TCP/IP

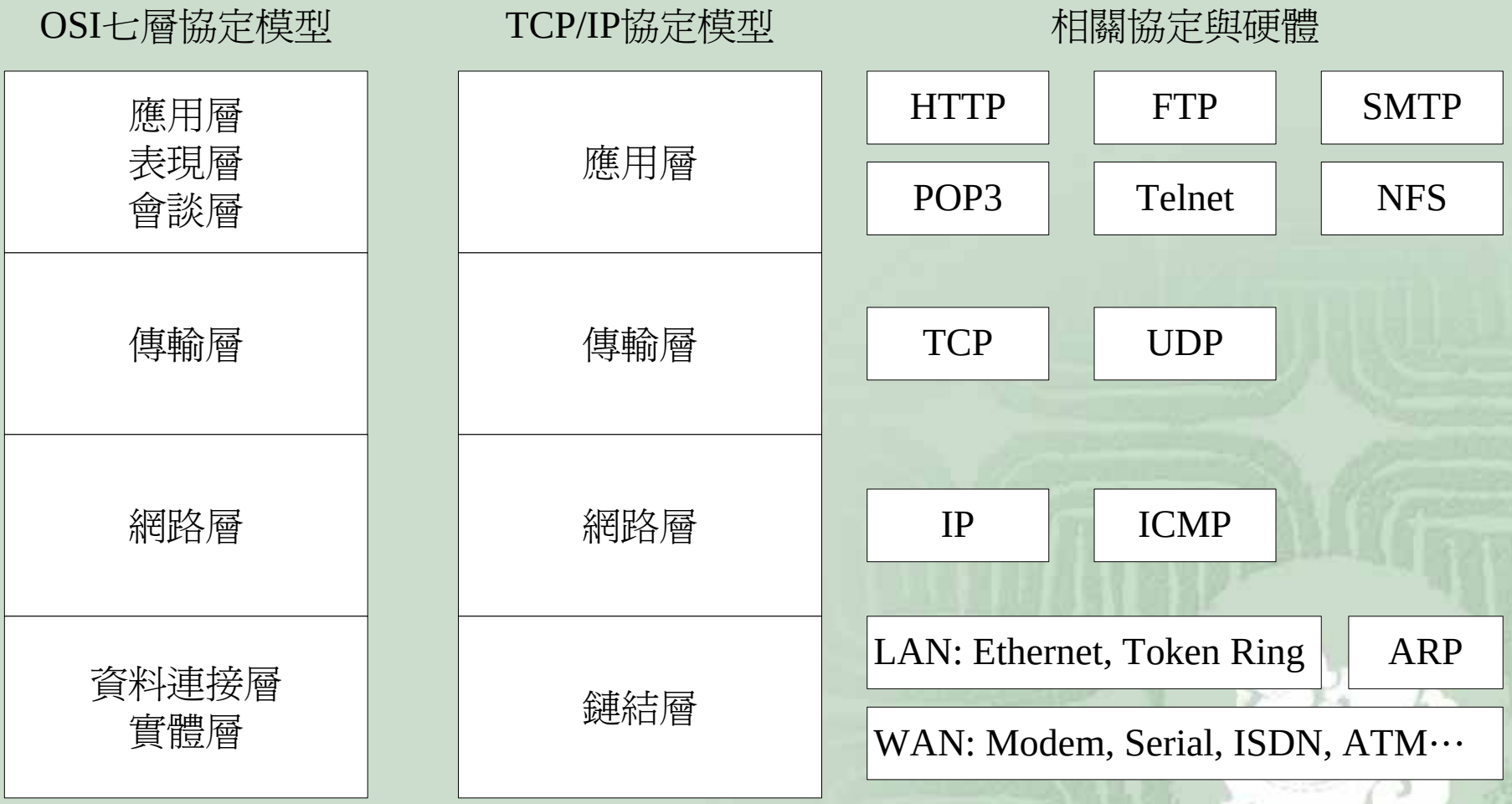
OSI七層協定與TCP/IP

- OSI七層協定的特色：
  - 分層堆疊，每層的任務是可以獨立的
  - 架構嚴謹，程式撰寫較不容易
  - 是一種標準，具有指導的意味。
- TCP/IP協定
  - 僅分四層，架構較爲鬆散
  - 程式撰寫容易
  - 應用廣泛

