘若上層應用軟體可自行驗證資料正確性的情況下，可考慮使用 UDP ( 如 RIP、DNS 之應用 ) 傳輸。UDP 之封包格式如圖 13-29 所示，各欄位功能也如同 TCP 格式，不另再贅言。

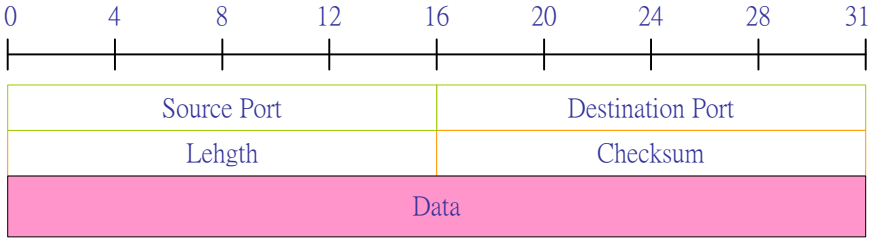


圖 13-29 UDP 之封包格式

# 13-8 IPv6 通訊協定

自從 1990 年網際網路風行之後，網路專家們漸漸感覺到所使用的 IP( IPv4，Version 4 ) 通訊協定已不敷使用。尤其隨著應用層次的提高，IP 網路不再只提供檔案傳送及遠端登入等簡單的應用，更進一步處理有關資料庫系統的查詢與更新，也進入電子商務的應用。因此，有必要再發展出功能更完整的通訊系統，『**IPv6**』( IP Version 6 ) 就在這迫切需求之下被發展出來。首先，我們用下列幾點來介紹 IPv6 如何彌補 IPv4 的不足。

IPv6 提供更寬廣的 IP 定址空間。IPv4 用 32 位元 ( 4 個位元組 ) 來表示 IP 位址空間，也漸不能滿足目前網際網路上主機電腦連結的成長。IPv6 提供 128 位元 ( 16 個位元組 ) 的空間來表示 IP 位址。

**(1) IPv6 提供認證服務。**一般 IP 封包在傳送當中，每經過一個中途路由器就必須被拆裝和重新包裝，又要經過許多不可預測的路由器 ( 無法事先預估 )。而且，為了要使封包能順利到達目的地，在封包上又無法做太多的保護措施。也就這樣，任何有心人士，皆可輕易地在網路上窺視，甚至竄改他人資料，使傳送的訊息失去正確性，尤其企業內的區域網路對資訊安全的需求更高，所以更為困擾。早期，跨區域的區域網路連接都透過專線，但為了節省費用及符合出差人員能以較快速、較便宜的連線，目前都希望能直接透過網際網路連線，如『**虛擬私人網路**』( Virtual Private Network, VPN )。雖然目前有許多技術可以克服，譬如，使用『**通道技術**』( Tunneling Technique ) 來保護資料在 IP 網路上不被偷竊，但這類技術大多必須利用上一層通訊協 ( TCP ) 定來完成，而且並非每一部路由器都提供到上一層的服務( 一般路由器只提供到 IP 層服務 )。IPv6 提供認證的功能，未經認證通過的連線， IPv6 路由器將不給予轉送或拆封，以保證資料的隱密性，也不需要透過上層協定的處理。

**(2) IPv6 提供『流量標籤』( Flow Label )。**一般 IPv4 網路上，封包每經過中途路由器，路由器只負責將封包轉送到適當的路徑上，並未做任何的紀錄。在 IPv6 網路上，每一個封包提供一個流量標籤，同一筆資料串列給予相同的標籤號碼，因此可以做流量控制及統計。

**(3) IPv6 提供『訊務等級』( Traffic Class ) 分類**。雖然在 IPv4 封包上有提供 ToS ( Type of Service )，但有關 QoS ( Quality of Service ) 的服務都由上層通訊軟體所提供，ToS 幾乎沒有發揮功能。IPv6 提供『**訊務等級**』的分類，再配合流量標籤使用，就可以依照每一個封包的服務性質，給予路徑選擇的優先次序及適合路徑，便可達到 QoS 的需求。

**(4) IPv6 減少封包分段 ( Fragmentation ) 的機率**。在 IPv4 的協定裡，每個封包大小並未嚴格限制，當封包經由不同網路存取層 ( Network Access Layer, NAL ) 時，會將封包分割成不同區段，並給予相同的分段號碼( Fragment Number )，好讓對方接收到後，依照相同的分段號碼，再組合回原來封包 ( 向上/向下多功能 )。但在同一序列的封包可能經由不同的 NAL 傳輸，其中若有任一封包沒有到達目的，則將使整串列資料失效，而全部都必須重傳。因此，在 IPv6 協定裡只允許傳送中的起始和終點可以做分割和組合，減少中途路由器的分割動作，不但可以減少中途路由器的負擔，對傳輸效率也較高。

**(5) IPv6 簡化封包標頭**。不像 IPv4 的標頭裡存放太多欄位，IPv6 捨棄不必要的欄位，作較有效率的處理。

## 13-8-1 IPv6 封包格式

圖 13-30 為 IPv6 的封包格式，各欄位功能如下：

**(1) 版本 ( Version )**：表示本封包的 IP 版本，如 IPv6 的值為 6。

**(2) 交通流量等級 ( Traffic Class )**：標示該封包的流量等級，等級愈高者優先轉送。可區分為 16 個等級，0 ~ 7 可以提供回應壅塞 ( 如 TCP )，8 ~ 15 則不提供回應壅塞 ( 如壅塞時便拋棄該封包 )。等級 0 ~ 7 所提供之服務如下：

- 0：非結構化交通流量 ( Uncharacterized traffic )
- 1：填滿型交通流量 ( Filler traffic )
- 2：未處理資料傳送 ( Unattended data transfer )
- 3：保留 ( Reserved )

- 4：經處理區塊傳送（Attended bulk transfer）
- 5：保留（Reserved）
- 6：交談式交通流量（Interactive traffic）
- 7：網路間控制交通流量（Internet control traffic）

**(3) 流量標籤（Flow Label）:** 同一筆資料給予相同的標籤，可作為流量控制。

**(4) 承載長度( Payload Length ):** 本封包所承載資料的長度。表示承載其他通訊軟體( TCP 或 UDP 等封包 ) 的長度。

**(5) 下一標頭 ( Next Header ):** 此欄位類似 IPv4 的 Protocol 欄位，表示本封包所承載的標頭型態，如 TCP 或 UDP 等等。

**(6) 跳躍次數（Hop Limit）:** 類似 IPv4 上的 TTL 欄位，每經過一個路由器其值就被減一，如路由器發現該值為一時，便將封包丟棄。在 IPv6 的封包標頭上沒有 Checksum 檢查，因此，路由器計算跳躍值後不用再重新計算 Checksum。

**(7) 來源位址（Source Address）:** 以 128 個位元（16 個位元組）表示。

**(8) 目的位址（Destination Address）:** 以 128 個位元（16 個位元組）表示。

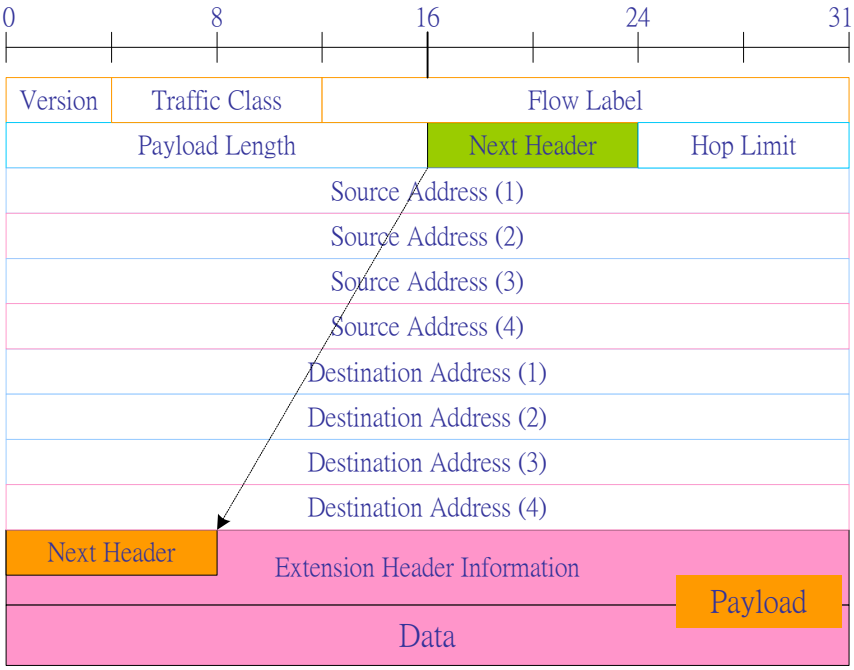



圖 13-30 IPv6 封包格式

## 13-8-2 IPv6 位址格式

IPv6 用 128 位元（16 個位元組）來表示位址，比 IPv4 增加許多，表示方法也相對複雜。IPv4 只將位址區分為兩個部份：網路號碼和主機號碼，但 IPv6 就有更多型態的區分。首先我們來看如何書寫這 128 位元，將其分成 8 組位置，每組 16 個位元又區分為 4 個字元，每個字元（4 個位元）以 16 進位法表示。如下面格式：

