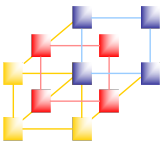
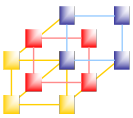
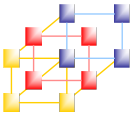


Unit 1
網路程式設計概念



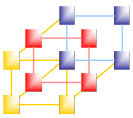
大綱

- 網路
- OSI 和 TCP/IP 模型
- 網路位址 (IP)
- 基本概念
- 主從式架構
- 解析網路封包

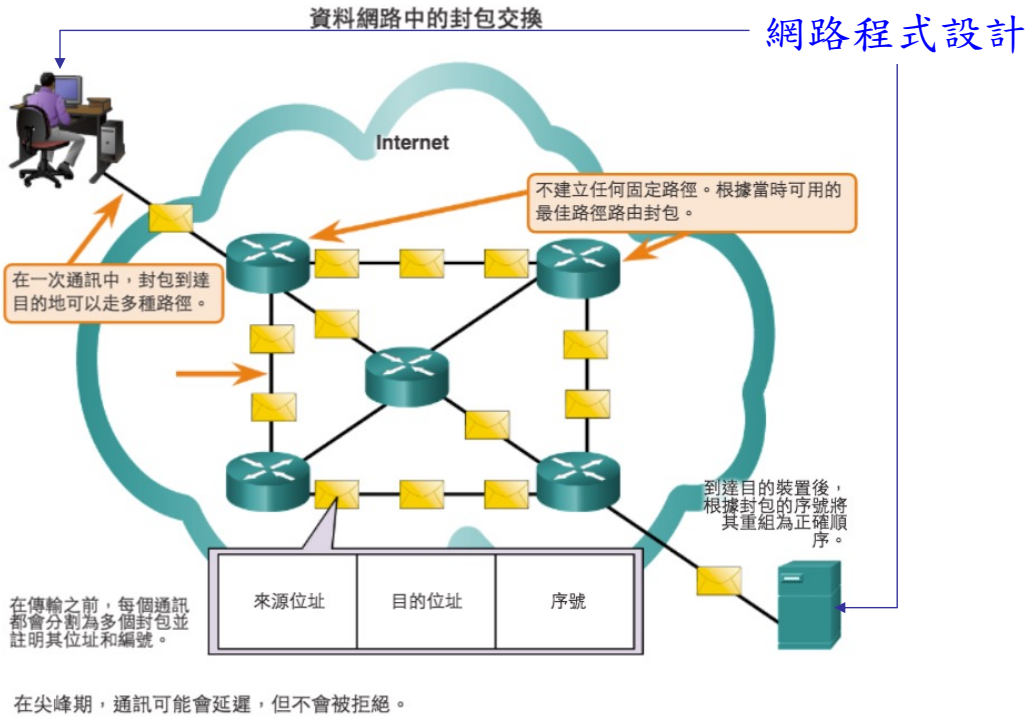


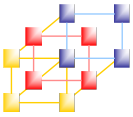
網路

- 網路是由網路設備 (Network devices)、電腦主機 (Computers) 及傳輸媒體 (Communication medias) 所共同組合而成，它們彼此之間透過一致的協定 (Protocol) 可以接收、傳送資料
  - 一般我們以節點 (Node) 來表示網路上的任何設備，以主機 (Host) 來表示一般電腦
  - 每一個在網路上的 node 都有一個位址 (Address)
- 目前的網際網路使用封包交換 (Packet-switching) 技術來傳送資料，每一個被傳送的資料都被切割成一個個的片段 (Segment)，再組成封包 (Packet) 傳送



