網路概論與 TCP/IP

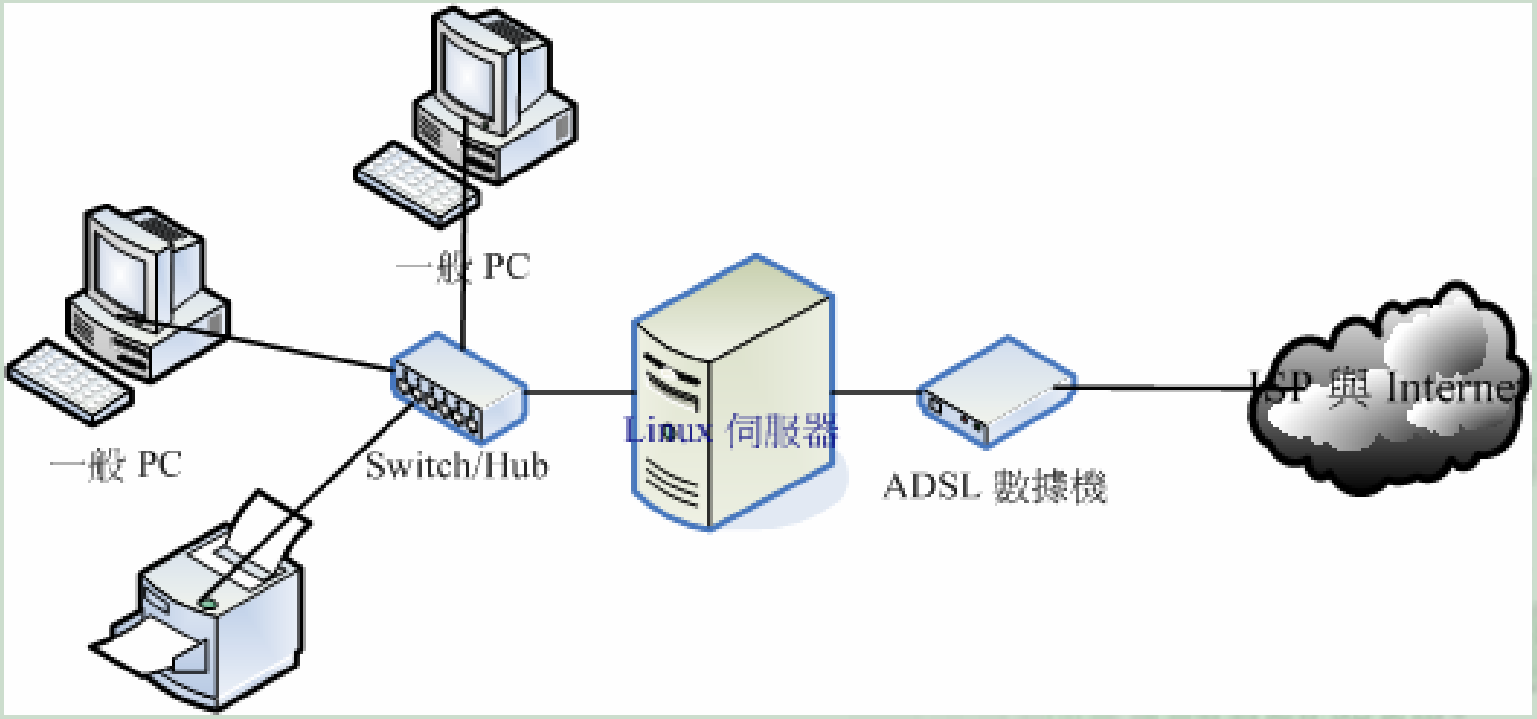
崑山科技大學資訊傳播系
蔡德明
(鳥哥, VBird)

分享指引

- 網路概論與OSI七層協定
- Ethernet 與 CSMA/CD
- TCP/IP
- Linux 與網路相關的檔案/指令

網路概論與OSI七層協定

電腦網路元件



硬體：各節點(node)、各用戶端主機(client)、各伺服器主機(server)、網路介面(Interface)與網卡(Network Interface Card)

通訊協定：各節點之間如何進行溝通？

網路的相關標準

- **IEEE 802 LAN/MAN Standards Committee**
  - http://grouper.ieee.org/groups/802/
  - 主要規範區域網路(LAN)都會網路(MAN)
  - 涵蓋乙太網路(Ethernet), 符記環狀(Token-Ring)
- 重要的標準規範
  - 802.3 Ethernet Working Group
  - 802.11 Wireless LAN Working Group

電腦網路的種類

- 廣域性電腦網路(wide area network, WAN)
  - 電腦網路連結的地區範圍較廣，如整個台灣構成網路或國際間網路
- 大都會網路(metropolitan area network, MAN)
  - 電腦網路分散在一個城市之範圍
- 區域網路(local area network)
  - 電腦分散在較小的區域範圍內，如一棟大樓或校園區域內

電腦網路的種類(續)

- 廣域性電腦網路(wide area network, WAN)
  - 傳輸距離較遠，因此採用的傳輸媒體較便宜、品質較差，如電話線、無線電波等等。
  - 網路可靠度(reliability)較低。
  - 傳輸速率較慢。
  - 應用上較受限制，一般應用於：e-mail、file transfer、 Web 瀏覽等等

電腦網路的種類(續)

- 大都會網路(metropolitan area network, MAN)
  - 傳輸距離雖稍遠但固定某一區域，可採用品質較高、可靠性較高的傳輸媒體。
  - 傳輸速率較快。
  - 一般應用於：辦公自動化、VOD (Video-on-Demand) 等等

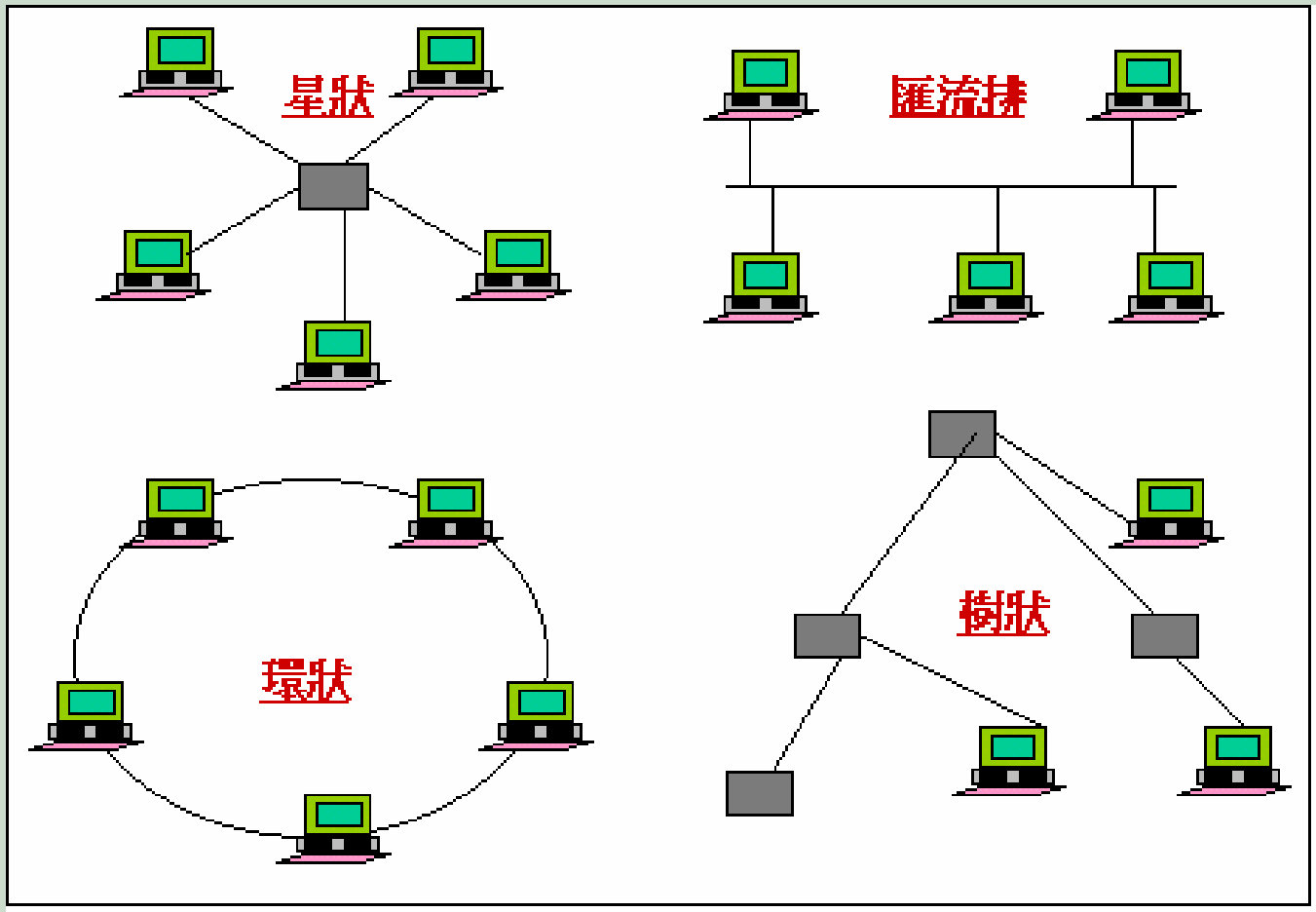
電腦網路的種類(續)