TCP/IP 的發展沿革

- 1960年代末期：由美國國防部尖端研究企畫署(DARPA)開發出一套名爲ARPANET的網路架構
- 1980：由ARPANET發展成爲TCP/IP協定
- 1983：TCP/IP協定取代ARPANET網路架構，並將TCP/IP稱爲Internet
- 1980年代中期：學術機構的BSD Unix內建TCP/IP的通訊協定技術
- 1980年代末期：TCP/IP已可被各主要作業系統所支援
- 1990年代：Internet上的應用被廣泛開發，如1993年的WWW協定

OSI與TCP/IP模型的比較



廣域網路(WAN)的PPP協定

- Point-to-Point Protocol的任務
  - 提供實體層與鏈結層的功能
  - 可將數據機(modem)當成網路卡來使用
  - 透過撥接取得IP後連線到Internet
  - PPP的特色：
    - 可支援多種協定，如TCP/IP、NetBEUI、IPX/SPX等
    - 可進行撥接身份的驗證(authentication)
    - 可進行連線協商(negotiation)與設定(configuration)

廣域網路(WAN)的ISDN

- Integrated Services Digital Network
  - 利用現有的電話線路來高速傳遞訊息之技術
  - 傳輸速率比數據機高，但花費比專線低
  - ISDN同樣以撥接達成連線，但連線兩端需有ISDN數據機
  - 一般速率可達 64Kbps

廣域網路(WAN)的ADSL

- Asymmetric Digital Subscriber Line
  - 利用電話線路中的高頻部分來達成網路連線
  - 其上行/下行的頻寬並不相等，故稱爲非對稱數位用戶迴路

區域網路(LAN)的乙太網路

- 透過廣播來傳遞訊框
  - 乙太網路的區域網路中，主要利用 MAC 訊框
  - MAC 訊框的標頭(header)重點在目標/來源卡號
  - MAC 網卡卡號佔有 6bytes
  - MAC 卡號不可跨路由

```
在 Linux 環境下
[root@linux ~]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:01:03:43:E5:34
          inet addr:192.168.1.100   Bcast:192.168.1.255   Mask:255.255.255.0
          inet6 addr: fe80::201:3ff:fe43:e534/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
.....

在 Windows 環境下
C:\Documents and Settings\admin..> ipconfig /all
....
        Physical Address. . . . . . . . . : 00-01-03-43-E5-34
....
```

