

經濟部資訊專業人員鑑定—開放式系統類

Linux 基礎運作—網路概論與 TCP/IP

崑山科技大學資訊傳播系

蔡德明

(鳥哥, VBird)

證書名稱與應考科目

- Linux維運管理專業人員
 - ☞Linux 基礎運作 (ILA)
 - ☞Linux 進階系統管理 (ILB)
- Linux服務整合專業人員
 - ☞Linux 基礎運作 (ILA)
 - ☞Linux 進階系統管理 (ILB)
 - ☞Linux 開放網路應用服務整合(ILC)



Linux基礎運作主要鑑定項目

- 電腦系統以及網路通訊的基本觀念技術與原理
- TCP/IP通訊協定原理與設定
- Linux安裝準備、安裝程序與安裝設定
- Linux基本常用指令與工具
- 硬碟、檔案、程序及印表機管理方式與工具
- 使用者帳號、群組帳號之建立與管理



『Linux基礎運作』細部規範

- Introduction to network
- TCP/IP protocol
- Linux installation and setup
- Introduction of shell and basic shell command
- Linux system configuration
- Basic command of disk management
- Account management
- Process introduction
- Printer setup and management
- X window
- Editor



分享指引

- Linux與自由軟體
- 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
- 精選範例





Linux 與自由軟體

什麼是自由軟體

- Free software，重點在Freedom
 - ∞自由的取得
 - ∞自由的修改與複製
 - ∞自由的運作
 - ∞自由的再發行



自由軟體的發展緣由

- 1984年，Richard Stallman (史托曼)
 - ∞ 因為想要保留駭客文化『共享』的精神；
 - ∞ 想要製作出一個『自由的作業系統』；
 - ∞ 利用Unix作為最初的啓始點；
 - ∞ 推展 GNU 計畫；
 - <http://www.gnu.org>；
 - **GNU's Not Unix** → 無窮迴圈啦！



GNU計畫的重要軟體

- 發展出許多可在**Unix**上面跑的重要軟體：
 - ☞ Bash shell (人與機器互動的介面)
 - ☞ GCC (程式編譯的編譯器)
 - ☞ Emacs (撰寫程式的編輯器)
 - ☞ Glibc (C程式語言的函式庫)
 - ☞ ...
 - ☞ <https://www.fsf.org/resources>



自由軟體的保護

- 如何保護自由軟體 → 透過授權
 - ☞ GNU 的 GPL (General Public License)
 - ☞ 也稱爲 Copyleft (針對 Copyright 來的)

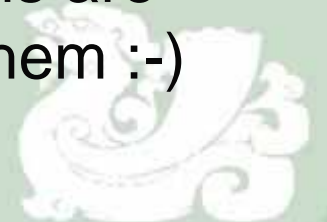


其他開放原始碼的授權

- GNU GPL (version 2, version 3)
 - ☞ <http://www.gnu.org/licenses/licenses.html#GPL>
- Apache License
 - ☞ <http://www.apache.org/licenses/LICENSE-2.0>
- BSD
 - ☞ <http://www.xfree86.org/3.3.6/COPYRIGHT2.html#5>
- FreeBSD
 - ☞ <http://www.freebsd.org/copyright/freebsd-license.html>

Linux的發明者

- Linus Torvalds自己的BBS說明：
 - ☞ Hello everybody out there using minix-
 - ☞ I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones.....
 - ☞ I've currently ported bash (1.08) and gcc (1.40), and things seem to work. This implies that i'll get something practical within a few months, and I'd like to know what features most people want. Any suggestions are welcome, but I won't promise I'll implement them :-)



Linus Torvalds

- http://en.wikipedia.org/wiki/Linus_Torvalds

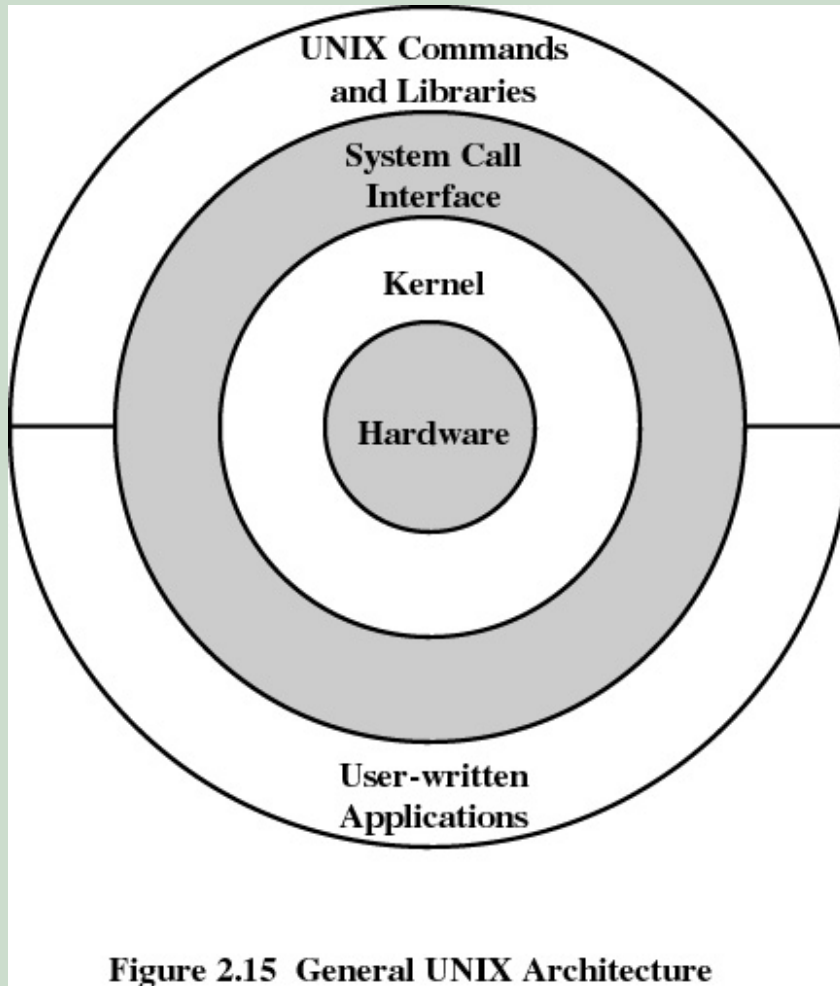


Linux是什麼？

- **Linux** 就是一套作業系統
 - ∞ 提供合理的硬體資源管理
 - ∞ 可驅動大部分的硬體配備
 - ∞ 提供很多的開發介面讓程式設計師使用
 - ∞ 程式設計師只要知道能夠使用何種程式語言在 **Linux** 上頭進行編譯即可。



軟體與作業系統



作業系統的功能：

1. 有效率、合理的管理硬體資源，就是Kernel的部分
2. 提供一個合適的開發介面，就是System Call的部分



Linux 發展簡史

- 1971 ~ 1973 Bell Lab 開發 C 寫出 Unix
- 1984 Minix 的發展(教育版本的Unix)
- **1984 GNU (Gnu is Not Unix) 計畫推行**
 - ☞ 發展 Free 的 Unix，推出多個軟體
- 1988 XFree86 計畫
 - ☞ X + Free + x86 → X11
- 1991 Linux 釋出 (386, Gnu bash gcc, minix)
- 1994 Linux version 1.0 釋出
- 1994 Linux distributions 開始發展



Linux distributions

- Linux distributions

 - ☞ kernel + software + tools + 完整安裝流程

- 企業版本

 - ☞ Red Hat Enterprise Linux (RHEL), Novel SuSE

- 社群版本

 - ☞ CentOS, Fedora, Debian, B2D, Ubuntu....