X:X:X:X:X:X:X:X

例如：A2E5:56EF:906B:4590:12EC:D532:7812:0001

在 IPv6 位址表示中常有許多組為 0 的情形，為了簡化組內數值都為 0 時，以「：：」來表示，例如：

0:0:0:0:0:0:0:1→ ::1 為 loop back 位址

0:0:0:0:0:0:0:0 → :: 為未指定位址

緊接著，我們來看 IPv6 的位址型態。在 IPv4 協定之下，將主機位址都設定為 1 時，表示針對這個網路號碼之下的所有主機廣播。但廣播封包容易造成風暴，嚴重影響網路效能。IPv6 不再使用這任意廣播的方式，而是使用『**所有節點**』的多點廣播位址。多重節點廣播並非所有節點都會處理廣播訊息，而是有關聯的節點才會處理，如此就可以減低所有節點對廣播訊息的處理。IPv6 將位址型態區分為下列三種：

**(1) 單一廣播位址（Unicast Address）**

**(2) 任一廣播位址（Anycast Address）**

**(3) 多點廣播位址（Multicast Address）**

以下分別介紹各種型態，對於 IPv6 前置位址以『**prefix/prefix-length**』表示之，例如：2000::/3 表示該 IPv6 位址的前置碼長度為 3，第一組字元為（0010），其餘皆為 0。

### (A) 單一廣播位址（Unicast Address）

單一廣播型態如同 IPv4 一樣，對每一個主機而言，都有一個獨一無二的位址。但 IPv6 採用 64 位元的介面位址，取代 IPv4 的主機位址。IPv6 期望如同 48 位元之 Ethernet 位址一樣可嵌入硬體介面上。單一廣播可區分為四種位址型態：

- **可集合式整體位址（Aggregatable Global Address）**
- **地區本地位址（Site-Local Address）**
- **鏈路本地位址（Link-Local Address）**
- **IPv4 相容（IPv4-Compatible）之位址格式**

以下分別介紹各位址格式之特性：

### (a) 可集合式整體位址（Aggregatable Global Address）

一般主機或網路設備都可被指定一個或一個以上以上的整體位址（Global Address），以便與其他電腦設備區分。它的位址格式如圖 13-31 所示，我們將 128 位址區分為三個部份，第一部份（Provider）表示網路連接的供應者，指一般的 ISP 位址；第二部分為區域，讓使用者自行區分網路，也就是一般所言的次網路。第三部份為主機，計有 64 位元，也希望使用類似 Ethernet 位址的方法。各欄位功能如下：

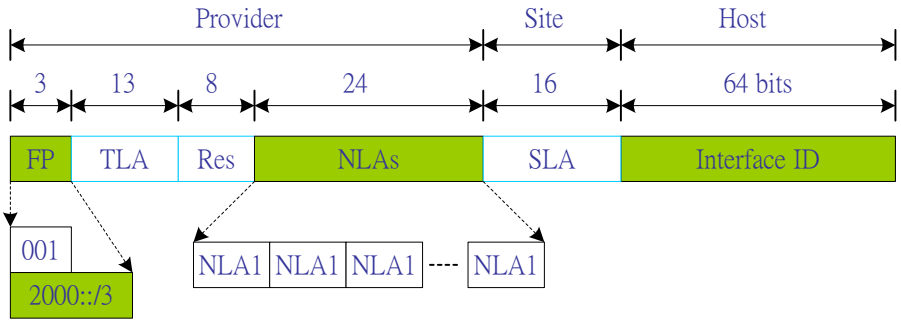



圖 13-31 可集合式整體位址格式

- **固定前置碼( Fixed Prefix, FP ):** 以 001 表示 IPv6 的可集合式整體位址格式，對整個位址表示為 2000::/3。
- **最上層集合碼（Top-Level Aggregator, TLA）:** 讓網路提供者做最上層的區分，類似電話號碼的國家碼區分法。
- **保留（Reserve, Res）:** 保留未使用。

- **下一層集合碼（Next-Level Aggregator, NLA）：**第二層次的集合碼，類似電話號碼的區域碼。它可以再區分若干個區域碼組合而成。
- **地區層次集合碼（Site-Level Aggregator, SLA）：**讓使用者環境區分集合碼，如 IPv4 的次網路（Subnet）位址碼。
- **介面識別碼（Interface ID）：**64 位元的主機位址。

### (b) 地區本地位址（Site-Local Address）

只要能在某特定區域裡自行構成網路，就可以使用 IPv6 的地區本地定址格式，對於該地區內所用的位址格式不同於整體位址（Global Address）(類似 IPX 定址)，IP 路由器不會將該類封包轉送出去，只在地區內廣播。至於需要轉送到地區外，則必須使用整體位址。它的位址格式如圖 13-32 所示。其固定前置碼為 FEC0::/10，並允許地區內再劃分多個小地區，因此有 Subnet-ID 欄位來表示次地區的編碼。Interface-ID 也是 64 位元組來表示。(但 IPv6 對 IPX 及 NASP 有另外定義位址)

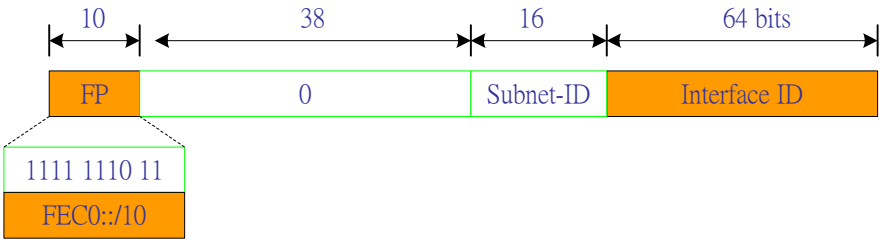



圖 13-32 地區本地位址格式

### (c)鏈路本地位址（Link-Local Address）

鏈路本地位址的特性類似地區本地位址，但鏈路本地位址是指在每一鏈路上而非地區，因此無法再區分次區域。鏈路本地位址可被自動規劃於任何網路介面上，並用來發現鄰近端點的協定或無狀態轉換的自動規劃使用。任何端點在本地網路上可用該位址互相通訊。路由器也不會將該類封包轉送出去，它的封包格式如圖 13-33 所示，其前置碼為 FE80::/10。

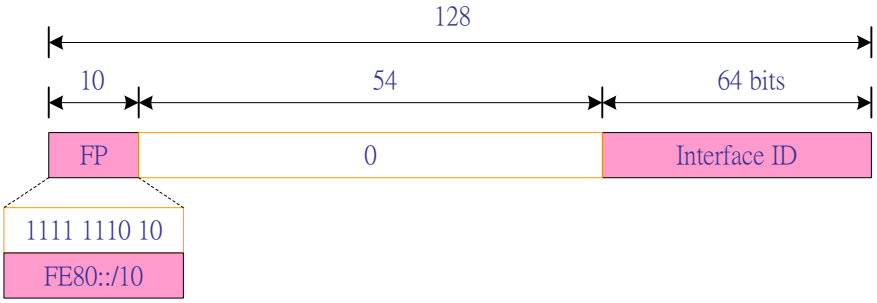



圖 13-33 鏈路本地位址格式

### (d) IPv4 相容（IPv4-Compatible）之位址格式

依目前 IPv4 的網路要轉換到 IPv6，可能需要一段長的時間，不僅封包格式需要修改，通訊協定也必須更新。因此，首先讓兩種協定能夠相容，再漸進式慢慢更新。IPv4 有 32 位元位置格式，IPv6 有 128 位元，其中介面位址為 64 位元，我們可將 IPv4 的 32 位元置入 64 位元的介面位址，所剩之位元皆放 0，如圖 13-34 所示。