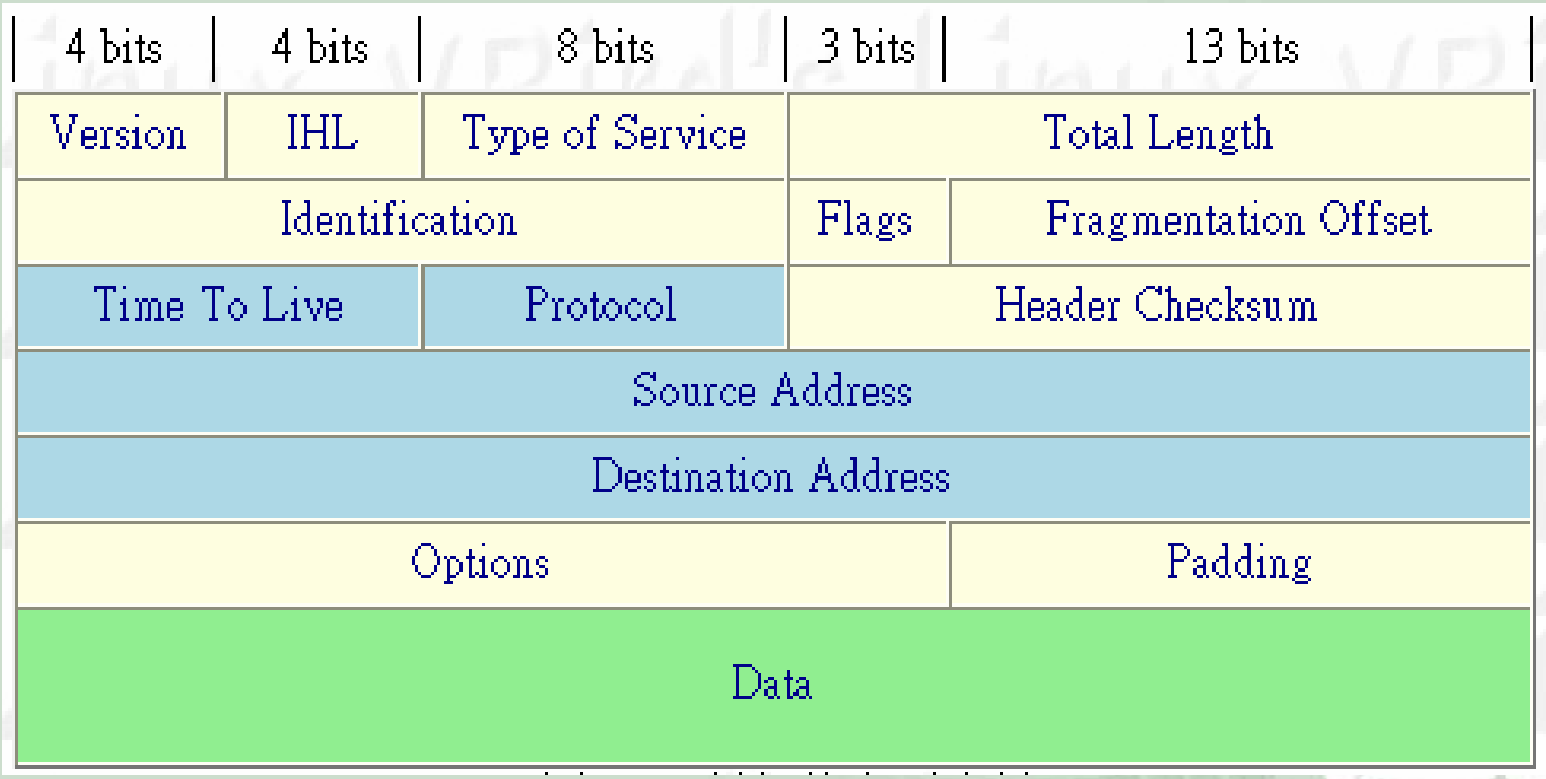
鏈結層的 ARP協定

- Address Resolution Protocol
  - 解析 MAC 與 IP 的對應
  - Linux 下可透過『 arp –n 』檢查
  - 每部主機都有 ARP table，記錄動態的ARP資訊

```
[root@linux ~]# arp -[nd] hostname
[root@linux ~]# arp -s hostname(IP) Hardware_address
參數：
-n ：將主機名稱以 IP 的型態顯示
-d ：將 hostname 的 hardware_address 由 ARP table 當中刪除掉
-s ：設定某個 IP 或 hostname 的 MAC 到 ARP table 當中
範例一：
[root@linux ~]# arp -n
Address                  HWtype  HWaddress           Flags Mask     Iface
192.168.1.100            ether   00:01:03:01:02:03     C              eth0
192.168.1.240            ether   00:01:03:01:DE:0A     C              eth0
192.168.1.254            ether   00:01:03:55:74:AB     C              eth0
```

網路層的IP

- Internet Protocol 封包表頭



IP 的組成

- 共 32 bits ，分四組十進位的數字組成
  - 00000000.00000000.00000000.00000000→0.0.0.0
  - 11111111.11111111.11111111.11111111→255.255.255.255

- 網域ID與主機ID(Net ID & host ID)

  192.168.0.0～192.168.0.255

  11000000.10101000.00000000.00000000→host全爲0(第一個IP)

  11000000.10101000.00000000.11111111→host全爲1(最後的IP)

  |----------Net_ID---------|-host--|

  - 同一網域內的機器，可直接傳送資料封包
  - 不同網域的機器，則需透過路由器(router)代爲傳送

IP網段

- 同一IP網段的特色
  - 必須是在『同一個物理網段』之內；
  - 同一網域的任何主機，可以透過廣播取得 MAC 與 IP 的對應表 (利用 arp 指令可以查詢到！)；
  - 同一個網段內，Net ID 是不變的，而 Host ID 則是不可重複
  - Host ID 在二進位的表示法當中，不可同時爲 0 也不可同時爲 1
    - 第一個是 network IP
    - 最後一個是 broadcast IP