Linux的成功之道

- Unix (Minix) 作業系統的設計概念
- GNU 周邊工具軟體的來源
- x86 實際運作的硬體配備
- Internet 虛擬團隊及錯誤回報的分享
- POSIX 核心設計的標準規範
- Distributions 尤其是一些知名的商業、社群



Linux的設計理念

- 將複雜的任務分給多個單純的小程式去負責
 - ∞ 因為每個小程式的功能單純，效能較佳
- Everything is file
 - ∞ 所有資源都以檔案的形態存在
 - ∞ 檔案主要依據目錄樹的方式來管理
 - ∞ 最頂層為根目錄 (/)，又稱為 root
 - ∞ 只要管理『裝置檔』的『權限』即可管理硬體

Linux的當前應用

- 個人環境的使用：
 - ☞ 桌上型電腦(Desktop)
 - ☞ 手持系統(手機、PDA等)
 - ☞ 一般家電設備
- 企業環境的利用：
 - ☞ 一般小型伺服器運作
 - ☞ 關鍵任務應用(金融資料庫、大企業網管環境)
 - ☞ 學術機構的高效能運算任務

學習的方法

- 學習軟體而不是學習指令
 - ☞ 每個軟體都有其任務，指令只是爲了達成任務
 - ☞ 指令都有 **man** 可用，每個軟體都有文件資料
 - **man** 有中文化的計畫喔！
 - <http://cle.linux.org.tw/CLDP/cldp.html>



man page 的範例

The image shows two terminal windows side-by-side. The left window displays the man page for 'bash', and the right window displays the man page for 'newgrp'.

```

vbird@dic-test:~ [54x26]
連線(C) 編輯(E) 檢視(Y) 視窗(W) 選項(O) 說明(H)
BASH(1)
          BASH(1)
NAME
  bash - GNU Bourne-Again Shell
SYNOPSIS
  bash [options] [file]
COPYRIGHT
  Bash is Copyright (C) 1989-2005 by the
  Free Software Foundation, Inc.
DESCRIPTION
  Bash is an sh-compatible command language
  interpreter that executes commands read
  from the standard input or from a file.
  Bash also incorporates useful features
  from the Korn and C shells (ksh and csh).

  Bash is intended to be a conformant
  implementation of the IEEE POSIX Shell
  and Tools specification (IEEE Working
  Group 1003.2). Bash can be configured to
  :

vbird@dic-test:~ [54x26]
Linux Programmer's Manual
NEWGRP(1)
          NEWGRP(1)
NAME
  newgrp - 登入到新的使用者組中
總覽 (SYNOPSIS)
  newgrp [ group ]
描述 (DESCRIPTION)
  Newgrp 改變調用者的使用者組標識，類似
  於 login(1)。調用者仍舊登入在系統
  中，當前目錄也不變，但是檔案的訪問權限
  將根據新的使用者組 ID 計算。

  如果沒有指定使用者組，GID 將變成登入
  的 GID。
檔案 (FILES)
  /etc/group
  /etc/passwd
另見 (SEE ALSO)
  login(1), group(5)
  :

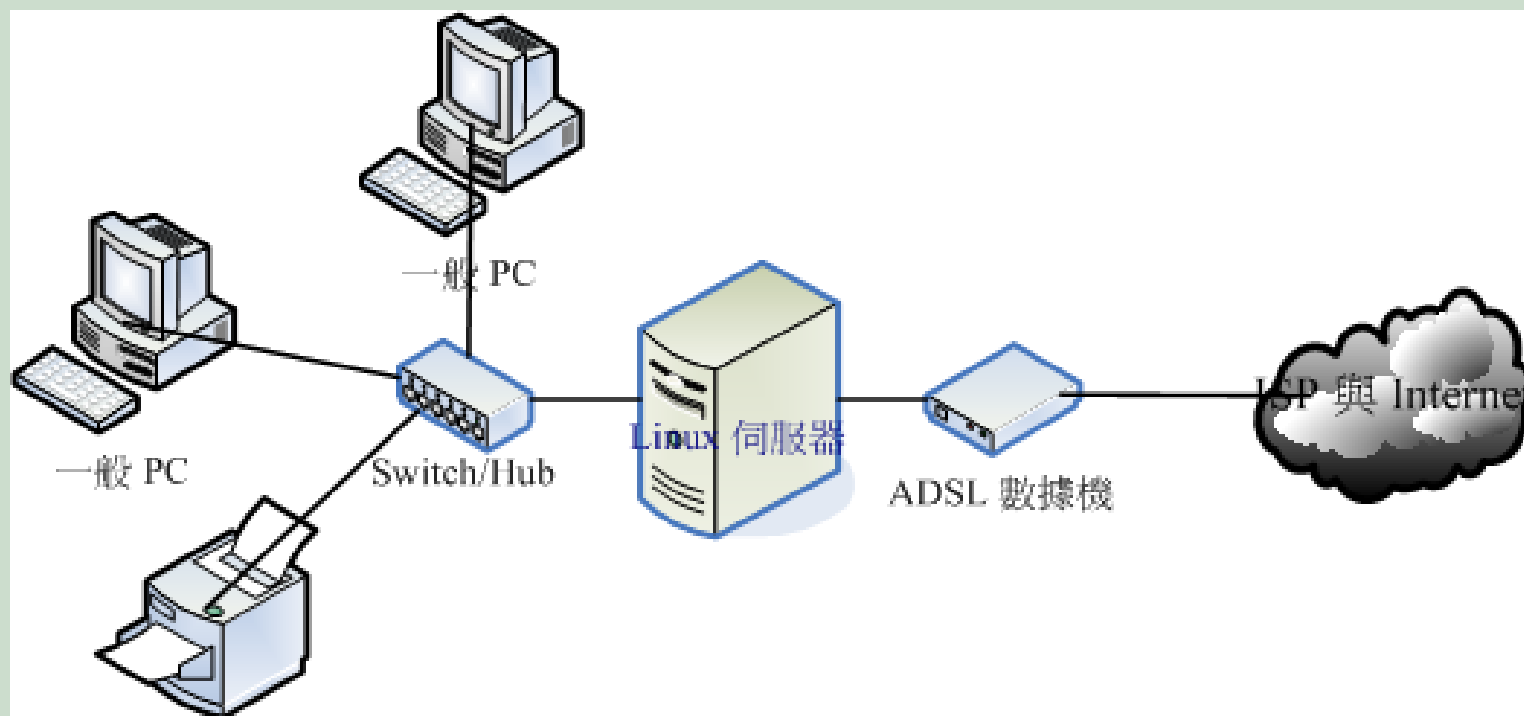
```