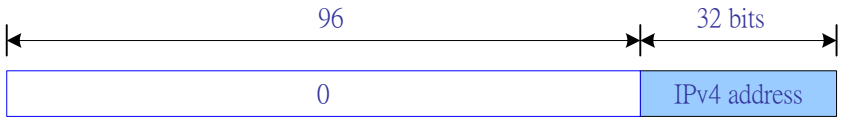



圖 13-34 IPv4 相容之 IPv6 格式

## (B) 任一廣播位址（Anycast Address）

在任一廣播位址型態下，一個位址可屬於多個介面共同使用，這些介面也允許在不同的端點上，當廣播任一廣播位址時，同一位址的介面都可收到。一般最常用是在路由器之間的廣播，不屬於該位址的網路設備就不用去拆裝封包，所以較 IPv4 的廣播方式更節省頻寬。圖 13-35 為次網路之路由器（Subnet router）的任一廣播位址格式，它是由可伸縮的前置碼（Prefix）欄位來代表次網路的位址。

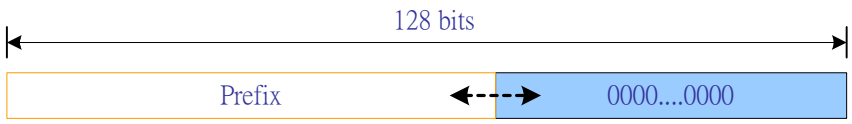



圖 13-35 次網路路由器任一廣播位址格式

## (C) 多點廣播位址（Multicast Address）

多點廣播可以指定較多的位址，可以針對若干個端點廣播，不像任一廣播只針對一個端點廣播。如採用多點廣播位址型式，IPv6 可向一組介面位址廣播，而每一個介面位址可以在不同的端點上。位址格式如圖 13-36 所示，它的前置碼為 FF00::/8；Lifetime 欄位表示該包產生的時機，其中 "0" 表示該位址為永久式（Permanent Unicast Address）；"1" 表示該位址為暫時性的（Temporary Unicast Address），使用後便不存在。另 Scope 欄位表示位址型態："1" 表示端點位址（Node Address）；"2" 表示鏈路（Link）位址；"5" 表示地區（Site）；"8" 表示組織（Organization）；"E" 表示整體（Global）位址。但在 IPv6 規格裡有一些特殊的多點廣播位址如下：

- FF02:0:0:0:0:0:0:1 為所有端點的多點廣播群組（All-node multicast group）。
- FF02:0:0:0:0:1:FF00:0000/104 為徵求端點的多點廣播群組（Solicited-node multicast group）。
- FF02:0:0:0:0:0:0:2 為所有路由器多點廣播群組（All-node multicast address），所有路由器都必須加入。

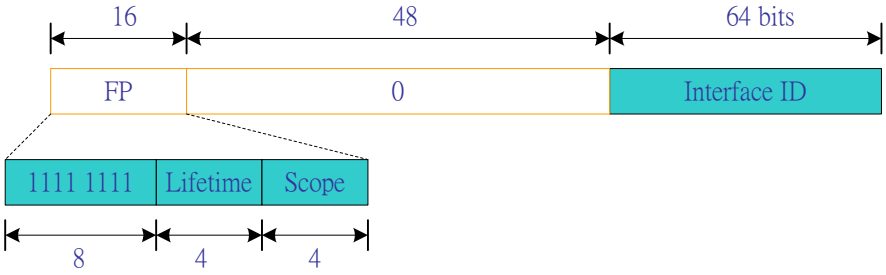



圖 13-36 多點廣播位址格式

## 13-8-3 ICMPv6 通訊協定

如同 IPv4 上的 ICMP 一樣，ICMPv6（Internet Control Message Protocol version 6）也是包裝在 IPv6 封包內（Next header = 58），用來測試或回報 IPv6 網路訊息。例如，某一路由器由於某種原因無法處理 IPv6 封包時，便發送該原因類別的 ICMPv6 給原始發送封包者，再由它做適當的處理。而其封包型態也如同 IPv4 包含終點無法到達、封包太大、時間超過、參數問題、回聲要求、以及回聲回應等。其封包格式也如同 ICMPv4（如圖 13-15）。

# 13-9 Internet 網路連結

『網際網路』（Internet）是目前全世界最大的網路系統，連結上億台電腦，分布於世界任何一個角落，本節就以 Internet 網路的基本架構來探討其連結技術。如果 Internet 網路採取像圖 13-10（IP 路徑選擇範例）一樣的擴充方式，隨著網路愈來愈大，要從網路中每一個路由器紀錄，來計算通往所有路由器的最短路徑已漸不可能。而且，當網路愈大，每個路由器內的路由表，則相對地變得愈長，每一個封包進入時，勢必浪費不少時間在於路由表上搜尋最短路徑，且路由表的維護也非常繁重。因此，Internet 網路上採用階層式路徑選擇的方法，類似目前電話系統之搜尋號碼位置的方式，以減低每個路由器的路由表建立及搜尋時間，提高路徑選擇的效率。

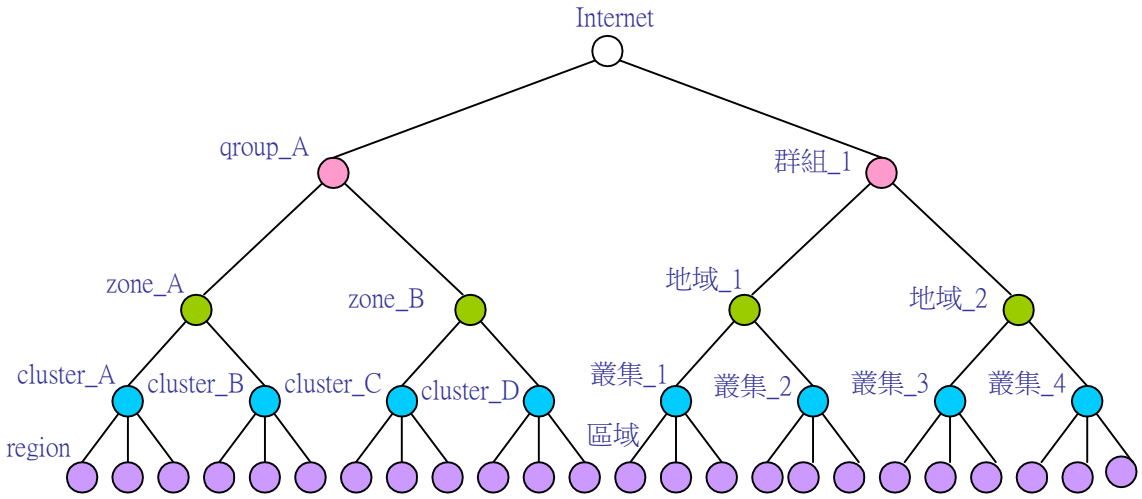



圖 13-37 Internet 網路架構圖

圖 13-37 表示 Internet 網路架構圖，使用階層式路徑選擇法，路由器則被劃分於所謂的區域（region）之內。每一個路由器不但非常清楚自己位於哪一個區域，對自己區域內其它路由器的路徑選擇也非常明白，但對本區域以外的路徑選擇便全然不知。至於和其它區域（region）之間的路徑選擇，就必須靠上層的路由器轉送，而無法直接繞徑（routing）。我們將若干個區域（region）集合成叢集（cluster），或又將若干個叢集組合成地域（zone），再將數個地域集合成群組（group），一直下去直到能完全分辨為止。其實，一般我們大型網路就是以階層式串接各地的區域網路，使用階層式路徑選擇法是最恰當不過的。

我們先以兩階層式路徑選擇法來介紹，如圖 13-38 所示。我們將一個組織單位（也許是一個公司、學校、教育部、國防部）的網路系統稱之為『自治系統』（Autonomous System，AS），它是由若干個稱之為『網域』（Domain）的網路所構成，這些網域是分佈在組織單位中的任何角落，也許是單位內小部門（如，分公司、系、所、學校）的網路系統。

每個網域上至少有一個『內部閘門』( Interior Gateway ) 和其它網域的內部閘門串接。一個自治系統就由這些內部閘門所串接而成，但至少有一個『**外部閘門**』( Exterior Gateway ) 連接至外部網路。內部閘門所串接的網路，一般就稱為骨幹網路 ( Backbone )。其實圖 13-38 也類似第十章中的圖 10-25 和 10-26 之傳輸骨幹。