- 區域網路(local area network)
  - 因傳輸距離較近，網路上可使用較昂貴的傳輸媒體，傳輸速率較高、線路品質較好穩定性較高，因此可較高階、較廣的應用。
  - 網路可靠性較高。
  - 一般應用於：分散式處理、負荷分擔、以及工廠自動化等等

電腦網路的種類(續)

- 如何區分這些網路架構？
  - 網路範圍大小牽涉到使用傳輸媒體的限制，因而影響到傳輸速率和網路的可靠度，也限制網路應用得層次
  - 評估一個網路的大小以區域範圍來區分並不完全正確，應以傳輸速率及品質來區分也許較正確。
  - 也因此近來談論網路架構大部分以速率來表示，不再以區域大小表示

區域網路之拓樸(topology)



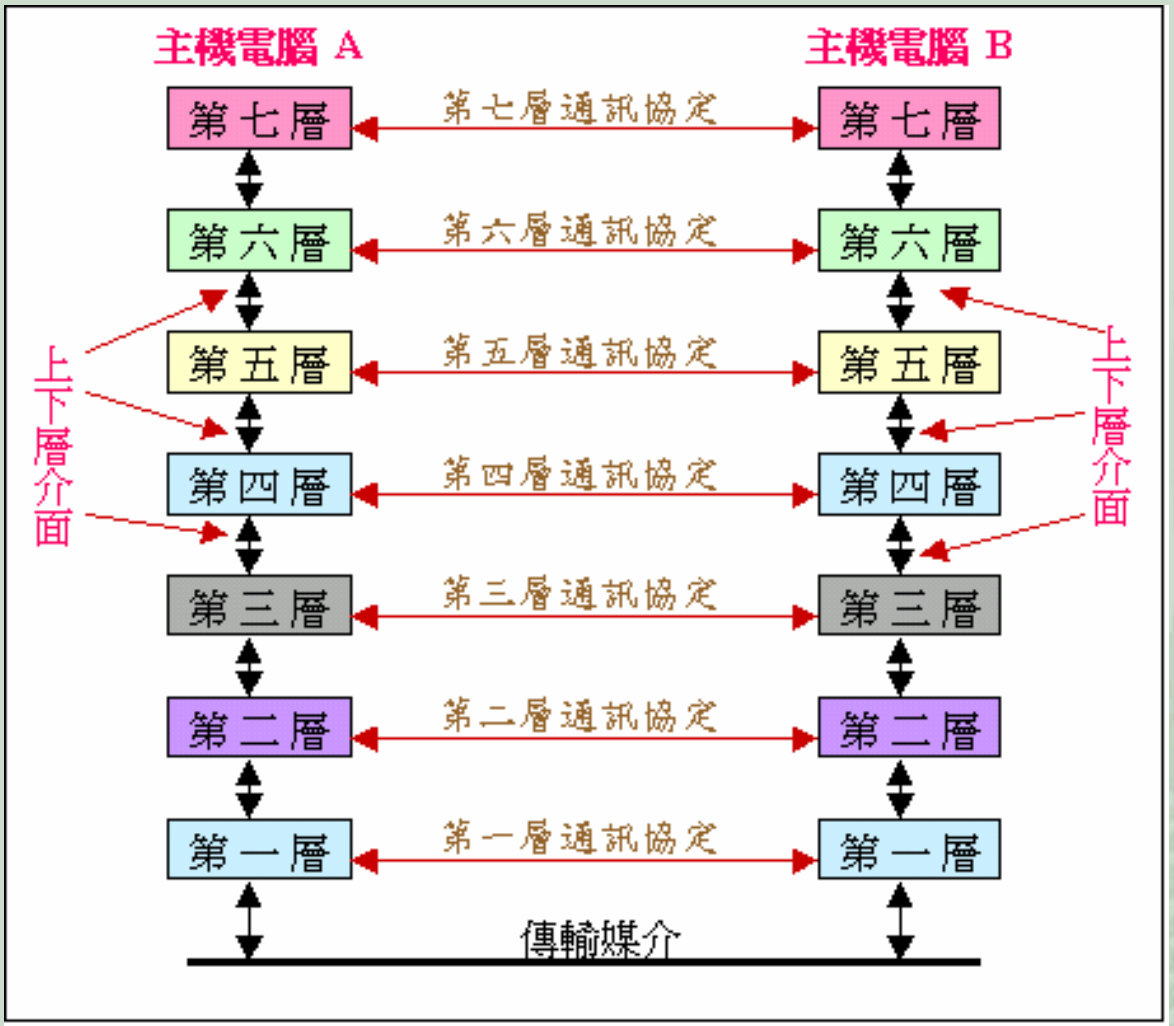
電腦通訊協定

- 何謂協定？
  - 以某種大家所認同的方法來互相溝通稱之爲協議，如果這些協議被大家所認定的固定標準稱之爲協定。
- 何謂電腦通訊協定
  - 定義電腦間互相通訊的共同認定之標準程序，網路上各個電腦依照此標準來互相通訊，使電腦間各個電腦能夠了解其它電腦的表達意思，並能完成其共同的任務(job)。

通訊協定的特性

- 階層性(Hierachical)或層次性(Layered)
  - 將一件非常大的事情 分割成許多獨立的實體，各個實體分別用各自獨立的程式來實現。
- 層次的功能性(Funcationality)
  - 每一層次處理某一特定功能，各個層次間的功能不與其他層相衝突。
- 層次的隔離性(Isolationality)
  - 上下層次間沒有絕對的從屬關係，不會因上下層的更動而影響本層次的功能。(堆疊的原理)

