



參考資料：<https://nordvpn.com/zh-tw/blog/tcp-udp-bijiao/>

IGMP (Internet Group Management Protocol, 互聯網群組管理協議) 是TCP/IP的協議族中負責的IP群播成員管理的協議，IP主機和與其直接相鄰的群播路由器之間建立，以便維護群播組成員關係。

ICMP是Internet Control Message Protocol的縮寫，這個網路協定運用在網路七層協定中的第三層。該協定的主要目的，是用來解析網路封包或是分析路由的情況，大多是透過所傳回來的錯誤訊息進行分析，而網路管理人員則利用這個協定的工具來了解狀況，進而使用其他措施解決所遇到的問題。

ARP 與 RARP 協定

在 Internet 網路下，每一部主機都有一個獨一無二的 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 位址只是一個網路位址，它是讓較高層的網路程式設計者（如應用層）在編寫程式時不用去考慮網路實際連線的問題（通訊協定的基本功能），但 IP 封包在網路上傳遞時，還是必須透過實體網路位址，才能送達目的位址。例如，IP 網路架設在 Ethernet 上，則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。但問題是當某部主機欲依照 IP 位址發送資料給另一主機時，它怎麼知道對方的 MAC 位址（如 Ethernet 位址）？一般主機當然知道自己的 MAC 位址，但如何得知自己的 IP 位址呢？

在 Internet 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的主機的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查詢其相對應的 IP 位址。