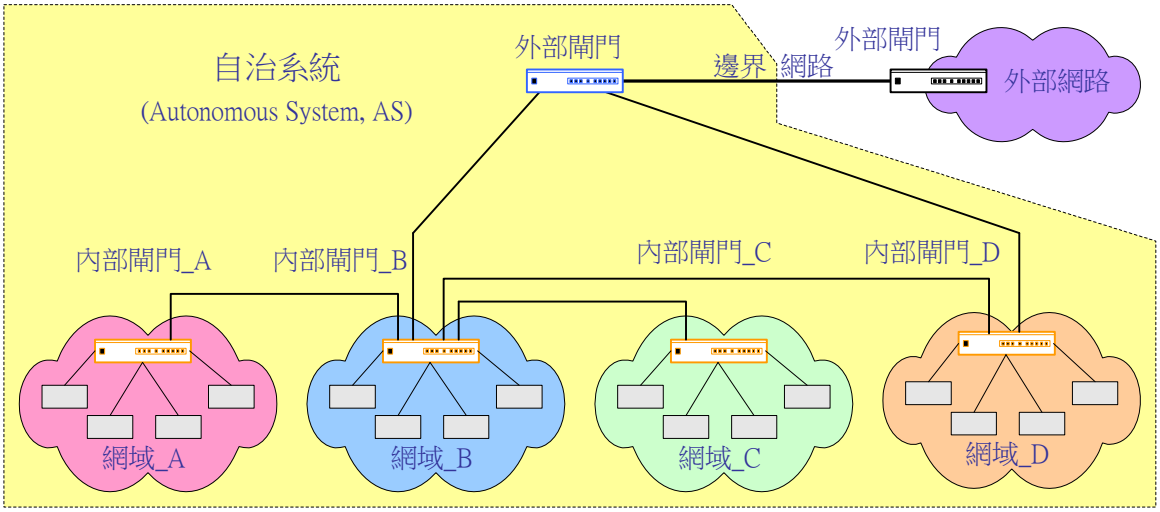



**圖 13-38 自治系統網路架構**

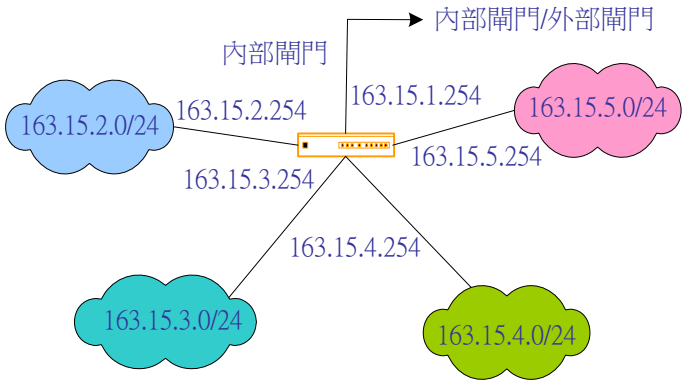
依照圖 13-38 的網路架構，有三種不同層次的路徑選擇方式：(a) 網域內路徑選擇；(b) 自治系統內路徑選擇；(c) 自治系統之間路徑選擇。以下就分別來介紹這三種路徑選擇方式。

# 13-10 網域內路徑選擇

網域內路徑選擇是電腦和內部閘門之間的路由方式之一。一般內部閘門都是使用『**多埠路由器**』( Multi-port Router )( 或由多個路由器所構成 )，每一個埠口設定一個網路位置，埠口所連接的電腦，都屬於該網路的一份子。系統管理者也對整個網路內的成員都非常清楚，因此內部閘門主要以『**靜態路徑選擇**』( Static routing ) 為主。又內部閘門至少有一個連接埠口，連結到其它網域的內部閘門或外部閘門，如果內部閘門有不認識的網路位址 ( 表示不在本網域內 )，便直接由該埠口發送出去，至於是否可以到達目的位址，這就不在管轄之內。

我們用圖 13-39 來說明網域內路徑選擇方式。圖中有一個多埠口路由器作為內部閘門，連接了四個網路 ( 由一個 Class B 網路分割的子網路 )，並有一個連接埠口接到外部網路，而以靜態路徑選擇方式，路由表 ( 固定路由表 ) 如圖中所示。當封包由任何一個埠口進入時，內部閘門依照它的網路位址，轉送到網路所屬的埠口上。例如，一個目的位址為 163.15.2.4 的封包進入，內部閘門就依照網路位址 ( 163.15.2.0/24 )，由路由表上查詢出，應該轉送到

163.15.2.254 的埠口上。假如另有一個目的位址為 138.14.3.2 的封包進入，內部閘門在路由表上無法找出相對應的路徑，便將該封包轉送到 163.15.1.254 埠口（Otherwise）上，該埠口連結至外部網路，至於該封包如何尋找出下一個路徑，就由外部之其它路由器負責了。（至於路由器如何設定，請參考拙著『**Internet 網路原理與實務**』）




內部閘門路由表

| 目的網路位址 | 轉送位址 |
|---|---|
| 163.15.2.0 | 163.15.2.254 |
| 163.15.3.0 | 163.15.3.254 |
| 163.15.4.0 | 163.15.4.254 |
| 163.15.5.0 | 163.15.5.254 |
| Otherwise | 163.15.1.254 |

**圖 13-39 網域內之路徑選擇範例**

# 13-11 自治系統內路徑選擇

如圖 13-38 所示，一個自治系統可由若干個網域所構成，每一個內部閘門管理一個網域。如果網域內所傳送的封包目的位址，是屬於本網域所管轄的網路內，封包將被留在內部傳送，但如果封包的目的位址超過網域所管轄範圍，該封包將會被送出該網域的內部閘門，且於若干個內部閘門（其它網域）之間，尋找出可到達目的地的最佳路徑。

一般來說，企業內之網路範圍較小，且多半屬於同一權責單位所管，所以通常選用『**鏈路狀態路徑選擇法**』（Link-State Routing, LS Routing）（請參考 4-7 節說明）或『**距離向量路徑選擇法**』（Distance–Vector Routing, DV Routing）（請參考 4-8 節說明）做為內部閘門之間的路徑選擇演譯法，。

兩者之間的不同點是內部閘門之間所互相傳遞的訊息，LS Routing 是傳遞本身和相鄰內部閘門之間的鏈路狀況；而 DV Routing 是計算所有可能到達目的地，所經過的「**跳躍次數**」（hop count）傳遞給其他內部閘門。每一個內部閘門接收到這些訊息後，再計算出最佳路徑填入路由表，至於進入內部閘門的封包就依照路由表上，查出最佳路徑，並發送到下一個內部閘門（next hop），再由下一個內部閘門決定往哪一個路徑傳送。因此，所有內部閘門之間

必須存在一個共通的通訊協定，以便傳遞網路之間的訊息，依此建立動態路由表，目前網際網路上較常用的『**路徑協定**』( Routing Protocol ) 有：

- Routing Information Protocol (RIP)
- Interior Gateway Routing Protocol ( IGRP )
- Enhanced Interior Gateway Routing Protocol ( EIGRP )
- Open Shortest Path First ( OSPF )

## 13-11-1 RIP 路徑協定

『**路徑訊息協定**』( Routing Information Protocol, RIP ) 是由 Xerox 公司的 Palo Alto Research Center ( PARC ) 所發展出來，目前是 Unix 電腦上的共通路徑選擇協定。RIP 採用『**距離向量路徑選擇法**』( Distance –Vector Routing )，首先路由器 ( 內部閘門 ) 紀錄每進入封包的來源位址和計算其所經過路徑的數目 ( hop ) ( 可由 IP 封包之 TTL 欄位數值計算出 )，在每一段時間 ( 一般設定 30 秒 ) 內廣播給相鄰的路由器。每一個路由器從自己所計算的訊息和其他路由器所傳遞過來的訊息之中計算出最佳路徑 ( 請參閱 4-8 節之演算法 )，再更新路由表。目前 RIP 協定在 Internet 網路上應用有兩種規格版本：RIP 和 RIP 2，以下分別介紹其封包格式。

圖 13-40 為 RIP 封包格式，各欄位功能如下：

**(1) 命令 ( Command, COM ) :** 表示此封包的命令是要求訊息 ( request ) 或回應訊息 ( response )。

**(2) 版本 ( Version, Ver ) :** 表示此封包的版本。

**(3) 位址家族標示 ( Address family Identifier, AFI ) :** 在 RIP 協定中允許不同網路之間的訊息傳遞，AFI 表示所傳遞訊息之網路型態或位址格式。

**(4) 位址 ( Address, Addr ) :** 訊息之位址，IP 位址表示之。

**(5) 路由值 ( Metric ) :** 到達位址欄位內之 IP 位址所必須經過的跳躍次數 ( hop count )。最高值為 15，如果超過 15 ( 16 ) 表示不可到達。

在一個 RIP 封包內最多可增列 25 筆訊息資料，每一筆訊息的長度為 20 Bytes，因此 RIP 訊息最長為 504 ( 20 × 25 + 4 ) Bytes，還不超過 UDP 封包最長 512 Bytes 限制，在一般環境下都可順利傳輸( MTU 限制 )。其實 RIP 封包內設計可存放 14 位元組長的位址，但使用 IP 位址格式只用到 4 個位元組，其餘都設為 0。

