

第 1 章

網路的基礎知識

本章整理了學習 TCP/IP 的必備基礎知識，說明電腦與網路的發展歷史及標準化、OSI 參考模型、瞭解網路所應具備的概念、構成網路的設備等。

7 應用層 (Application Layer)	〈應用層〉 TELNET, SSH, HTTP, SMTP, POP, SSL/TLS, FTP, MIME, HTML, SNMP, MIB, SIP, RTP,...
6 表現層 (Presentation Layer)	
5 交談層 (Session Layer)	
4 傳輸層 (Transport Layer)	〈傳輸層〉 TCP, UDP, UDP-Lite, SCTP, DCCP
3 網路層 (Network Layer)	〈網路層〉 ARP, IPv4, IPv6, ICMP, IPsec
2 資料連結層 (Data-Link Layer)	乙太網路、無線網路、PPP、… (雙絞線、無線、光纖、…)
1 實體層 (Physical Layer)	

1.6 利用 OSI 參考模型進行通訊處理的範例

▼主機 (Host)

這裡的主機是指連接網路的電腦。在 OSI 的相關專有名詞中，進行通訊的電腦，稱作節點。但是在 TCP/IP 中，稱為主機。本書的主題是 TCP/IP，所以對於進行通訊的電腦，主要稱作「主機」，請參考 P135 的專欄說明。

以下將用一個具體的通訊範例，說明七個層級的功能。假設主機 A 的使用者 A，要傳送電子郵件給與主機 B 的使用者 B。

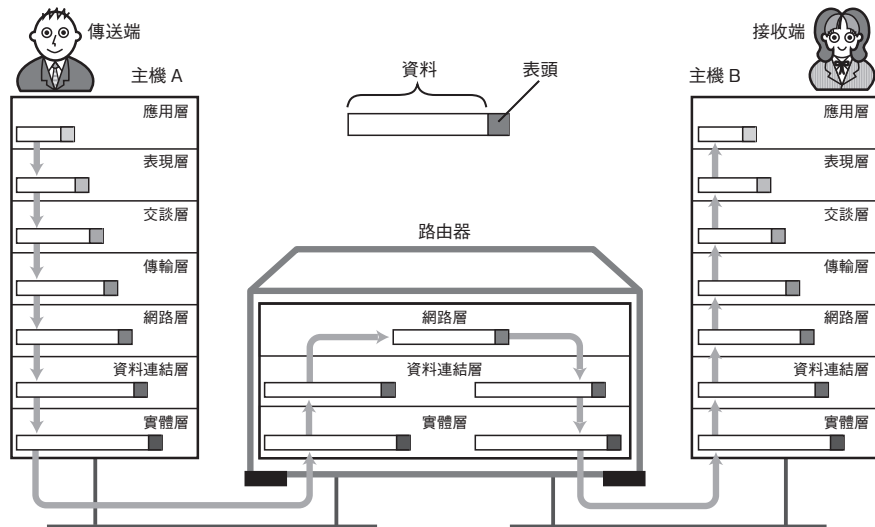
嚴格來說，OSI 或網際網路的電子郵件結構並非如以下所示這麼簡單。請把它當成是為了容易瞭解 OSI 參考模型而設計的範例。

1.6.1 七層通訊

在 OSI 的七層模型中，如何將通訊模組化？

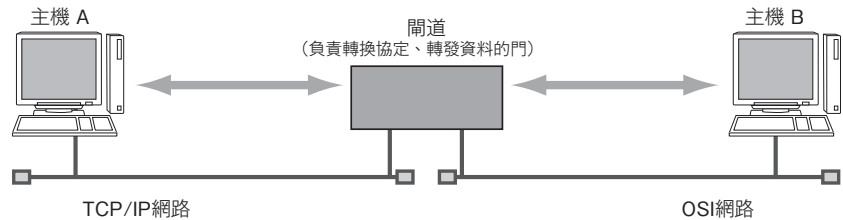
分析方法和圖 1-17 (P21) 介紹過的語言及電話等兩層模型一樣。傳送端從第七層、第六層依序由上層往下層傳送資料，接收端是由第一層、第二層依序往上層傳送資料。每一層會在上層傳來的資料中，以「表頭」的形式，加上本層協定處理所需的資料。接收端將接收到的資料分離成「表頭」與傳給上層的「資料」，再把資料傳送給上層。最後將傳送的資料恢復成原狀。