Peer-to-Peer Protocol



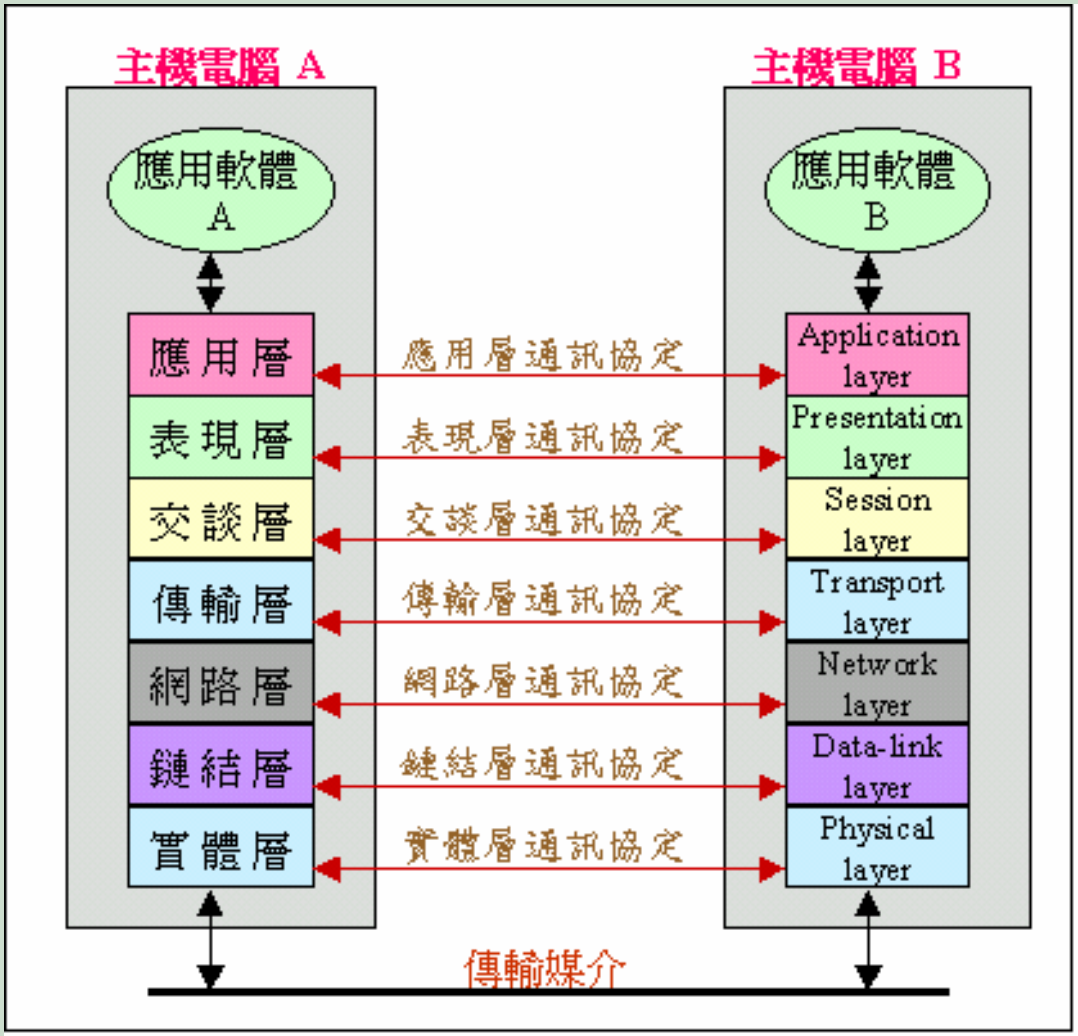
電腦間同一階層次 (如第六層對對方第六層) 的通訊協定，亦是電腦間相對(peer-to-peer)層次間必須協議出共同的工作模式稱爲前端對前端協定。

不對稱的層次間 (如第六層和對方第七層或第五層) 沒有關係。

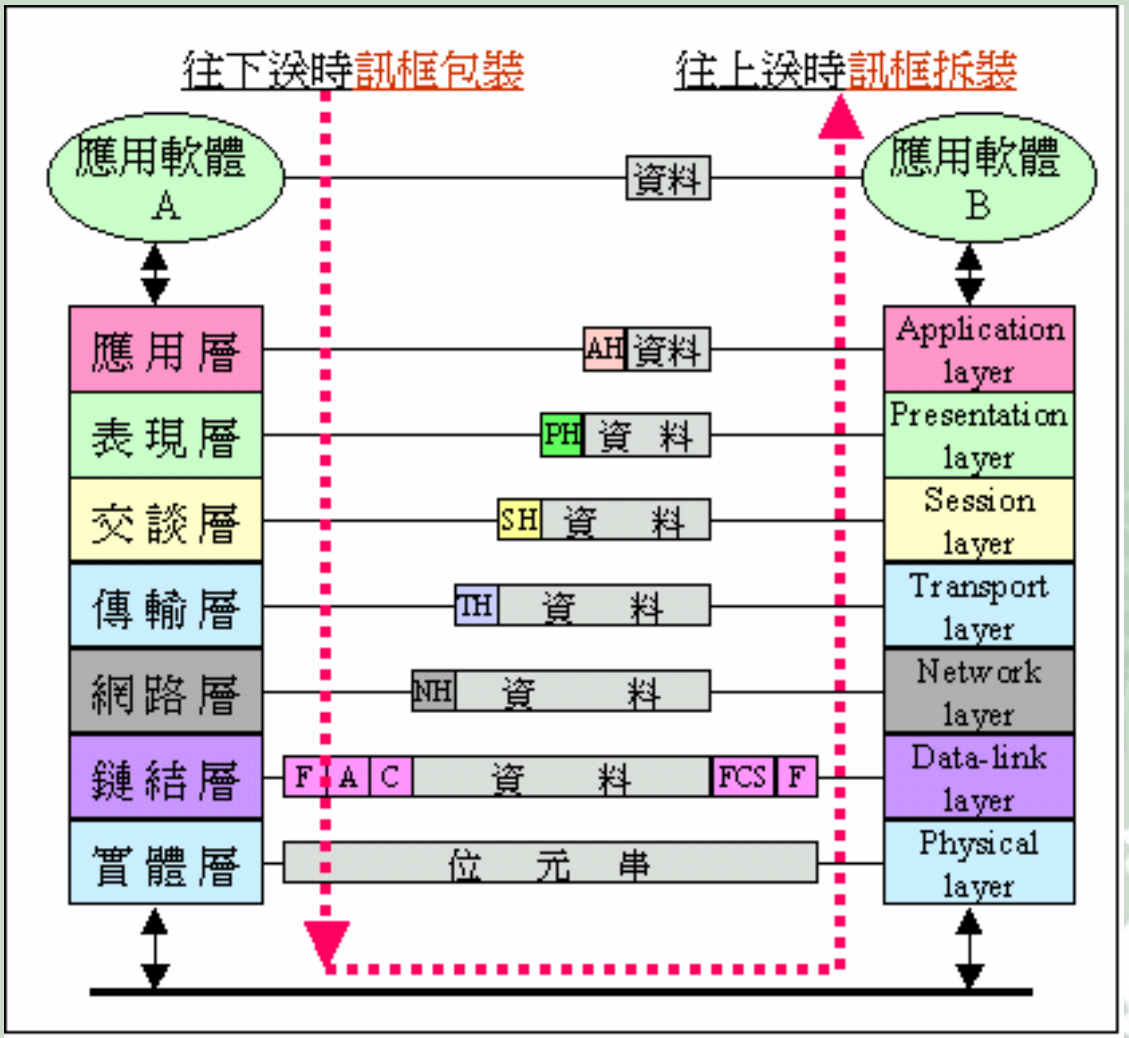
OSI七層協定

- 國際標準組織(International Standards Organization, ISO)
  - 1978年制定『開放式系統連結』 (OSI, Open System Interconnected)