封包交換網路

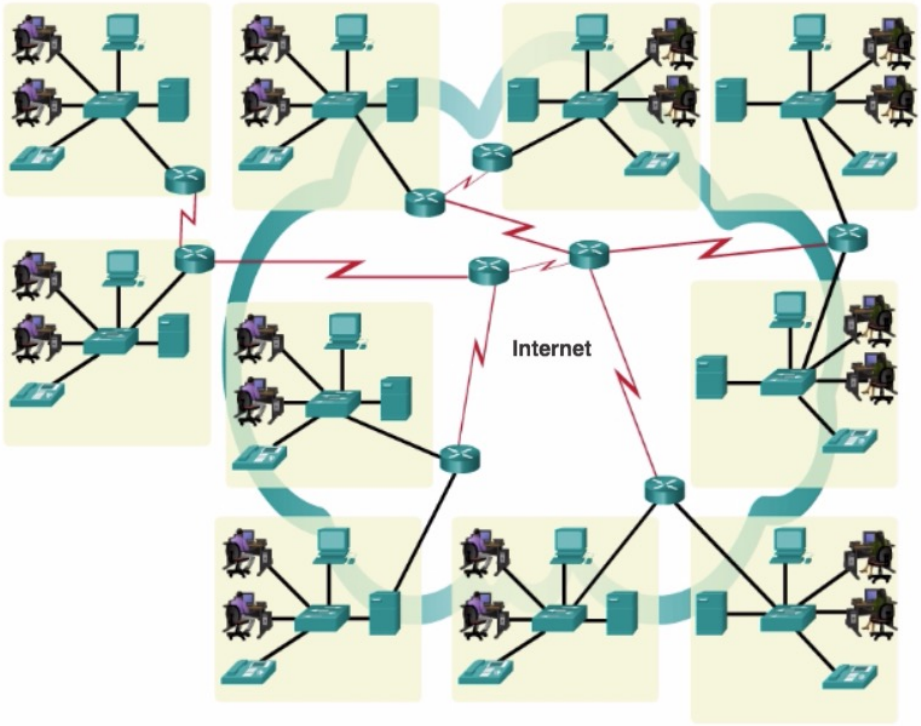




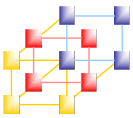
Internet

Internet 是大量網路的聚合體，並不屬於任何個人或組織

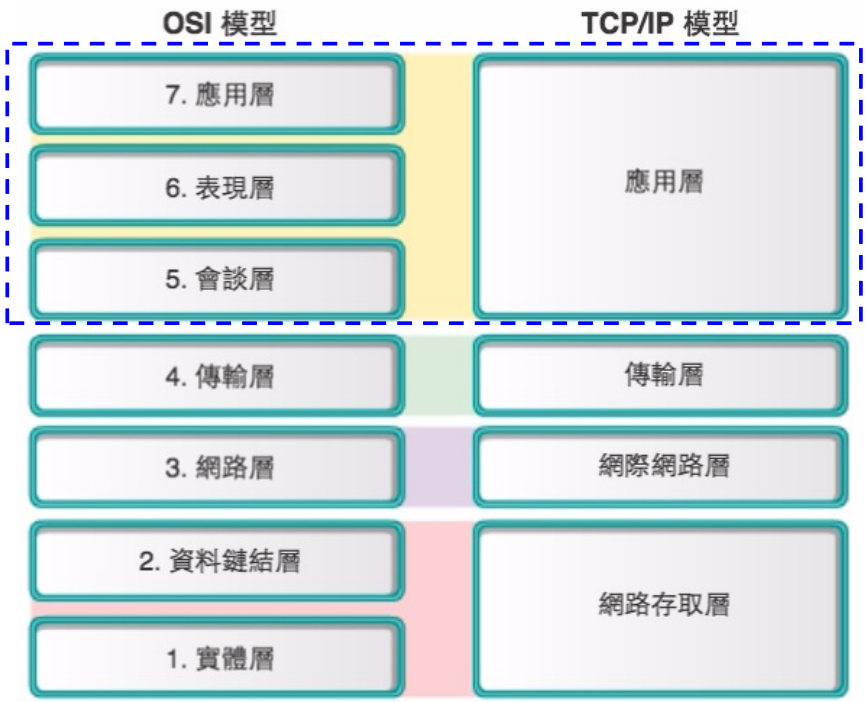
- 採用統一的公認技術和標準
- 眾多網路管理機構相互合作



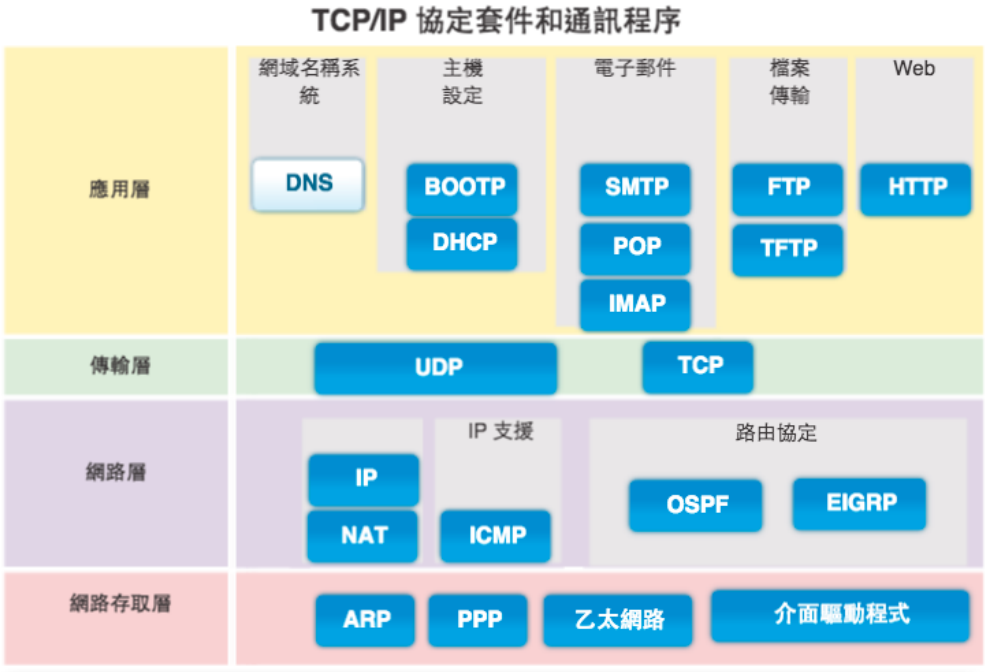
LAN 和 WAN 可以連接成互連網路



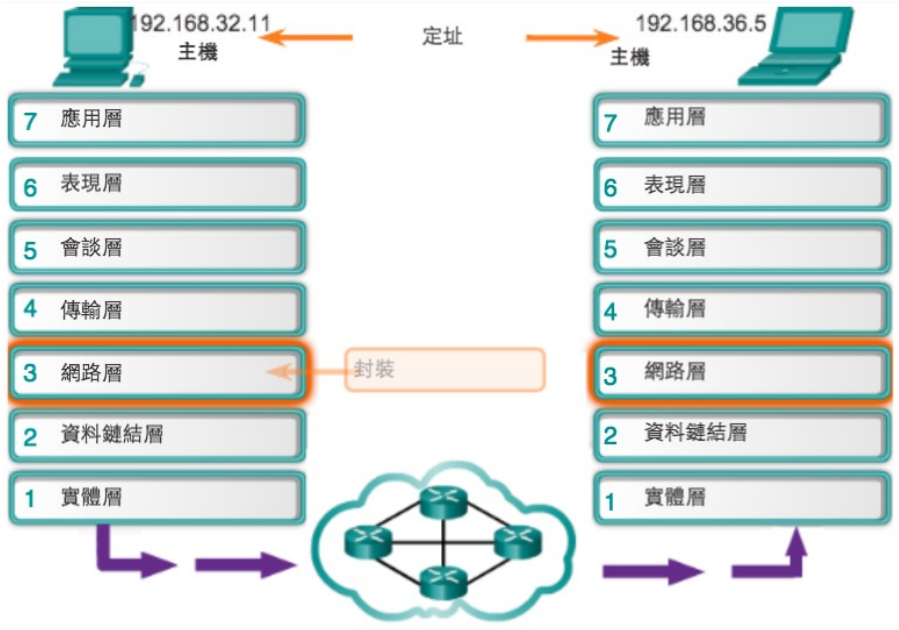
OSI 和 TCP/IP 模型



TCP/IP 協定套件

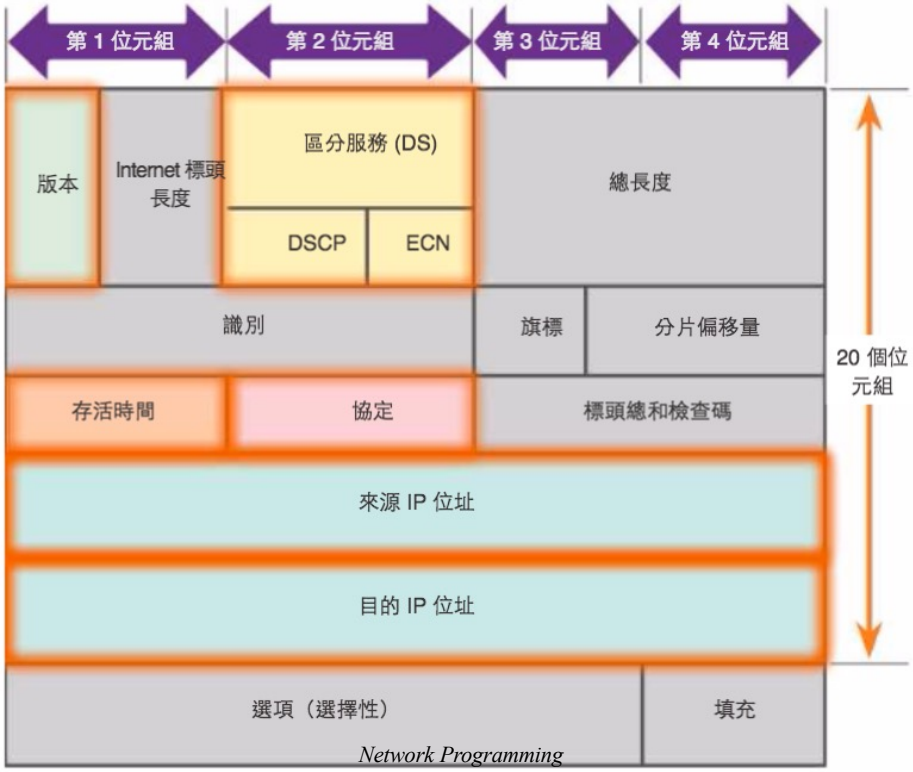


網路位址 (IP)

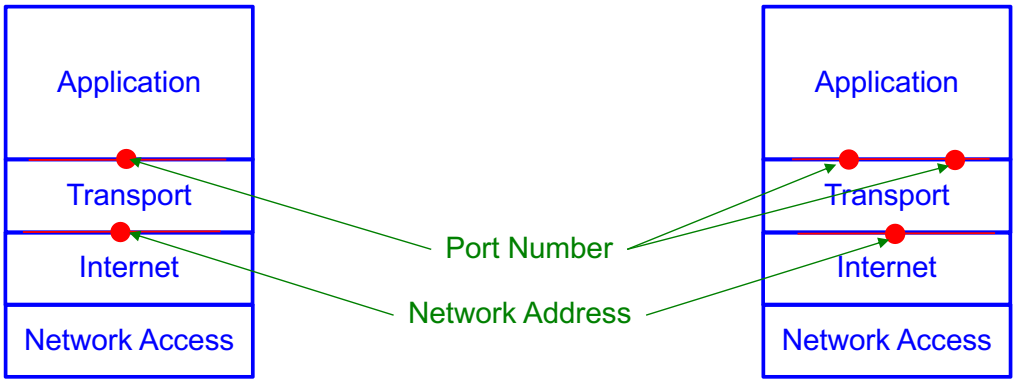


網路層協定在主機之間轉送傳輸層 PDU。

IPv4 封包標頭



IP 與 Port Number



服務 (Service) 是在主機背景執行的一支程式，通常系統服務都會占用一個埠號 (Port)，等待外部連線的要求

常用連接埠

連接埠號範圍	連接埠組