IP的分類

- A,B,C class 的網域分類：
  - 以二進位說明 Net ID 第一個數字的定義：

```
A Class : 0xxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx  ==>開頭是 0
          |--net--|---------host------------|
B Class : 10xxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx  ==>開頭是 10
          |------net-------|------host------|
C Class : 110xxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx  ==>開頭是 110
          |-----------net-----------|-host--|
```

  - 以十進位說明 Network 的定義：
    - A Class : 0.xx.xx.xx ~ 126.xx.xx.xx
    - B Class : 128.xx.xx.xx ~ 191.xx.xx.xx
    - C Class : 192.xx.xx.xx ~ 223.xx.xx.xx
    - 127.0.0.0 這個網域被作爲系統的內部迴圈(loopback)測試網路！

IP網域的定義：Netmask

- Netmask, 子遮罩網路(也有翻譯成子網路遮罩等等)
  - 可用來規範『網域』的區間
  - Netmask 就是 Net ID 均爲 1, 而 Host ID均爲 0 時
  - ex> 192.168.0.0~192.168.0.255 這個 C Class 的 netmask 就是 255.255.255.0
    - IP： 11000000.10101000.00000000.00000001 →192.168. 0.1
    - Netmask：11111111.11111111.11111111.00000000 →255.255.255.0

IP網域的定義：Netmask

- 網域或 IP 的表示法：
  - network IP / netmask (or bits)
  - 192.168.0.0/255.255.255.0
  - 192.168.0.0/24
  - 務必以 32 bits 來思考～

子網域的切分

- 若將 192.168.0.0/24 再細分爲兩個子網域？
  - Network1：11000000.10101000.00000000.0**0**000000 →192.168. 0.0
  - Network2：11000000.10101000.00000000.1**1**000000 →192.168. 0.128
  - Netmask ：11111111.11111111.11111111.10000000 →255.255.255.128
  - Network1：192.168.0. 0~192.168.0.127 (192.186.0.0/25)
  - Network2：192.168.0.128~192.168.0.255 (192.168.0.128/25)
- 思考：
  - 說明 192.168.100.30/26 的相關網路參數：
    - IP： ***192.168.100.30***
    - Netmask： ***255.255.255.192***
    - Network： ***192.168.100.0***
    - Broadcast： ***192.168.100.63***