中文化Linux文件計畫 (CLDP)

The screenshot shows a Mozilla Firefox browser window displaying the CLDP website. The browser's address bar shows the URL <http://cde.linux.org.tw/CLDP/HOWTO/admin.html#admin>. The website content includes the title "CLDP" and the subtitle "Chinese Linux Documentation Project". A navigation menu lists links for [首頁\(H\)](#), [HOWTO\(T\)](#), [指南\(G\)](#), [FAQ\(F\)](#), [手冊頁\(M\)](#), [Linux電子報\(L\)](#), and [LinuxFocus\(S\)](#). A highlighted section titled "和系統管理相關的 HOWTO" contains a list of links: [HOWTO](#), [作業系統](#), [系統管理](#), [硬體](#), [網路](#), [應用](#), [程式設計](#), [其它](#), and [雜項](#). Below this, a list of specific HOWTO documents is provided, each preceded by a bullet point: [HOWTO : Beowulf](#), [HOWTO : The Linux Bootdisk](#), [HOWTO : Configuration](#), [HOWTO : LILO, Linux Crash Rescue](#), and [HOWTO : Linux Shadow Password](#). The footer of the website repeats the main navigation menu. The browser's taskbar at the bottom shows the date and time as "2008/01/10 10:00:00 AM" and the status "完成".

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

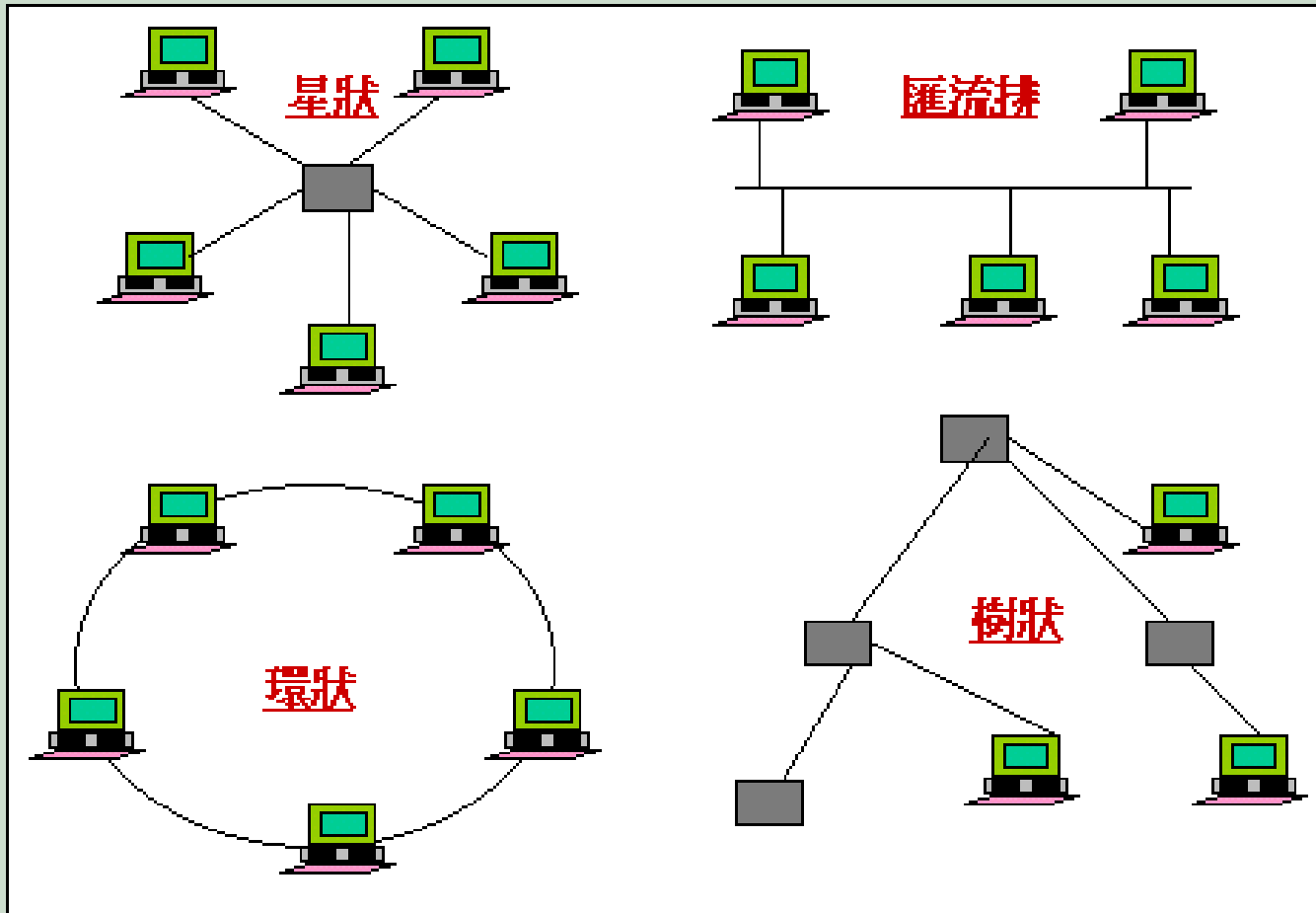


電腦網路的種類(續)

- 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為協議，如果這些協議被大家所認定的固定標準稱之為協定。