0 到 1023	公認連接埠
1024 到 49151	註冊連接埠
49152 到 65535	私有和/或動態連接埠

已註冊的 TCP 連接埠：
1863 MSN Messenger
2000 Cisco SCCP (VoIP)
8008 備用 HTTP
8080 備用 HTTP

公認的 TCP 連接埠：
21 FTP
23 Telnet
25 SMTP
80 HTTP
143 IMAP
194 Internet 中繼聊天 (IRC)
443 安全 HTTP (HTTPS)

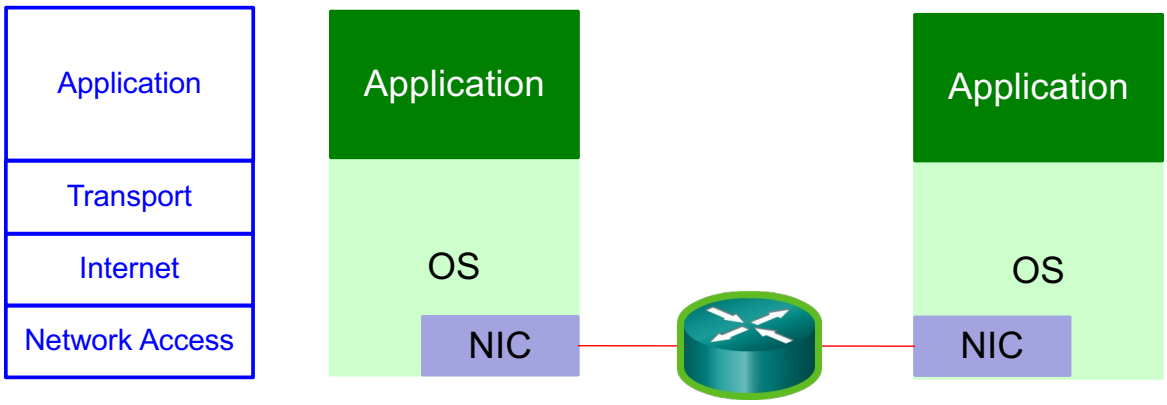
已註冊的 UDP 連接埠：
1812 RADIUS 驗證協定
5004 RTP（語言和視訊傳輸協定）
5060 SIP (VoIP)

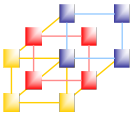
公認的 UDP 連接埠：
69 TFTP
520 RIP

已註冊的 TCP/UDP 通用連接埠：
1433 MS SQL
2948 WAP (MMS)

公認的 TCP/UDP 通用連接埠：
53 DNS
161 SNMP
531 AOL Instant Messenger，IRC

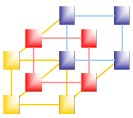
基本觀念(1/2)