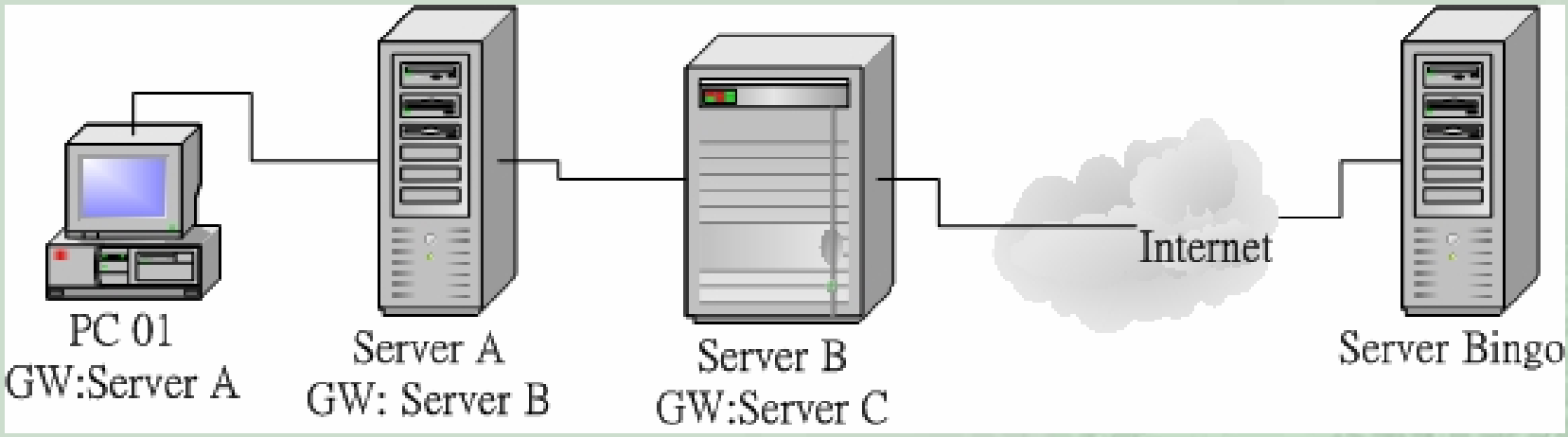
IP 的種類

- Public IP (可直接連上 Internet)
- Private IP(不可與 Internet 交換路由, 需 NAT)
  - A Class：10.0.0.0 - 10.255.255.255
  - B Class：172.16.0.0 - 172.31.255.255
  - C Class：192.168.0.0 - 192.168.255.255

網路層的route概念

- 路由(route)：
  - 相同網域的電腦可透過廣播傳送封包
  - 不同網域的電腦，則資料封包將透過：
    - 經由：本機的路由設定傳送到本網域的路由器
    - 經由：本網域的路由器自己的路由設定，傳送到下一個路由器
    - 持續傳送到目的地。
  - 若沒有路由設定，則不同網域的封包無法順利互相傳送，設定錯誤也會導致封包無法正確投遞。

網路層的route概念



Linux 路由狀態的觀察

- 利用 route 可查閱路由設定，如：

```
[root@localhost ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use
   Iface
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U     0      0        0 eth0
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
```

  - 路由查詢由小網域至大網域(由上而下排列)
  - 最後一個 0.0.0.0 的是預設路由！(default gateway)

基本網路的 IP 參數

- 一組成功可連上 Internet 的網路設定需要：
  - IP
  - network
  - netmask
  - broadcast
  - gateway (router)
- 可利用指令：
  - ifconfig 來查閱 MAC 與 IP 的設定值
  - arp 查閱MAC與IP的對應表，或設定靜態 MAC 對應表
  - route 查詢目前的路由狀態；

網路層的ICMP協定

- Internet Control Message Protocol
  - ICMP 是一個錯誤偵測與回報的機制，最大的功能就是可以確保我們網路的連線狀態，與連線的正確性！
  - ICMP 本身並沒有傳送的能力，需要藉由 IP 來進行傳送
  - 指令 ping 爲重要的使用 ICMP 封包的指令
  - 若設定防火牆，並非所有的 ICMP 都要關閉，容易發生問題～

ICMP封包的類型

類別代號	類別名稱與意義
0	**Echo Reply (代表一個回應信息)**
3	Distination Unreachable (表示目的地不可到達)
4	Source Quench (當 router 的負載過高時，此類別碼可用來讓發送端停止發送訊息)
5	Redirect (用來重新導向路由路徑的資訊)
8	**Echo Request (請求回應訊息)**
11	Time Exceeded for a Datagram (當資料封包在某些路由傳送的現象中造成逾時狀態，此類別碼可告知來源該封包已被忽略的訊息)
12	Parameter Problem on a Datagram (當一個 ICMP 封包重複之前的錯誤時，會回覆來源主機關於參數錯誤的訊息)
13	Timestamp Request (要求對方送出時間訊息，用以計算路由時間的差異，以滿足同步性協定的要求)
14	Timestamp Replay (此訊息純粹是回應 Timestamp Request 用的)
15	Information Request (在 RARP 協定應用之前，此訊息是用來在開機時取得網路信息)
16	Information Reply (用以回應 Infromation Request 訊息)
17	Address Mask Request (這訊息是用來查詢子網路 mask 設定信息)
18	Address Mask Reply (回應子網路 mask 查詢訊息的)