OSI七層協定


主機電腦 A
主機電腦 B
應用軟體 A
應用軟體 B
應用層
表現層
交談層
傳輸層
網路層
鏈結層
實體層
Application layer
Presentation layer
Session layer
Transport layer
Network layer
Data-link layer
Physical layer
應用層通訊協定
表現層通訊協定
交談層通訊協定
傳輸層通訊協定
網路層通訊協定
鏈結層通訊協定
實體層通訊協定
傳輸媒介

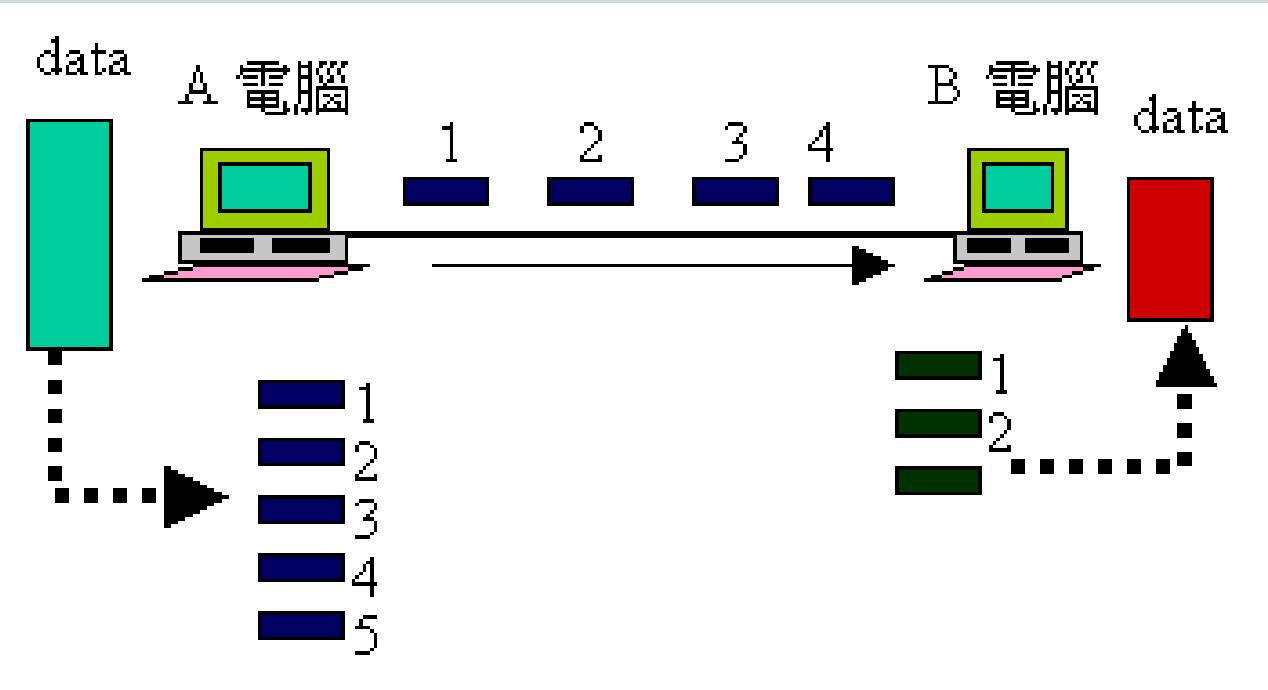
OSI協定的包裝/拆解流程



OSI-實體層

- 實體層任務：
  - 透過編碼將來自上層的資料以電子訊號傳送出去
- 常見的傳輸媒體
  - 雙絞線➔如 RJ45 網路線
    - 雙絞線是包含有兩條絞在一起、互相絕緣的導線，價格較便宜、佈線簡單
    - 可分爲『遮蔽式雙絞線』(Shielded Twisted Pair, STP)和『無遮蔽式雙絞線』(Unshielded Twisted Pair, UTP)
  - 同軸電纜線
  - 光纖
  - 無線傳輸：無線電廣播、微波、紅外線、衛星

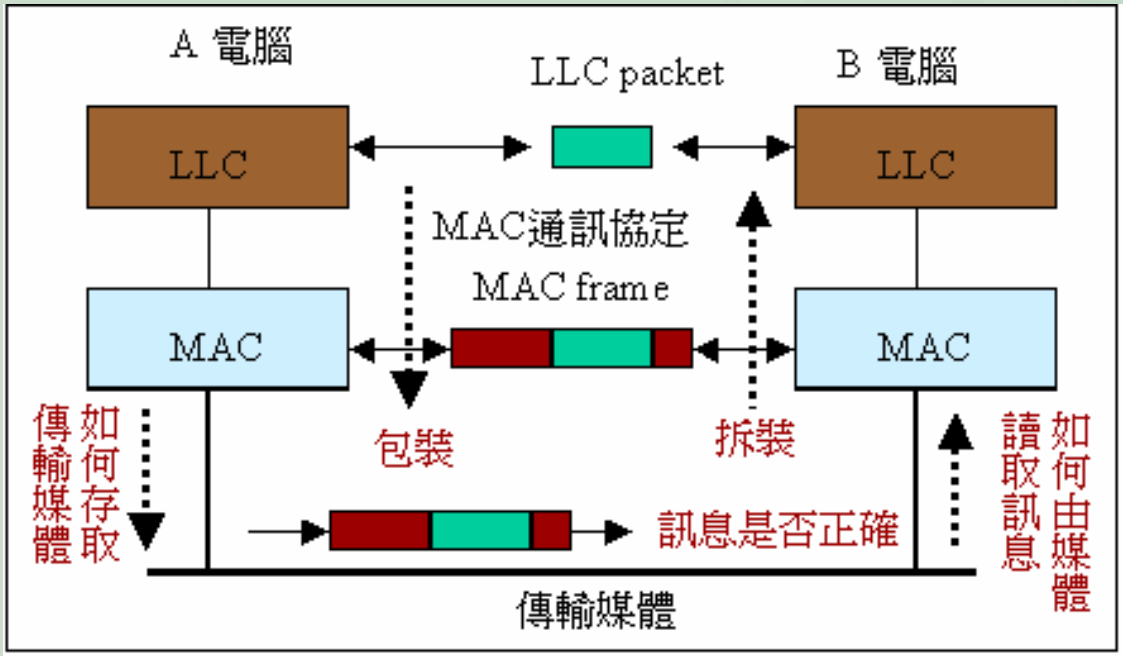
OSI-資料連結層



- 封包(packet)
  - 大的檔案會被拆解成數個小封包再一個個傳送到網路媒體傳輸出去
- 訊框(frame)
  - 儲存媒體所能傳輸的資料包稱爲訊框

OSI-資料連結層

- 資料連結層的MAC (Media Access Control)
  - MAC必須依照某種通訊協定來取得傳輸媒體的使用權，例如 802.3 的乙太網路標準。



OSI-網路層

- 網路層功能：
  - 負責處理如何將資料由一部電腦傳給另一部電腦的路徑選擇 (routing)的問題。
  - 建立、維護、以及結束兩部電腦間的連線 (connection)。
- 重要資料項目
  - Internet Protocol (IP)：含network, broadcast, netmask 等IP參數
  - Route ：路由判斷機制

OSI-傳輸層

- 傳輸層任務：
  - 當Server/Client之間的連線建立後，傳輸層要提供適當的通訊品質，並且監督資料傳輸的過程以保證該通訊品質的維持。如無法達到必須通知使用者。
  - 讓某一電腦中的某一程式(如telnet)和另一部電腦內的某一程式(telneted)連線，這便是傳輸層所主要提供的服務。(需要有 port)

OSI-傳輸層

- 傳輸層主要服務類型：
  - 連接導向(connection-oriented)：
    - 資料傳送前，雙方先要求連線並經對方同意後再傳送資料。如 TCP 封包
  - 非連接導向(connectionless, or datagrame)：
    - 資料傳送前，雙方並未先前連線。如 UDP 封包
- 定址方式：
  - 透過 port number
  - 168.95.1.1:53