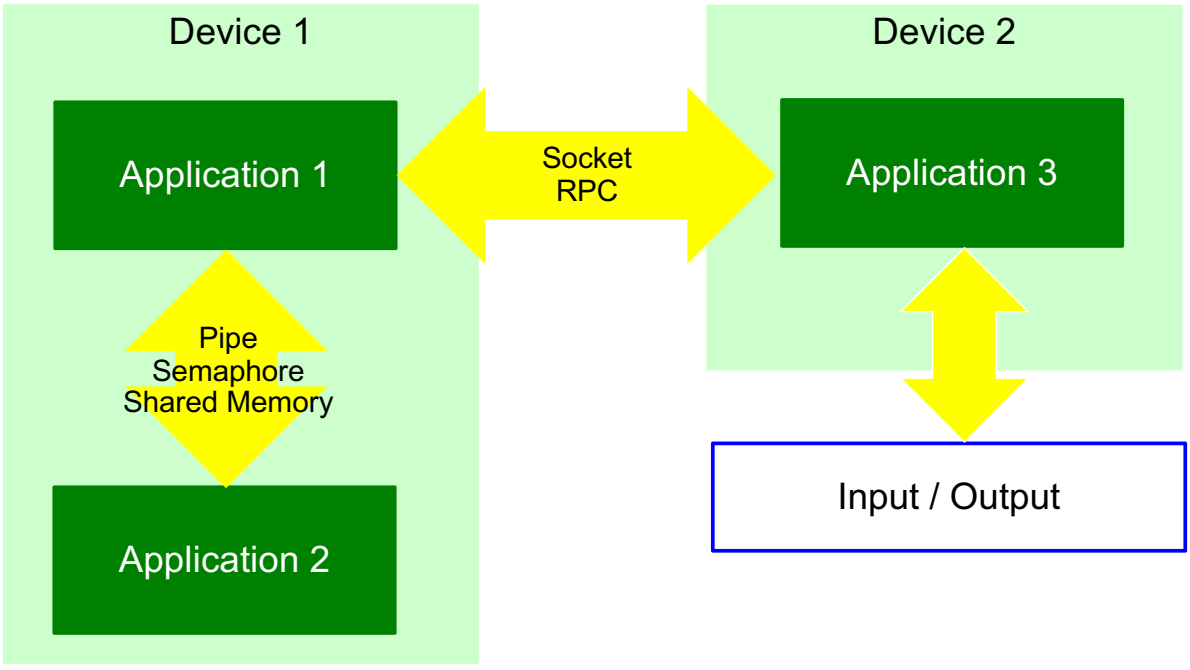


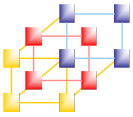
基本觀念(2/2)

- 應用程式的網路通訊主要透過系統呼叫 (System Call) 或函式庫 (Library) 來進行
  - 以 Python 來說，主要使用 socket package
  - 函式庫也是透過呼叫作業系統的服務來啟動網路通訊的指令
  - 通訊的方式主要依照 TCP/IP 網路協定的標準
- 常用的網路通訊函式庫有兩種
  - 通訊槽介面 (Socket interface)
  - 遠端程序呼叫 (RPC, Remote procedure call)



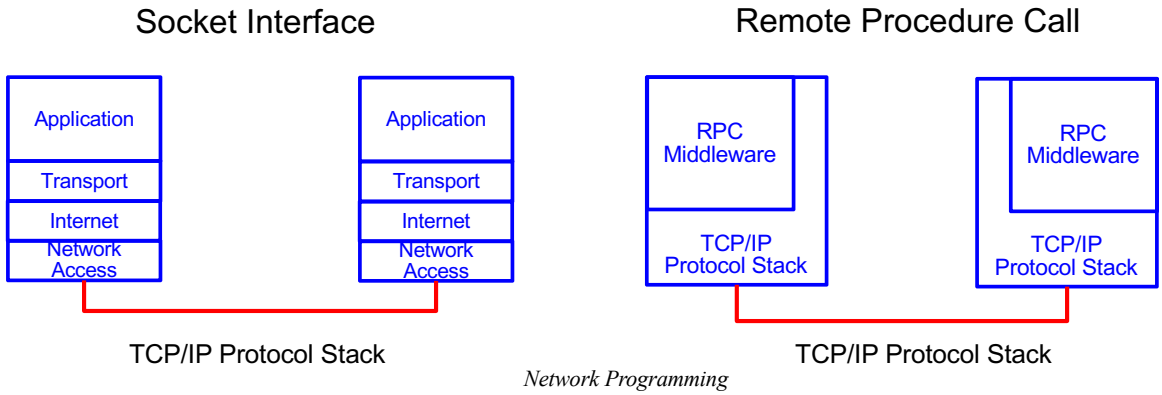
程式間訊息溝通的方法

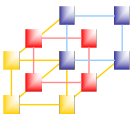




網路通訊函式庫的種類

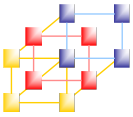
- Socket interface
  - 須考慮各種通訊的細節（例如資料型式與結構的轉換、連線的管理等）
- Remote Procedure Call (RPC)
  - 將網路通訊看成是程式中的程序
  - 對應於 Java 的 Remote Method Invocation





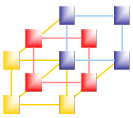
通訊槽 (Socket) 介面

- TCP 與 UDP 都支援 Socket interface
  - 目前除了 UNIX 作業系統之外，其他的各種硬體平台及作業系統，也都支援 TCP/IP 與 Socket
- Socket 介面的主要內涵是提供通訊的功能，並且藉由程序中參數的設定使呼叫程式有各種調整的彈性
- 軟體層面通訊管道
  - 連線導向 (Connection-oriented) 的軟體通訊管道
  - 非連線導向的 (Connectionless) 軟體通訊管道

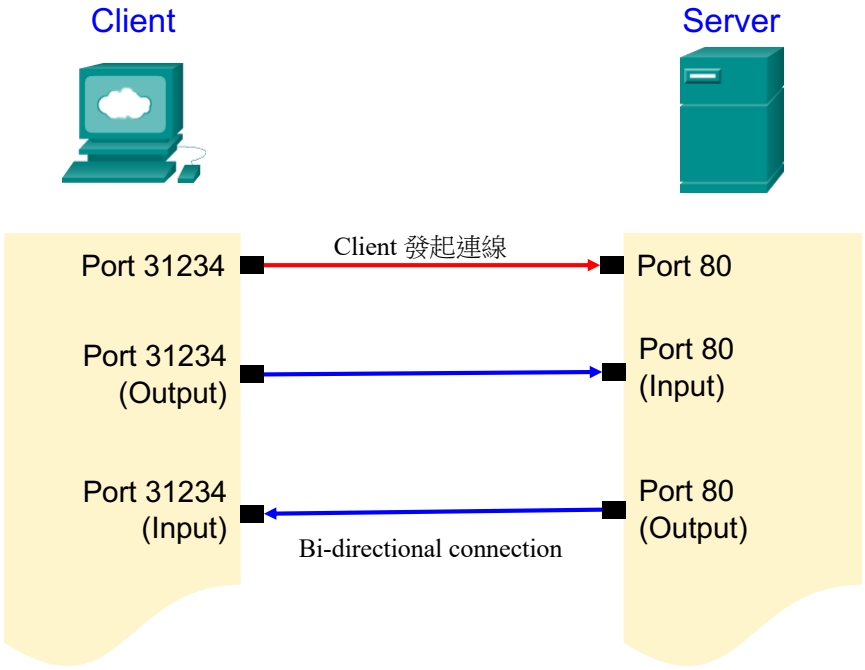


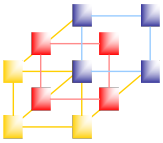
傳輸層 (Transport Layer)