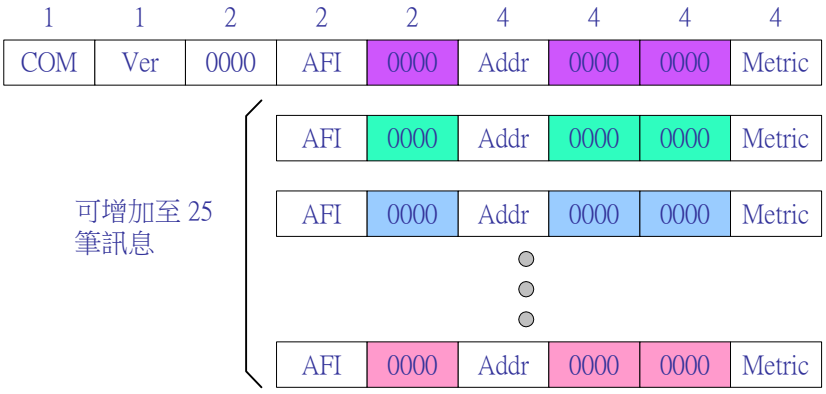



**圖 13-40 RIP 封包格式**

圖 13-41 為 RIP 2 封包格式，由圖中我們可發現 RIP 2 充分利用 RIP 的位址的空白欄位，填入更多的訊息。以下介紹所增加的 3 個訊息欄位：

**(1) 路由標籤 ( Route Tag, RT )：**用來區分內部閘門和外部閘門之間的路徑訊息。

**(2) 次網路遮罩 ( Subnet Mask, SM )：**提供該筆訊息的次網路遮罩，如都為 0 表示沒有提供 SM 資料。

**(3) 下一路徑 ( Next Hop, NH )：**到達該筆訊息之位址的下一路徑。

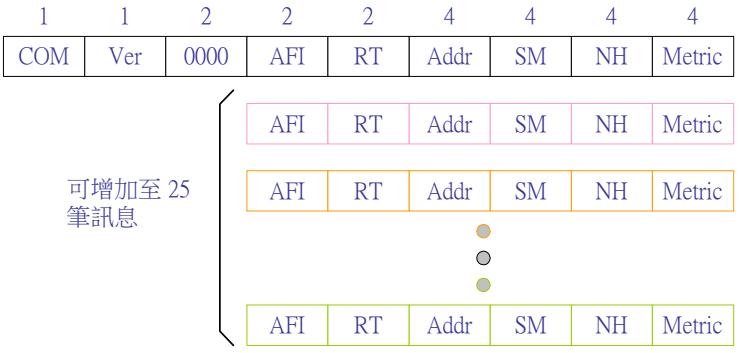



**圖 13-41 RIP 2 封包格式**

RIP 協定的最大限制就是跳躍距離最大為 15 個區段，目前網路中自治系統環境愈來愈大，一個自治系統的路由器也許就會超過這個數目。又因採用距離向量法可能會發生訊息過

慢收斂問題，也就是說當網路變更或故障時，無法在快速的時間內傳遞及更新所有路由器上的路由表，造成封包回繞或到達不了目的地。解決方法有水平分割法、以毒攻毒法等等（請參閱 4-8-2 節）。

## 13-11-2 IGRP 路徑協定

『**內部閘門路徑協定**』( Interior Gateway Routing Protocol, IGRP )是由 Cisco 公司於 1980 年中期發展出來，提供比較完整的自治系統（Autonomous System, AS）內之路徑選擇，也是針對 RIP 協定的功能增強。RIP 提供使用較小自治系統內，而且是在同等級( Homogeneous ) 網路之間使用，也限制 16 個跳躍距離。IGRP 提供較大型且複雜的自治系統內的路徑選擇協定。IGRP 和 RIP 的不同點如下：

- IGRP 可以服務較大的自治系統，跳躍距離不受限於 16。
- IGRP 可以提供多條路徑選擇，RIP 只提供單一最佳路徑。
- IGRP 可以重新配置於 RIP、OSPF、EIGRP 之協定內，也就是說可以共同使用及轉換。
- IGRP 提供快速更新資料計時器（Flush timer），如有資料變動，將更新之資料於迅速告知相鄰路由器（一般設定 10 秒）。
- IGRP 廣播訊息週期是每 90 秒一次。

基本上，IGRP 也是採用『**距離向量演算法**』來計算最佳路徑，但它的向量值（metric）不只使用跳躍距離。IGRP 的向量值可由下列參數的組合：網路間延遲時間（internetwork delay）、頻寬（bandwidth）、可靠度（reliability）與負載（load）。網路間延遲時間可由進入封包內所紀錄的發送時間和實際接收到時間的差異計算出來。頻寬可以將傳輸速率分為不同等級 1 到 255 之間來計算，例如將 1200 bps 到 10Mbps 的傳輸速率以 1 到 24 的級數之間來分別。至於向量值（metric）對於這些參數的權重比率值必須由系統管理員來設定，一般內定值（default）只會採用 delay 和 bandwidth 兩個參數，並以最佳權重比率計算。

路由器利用與其他路由器相互傳遞的訊息來建立路由表，其中最大的困擾就是收斂問題。網路上任何區段發生故障，或網路架構變更之訊息，無法立即傳遞給有關的路由器，造成網

路之傳遞訊息暫時性的不正確，必須經過一段時間的訊息更新後，才能到達穩定狀況，這段時間稱之為『**收斂時間**』。IGRP 為提高路由選擇效率，採取多種方法來縮短收斂時間，以及預防網路不穩定，方法如下列說明：( 如圖 13-42 所示 )

- **Flash Update**：使用 Flash Update 訊息，以便快速通知相鄰路由器網路有變更，使加快收斂時間。
- **Hold-Down Timer**：使用 Hold-Down Timer 計時器，以預防路徑回繞。
- **Split Horizon**：用來防止傳回不正確訊息。
- **Poison Reverse**：用來移除不正確路徑。

在圖 13-42 中，假設網路 C 發生故障，Router_4 發現通往網路 C 的路徑已不通，立即廣播 Flash Update 訊息給相鄰之路由器。Router_3 接收到 Flash Update 訊息，知道經由 Router_4 到達網路 C 路徑已不通，立即啟動 Hold-Down Timer 並將往網路 C 之路徑刪除。並且啟動 Split Horizon ，將欲往網路 C 的路徑隔離，以防止任何封包欲經由 Router_3 傳送到網路 C。也就是說，要到網路 C 的封包不可再經由 Router_3 送往 Router_4，必須經由其他路徑。如果 Router_1 還未更新路由表，發送 Update Router 訊息給 Router_3，並告知經由 Router_3 可到達網路 C。則 Router_3 回應 Poison Reverse 給 Router_1 經由 Router_3 到達網路 C 的路徑為無限大。因此，Router_1 便知道必須移除該路徑。

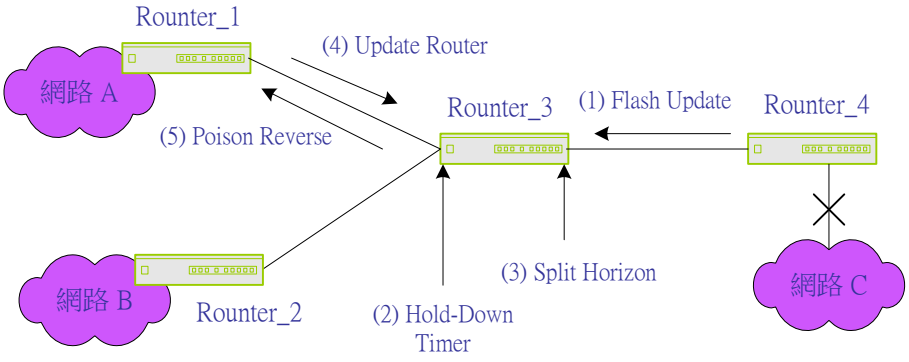



**圖 13-42 IGRP 預防網路震盪範例**

## 13-11-3 EIGRP 路徑協定

『**加強型內部閘門路徑協定**』( Enhanced Interior Gateway Routing Protocol, EIGRP ) 是 Cisco 公司加強 IGRP 功能以求更適合較大型網路的路徑選擇協定。EIGRP 的路徑選擇演算

法是整合『**鏈路狀態法**』( LS Routing ) 和『**距離向量法**』( DV Routing )，成為一個稱之為『**擴張型更新演算法**』( Diffusing-Update Algorithm, DUAL )。另外，EIGRP 和其他路徑選擇協定有下列四個主要不同點：