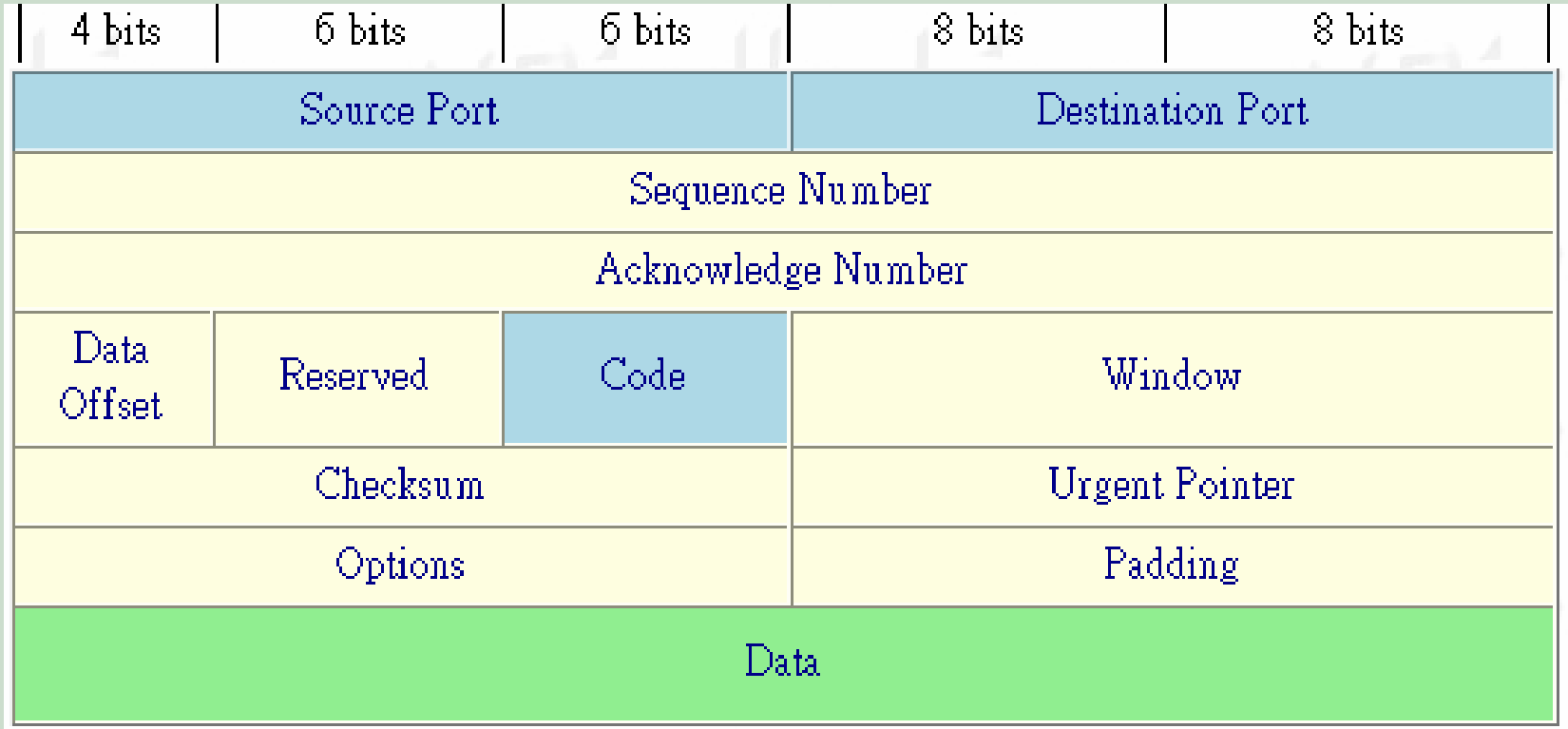
使用 ping 檢測網路狀態

```
範例一：偵測一下 168.95.1.1 這部 DNS 主機是否存在？
[root@linux ~]# ping -c 3 168.95.1.1
PING 168.95.1.1 (168.95.1.1) 56(84) bytes of data.
64 bytes from 168.95.1.1: icmp_seq=0 ttl=243 time=9.16 ms
64 bytes from 168.95.1.1: icmp_seq=1 ttl=243 time=8.98 ms
64 bytes from 168.95.1.1: icmp_seq=2 ttl=243 time=8.80 ms

--- 168.95.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 8.807/8.986/9.163/0.164 ms, pipe 2
```