- 傳輸層主要的功能是提供通訊的兩個節點之間一種穩定又節省成本的資料傳輸服務
  - 不管底下的實體網路是那一種，都能維持一樣的服務品質
  - 傳輸層中負責主要工作的軟硬體也稱為傳輸主體(Transport entity)
- 傳輸層的服務
  - Connection-oriented connection – TCP
    - Stream Socket
  - Connectionless connection – UDP
    - Datagram socket

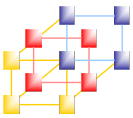


主從式架構



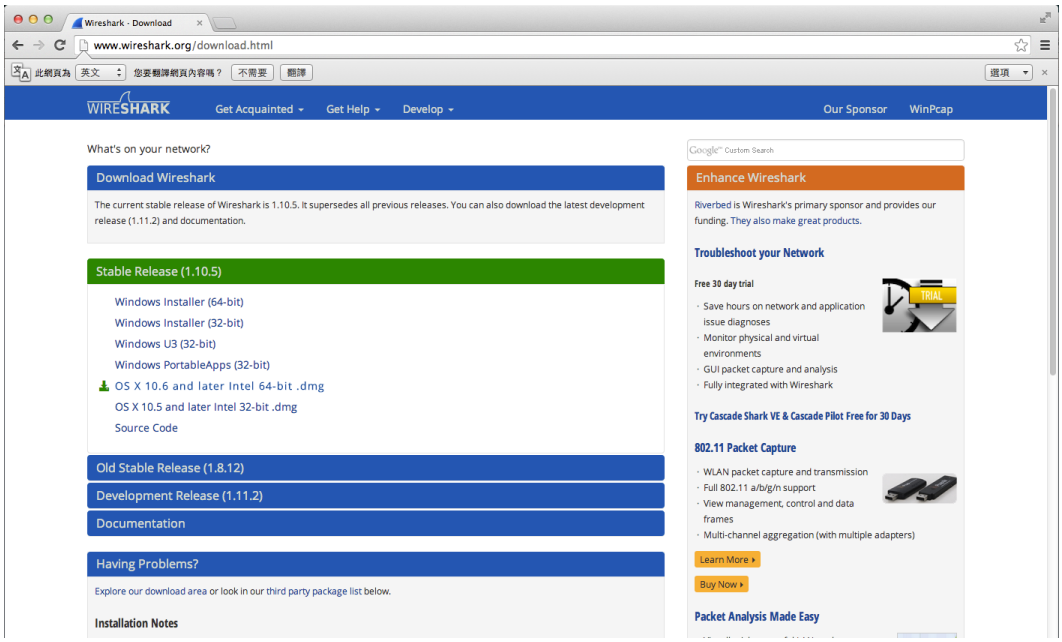


解析網路封包



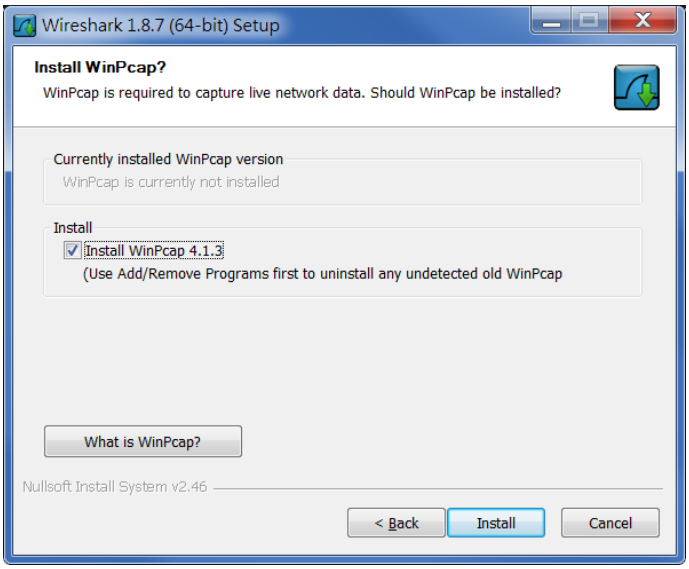