圖 1-20
通訊與七個層級



1.9.7 閘道

圖 1-46
閘道



- 閘道可以進行轉換或中繼協定。
- 同在相同的協定之間，進行轉換的閘道，稱作應用程式閘道。

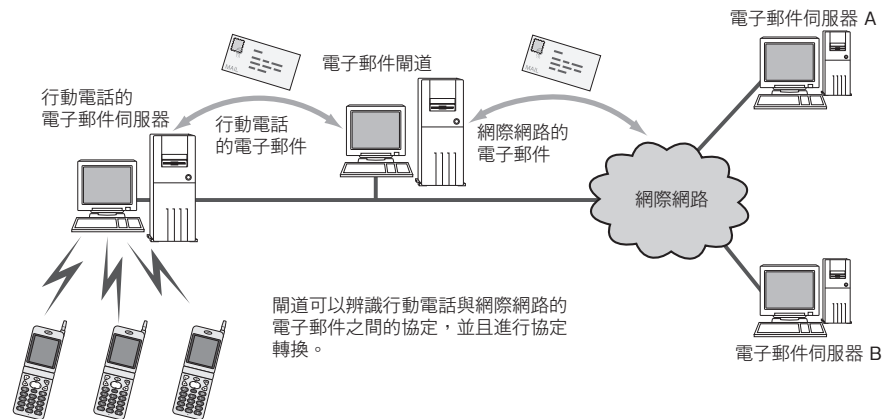
▼依照慣例，有時路由器的功能會用「閘道」來表現，但是本書把在 OSI 參考模型傳輸層以上的層級，進行協定轉換的部分，稱作「閘道」。

閘道是在 OSI 參考模型的傳輸層到應用層，負責轉換資料再轉發的設備▼。和第 4～7 層交換器一樣，會檢視傳輸層以上的資料，進行封包處理。但是閘道不僅負責轉發資料，還負責轉換資料。尤其是，對於彼此無法直接通訊的兩種不同協定，閘道會執行翻譯工作，讓彼此互相通訊，所以我們很常使用閘道來處理表現層或應用層。

最簡單的例子應該是，網際網路與行動電話的電子郵件之間的轉換服務。部分行動電話的電子郵件可能與網際網路的電子郵件不相容，交換電子郵件的步驟也不一樣。換句話說，這是因為應用層或表現層的「電子郵件協定」不同的關係。

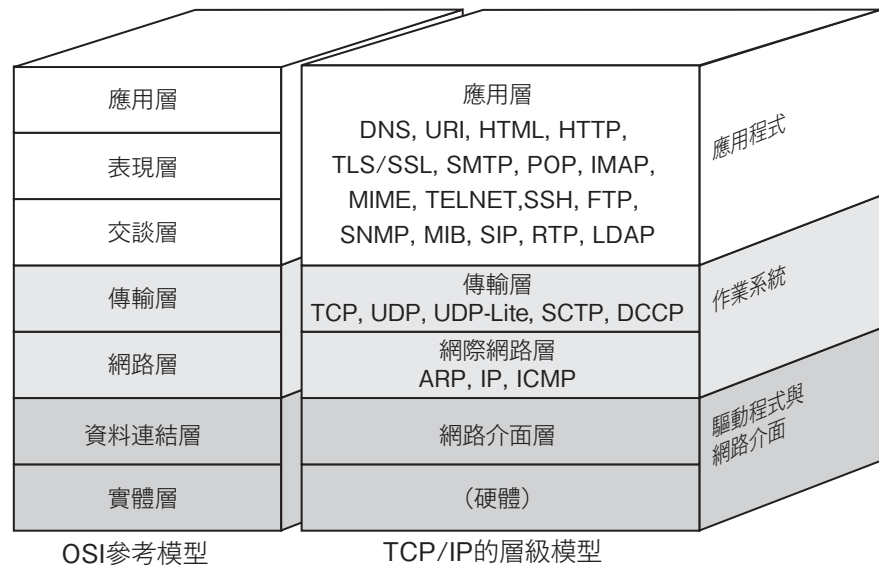
為什麼連接網際網路的電腦與行動電話之間，可以彼此通訊呢？這是因為，網際網路與行動電話連接的接點，有閘道存在的緣故。閘道可以解讀、轉換、轉發各個電子郵件的協定。結果，能讓使用不同電子郵件協定的電腦與行動電話之間，彼此發送電子郵件。