**(1) 提供重新配置( Redistribution )功能**以整合不同網路的路徑選擇協定，如 Apple-Talk、IP 和 Novell Netware 之間。在 Apple-Talk 網路之下，重新配置是由 RTMP( Routing Table Maintenance Protocol ) 所建立的路由表；在 IP 網路下，重新配置是由 RIP 、OSPF ( Open Shortest Path First )、EGP ( Exterior Gateway Protocol )、或 BGP ( Border Gateway Protocol ) 等協定所建立的路由表；Novell 網路下，重新配置是由 Novell RIP 等協定所建立的路由表，使這些異質網路( Heterogeneous Network )之間可經由 EIGRP 作最佳路徑選擇。

**(2) 快速收斂。**在 EIGRP 之下的所有路由器皆有儲存其相鄰路由器之路由表，因此它可以快速更新替代路徑，如果沒有適當路徑，路由器會發送查詢訊息給相鄰的路由器，這查詢訊息會一直被傳遞，直到找出適當路徑為止。

**(3) 提供可變長度的網路遮罩。**路由器會自動收集網路號碼的範圍，更進一步，EIGRP 可以被規劃為總結 ( summarize ) 任意位元長度的遮罩。

**(4) EIGRP 並非週期性的廣播訊息**，而是當本身路由表有所變更時，才將更新部份廣播給其他路由器，因此 EIGRP 使用頻寬比 IGRP 用的少。

為增強 EIGRP 的功能，它使用了四個主要技術：

**(1) 鄰居發現與復原 ( Neighbor discovery/recovery )。**路由器必須隨時注意相連接網路之間是否有發生不可到達或停止工作的情況，當它發現某一路徑的負載特別低，便週期性發送 Hello 封包詢問對方，如一直沒有收到回應，表示該網路已不正常工作，則必須更新路由表並通知其他相鄰路由器。任何路由器接收到 Hello 封包必須即時回應。

**(2) 可靠的傳輸協定 ( Reliable Transport Protocol )。**為了保證訊息封包都能按順序及安全到達相鄰路由器，EIGRP 提供多點廣播 ( Multicast ) 和單一廣播 ( Unicast ) 兩種封包。對於多重存取 ( Multiaccess ) 網路，則使用多點廣播封包；如是單一存

取網路（如 Ethernet），則使用單一廣播封包。當廣播封包是 Hello 時不用回應確認訊息；但廣播更新（Update）封包時，接收者必須回應確認訊息。

**(3) DUAL 狀態轉換（DUAL Finite-State Machine）**被崁入計算和搜尋最佳路徑演算法內。DUAL 整合距離向量演算法和鏈路狀態演算法，能隨時找出最佳路徑更新路由表。

**(4) 協定相依模組（Protocol-Dependent Module）**。特定網路層路徑選擇協定之間的連結可採用不同模組，這對網路的擴充性較高。

## 13-11-4 OSPF 路徑協定

**『開放式最短路徑優先』（Open Shortest Path First, OSPF）**是在 1980 年中期由 IETF（Internet Engineering Task Force）發展出來，主要應用於 IP 網路中內部閘門之間的路徑選擇協定。和 RIP 相比較，OSPF 能適用於較大網路或異質網路上。OSFP 有兩個重要特性：(1) 是開放性架構（Open），它的規格是公開性的（RFC 1247），任何廠商可任意安裝在自家電腦上，並修改或增加其功能。(2) 使用最短路徑演算法（SPF），找出所有路徑中的最短路徑，一般會參考採用 Dijkstra Algorithm（請參考 4-7-4 節）。

和其他路徑選擇協定的另一不同點是，OSPF 採用**『鏈路狀態路徑選擇法』**（Link-State routing）。在 OSPF 下的路由器定時傳送**『鏈路狀態宣傳』**（Link-State Advertisement, LSA）訊息給同等階級地區的其他路由器，LSA 訊息包含有連接介面、路由值（Metric）、以及其他相關變數值。OSPF 路由器計算這些參數後，並以最短路徑演算法找出，針對網路上（自治系統內）所有路由器中的最短路徑。另外和使用距離向量法的 RIP 或 IGRP 有很大的不同，它們皆傳送某部份（或更新部份）的路由表給其他路由器；而 OSPF 是傳遞路由器所管轄內之**『路由拓樸圖』**給相鄰之路由器。

OSPF 能將自己管轄的自治系統（Autonomous System, AS）以階層式分割為若干個小區域（如圖 13-43 所示）。基本上，OSPF 是負責自治系統內（intra-AS）路徑選擇的功能，但它也有能力處理接收和傳送自治系統之間（inter-AS）的路徑選擇問題。被分割的小區域一般都稱為網域（Domain），一個網域內也許連接數個路由器和若干個主機。網域之間連接的路由器稱之為**『邊界路由器』**（Border Router）或稱**『骨幹路由器』**（Backbone Router），如圖中

的 Router_4、Router_5、Router_12、Router_11、Router_10、以及 Router_6，它們之間連線稱為骨幹（Backbone）。骨幹路由器和一般網域內路由器（如 Router_3 等）處理不同的拓樸圖資料庫（Topological Database）。

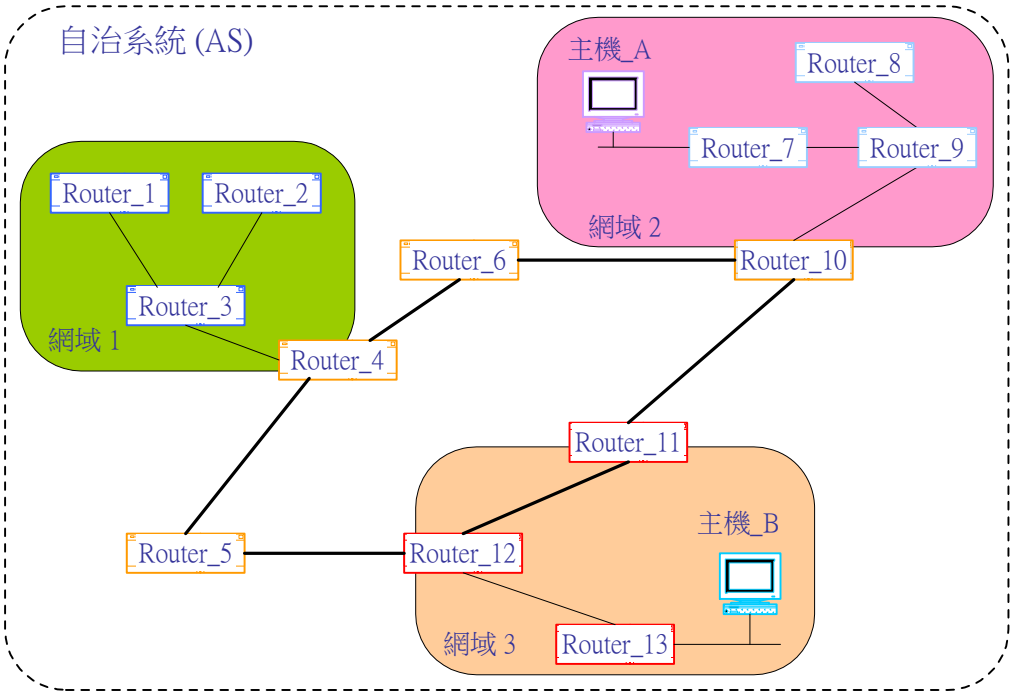



**圖 13-43 自治系統內 OSPF 的拓樸圖**

網域內所有路由器接收網域內其他路由器所傳送的 LAS 建立網路架構圖，並將其建構於拓樸圖資料庫內。骨幹路由器不僅必須建構網域內的拓樸圖，還必須建立骨幹的拓樸圖資料庫，因此在任一部骨幹路由器上可觀察到所有網域和骨幹網路的拓樸圖。在 OSPF 中有兩種路徑選擇功能：

**(1) 網域內（intra-domain）**，處理封包的目的和來源位址皆屬於本網域之路徑選擇；

**(2) 網域間（inter-domain）**，跨越不同網域必須透過骨幹路由器轉送。

如圖 13-43 網域 3 的主機_B 欲傳送封包到網域 2 的主機_A，該封包被傳送到 Router_13、再往前送到 Router_11、再送到 Router_10（inter-domain）；之後再經由 Router_9 轉送到 Router_7 到達主機_A（intra-domain）。

因此，骨幹路由器在做跨越不同網域的路徑選擇時，必須搜尋較複雜的拓樸圖資料庫，尤其做連續封包傳送的時候，每個封包都必須搜尋資料庫。為了節省搜尋時間及次數，骨幹路由器可以建立虛擬鏈路（Virtual Link），來連結經常使用的路徑。但網域內路由器之間的虛

