

TCP/IP 簡介

李宗育

a5000ml@yahoo.com.tw

0932-953-725

TCP/IP 分層架構

應用層 (http, ftp, telnet, ssh, sendmail, VoIP ...)

傳輸層 (UDP, TCP)

網路層 (IP, ICMP, RIP ...)

鏈結層 (網路介面, ARP, RARP)

網路實體

A diagram of the TCP/IP layer structure. It consists of four stacked rectangular boxes representing the layers: Application Layer (top), Transport Layer, Network Layer, and Link Layer (bottom). A vertical line connects the bottom of the Link Layer to a wider rectangular box at the very bottom labeled 'Network Entity'.

鏈結層 (Data Link Layer)

- 資料單元稱為**框架 (Frame)**
- 負責網路的**實體傳輸**。
- 框架表頭記錄的位址是「**網路實際傳輸的位址**」，在乙太網路上就是所謂的 **MAC** 位址。
- 依網路實體有不同的鏈結層協定
例：乙太網路、記號環、**SLIP**、**PPP** ...。

網路層 (Network Layer)

- 資料單元稱為**封包** (Packet)
- 負責網路封包的**繞送**(Routing)
- IP 表頭記錄的位址是**來源和目的地 IP 位址**。
- ICMP 輔助**調節繞送資訊**。
- 和實際網路傳輸媒體無關。

傳輸層 (Transport Layer)

- 主要負責連接埠多工 (Port)。
- **TCP** 具有**傳輸控制**，可將資料的每一個位元組按照順序如實地送達目的地。
- **UDP** **不具傳輸控制**，無法保證資料順序與一定能送達，但無 **TCP** 的延遲。

應用層 (Application Layer)

- 架於 **TCP** 和 **UDP** 上的各式應用程式。
- 諸如 **http**、**ftp**、**telnet**、**ssh** ...。
- 由於傳輸層的多工，使得我們的同一台機器可以開啓多種服務和應用軟體，每一個應用程式用不同的連接埠。

在網路上實際傳輸的訊息框

TCP 訊息框



UDP 訊息框



ICMP 訊息框



乙太網路資料鏈結層協定

- IEEE 802 : 10Mbit, 48bit Address
- IEEE 802.2 : LLC
- IEEE 802.3 : CSMA/CD Network
- IEEE 802.4 : Token Bus
- IEEE 802.5 : Token Ring

-
- LLC : Logical Link Control 和實體無關 (802.2)
 - MAC : Media Access Control (802.3 ~ 802.5)
 - 可以選擇 LLC + 任意 MAC 形成一組資料鏈結層協定。
例如 802.3/802.3 框架的表頭為

目的位址(48)	來源位址(48)	長度(16)	802.2 LLC (64)	資料...
----------	----------	--------	----------------	-------

IP 封包表頭

版本 (4)	表頭長度(4)	服務類型 TOS (8)	封包總長度 (16)	
認證 (16)			旗標 (3)	區段位移 (13)
存活時間 TTL (8)	通訊協定 (8)		表頭總和檢查 (16)	
來源端IP位址 (16)				
目的端IP位址 (16)				
選項 (如果有)				
資料				

IP 表頭摘要

- 版本：(IPv4)
- 表頭長度：以32bit為單位，涵蓋到所有選項。
- 服務類型：3bit priority + 4bit TOS + 1bit null (全為 0 表正常服務)
4bit TOS 表示(最小延遲、最大處理量、最大可靠度、最小花費)
例如：telnet 要最小延遲位元、FTP要最大處理量位元等
- 認證、旗標、區段位移：和封包分段有關。
- 存活時間：封包繞送時，經過一個路由器就減1，減至0就丟棄封包，亦即封包繞送的上限值，避免垃圾封包在網路上漂浮。
- 通訊協定：TCP、UDP、ICMP、IGMP。
- 表頭總和檢查：不包括資料。
- 選項：記錄路由、時間標記、安全限制等。