OSI-會談層

- 會談層負責的任務：
  - 提供服務來達成許多使用者之間對談(dialog)的組成、同步、以及管理使用者之間資料的傳送。
  - 根據使用者可否同時傳送資料或接收資料，來控制使用者何時可以傳送或接收資料，既達到所謂的同步交談的功能。

OSI-會談層

- 對談連線 (dialog-to-dialog connection) ：
  - 提供應用層通訊的控制結構，包括交談的建立、管理、終止、並支援檢查點、重新啓動等功能。
  - 各層連線的意義：
    - 網路層提供工作站對工作站間的連線；
    - 傳輸層提供工作站內使用者(程式)對使用者間的連線；
    - 交談層提供使用者內對話的連線(dialog-to-dialog connection)。

OSI-表現層

- 表現層任務：
  - 負責將資料以有意義的型式表達給網路使用者，其工作可能包含：
    - 字元碼的轉換 (如 ASCII 轉換成 EBCDIC 碼
    - 資料的壓縮(compression)以及還原(expansion)
    - 資料的加密(encryption)以及解密(decryption)。

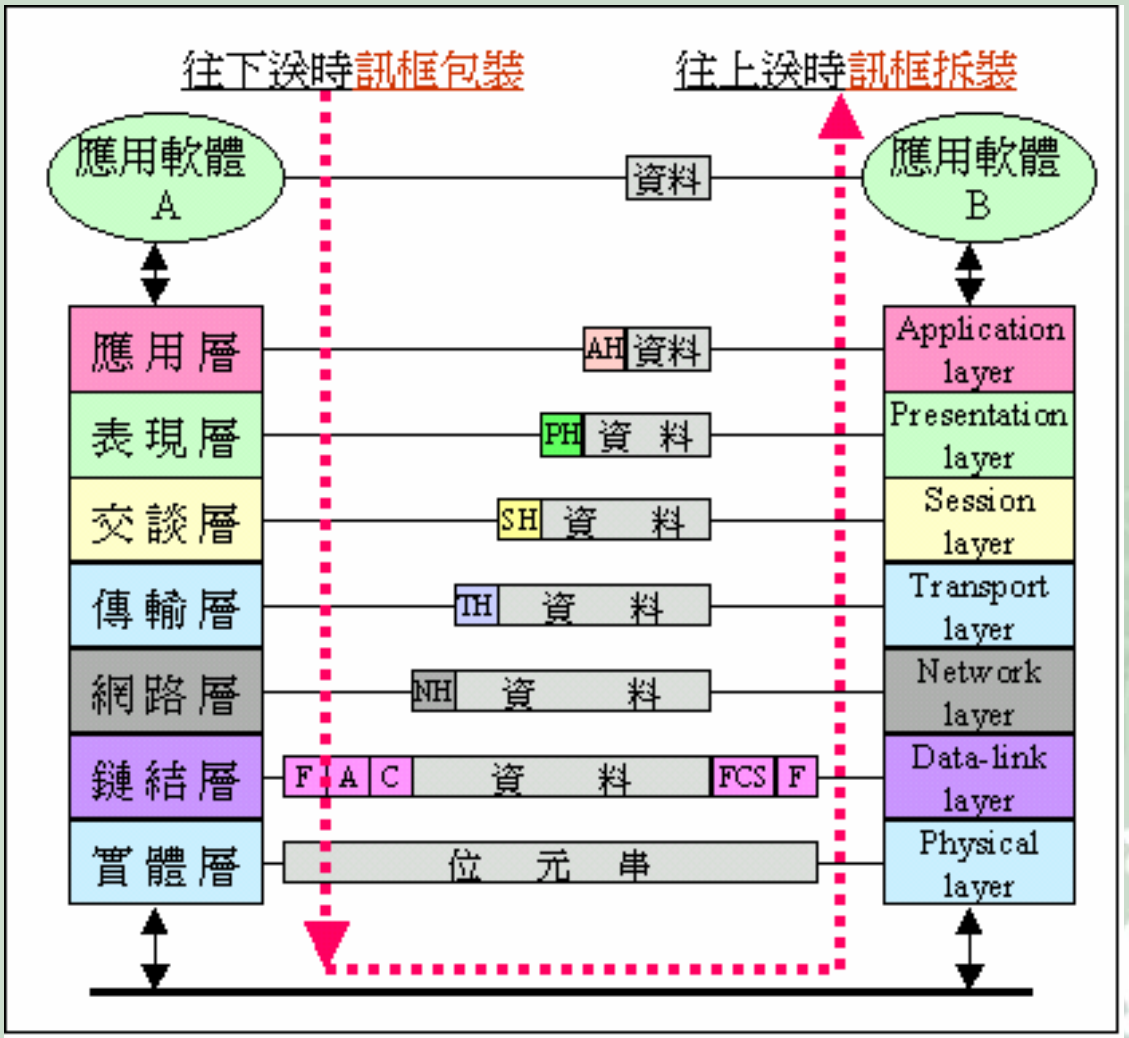
OSI-應用層

- 應用層任務：
  - 負責提供各種服務給應用程式 (application processes)，使其能夠使用系統之連結功能來達到和其他應用程式交換資料的目的。
  - 應用層提供了使用者或使用者程式與網路溝通的介面。例如：
    - 檔案傳送通訊協定 (file transfer protocol)，
    - 網路管理軟體 (network management)。

OSI-應用層

- 網路應用程式：
  - Server：提供網路各項資源讓其他用戶端使用，如FTP, WWW, Mail, Printer server 等
  - Client：使用程式連結到伺服器以取得所需資源，如gftp, browser (firefox..), thunderbird
- 常見公用程式：
  - 網路偵測： ping, traceroute
  - IP參數設定： ifconfig, ifup, ifdown
  - 路由觀察與設定：route
  - 埠號與連線查閱： netstat

OSI協定的包裝/拆解流程



Ethernet 與 CSMA/CD

乙太網路(Ethernet)

- 乙太網路由來：
  - 1972年由Digital公司、Intel公司和Xerox公司共同制定Ethernet規格。
  - 與IEEE 802.3 CSMA/CD標準相容性高。
  - 目前所談的**CSMA/CD**規格反而以Ethernet標準爲主。
  - 目前區域網路架構絕大部份以架設Ethernet網路爲主，已成爲標準介面可裝設在各種不同網路作業系統上。

CSMA/CD 協定

- 透過廣播：共享媒體上任何電腦皆可接收到
- Carrier Sense：傳送資料前需經過監聽(listen)
- Collision Detection：判斷是否有跟其他工作站碰撞
  - 如有碰撞便馬上退回不再傳送，等待某一隨機時間 (Random Time) 再繼續listen；否則繼續傳送。
- 在同一網路上可能有多個工作站在 carrier sense 準備要傳送，也可能在傳送途中與其他工作站發生碰撞。
- 任何一部工作站，其不是在傳送資料時，便是在接收資料。若收到的資料非為自己則予以丟棄。

乙太網路訊框格式

前導碼 8 Bytes	目的位址 6 Bytes	來源位址 6 Bytes	資料欄位通訊 2 Bytes	主要資料 46-1500 Bytes	檢查碼 4 Bytes

- 資料長度
  - 資料長度最大爲 1500bytes，最小需要 46bytes
  - 46bytes的來源：
    - 由CSMA/CD的原理，選相隔最遠的兩點可能發生碰撞的情況下，計算出最小的訊框需要**64bytes**；
    - 46=64-6-6-2-4(不含前導碼)
- 位址的格式：
  - 00:11:22:33:BB:FF