圖 1-47
行動電話與網際網路的電子郵件轉換



2.4.1 TCP/IP 與 OSI 參考模型

圖 2-8
OSI 參考模型與 TCP/
IP 的關係



第 1 章我們介紹了 OSI 參考模型的各層功用，而 TCP/IP 中的各種協定，基本上也能與 OSI 參考模型對應。知道各個協定對應到 OSI 參考模型的哪一層，就可以瞭解該協定的用途，之後只要理解技術方面的結構運作即可。關於各協定的詳細說明，請參考第 4 章之後的介紹。這裡先說明 TCP/IP 的各個協定與 OSI 參考模型的對應關係。

圖 2-8 是 TCP/IP 與 OSI 層級模型的比較圖。TCP/IP 與 OSI 的層級模型有些許差異，OSI 參考模型以「哪些是通訊協定的必要功能」為主，進行模型化；相對來說，TCP/IP 的層級模型是以「安裝在電腦中的協定，該如何進程式設計」為主，進行模型化。

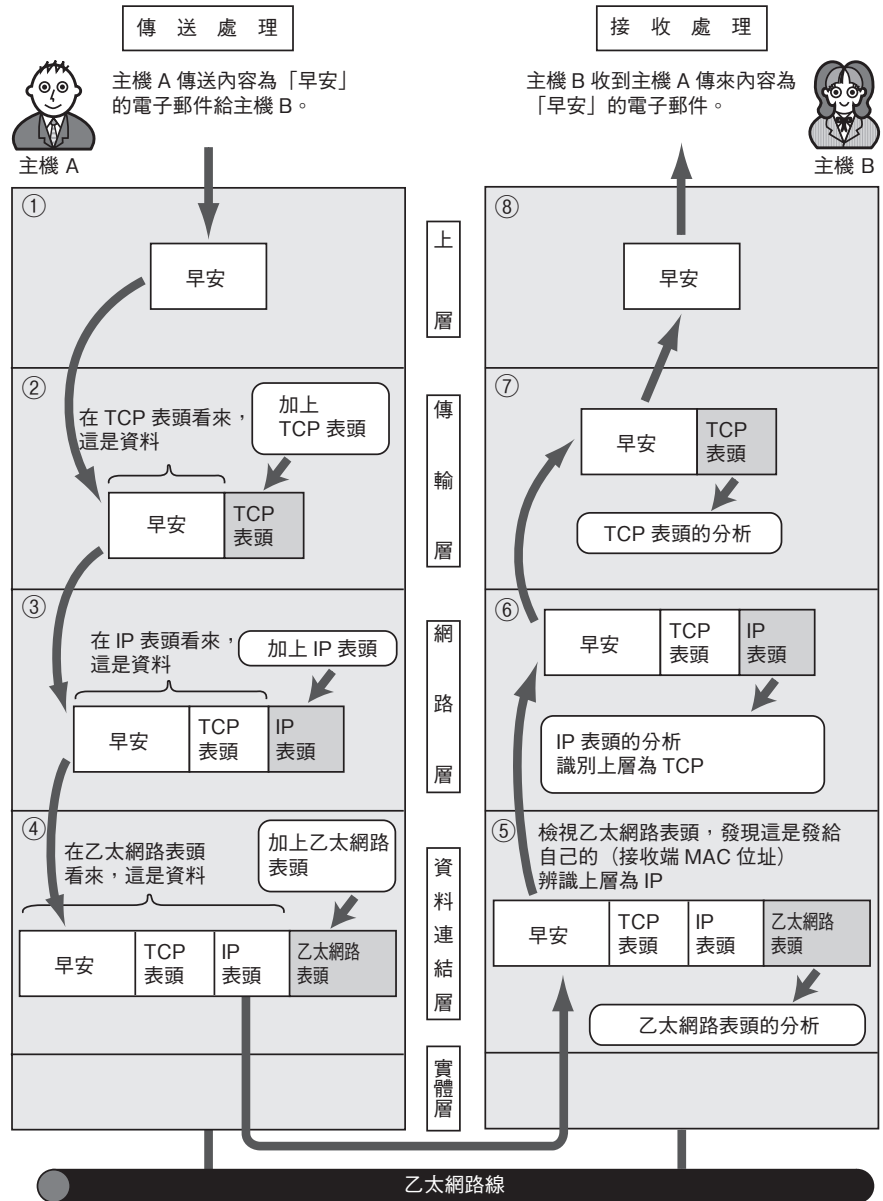
2.4.2 硬體（實體層）

在 TCP/IP 的層級模型中，最下層是負責傳輸物理性資料的硬體。這個硬體是指乙太網路、電話線路等實體層，可是該內容沒有明確定義。使用的通訊媒體可以有線，也可以是無線。進行通訊時的可靠性與安全性、頻寬、延遲時間等使用上沒有特別限制。總之，TCP/IP 是以網路連線的設備之間，可以通訊為前提而建立的協定。

應用層在傳送電子郵件時，指示建立 TCP 連接。建立 TCP 連接之後，再利用該連接傳送電子郵件。

接著將應用層的資料傳遞給下層的 TCP，進行轉發處理。

圖 2-18
TCP/IP 各層的電子郵件收送處理



3.4 無線通訊

一般無線通訊是透過電波、紅外線、雷射光線來進行傳輸。在辦公室的區域網路範圍內，能進行高速無線通訊的部分，稱作無線區域網路（WLAN）。