擬路徑是共享而非專屬。骨幹路由器也可以學習經由外部閘門所傳過的路徑訊息，作自治系統之間的路徑選擇功能。

圖 13-44 為 OSPF 的封包格式，其中各欄位功能如下：

**(1) 版本（Version, Ver）：**表示該封包之 OSPF 的版本。

**(2) 型態（Type）：**表示該封包的工作型態，有下列四種型態：

- Hello：建立和管理相鄰路由器關係。
- Database Description：描述拓樸圖資料庫的內容。這些訊息將因調整資料庫而被改變。
- Link-state Request：向相鄰路由器要求傳遞某些片段的拓樸圖資料庫。這些訊息被傳送是因為某些路由器發現資料庫的內容已經失去時效性，要求重新更新。
- Link-state Update：回應 Link-state Request 要求。傳送中的訊息可能經由 LSA 訊息修正過。
- Link-state Acknowledge：確認接收到回應訊息。

**(3) 封包長度（Length, Len）：**整個封包的長度，以位元組為單位。

**(4) Router ID：**發送封包的來源路由器之識別碼。

**(5) Area ID：**來源封包之區域（或網域）的識別碼。

**(6) Checksum（CS）：**檢查集之檢查碼。

**(7) 認證型態（Authentication Type, AT）：**內容為認證型態。所有 OSPF 的交換訊息都必須經過認證，任何區域可自行規劃認證型態。

**(8) 認證（Authentication, Auth）：**內容為認證訊息。

**(9) 資料（Data）：**傳送給上層通訊協定之包裝資料。

| 1 | 1 | 2 | 4 | 4 | 2 | 2 | 8 | variable |
|---|---|---|---|---|---|---|---|---|
| Ver | Type | Len | Router ID | Area ID | CS | AT | Auth | Data |

圖 13-44 OSPF 封包格式

未來 OSPF 將被加入適當價格( equal-cost )與多重路徑選擇( multipath routing )的功能，使路徑選擇能依照上層服務型態 ( Type-of-Service, ToS ) 的要求來配置路徑。ToS 路徑選擇是由上層通訊協定依照服務的特殊需求而制定，因此可達到服務品質（ Quality of Service, QoS ）的需求。在應用上，譬如某個封包特別緊急，如果 OSPF 採用不同優先等級鏈路，就可讓它優先通過。OSPF 提供一個或多個路由值 ( metric ) 計算路徑效率，如果只採用一個路由值，將沒有所謂 ToS 功能，我們可按照 ToS 的需求採用多種有關的路由值。例如在 IP ToS 之下，我們可採用延遲、傳輸量、可靠度等等參數，再由 OSPF 計算出適當價格（ equal-cost ）的路徑。

# 13-12 自治系統之間路徑選擇

若傳送封包的目標網路位址不在自治系統（ Autonomous System, AS ）內，則必須被傳送到自治系統外部，由『**外部閘門**』( Exterior Gateway ) 之間尋找適合的路徑傳送，如圖 13-45 所示。外部閘門之間必須按照某個共通的協定來互相傳送路徑訊息及尋找路徑，此協定稱之為『**外部閘門協定**』( Exterior Gateway Protocol, EGP )。外部閘門和自治系統之間宛如國家邊界，因此又稱為『**邊界閘門**』( Border Gateway )。邊界閘門所扮演的角色非常的重要，它就像國家的邊界之出入境管理局一樣，負責審核各種封包是否可以進出自治系統。一般自治系統的封包進出都有依其政策型態 ( Policy dependent ) 規定，好比如研究機構、或國防單位的管理就更加嚴謹；然而一般環境也必須預防破壞份子的入侵 ( 至於如何防患並不是本書探討的範圍 )，一般外部閘門之間的都採用『**距離向量路徑選擇法**』( Distance Vector Routing )，目前在 Internet 網路上較常用的是『**邊界閘門協定**』( Border Gateway Protocol, BGP )，我們就以 BGP 協定協定介紹外部閘們之間路徑選擇之功能。( 注意 BGP 是 EGP 協定中的一個，兩者名稱不要混擾 )

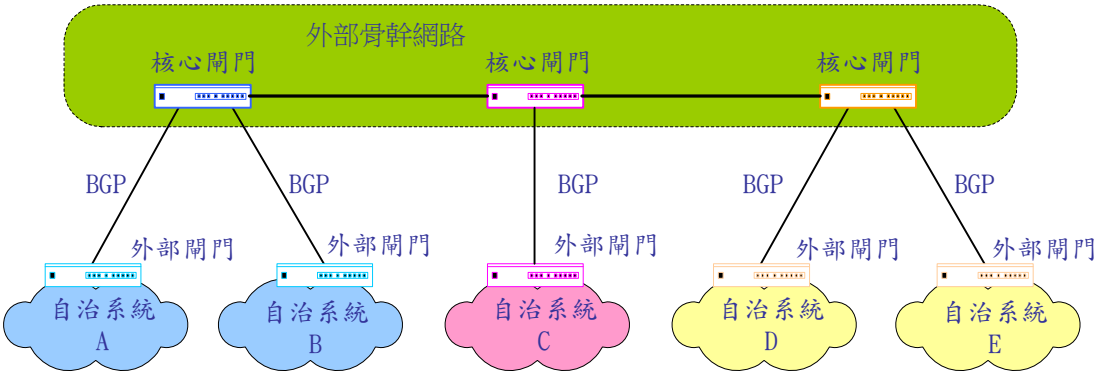



圖 13-45 自治系統之間網路架構

在 Internet 網路上的外部閘門的路由器又被分為『**核心閘門**』( Core Gateway ) 和『**非核心閘門**』( Non-core Gateway )( 即是一般外部閘門 ) 兩種。非核心閘門必須紀錄自己管轄內，自治系統的網路拓樸之路徑選擇資料，以及與核心閘門之間的路徑選擇資料，核心閘門只負責核心閘門之間的路由資料。一般核心閘門是由『**網際網路操作中心**』( Internet Network Operation Center, INOC ) 所管理，各自治系統之外部閘門 ( 非核心閘門 ) 都要連接到 INOC，由 INOC 管理整個核心骨幹。

## 13-12-1 BGP 路徑協定

『**邊界閘門協定**』( Border Gateway Protocol, BGP ) 有三種路徑選擇型態：

**(1) 自治系統之間路徑選擇 ( Inter-autonomous System Routing )**。用於若干個外部閘門之間的路徑選擇。外部閘門必須使用 BGP 去紀錄及管理整個網路間拓樸關係，相鄰之間的外部閘門必須負責傳遞網路訊息。

**(2) 自治系統內路徑選擇 ( Intra-autonomous System Routing )**。用於在同一個自治系統內一個或多個外部閘門之間的路徑選擇。因此，在每一個路由器上必須可觀察到整個自治系統內所有網路的拓樸資料。對於路由器自行管理的區域內 ( 網域內 ) 必須負責管理及建立網路拓樸圖。也因此 BPG 可提供自治系統內或自治系統之間的路由管理。

**(3) 貫穿自治系統路徑選擇 ( Pass-through Autonomous System Routing )**。如果封包目的位址不在自治系統內，而能直接丟往外部閘門上那就比較單純。但如果邊界網路或外部閘門貫穿自治系統內，那對於路徑選擇就較複雜，如圖 13-46 所示。如圖中，主

機 A 欲傳送封包給主機 B，首先必須經過 BGP 找到自治系統的前端路由器，再由自治系統內路徑選擇功能（也許是 RIP 或 OSPF）尋找出另一個前端路由器，再經過 BGP 尋出主機 B 的位址。