- ttl：每經過一個結點就會減一
- time：傳輸的時間，越小越好

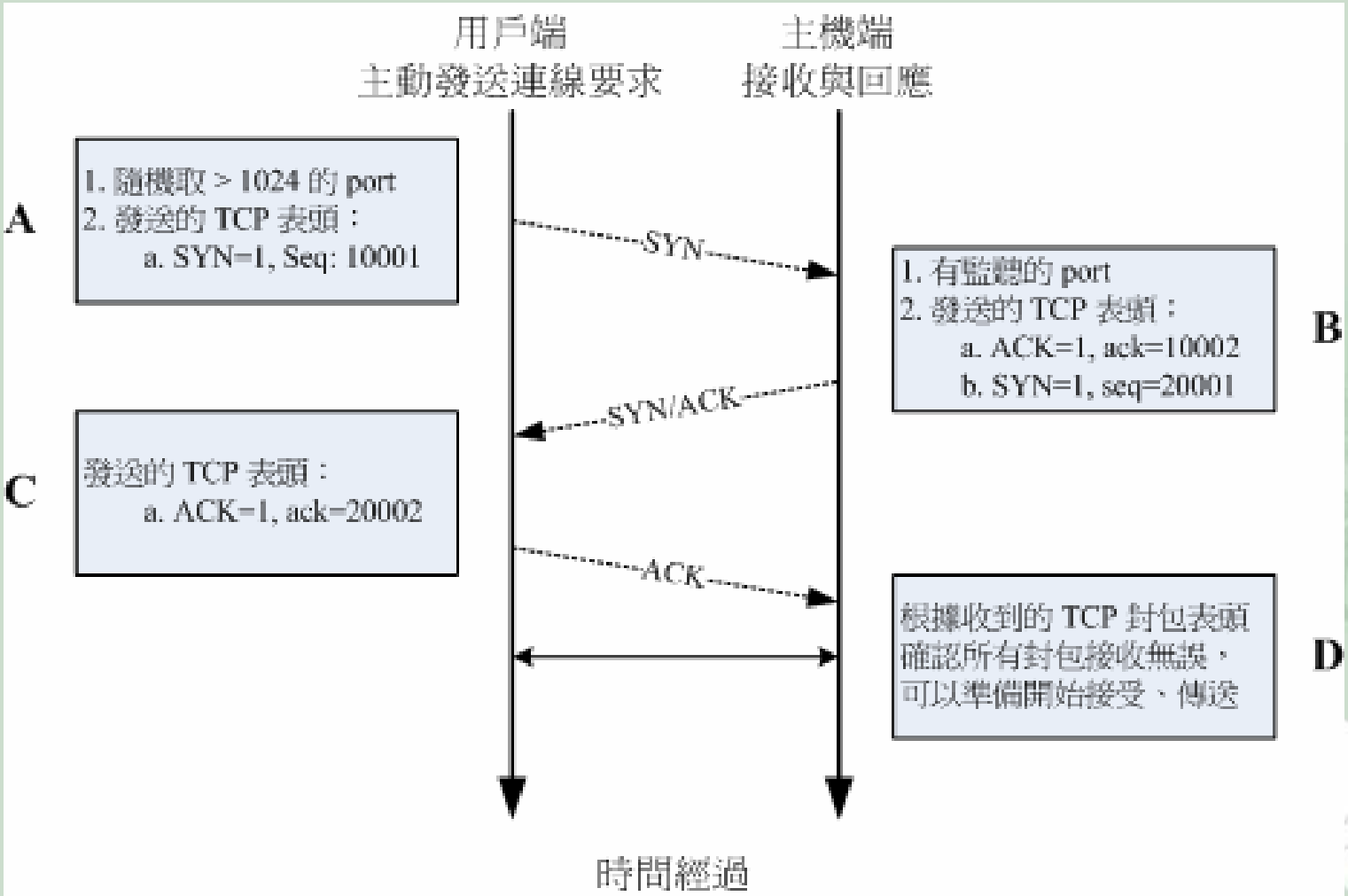
傳輸層的 TCP 封包協定



Port 的功能

- TCP 封包的 port 由應用程式所開啓
- 透過此 port 可讓該應用程式提供服務
- Server端
  - 透過伺服器軟體啓動固定的埠口
  - 常見的服務與埠號定義於 /etc/services
- Client端
  - 由用戶端程式隨機啓動 > 1023 以上的埠口