下載 Wireshark

- http://www.wireshark.org/download.html

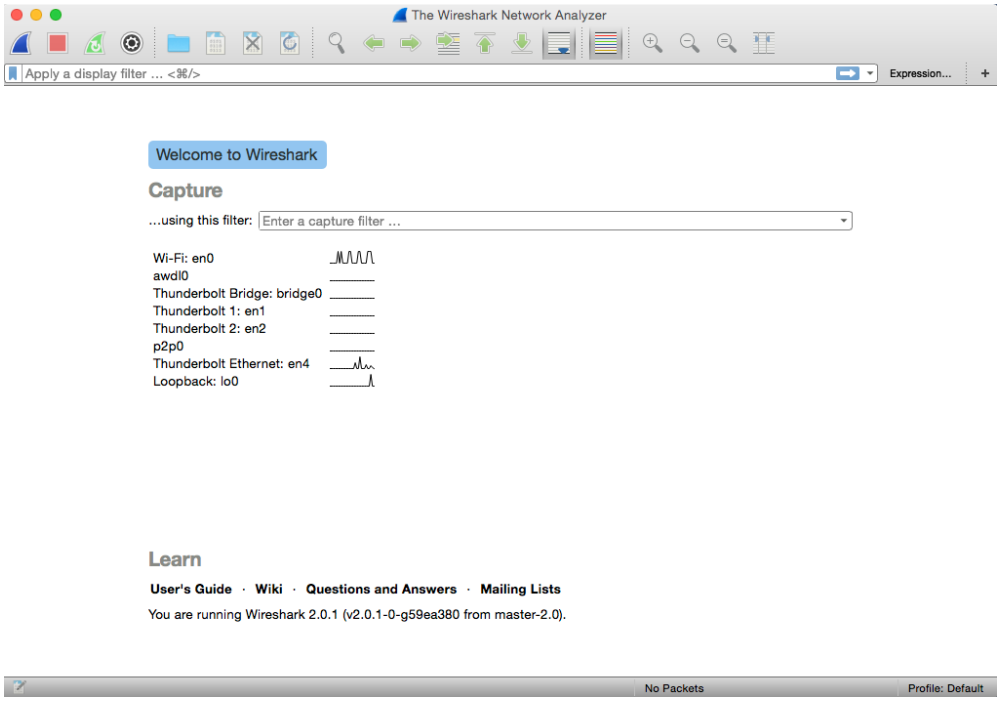


WinPcap

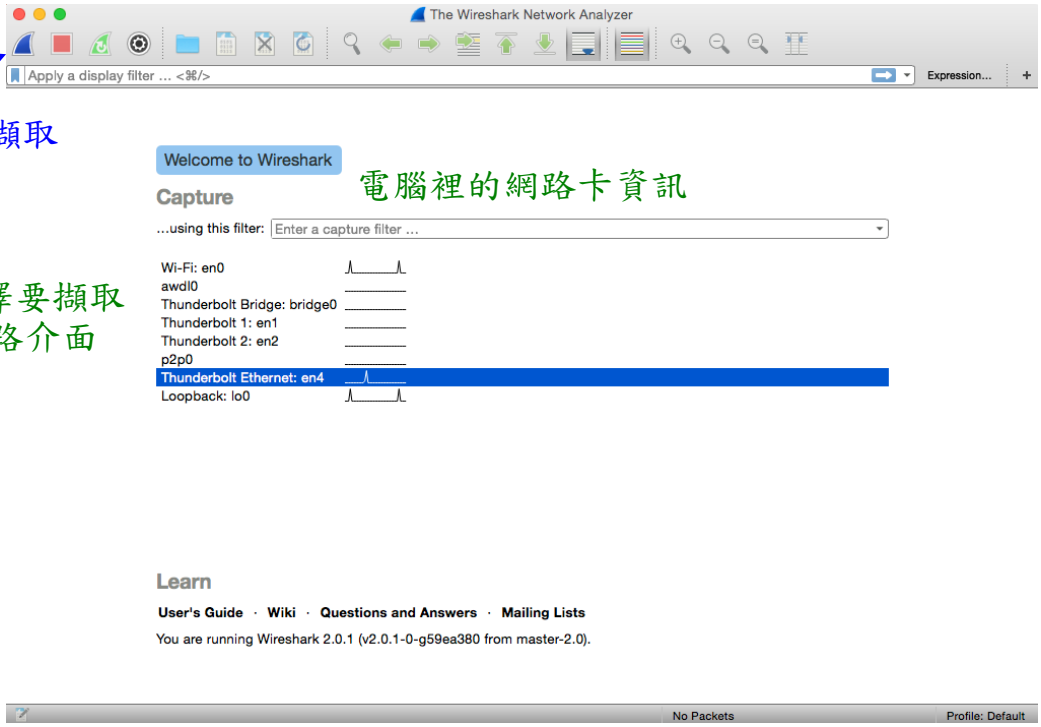
- WinPcap 是 Windows 版本的 lippcap 函式庫
  - Wireshark使用WinPcap函式庫抓取網路上的封包



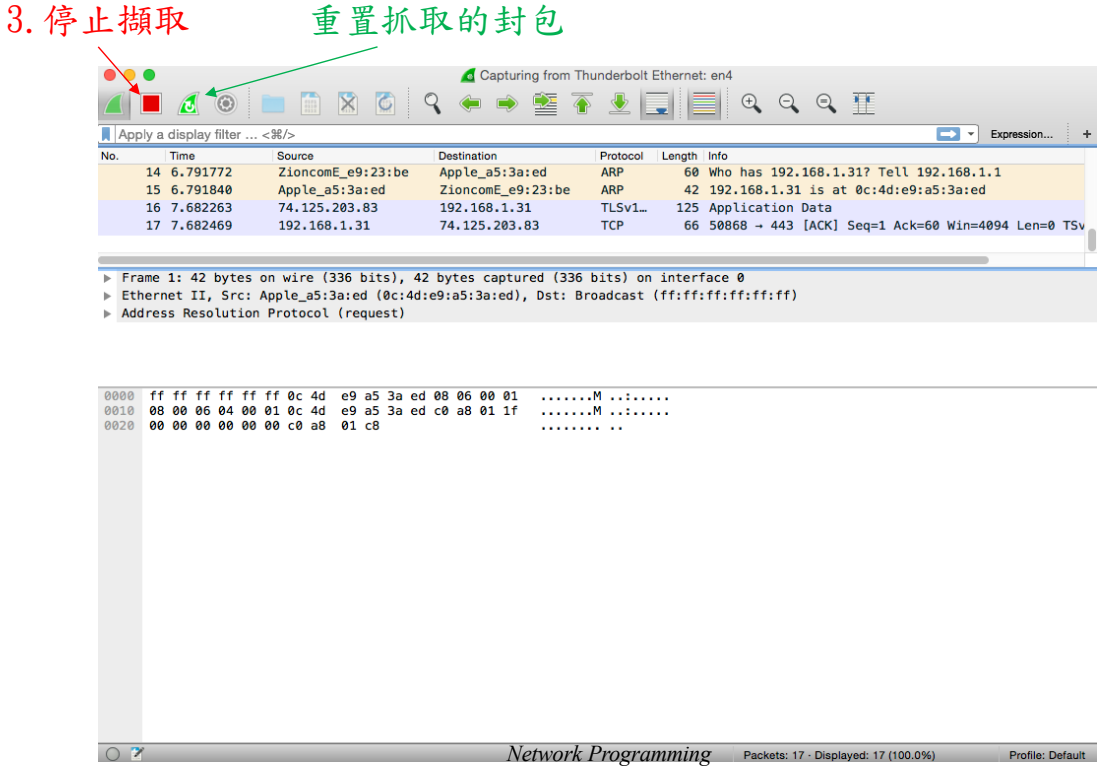
Wireshark 起始畫面

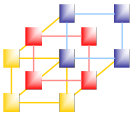


封包截取 (1/2)



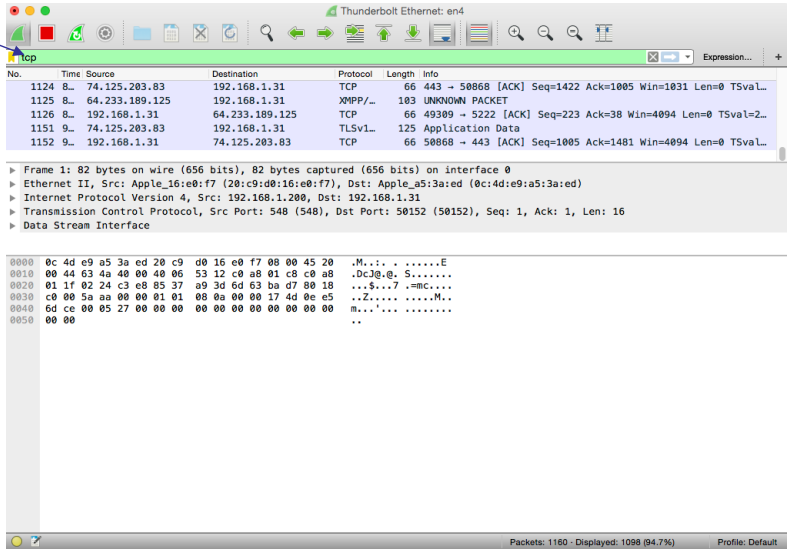
封包截取 (2/2)