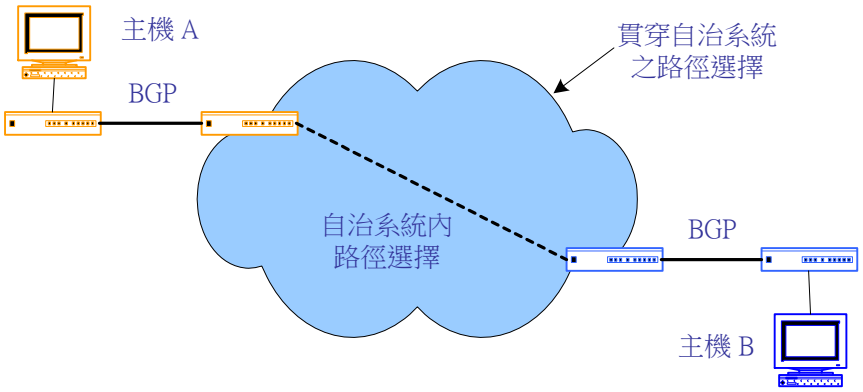



圖 13-46 貫穿自治系統之路徑選擇

在 BGP 協定下外部閘門之間有四個訊息：(1) Open Message：建立兩個閘門之間的交談連線，它是連線後第一個訊息，如欲傳送其他訊息之前，必須使用 Open Message 建立雙方對談連線；(2) Update Message：被用來更新外部閘們之間的網路訊息，使各個路由器都能建立一個可觀察整個網路的拓樸圖。Update Message 是由 TCP 連線完成已確定訊息的可靠度。當網路上有任何路徑被抽離，該相連之外部閘門便利用 Update Message 告知相鄰之閘門；(3) Notification Message：當外部閘門發現任何異常狀態，便使用該訊息告知相鄰閘門，或被使用於中斷連線；(4) Keep-alive Message：用來測試前端外部閘門是否還存在，當路由器發現前端閘門不再週期性的發送訊訊息時，便發送該訊息以做測試。

為了能發送以上四種訊息，BGP 有四種封包格式。首先我們來介紹這四種格式的共通封包標頭，這封包標頭如圖 13-47 所示，其中各欄位功能如下：

- Marker：內容為一個認證值，讓訊息接收者可以預定該值。
- Length：表示整個封包的長度。
- Type：表示為 Open、Update、Notification、或 Keep-alive 的訊息封包。
- Date：內容為上層之資料（Open、Update、Notification、或 Keep-alive 訊息）。

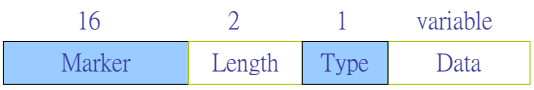


圖 13-47 GRP 之封包標頭

圖 13-48 為 Open Message 之封包格式，其中各欄位功能如下：

- Version（Ver）：表示該封包的 BGP 版本。
- Autonomous System（AS）：表示該發送封包者所在的自治系統編號。
- Hold-Time（HT）：表示扣留時間，在這時間內沒有回應的路由器，都被假設已失去功能。
- BGP Identifier（BGP）：傳送該封包的外部閘門號碼（IP 位址）。
- Optional Parameter Length（O-Len）：表示緊接在後的 Optional 欄位的長度。
- Optional Parameter：任意參數。目前僅使用於認證（Authentication）訊息，有兩個部份：Authentication code 和 Authentication data。


圖 13-48 Open Message 之封包格式

圖 13-49 為 Update Message 之訊息封包格式，各欄位功能如下：

- Unfeasible Router Length（URL）：表示緊接著後面 Withdrawn Router 欄位的長度。
- Withdrawn Router（WR）：表示有那些已被抽離的路由器（IP 位址表示），可變長度表示之。
- Total Path Attribute Length（TPAL）：表示後面緊接著兩個有關屬性欄位的長度。
- Path Attribute（PA）：路徑屬性。描述該路徑之特性有能是下列屬性：
  - **Origin**：指派屬性（Mandatory attribute）。為原系統指定之路徑。
  - **AS Path**：經系統指定之經由多個自治系統片段所構成的路徑。
  - **Next Hop**：指派屬性。指定經由邊界網路的下一路徑可到達目的位址。

- **Mult Exit Disc**：選擇屬性（Option attribute）。在多點路徑之中辨別可到達鄰近自治系統之路徑。
- **Local Pref**：任意屬性（Discretionary attribute）。 描述任意路由的級數。
- **Atomic Aggregate**：任意屬性。被使用在表現有關路徑選擇的訊息。
- **Aggregator**：選擇屬性。包含有關路徑聚集的訊息。

- Network Layer Reachability Information（NLRI）:包含一串列的 IP 位址的網路位址，表示路徑區段

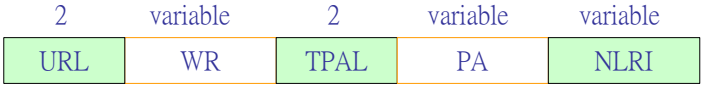



**圖 13-49 Update Message 之封包格式**

Notification Message 是被用通知路徑狀況的封包，封包格式如圖 13-50 所示，各欄位功能如下：

- **Error Code（EC）**：該封包表示錯誤的種類，如下列：
  - **Message Header Error**：所傳送的封包標頭發生錯誤。
  - **Open Message Error**：所傳送的 Open Message 錯誤，如版本、自治系統或 IP 號碼、或認證錯誤。
  - **Update Message Error**：所傳送的 Update Message 錯誤，如屬性不合等。
  - **Hold Time Expired**：表示 Hold Time 溢時，將該區段之 BGP 被視為沒有功能。
  - **Finite State Machine Error**：協定流程錯誤。
  - **Cease**：結束 BGP 連線，
- **Error Subcode**：錯誤型態的附加描述碼。
- **Error Data**：內容為有關錯誤型態的資料。


圖 13-50 Notification Message 之封包格式

由上述幾節的介紹，我們大略可以了解 Internet 網路的架設和基本理論。但隨著 Internet 應用的普及，所使用的層次也漸漸提高，我們不僅要架設一個穩定性好、傳輸率高的網路外，也必須加強網路的保密性，另外要做好網路頻寬管理，除了必須有良好的網路觀念外，實務方面的經驗也非常重要。

# 習 題

1. 請敘述 IP 通訊協定的特性。
2. 何謂 TCP/IP 網路？為何這兩個通訊協定要結合在一起？有何功能？
3. 何謂『IP 分級』（IP Classic）？並請敘述每一級（Class）的網路範圍。
4. 何謂『網路遮罩』（Network Mask）？
5. 如果有一網路位址為 138.45.0.0/16，請設計增加 16 個次網路位址，並請列出次網路遮罩及各網路範圍之主機的 IP 位址。
6. 當某一路由器收到封包時，請敘述其路徑選擇機制的運作程序。
7. 如下圖（圖 13-51）之 IP 網路架構，請規劃出各主機電腦的 IP 位址，並設計出路由器（主機 A）的路由表。

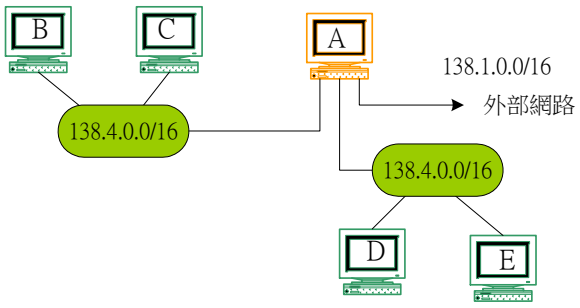



圖 13-51 IP 網路範例

8. 同上題，請利用一部 Linux 作業系統之電腦，安裝成主機 A 之路由器，並測試其路徑選擇之結果。
9. 同上題，請利用 Windows 2000 伺服器安裝。

10. 何謂 ARP 通訊協定？並說明其運作程序。

11. 何謂 RARP 通訊協定？並說明其運作程序。

12. 何謂 ICMP 通訊協定？並說明其運作程序。

13. 請說明下列 IP 網路之命令的功能，並列出在電腦上執行的結果。

    (1) ping

    (2) ifconfig

    (3) netstat

    (4) route

    (5) arp

    (6) traceroute

    (7) finger

14. 何謂『TCP 埠口』( TCP Port ) ？並請說明 TCP 和 IP 的多工關係。

15. 何謂『三向握手式連絡法』( Three-way Handshake ) ？

16. 請說明 TCP 的連線建立的運作程序。

17. 請說明 TCP 的資料傳送的運作程序。

18. 請說明 TCP 的連線終止的運作程序。

19. 請敘述 IPv6 比 IPv4 增加了哪些功能。

20. 請說明 IPv6 的定址模式。

21. IPv6 位址模式如何相容於 IPv4 的定址方式？

22. 請設計一個 Internet 網路架構圖，並說明網域網路、自治系統和自治系統之外的範圍。

23. 何謂網域內之路徑選擇？一般都採用何種方式？

24. 何謂『路徑協定』( Routing Protocol ) ？請敘述其功能。

25. 請說明『路徑訊息協定』( Routing Information Protocol, RIP ) 的運作原理。

26. 請說明『內部閘門路徑協定』( Interior Gateway Routing Protocol, IGRP ) 的運作原理。

27. 請說明『加強型內部閘門路徑協定』( Enhanced Interior Gateway Routing Protocol, EIGRP ) 的運作原理。

28. 請說明『開放式最短路徑優先』( Open Shortest Path First, OSPF )之路徑協定的運作原理。

29. 請說明『邊界閘門協定』( Border Gateway Protocol, BGP ) 的運作原理。