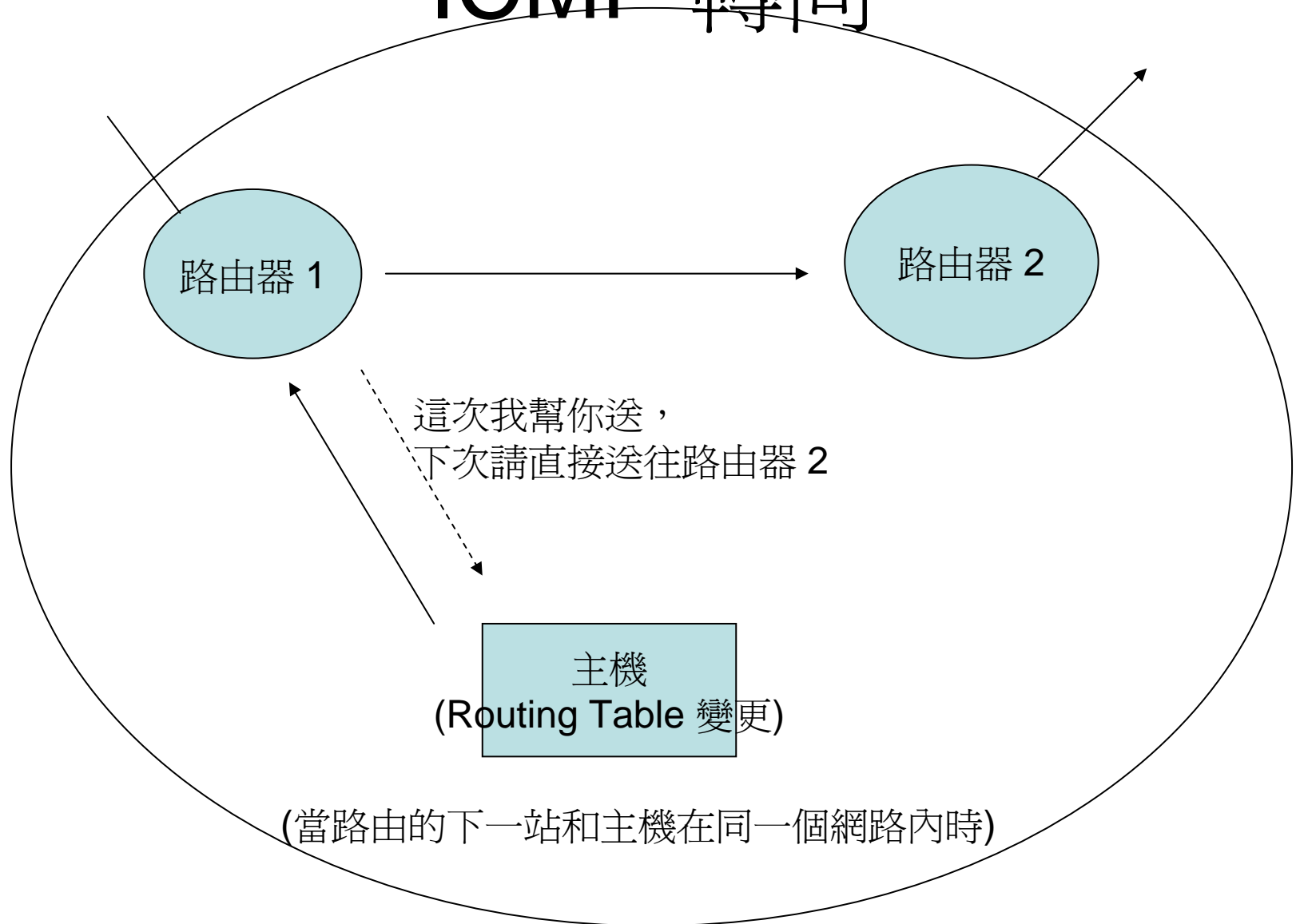
位址解析協定 (ARP)

- **ARP** 架構在鏈結層和網路層之間，主要負責將 **32bit** 的 **IP** 位址解析成 **48 bit** 的 **MAC** 位址。
- 主機上通常有一份 **ARP** 快取，記錄了 **IP** 和 **MAC** 位址的對應。
- 以廣播的方式發出 **ARP** 請求，而 **ARP** 的回應則直接送達發出請求的 **MAC** 位址。