使用無線通訊的電腦設備，不需要使用網路線來連接網路。因此，一開始主要用於適合移動、體積輕巧的設備上。隨著通訊速度提升，再加上省空間、可以節省配線費用等優點，因而廣泛運用在辦公室、家庭、門市、車站、機場等地方。

- ▼ WPAN
(Wireless Personal Area Network)
- ▼ WLAN
(Wireless Local Area Network)
- ▼ WMAN
(Wireless Metropolitan Area Network)
- ▼ WRAN
(Wireless Regional Area Network)
- ▼ WWAN
(Wireless Wide Area Network)

3.4.1 無線通訊的種類

無線通訊可以依照通訊距離來分類，結果如表 3-3 所示。IEEE802 標準協會制定了無線個人區域網路 WPAN▼（802.15）、無線區域網路 WLAN▼（802.11）、無線都會網路 WMAN▼（802.16、802.20）、無線地區網路 WRAN▼（802.22）等規格。廣域無線區域網路 WWAN▼最具代表性的，就是手機通訊。手機透過基地台，可以進行長距離通訊。

表 3-3
無線通訊的分類與性質

分類	通訊距離（例）	制定規格的組織	相關組織及技術名稱
短距離無線	數公尺	個別	RF-ID
WPAN	10 公尺左右	IEEE802.15	Bluetooth
WLAN	100 公尺左右	IEEE802.11	Wi-Fi
WMAN	數公里～100 公里	IEEE802.16、IEEE802.20	WiMAX
WRAN	200 公里～700 公里	IEEE802.22	—
WWAN	—	GSM、CDMA2000、W-CDMA	3G、LTE、4G、下一代行動通訊規格