標準速度

- 乙太網路的標準速度爲
  - 乙太網路： 10Mbps(Mbits/second)
  - 高速乙太網路： 100Mbps(Mbits/second)
  - 超高速乙太網路： 1000Mbps(Mbits/second)

TCP/IP

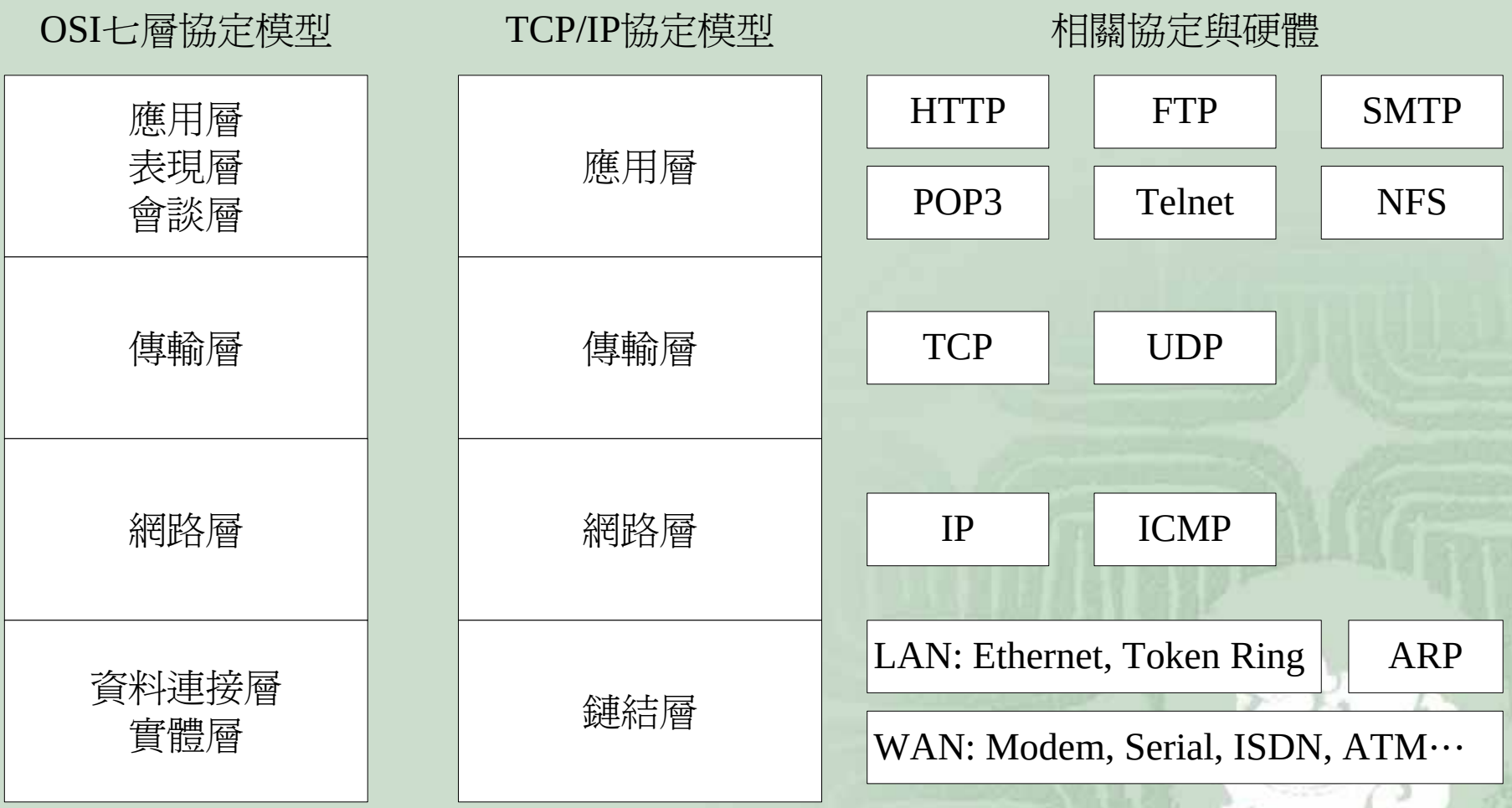
OSI七層協定與TCP/IP

- 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



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