IP 繞送機制

- 透過繞送表(Routing Table) 達成
- 若目的和主機在同一個網路內，則直接送達 (鏈結層的目的 MAC 位址為和網路層的目的 IP位址指向相同機器)；
否則就送往路由器，由路由器決定(鏈結層的目的 MAC 位址指向路由器，而網路層的目的 IP位址仍為原來的目的)。
- 繞送表由以下等因素決定
 1. 主機初始設定
 2. 路由器傳來的 ICMP 轉向訊息
 3. 路由器不定期發出的 ICMP 廣告
 4. 主機發出的 ICMP 路由需求
 5. RIP 等動態繞送協定
- 路由器對網路拓樸的了解比主機多很多，主機藉由和路由器的學習，改變內建的繞送表而逐漸累積繞送知識。

ICMP 轉向



UDP 表頭

來源端 port (16)	目的端 port (16)
總長度 (16)	總和檢查 (16)
資料	

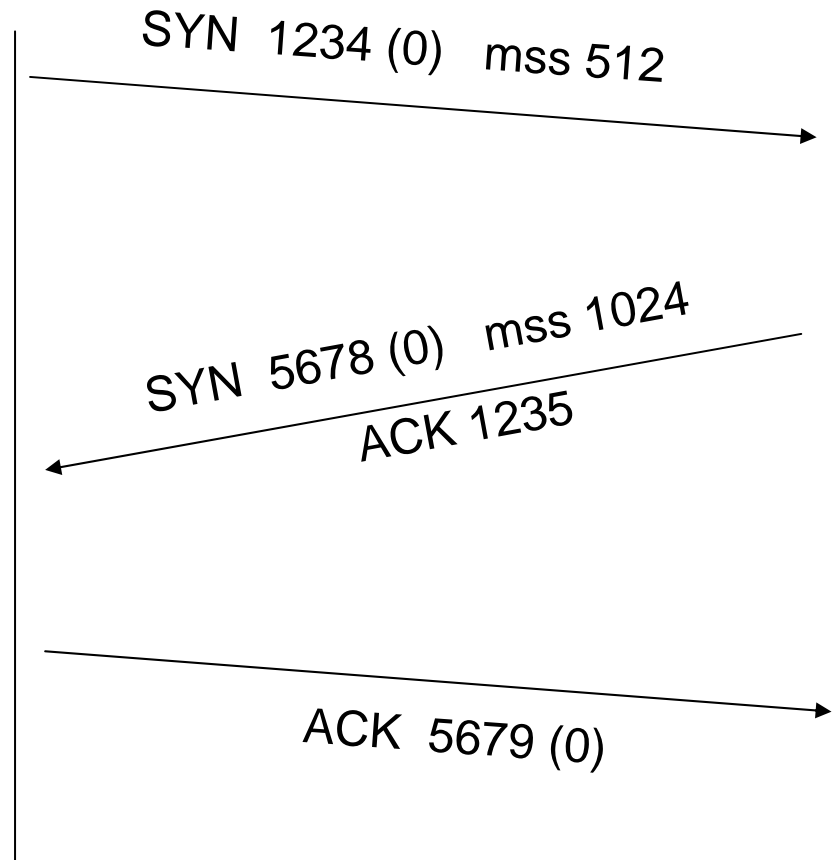
TCP 表頭

來源端 port (16)				目的端 port (16)				
序號 (32)								
回報序號 (32)								
表頭長 (4)	反向 (6)	U R G	A C K	P S H	R S T	S Y N	F I N	窗口大小 (緩衝區容量) (16)
總和檢查 (16)				緊急指標 (16)				
選項 (如果有)								
資料								