※ 通訊距離會隨著設備的規則而異。

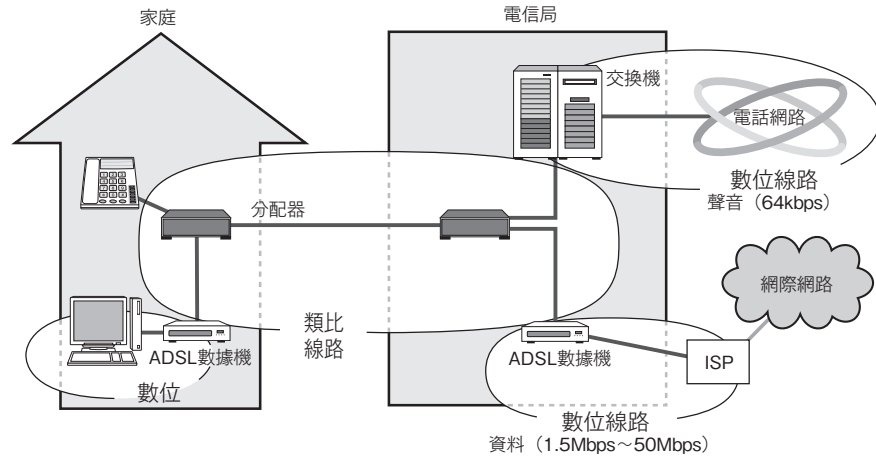
3.4.2 IEEE802.11

IEEE802.11 是定義 WLAN 協定的實體層與部分資料連結層（MAC 層）的規格。IEEE802.11 這個編號可以當作多數規格的總稱，以及作為 WLAN 的一種通訊方式。

IEEE802.11 是 IEEE802.11 相關規格的基礎，這裡規定的部分資料連結層（MAC 層），適用於 IEEE802.11 的所有規格。在 MAC 層中，和乙太網路一樣是使用 MAC 位址，並且採取與 CSMA/CS 非常類似的 CSMA/

通訊方式、電話線的品質、與電信局的距離，都會影響到線路的速度，但是基本上，ISP → 家庭或辦公室是 1.5Mbps ~ 50Mbps、家庭或辦公室 → ISP 是 512kbps ~ 2Mbps。

圖 3-34
ADSL 撥接



3.7.4 FTTH (Fiber To The Home)

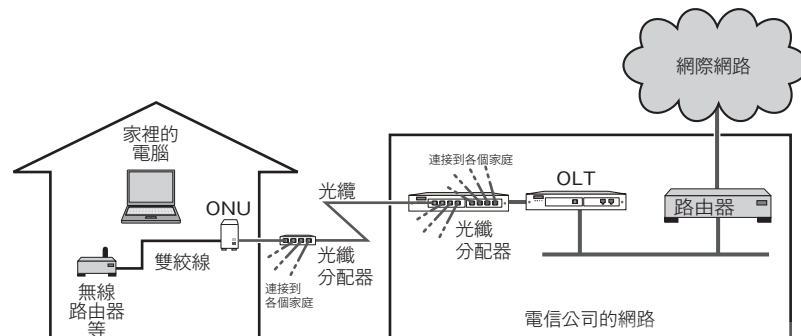
FTTH 是 Fiber To The Home 的縮寫，中文是「光纖到府」。這是直接將高速光纖連接到使用者家裡或公司建築物內的方法。雖然光纖是連接到建築物內，但是一般並非直接與電腦連接，而是透過稱作 ONU 的設備，將光轉換成電子訊號，再連接到電腦或路由器上。使用 FTTH，可以進行穩定的高速通訊，但是線路速度、服務等，將隨著各電信服務供應商提供的內容而異。

▼ ONU
(Optical Network Unit)
光網路單元。電信公司的終端設備稱作 OLT (Optical Line Terminal)。

另外還有一種方法稱作 FTTB (Fiber To The Building)，中文是「光纖到建築」。這種型態是，光纖連接到公寓、公司、飯店的建築物，之後在建築物內佈線，連接到每一戶。另外，還有光纖連接到住宅附近，再透過網路佈線，讓週邊住家共同使用的型態，稱作 FTTC (Fiber To The Curb)，中文是「光纖到路邊」。

▼ Curb 這個字的意思是，住家附近道路的石頭。

圖 3-35
FTTH 連線



▼ 3.7.6 專線

隨著網際網路的使用者急速增加、專線服務的價格降低、頻寬更廣、更多樣化，而出現各式各樣的「專線服務」。以 NTTGroup 為例，他們提供 Mega Data Net、ATM Mega-Link Service、Giga Steam 等服務。在 Mega Data Net 中，透過 ATM 介面，可以使用 3Mbps 到 42Mbps 的專線連接服務。Giga Steam 是利用乙太網路或 SONET/SDH 介面，提供 0.5Mbps 到 135Mbps 的專線連接。