....
```

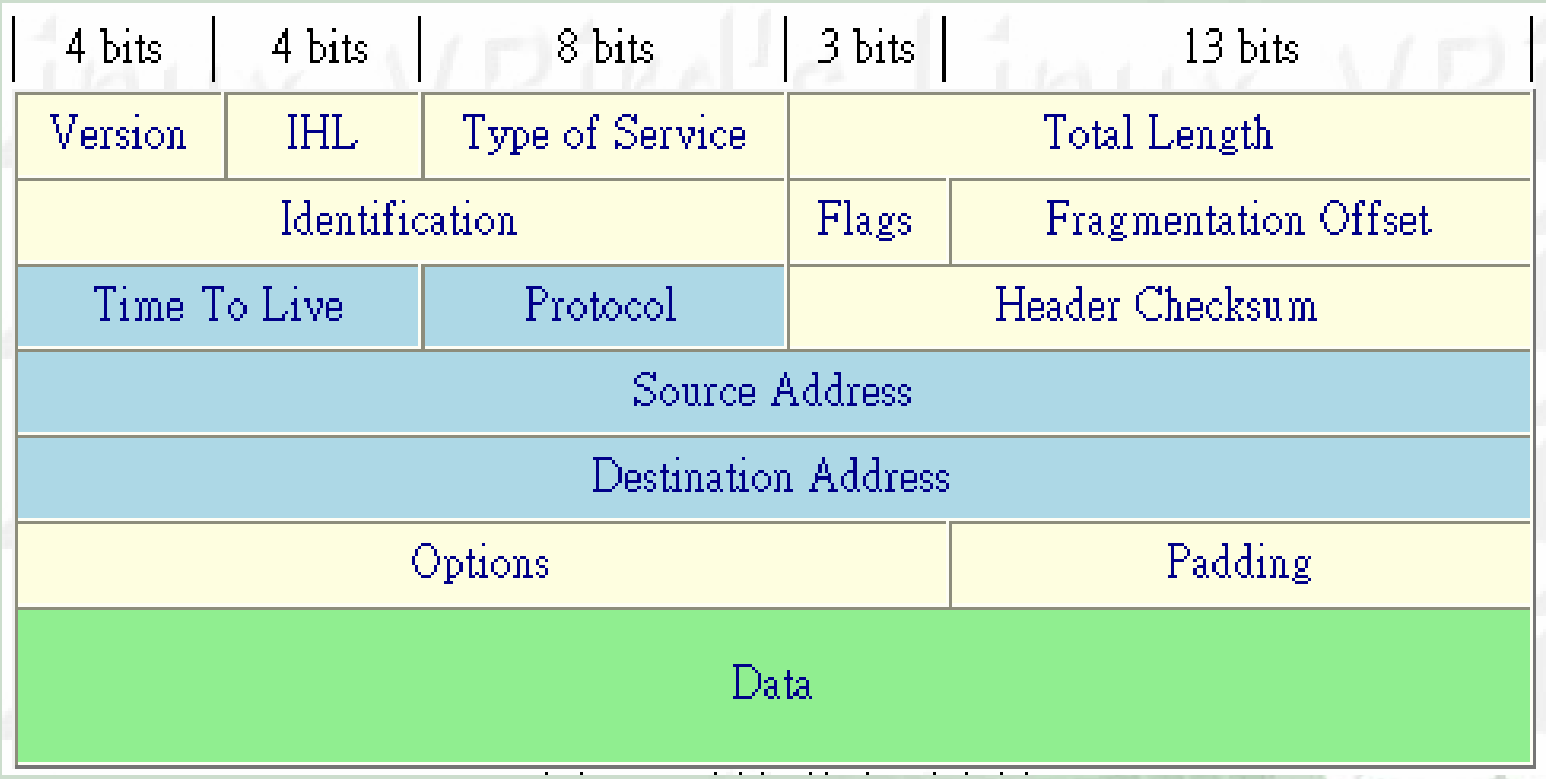
鏈結層的 ARP協定

- 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***

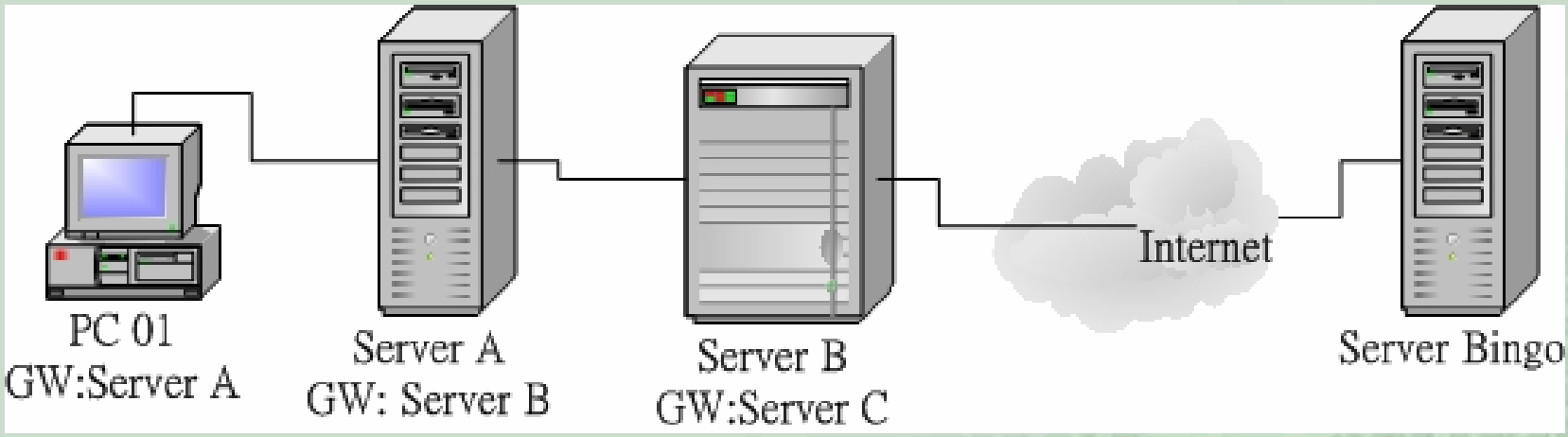
IP 的種類

- 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)

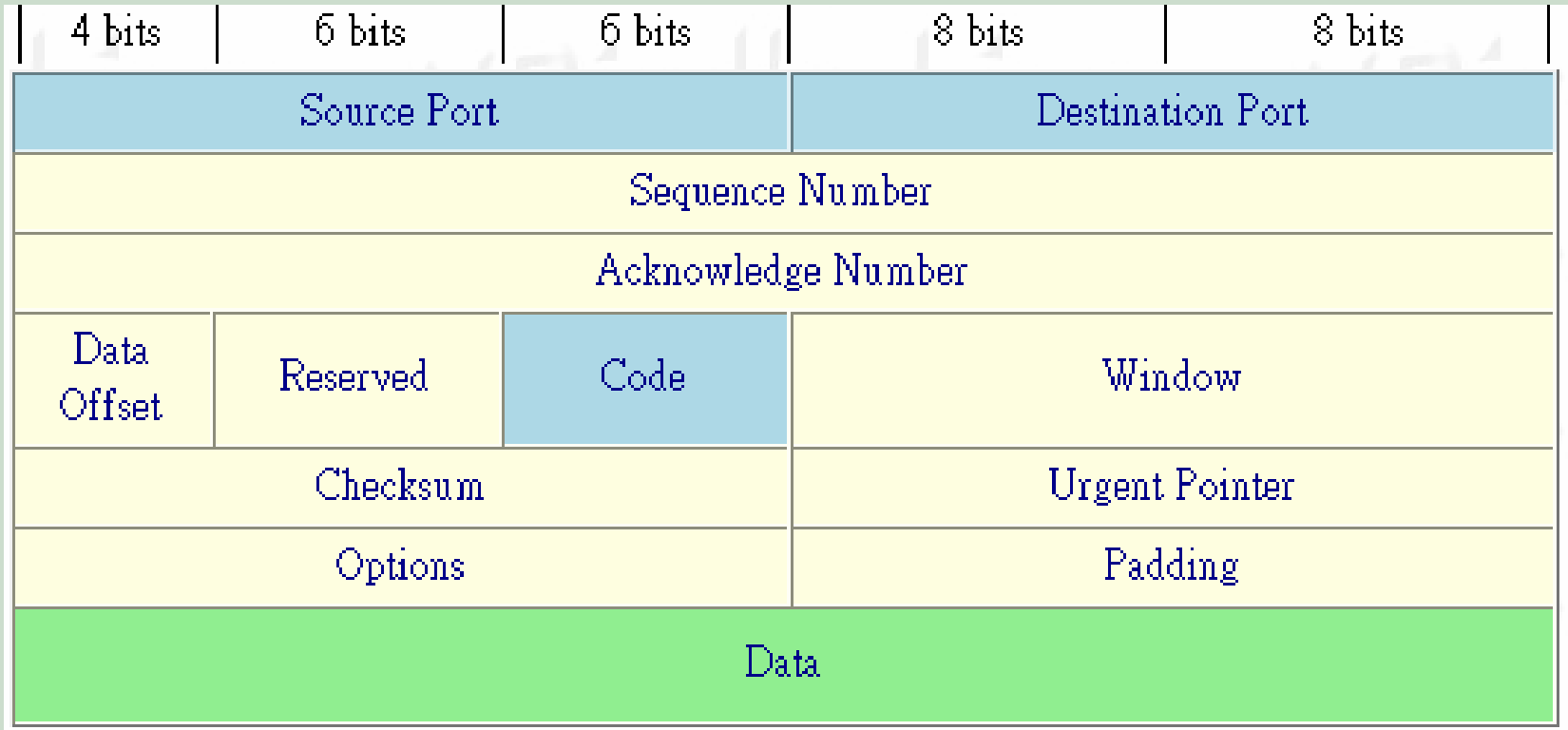
使用 ping 檢測網路狀態