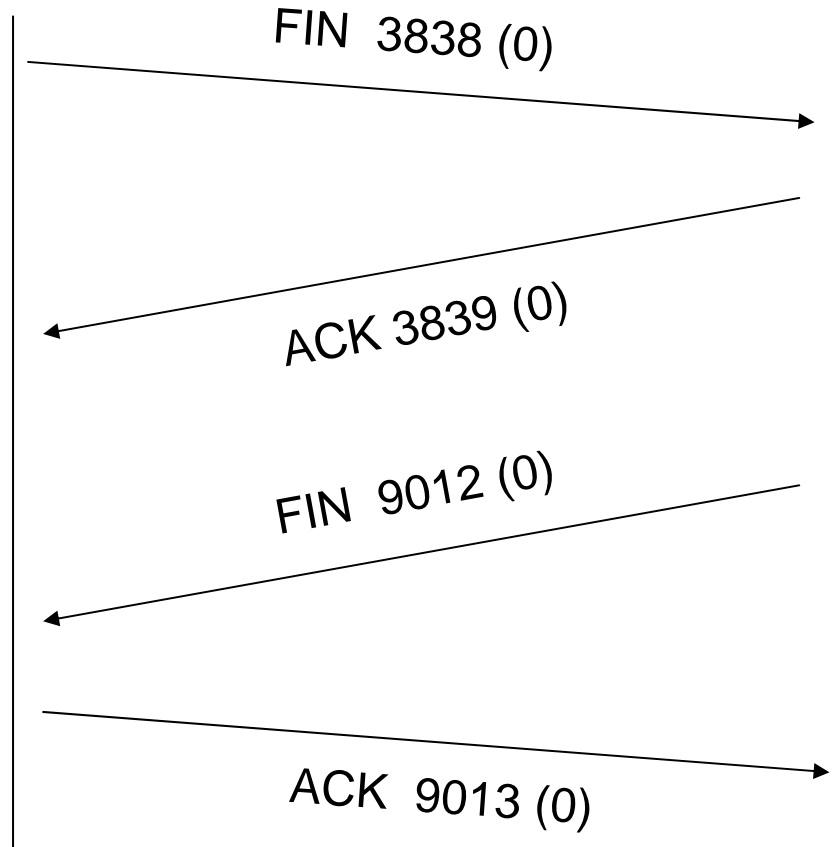
TCP表頭摘要

- 序號：資料的每個位元組都被賦予一個編號，此序號即封包中資料開頭的編號。
- 回報序號：ACK 回報已收取的資料編號加 1，亦即下一個傳送的資料編號。
建立連結的 SYN 和結束連結的 FIN 都要用掉一個序號。
- URG 緊急指標
- ACK 回報指標
- PSH 接收端要儘快把資料給應用程式
- RST 重置連線
- SYN 同步序號，起始連線
- FIN 完成傳送，結束連線
- 窗口大小：告知對方這邊的可用緩衝區容量。
- 常出現在選項中的為最大節區大小 MSS，即最大的資料塊大小，於建立連線的第一個封包(SYN)，互相告知對方。
- 資料的長度由 IP 表頭定義，所以 TCP 不需記錄。