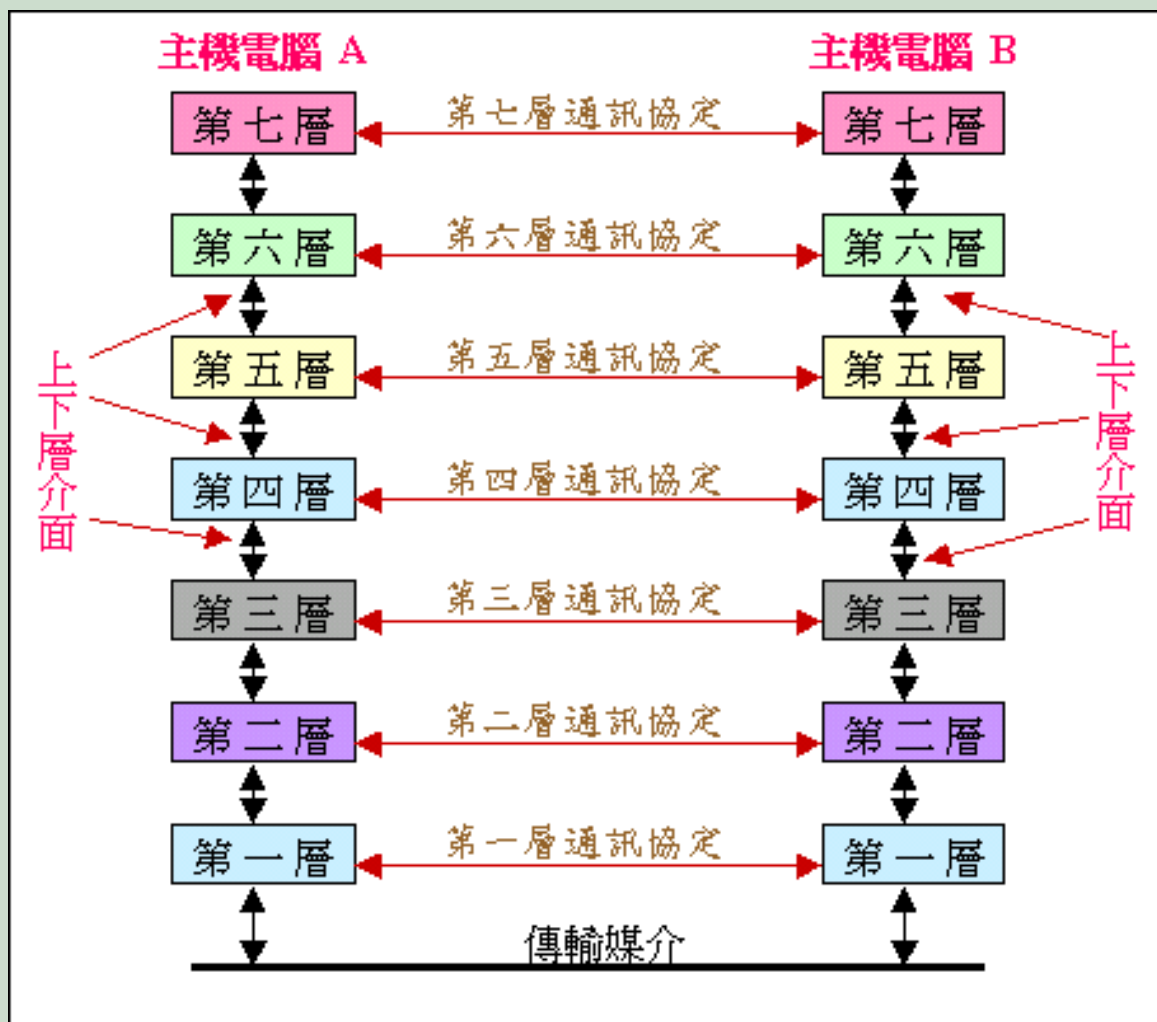
■ 何謂電腦通訊協定

☞ 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(Funcnctionality)
 - ∞ 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為前端對前端協定。