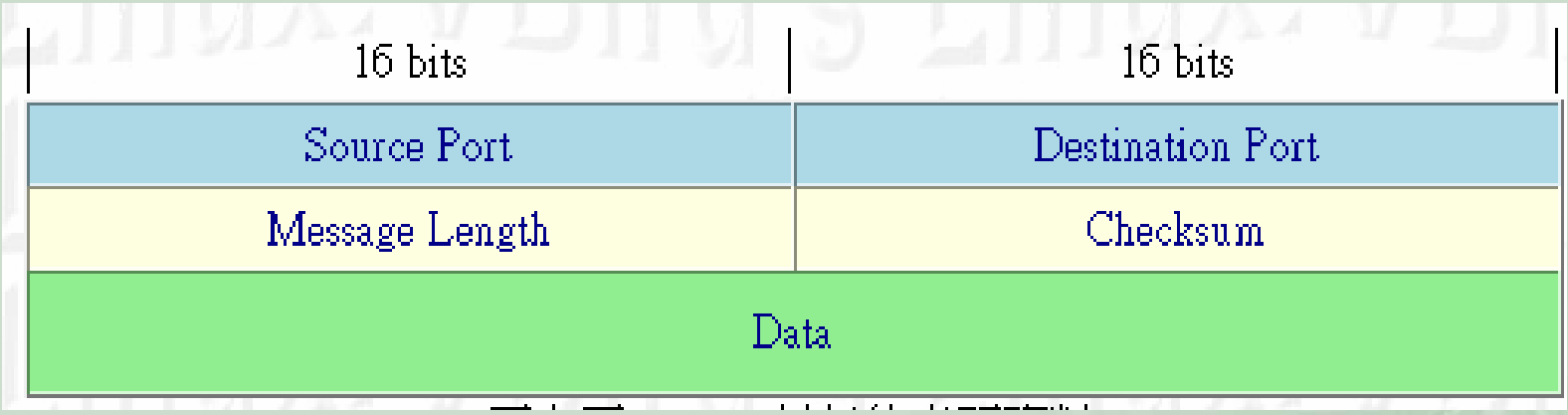
可靠的TCP傳輸機制


用戶端
主動發送連線要求
主機端
接收與回應
A
1. 隨機取 > 1024 的 port
2. 發送的 TCP 表頭：
a. SYN=1, Seq: 10001
SYN
B
1. 有監聽的 port
2. 發送的 TCP 表頭：
a. ACK=1, ack=10002
b. SYN=1, seq=20001
SYN/ACK
C
發送的 TCP 表頭：
a. ACK=1, ack=20002
ACK
D
根據收到的 TCP 封包表頭
確認所有封包接收無誤，
可以準備開始接受、傳送
時間經過

Socket Pair

- 主從架構(Server/Client)常見的網路連線
  - 需要有以下的重要表頭資料
    - 來源 IP
    - 來源 Port
    - 來源協定 (TCP/UDP)
    - 目標 IP
    - 目標 Port
    - 目標協定 (TCP/UDP)

傳輸層的UDP封包



- 表頭資料較少，可容納的Data較多
- 不需透過三向交握，速度較快
- 常用於類似即時通訊軟體的封包格式中

常見 port number 與協定

連接埠口	服務名稱與內容
20	FTP-data，檔案傳輸協定所使用的主動資料傳輸埠口
21	FTP，檔案傳輸協定的命令通道
22	SSH，較爲安全的遠端連線伺服器
23	Telnet，早期的遠端連線伺服器軟體
25	SMTP，簡單郵件傳遞協定，用在作爲 mail server 的埠口
53	DNS，用在作爲名稱解析的領域名稱伺服器
80	WWW，這個重要吧！就是全球資訊網伺服器
110	POP3，郵件收信協定，辦公室用的收信軟體都是透過他
443	https，有安全加密機制的WWW伺服器

主機名稱解析

- 人們不擅長記 IP ，便想出以 hostname 取代 IP 的方法
- 早期以 /etc/hosts 翻譯；
- DNS 系統：
  - 利用一部合法授權的主機來記錄該主管轄範圍內的主機名稱與IP的對應；
  - 當 client 端想要瞭解某主機名稱與 IP 的對應時，就需要到這部 DNS 主機查詢。
  - 若這部主機沒有相關的紀錄，則往上層 DNS 主機去查詢
  - Hostname ←→IP