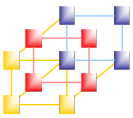




過濾器

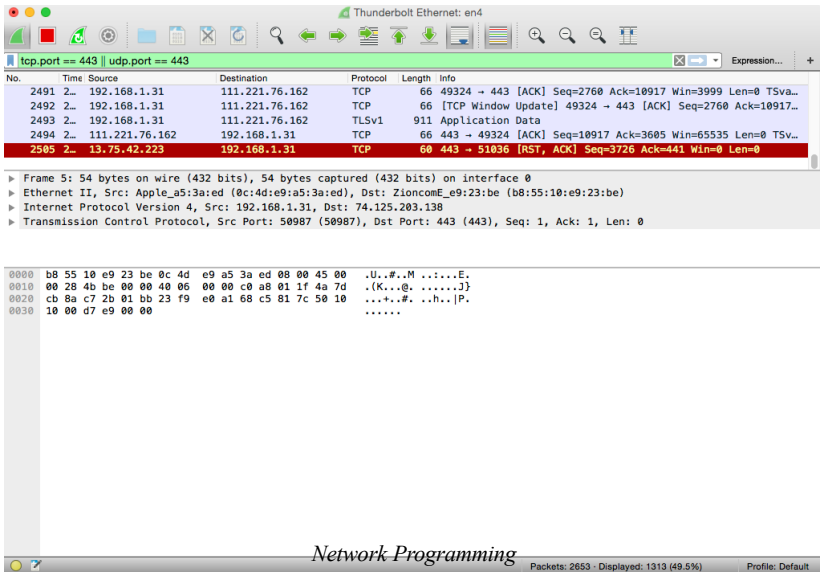
- 從擷取的封包中過濾出我們要的封包
  - 語法：[通訊協定][運算元][數值]
- 通訊協定
  - tcp 、udp、dns、ftp、ip、ssh、…
- 運算元
  - == 、!= 、> 、< 、>= 、<=
- Example
  - dns
  - ip.addr == 192.168.1.22
  - tcp.port >= 80



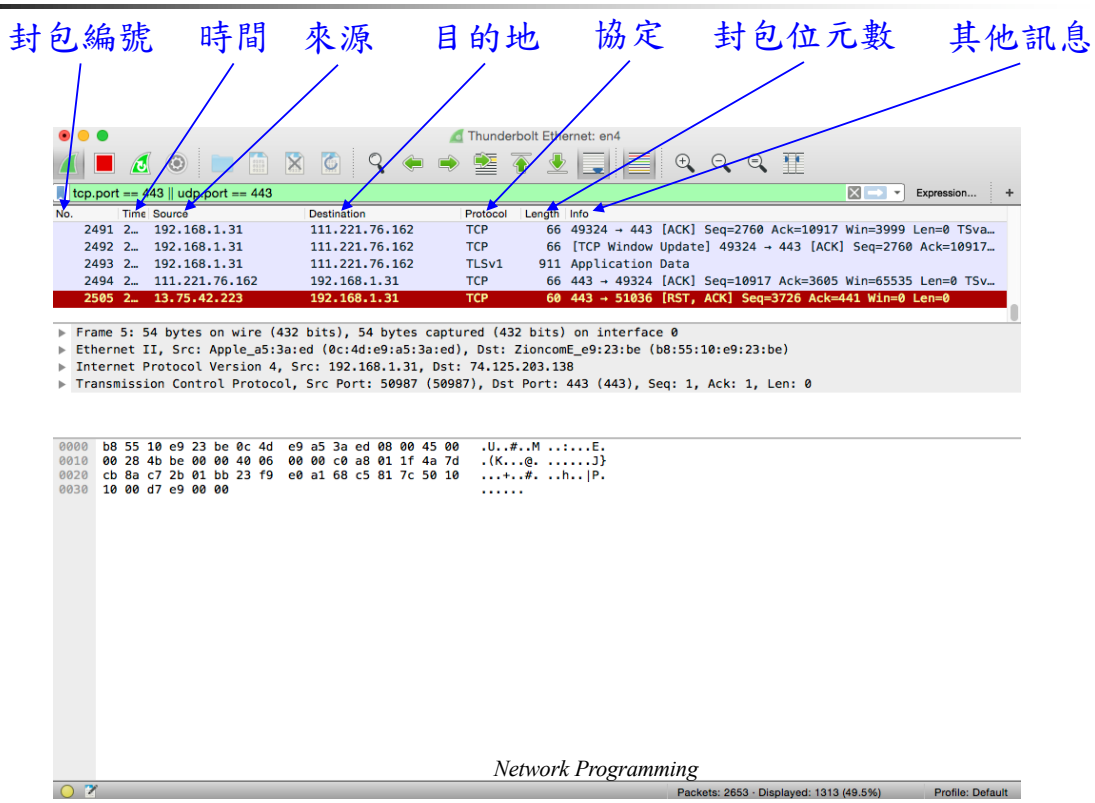


多條件過濾

- 語法：[表達式] [邏輯運算符] [其他表達式]
  - 邏輯運算符
    - && 、|| 、^^ 、!