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。

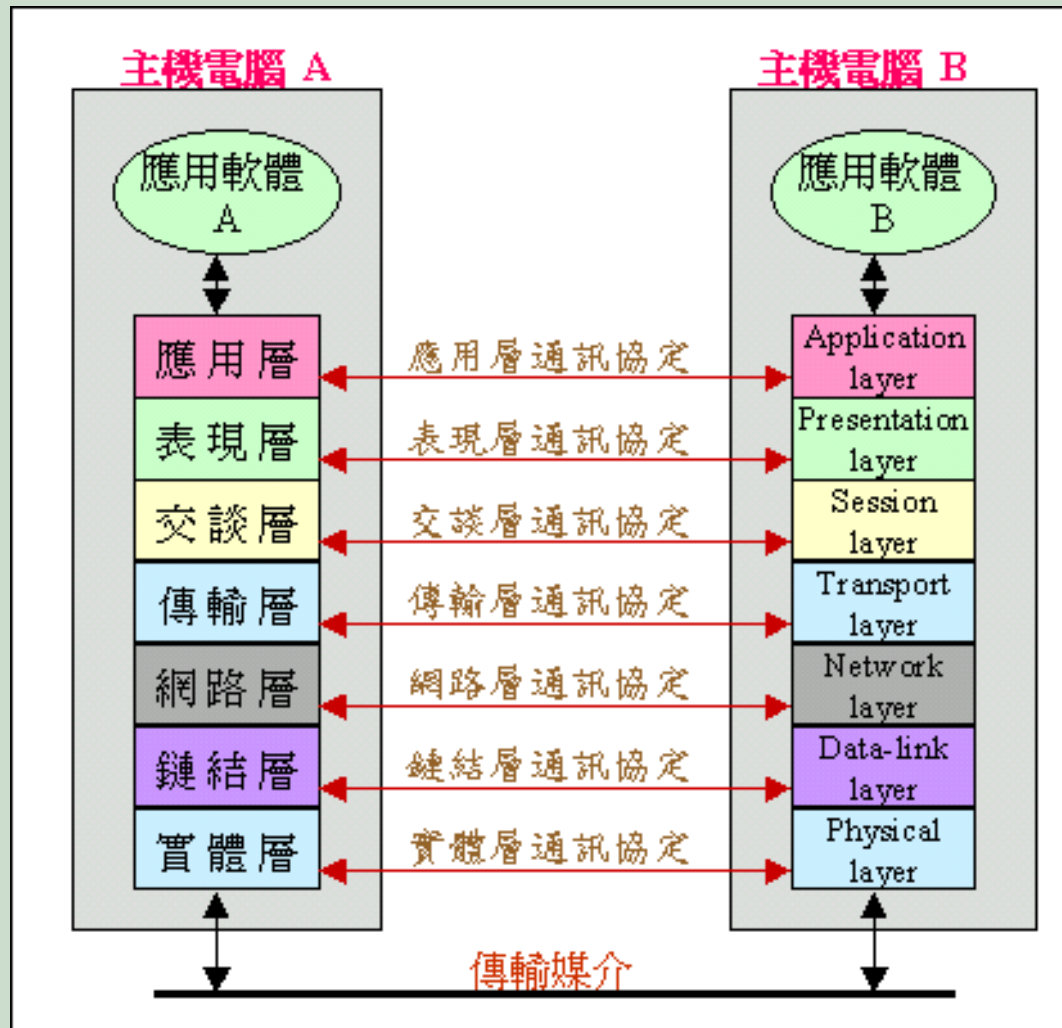


OSI七層協定

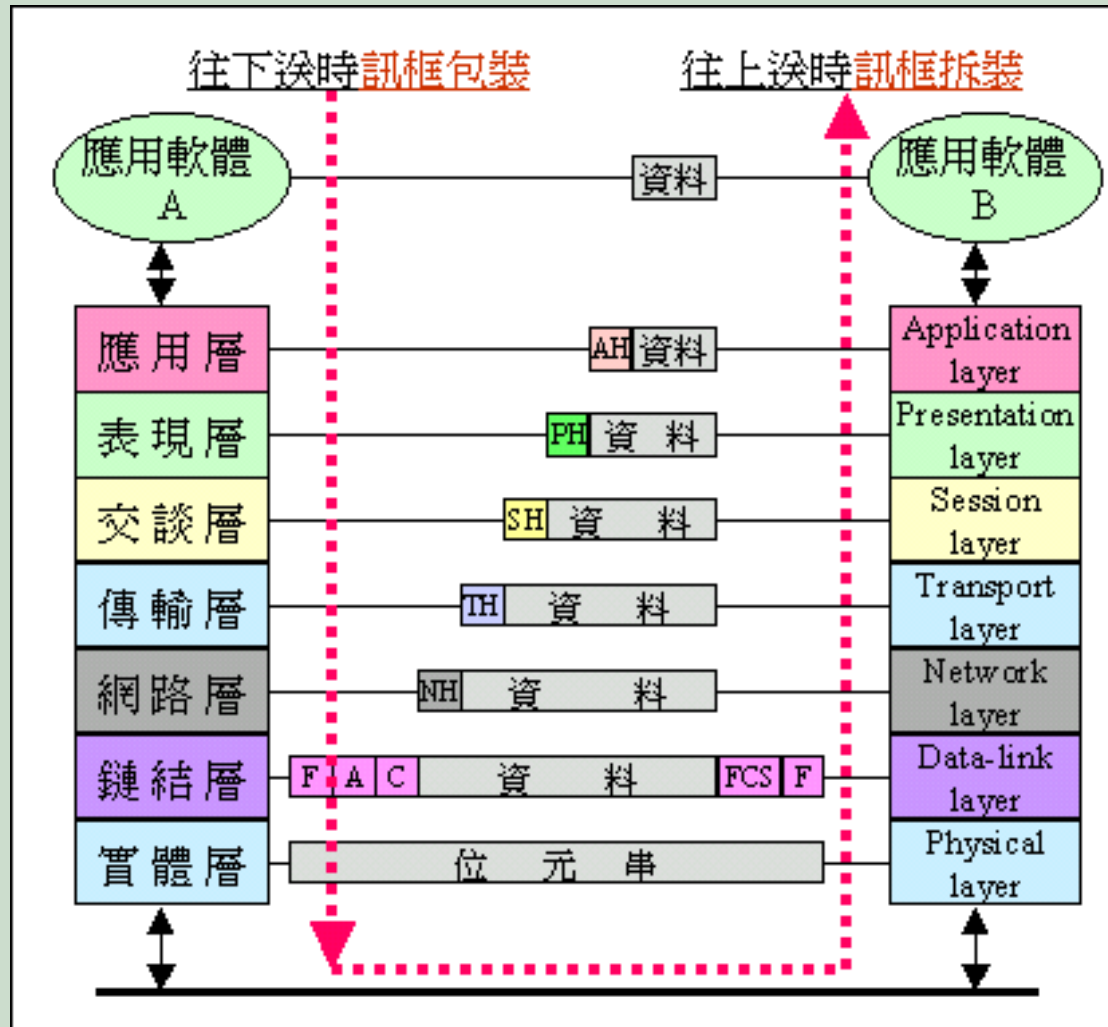
- 國際標準組織(International Standards Organization, ISO)
 - ∞ 1978年制定『開放式系統連結』(OSI, Open System Interconnected)



OSI七層協定



OSI協定的包裝/拆解流程

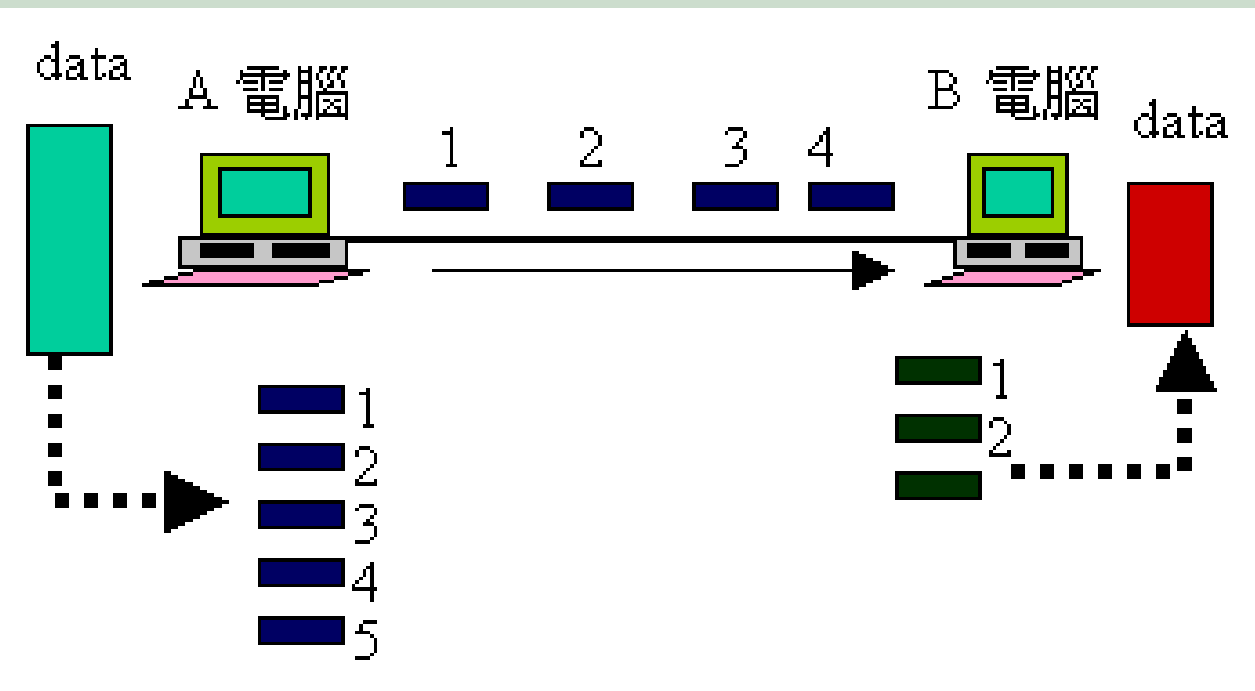


OSI-實體層

- 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
 - 可分為『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