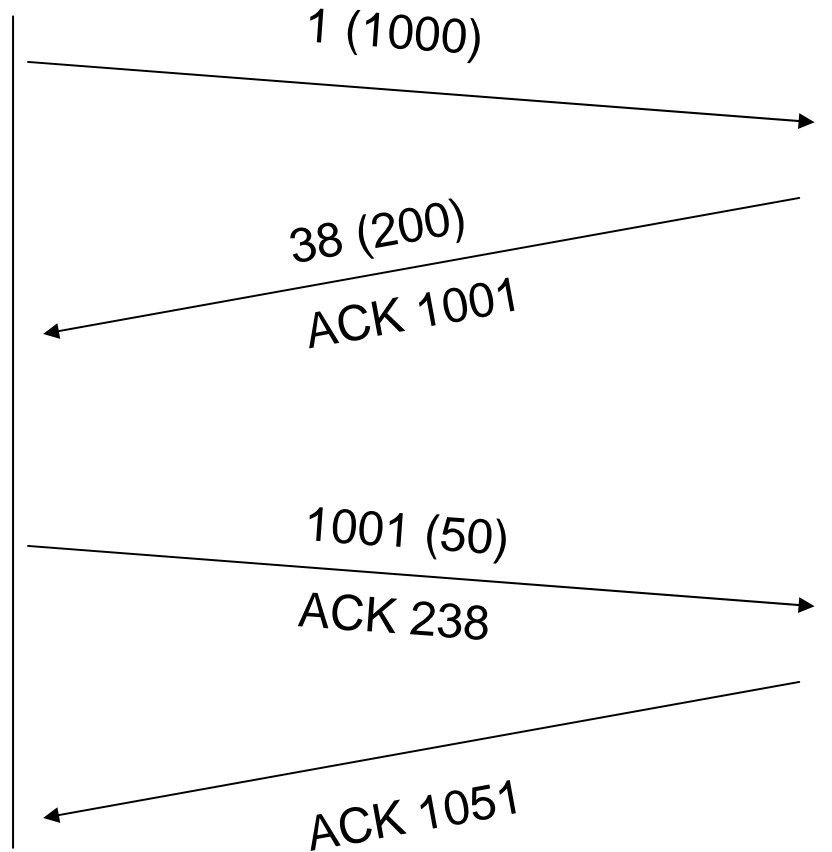
TCP 連線的建立



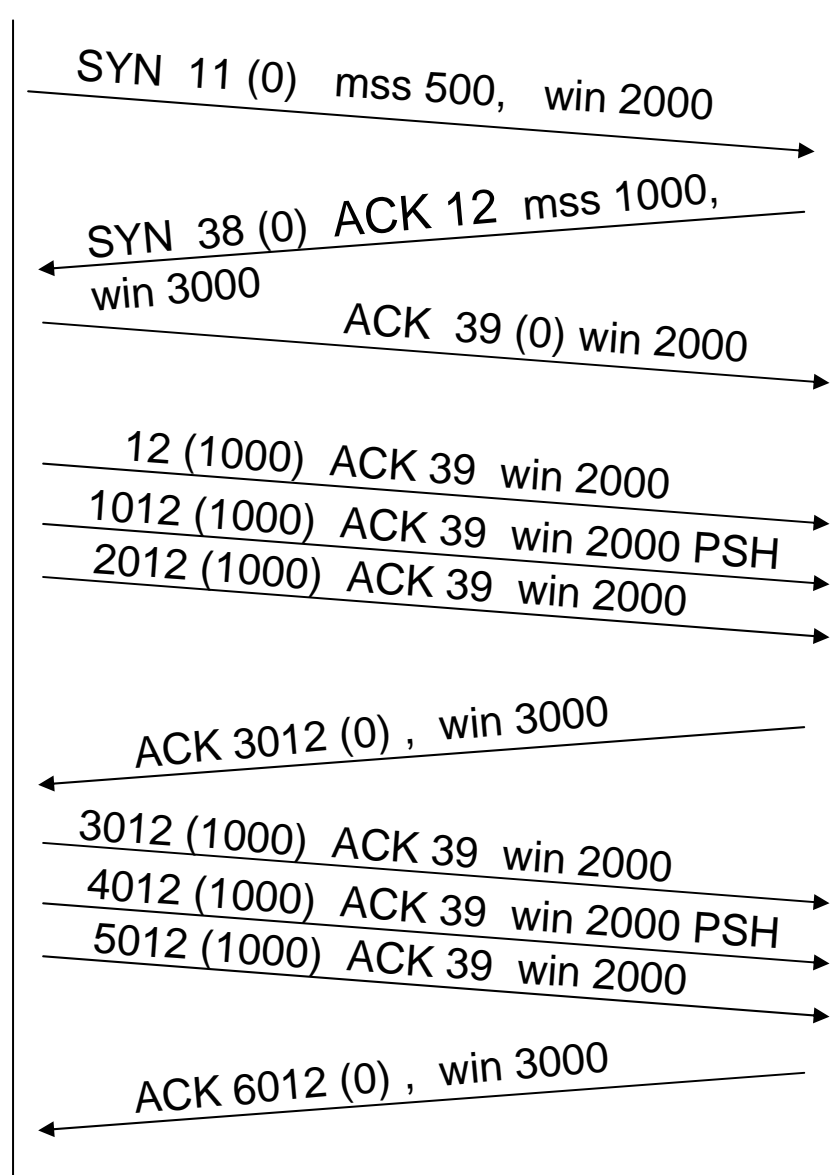
TCP 連線的結束



TCP 的雙向傳輸



TCP 的大量傳輸 (滑動窗口)



實驗

- Ethereum 示範
- PackETH 示範