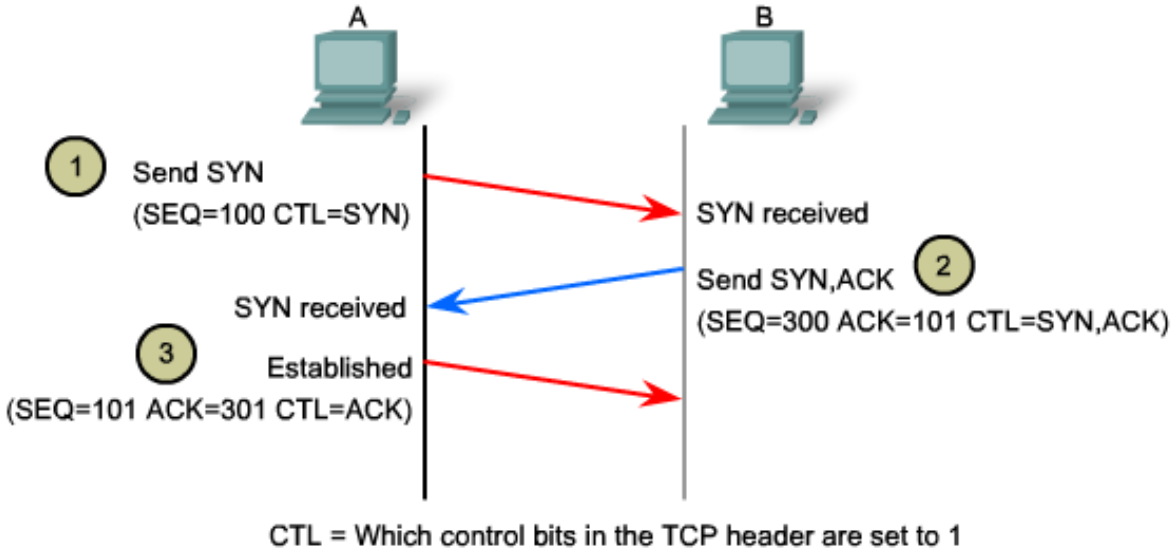


封包追蹤



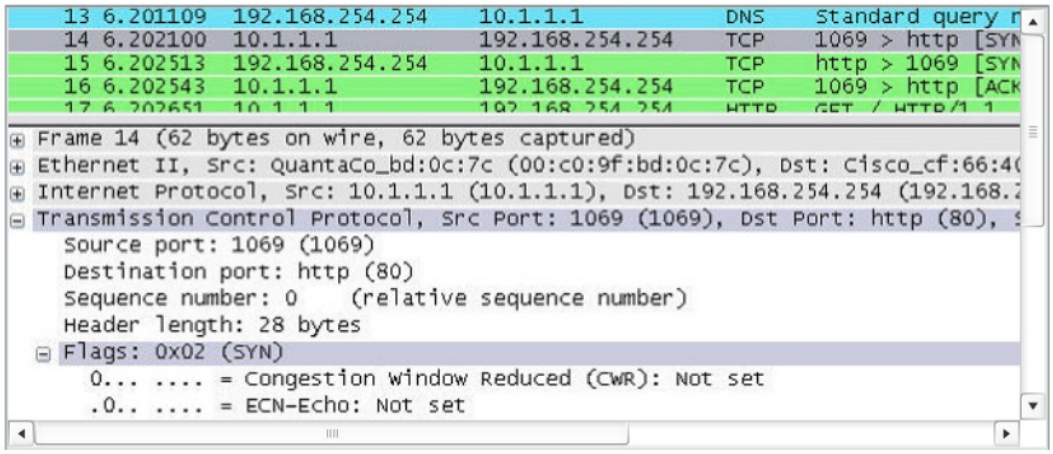
Steps in the TCP Handshake (1/5)

- TCP Connection Establishment



Steps in the TCP Handshake (2/5)

TCP 三向交握 (SYN)

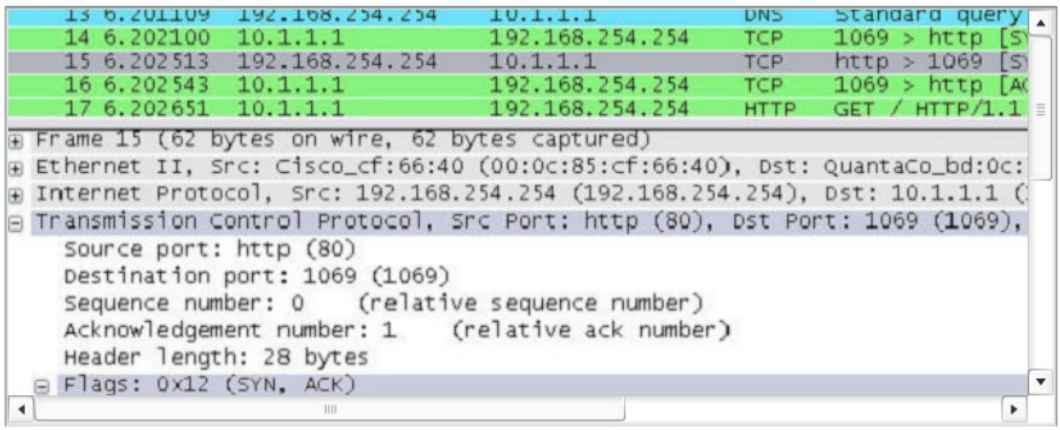


通訊協定分析器顯示了訊框 14 中的用戶端初始會談請求。

此訊框中的 TCP 資料段顯示：
- SYN 旗標設置以使初始序號生效
- 採用隨機序號有效（相對值為 0）
- 隨機來源連接埠 1069
- 公認目的連接埠 80（HTTP 連接埠）表示 Web 伺服器 (http)

Steps in the TCP Handshake (3/5)

TCP 三向交握 (SYN, ACK)



通訊協定分析器顯示了訊框 15 中的伺服器回應

- ACK 標誌設置以表示有效的確認號
- 確認號以相對值1來回應初始序號
- SYN 標誌設置以表示從伺服器到用戶端會談的初始序號
- 目的連接埠號 1069 與用戶端來源連接埠對應
- 來源連接埠號 80 (HTTP) 表示 Web 伺服器服務 (http)

Steps in the TCP Handshake (4/5)

TCP 三向交握 (ACK)

```
   13 6.201109   192.168.254.254   10.1.1.1          DNS    Standard query re
   14 6.202100   10.1.1.1          192.168.254.254   TCP    1069 > http [SYN]
   15 6.202513   192.168.254.254   10.1.1.1          TCP    http > 1069 [SYN,
   16 6.202543   10.1.1.1          192.168.254.254   TCP    1069 > http [ACK]
   17 6.202651   10.1.1.1          192.168.254.254   HTTP   GET / HTTP/1.1
⊞ Frame 16 (54 bytes on wire, 54 bytes captured)
⊞ Ethernet II, Src: QuantaCo_bd:0c:7c (00:c0:9f:bd:0c:7c), Dst: Cisco_cf:66:40
⊞ Internet Protocol, Src: 10.1.1.1 (10.1.1.1), Dst: 192.168.254.254 (192.168.25
⊟ Transmission Control Protocol, Src Port: 1069 (1069), Dst Port: http (80), Se
    Source port: 1069 (1069)
    Destination port: http (80)
    Sequence number: 1    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊟ Flags: 0x10 (ACK)
```

通訊協定分析器顯示了訊框 16 中用戶端對會談的回應

此訊框中的 TCP 資料段顯示：
- ACK 標誌設置以表示有效的確認號
- 確認號以相對值1來回應初始序號
- 來源連接埠號為對應的 1069
- 目的連接埠號 80 (HTTP) 表示 Web 伺服器服務 (http)

Steps in the TCP Handshake (5/5)

- TCP Connection Termination