專線的連接類型一定是一對一。ATM 原本設計成允許多個連接目標，但是以專線服務提供的 ATM Mega-Link Service，只能選擇一個連接目標。無法像 ISDN 或訊框中繼一樣，只要一條電纜就可以連接多個目的地。

▼ 3.7.7 VPN (Virtual Private Network)

在連接遠距離地區的 VPN (Virtual Private Network) 服務中，包括 IP-VPN 及廣域乙太網路。

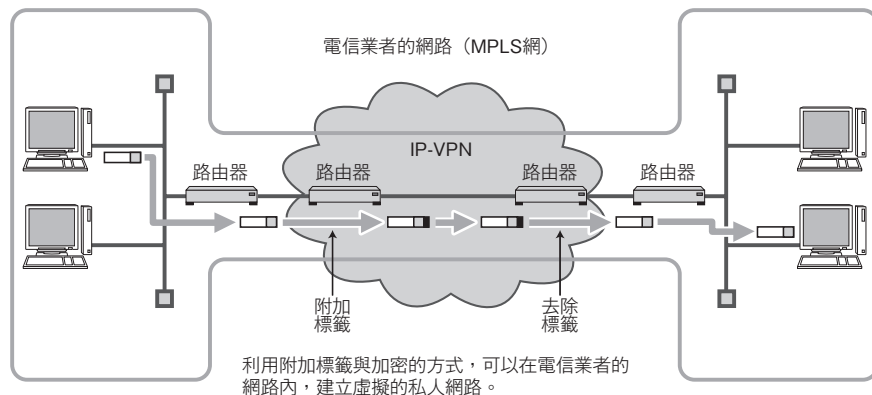
■ IP-VPN

這是指在 IP 網路（網際網路）建構 VPN。

部分電信業者提供在 IP 網路上使用 MPLS 技術，建構 VPN 的服務。7.7 節說明的 MPLS (Multiprotocol Label Switching)，是在 IP 封包中加上稱作標籤 (Label) 的資料來控制通訊。依照每個客戶設定不同標籤，通過 MPLS 網路時，利用這個標籤來判斷目的地。因此，在一個 MPLS 網路上，可以劃分出多位顧客的 VPN，形成受到保護的封閉私人網路。另外，還可以依照每位顧客的需要來控制頻寬。

▼有時也稱作 tag。

圖 3-37
IP-VPN (MPLS)



4.1 IP 是網際網路層的協定

網際網路層是 TCP/IP 的心臟，而這一層是由 IP（Internet Protocol）與 ICMP（Internet Control Message Protocol）兩個協定所構成。本章主要將針對 IP 來做介紹，至於 DNS、ARP、ICMP 等與 IP 相關的協定，會在第 5 章說明。

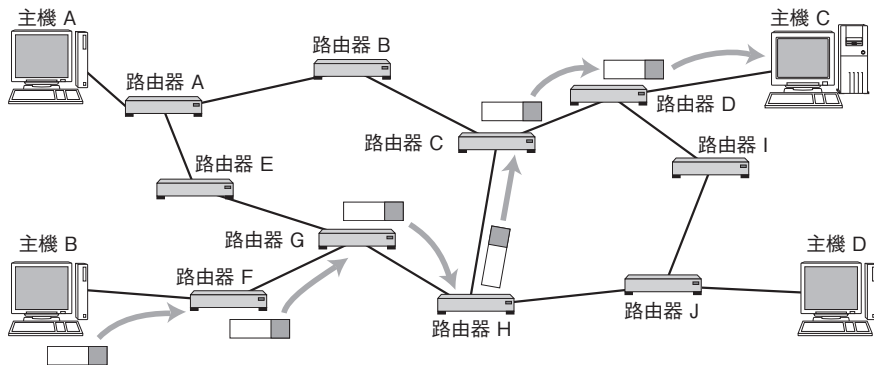
現在使用的 IP，日後恐怕不足以因應愈來愈發達的網際網路，因而提出了新版本的 IP 協定，稱作 IPv6（IP version 6）。本章先介紹 IP（IP version 4、IPv4），之後再介紹 IPv6。