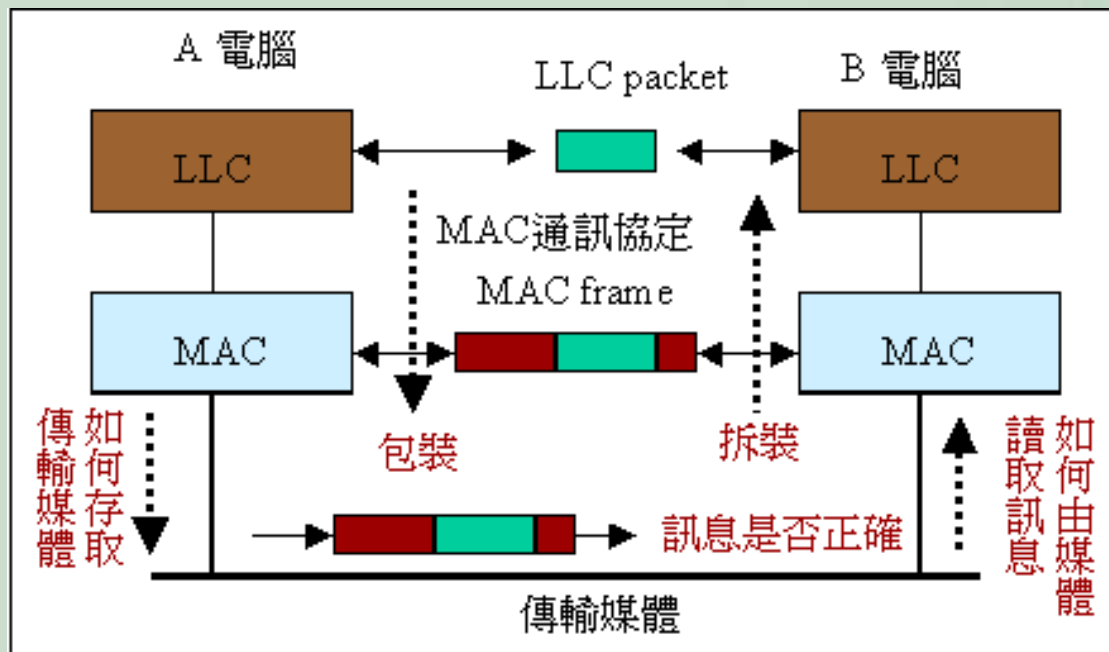
OSI-資料連結層



- 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為訊框

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 datagram)：

- 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**)。

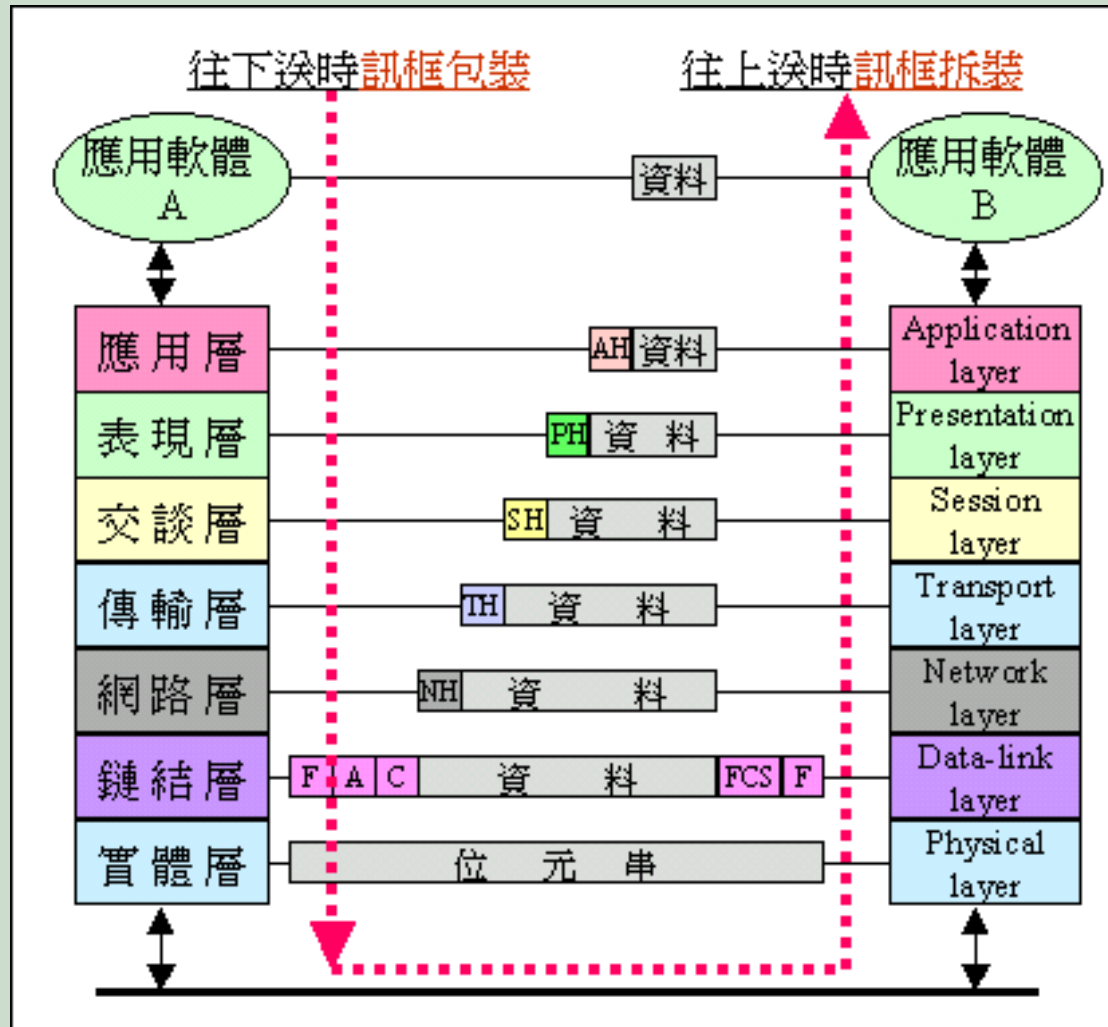


OSI-應用層

- 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)