```
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

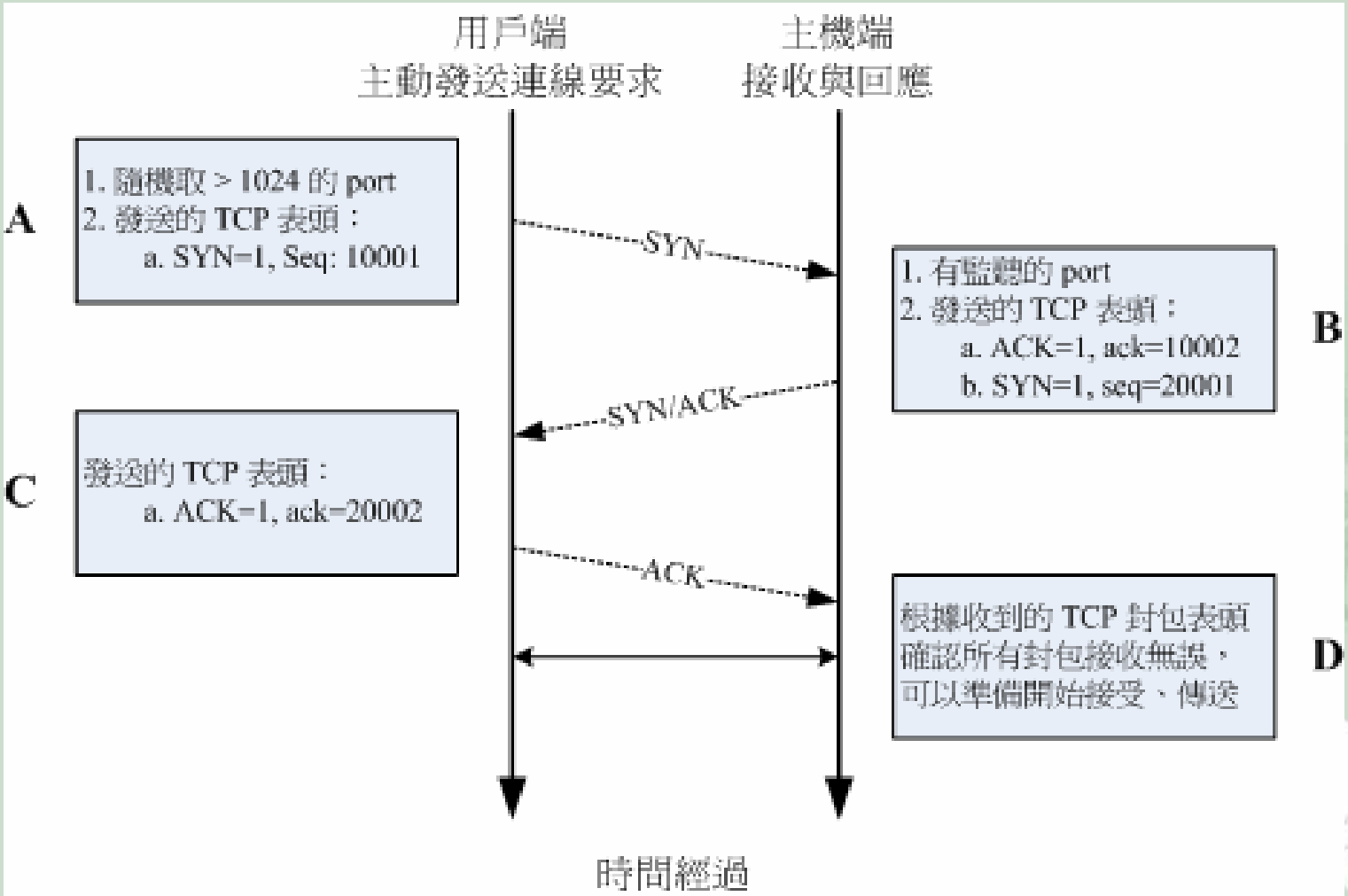
傳輸層的 TCP 封包協定



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

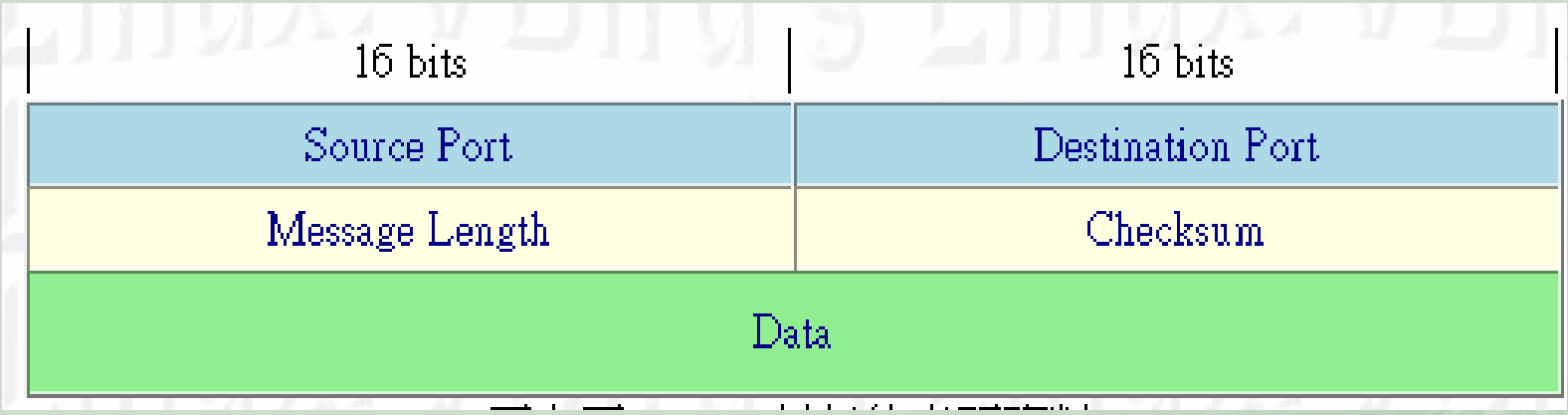
可靠的TCP傳輸機制


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
1. 有監聽的 port
2. 發送的 TCP 表頭：
a. ACK=1, ack=10002
b. SYN=1, seq=20001
B
SYN/ACK
C
發送的 TCP 表頭：
a. ACK=1, ack=20002
ACK
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
D
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

Linux 與網路相關的檔案/指令

所需要的網路參數

- TCP/IP 的網路參數
  - IP
  - Netmask → 可由 IP/Netmask 算出Network, Broadcast
  - Gateway (router)
- 需要主機名稱(如網址列)
  - 私有IP的主機名稱對應
  - Internet的IP與主機名稱對應 (DNS系統)

與網路相關設定檔

參數	檔案
主機名稱	/etc/sysconfig/network
IP參數	/etc/sysconfig/network-scripts/ifcfg-eth0
DNS	/etc/hosts
	/etc/resolv.conf
啓動腳本	/etc/init.d/network restart

主機名稱設定

- /etc/sysconfig/network
  - NETWORKING=yes
  - NETWORKING_IPV6=no
  - HOSTNAME=localhost.localdomain
  - GATEWAY=192.168.1.254
- 指令的依據
  - reboot
  - hostname localhsot.localdomain
  - route -n → netstat -r

IP參數的設定

- /etc/sysconfig/network-scripts/ifcfg-eth0
  - DEVICE=eth0
  - HWADDR=00:08:A1:04:98:88
  - IPADDR=203.71.39.250
  - NETMASK=255.255.255.0
  - ONBOOT=yes
- 指令依據
  - ifconfig eth0 up → ifconfig eth0 down
  - ifup eth0 → ifdown eth0
  - /etc/init.d/network restart

主機名稱解析的檔案

- 內部私有 IP ➔ /etc/hosts
  - 127.0.0.1　　localhost　　localhost.localdomain
  - 10.0.0.1　　mysite kiki
- Internet 的主機名稱對應 ➔ /etc/resolv.conf
  - search dic.ksu.edu.tw
  - nameserver 168.95.1.1
- 測試指令
  - dig linux.vbird.org
  - host linux.vbird.org
  - nslookup linux.vbird.org

網路偵測的指令

- 偵測兩部主機間的連線情況
  - ping –c 次數 主機名稱或IP
  - ping –c 3 168.95.1.1
- 兩部主機間各節點的連線狀態
  - traceroute 主機名稱或IP
  - traceroute 168.95.1.1
- 監聽網路介面所能聽到的所有封包資料
  - tcpdump –i eth0 參數
  - tcpdump –i eth0
  - tcpdump –i eth0 port 25

參考資料

- 粘添壽老師個人網站：http://www.tsnien.idv.tw/
- IEEE官網：http://grouper.ieee.org/groups/802/dots.html