4.1.1 IP 相當於 OSI 參考模型的第 3 層

IP（IPv4、IPv6）相當於 OSI 參考模型的第 3 層網路層。若用一句話來說明網路層的作用，就是「達到終點節點之間通訊」。終點節點之間的通訊，又稱為端對端（end-to-end）通訊，是網路層最重要的功能。

位於網路層的下層的資料連結，只負責在相同種類資料連結的節點之間傳送封包。但是要跨越資料連結進行通訊時，就需要網路層。網路層會隱藏通訊路徑的資料連結差異，即使資料連結的種類不同，也可以取得合作，轉發封包，讓連接到與其他資料連結的電腦之間，能進行通訊。

圖 4-1
IP 的作用



IP 的目的是在複雜的網路中，最後仍能將封包寄送到目的地。

▼ 起站相當於傳送端的 MAC 位址，終站相當於接收端的 MAC 位址。

這些車票及機票的功能，其實是在各個區間內控制移動用的東西。這裡的「區間內」，等同資料連結。寫著區間內起站到終站的車票，相當於記載著資料連結目標與傳送來源的表頭▼。說明旅行全程的行程表，其作用等同網路層。

有行程表卻沒有車票，就無法搭乘交通工具，也無法到達目的地。相對來說，即使有車票，也很難抵達最終的目的地。因為不曉得該依照何種順序來搭乘這些交通工具。如果要成功到達目的地，就得同時準備好車票與行程表。要進行網路通訊如同去遠方旅行，電腦網路中必須同時具備網路層與資料連結層。

4.2 IP 的基礎知識

IP 主要的功能有三個，包括 IP 位址、傳送封包給最終主機（路由選擇）、IP 封包的分割處理與重組處理，以下將針對各點簡單說明。

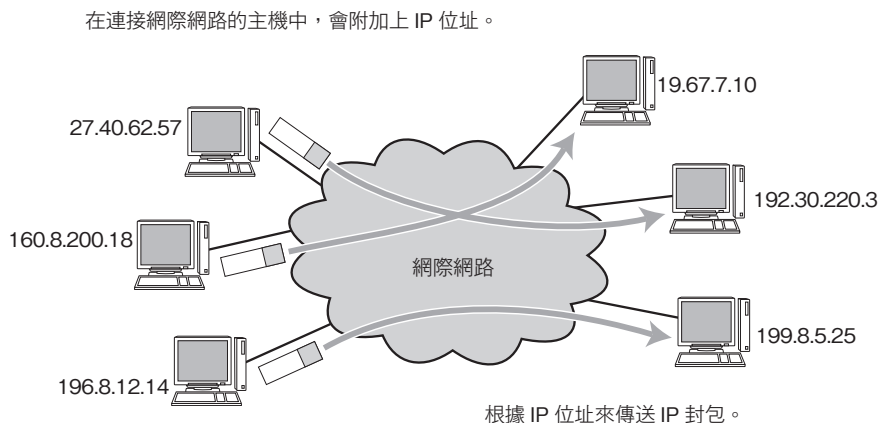
4.2.1 IP 位址是網路層的位址

在電腦通訊中，會使用位址等識別碼來辨識通訊對象。第 3 章介紹了資料連結層的 MAC 位址。MAC 位址是用來識別在同一資料連結內的電腦。

網路層的 IP 也是使用位址來識別，這個部分稱作 IP 位址，主要用於「從連接網路的所有主機中，識別進行通訊的目標對象」。利用 TCP/IP 進行通訊的所有主機或路由器，一定要設定 IP 位址▼。