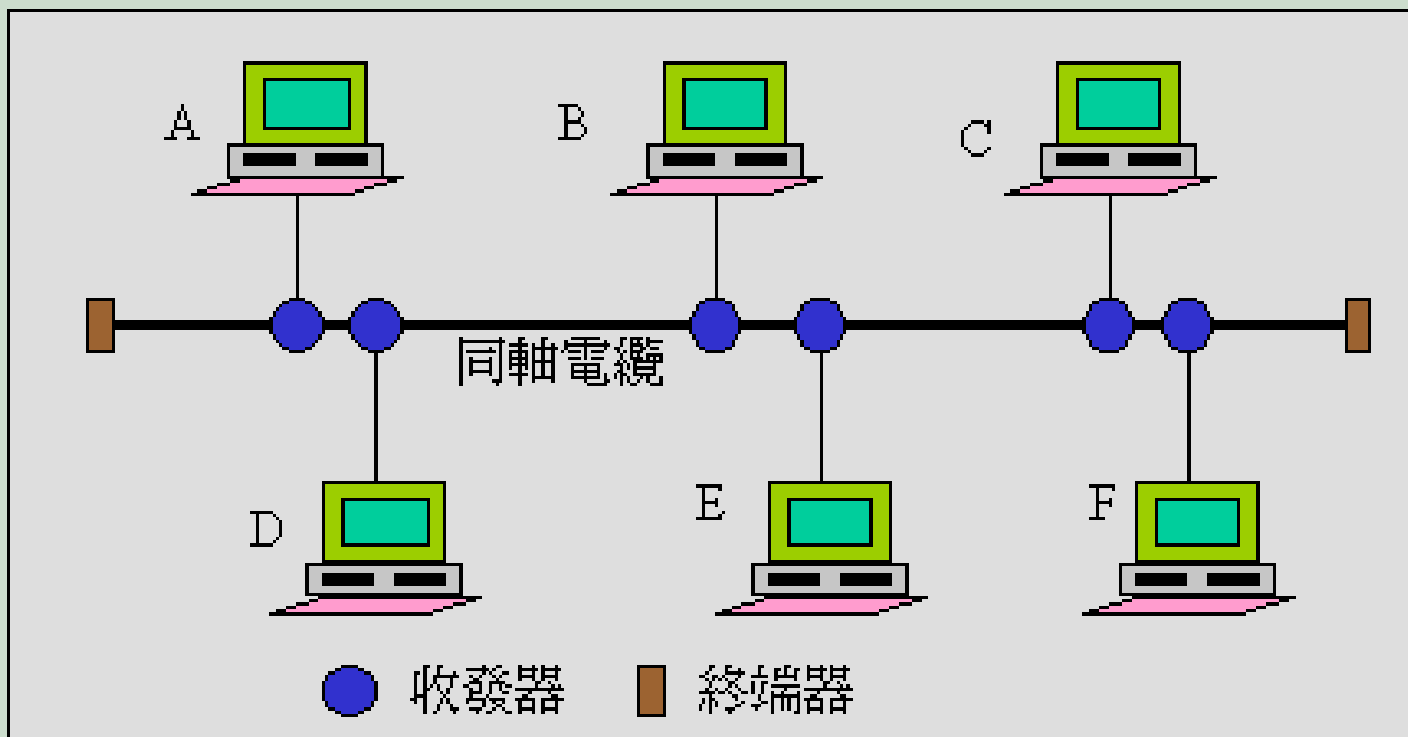
■ 乙太網路由來：

- ∞ 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標準為主。
- ∞ 目前區域網路架構絕大部份以架設Ethernet網路為主，已成為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)
- **Carrier 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。

CSMA/CD 協定



- 示意圖：每部主機都可能同時發送資料在這個共享的bus媒體上

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

☞ 資料長度最大為 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為
 - ⌘ 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)
- 每傳送 1 bit 所花的時間稱為 bit time
- 每個 frame 傳送到網路媒體上，需要等待至少96 bit time才能夠繼續傳送。



訊框傳輸速率

- 最大與最小訊框的資料量：
 - ∞ 最大： $8+6+6+2+1500+4=1526\text{bytes}=12208\text{bits}$
 - ∞ 最小： $8+6+6+2+46+4=72\text{bytes}=576\text{bits}$
- 每個訊框傳輸的時間(需加上等待的96bit time)
 - ∞ 最大： $12208+96=12304\text{ bit time}$
 - ∞ 最小： $576+96=672\text{ bit time}$
- 每秒鐘最大的傳輸訊框數(標準乙太網路)
 - ∞ 最大： $10\text{Mbps}/12304=812.7\text{個/秒}$
 - ∞ 最小： $10\text{Mbps}/672=14880\text{個/秒}=14.88\text{K個/秒}$
- 最大傳輸資料量(不含前導碼8bytes)
 - ∞ 最大： $812.7*1518*8=9.87\text{Mbps}$
 - ∞ 最小： $14.88\text{K}*64*8=7.62\text{Mbps}$ ←越大的封包，網路使用率越高



TCP/IP

OSI七層協定與TCP/IP

- OSI七層協定的特色：
 - ∞ 分層堆疊，每層的任务是可以獨立的
 - ∞ 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，架構較為鬆散
 - ∞ 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

OSI七層協定模型

應用層 表現層 會談層
傳輸層
網路層
資料連接層 實體層

TCP/IP協定模型

應用層
傳輸層
網路層
鏈結層

相關協定與硬體

HTTP	FTP	SMTP
POP3	Telnet	NFS
TCP	UDP	
IP	ICMP	
LAN: Ethernet, Token Ring		ARP
WAN: Modem, Serial, ISDN, ATM...		

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，故稱為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

4 bits	4 bits	8 bits	3 bits	13 bits
Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragmentation Offset
Time To Live	Protocol		Header Checksum	
Source Address				
Destination Address				
Options			Padding	
Data				

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全為0(第一個IP)

11000000.10101000.00000000.11111111→host全為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)代為傳送

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，不可同時為 0 也不可同時為 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 這個網域被作為系統的內部迴圈(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 均為 1, 而 Host ID均為 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 再細分為兩個子網域？

⊗ Network1 : 11000000.10101000.00000000.00000000 → 192.168. 0.0

⊗ Network2 : 11000000.10101000.00000000.10000000 → 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

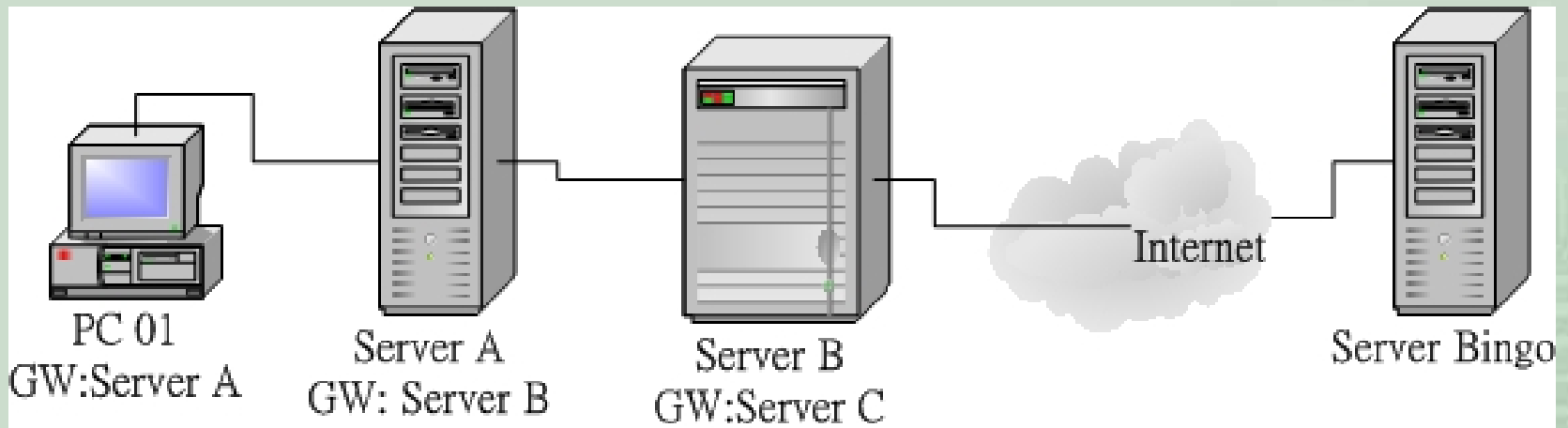


網路層的route概念

■ 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
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 為重要的使用 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