▼ 嚴格來說，每張網卡至少要加上一個以上的 IP 位址。

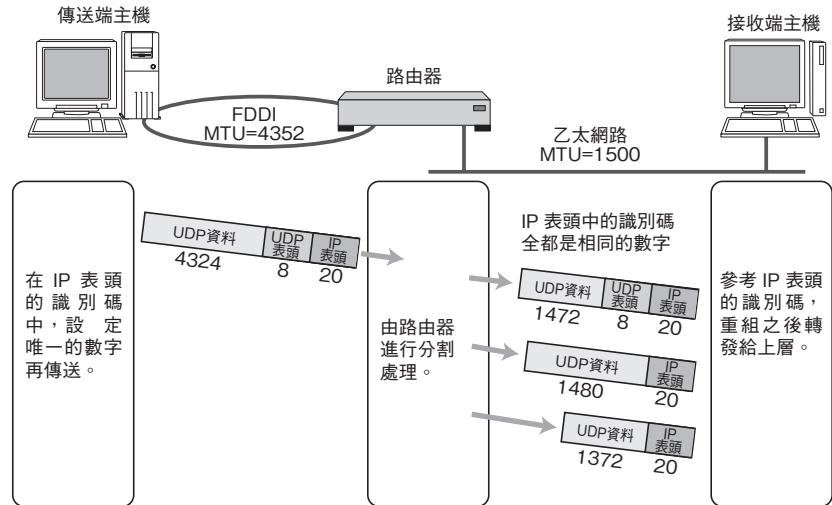
圖 4-3
IP 位址



4.5.2 IP 資料包的分割處理與重組

主機或路由器必須視狀況，進行 IP 資料包的分割處理（Fragmentation）。對網路傳送資料包時，若無法按照原本的大小直接轉發，就要進行分割處理。

圖 4-24
IP 資料包的分割處理與重組



在 IP 表頭中，含有分割後的碎片位置，以及顯示該封包後面還有接續其他碎片的旗標。根據這個旗標，可以瞭解 IP 資料包是否被分割，以及這是碎片的開頭、中間，還是結尾。（數字代表資料的長度，單位是位元組）。

圖 4-24 是在網路中進行分割處理的範例。乙太網路的 MTU 是 1500 位元組，因此 4324 位元組的 IP 資料包無法只用一個訊框來傳送，所以路由器把 IP 資料包分割成 3 個後再傳送。只要有需要，可以重複執行多次分割處理▼。

▼分割處理是以 8 位元組的倍數為單位。

分割後的 IP 資料包只會在終點的目標主機進行還原成 IP 資料包的重組處理。雖然過程中的路由器可以進行分割，卻無法執行重組處理。

這樣做的理由有很多。例如，分割後的 IP 資料包不保證是透過相同路徑來傳送。因此，就算在中途等待，也可能等不到其他封包。此外，分割後的碎片可能在半途遺失而無法送達▼。即使中途重組，通過別的路由器時，仍必須進行分割。結果，途中的細節控制，只會給路由器帶來沉重的負擔，而變得沒有效率。基於這些理由，只有終點的目標主機才能重組分割後的封包。

▼目標主機進行重組處理時，即使沒有收到部分封包，仍有可能只是延後送達而已。因此，最初收到資料包之後，大概會等待 30 秒再進行處理。

4.6.4 IPv6 位址的架構

IPv6 和 IPv4 的層級類似，也是以 IP 位址開頭的位元類型來區分 IP 位址的種類。

在網際網路的通訊中，使用的是全球單播位址（Global Unicast Address）。

全球單播位址是在網際網路內唯一的位址，因此必須使用接受正式分割的 IP 位址。

如果是控制類網路等不直接與網際網路通訊的私有網路，可以使用唯一本地位址（Unique Local Address）。唯一本地位址必須在網址內包含利用演算法隨機產生的亂數，和 IPv4 的私有位址一樣，都可以自由使用。

如果只在乙太網路相同區段中通訊沒有路由器等時，可以使用連結本地單播位址（Link Local Unicast Address）。

假如建構了可以使用多種 IP 位址的網路環境，即使在相同連結上，也可以使用全球單播位址或唯一本地位址來通訊。

IPv6 可以對一個 NIC 同時分配多個 IP 位址，因此可以視狀況來分別使用這些 IP 位址。

圖 4-27
IPv6 的通訊