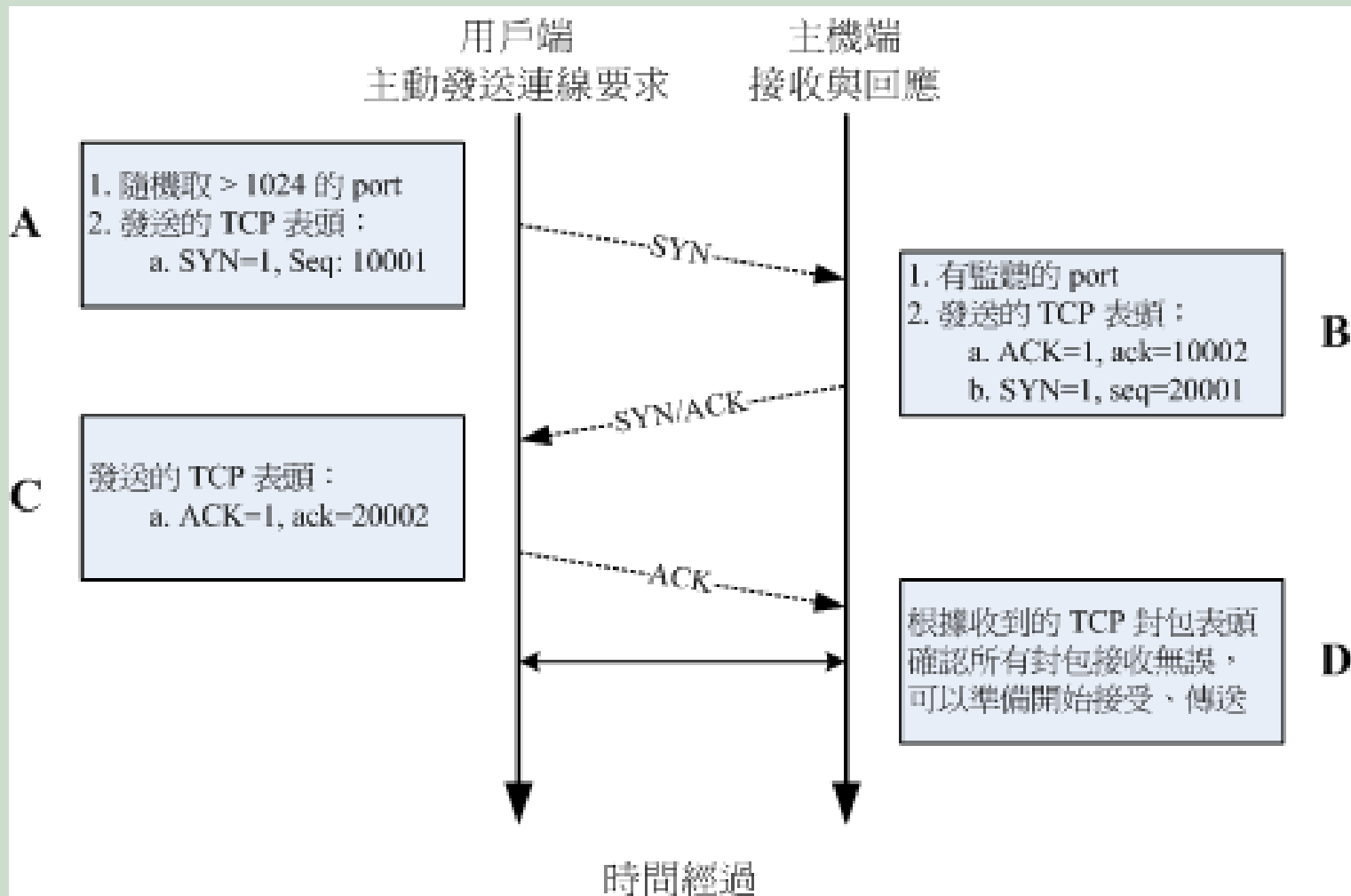
傳輸層的 TCP 封包協定

4 bits	6 bits	6 bits	8 bits	8 bits
Source Port			Destination Port	
Sequence Number				
Acknowledge Number				
Data Offset	Reserved	Code	Window	
Checksum			Urgent Pointer	
Options			Padding	
Data				

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

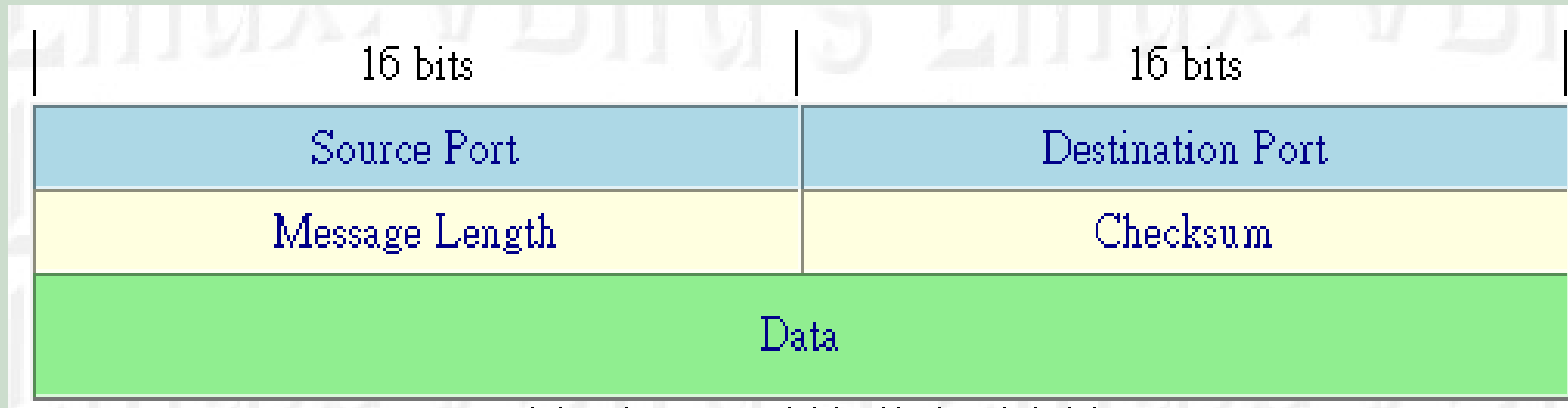


Socket Pair

- 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，較為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，用在作為 mail server 的埠口
53	DNS，用在作為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** \leftrightarrow **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	<code>/etc/sysconfig/network</code>
IP參數	<code>/etc/sysconfig/network-scripts/ifcfg-eth0</code>
DNS	<code>/etc/hosts</code> <code>/etc/resolv.conf</code>
啓動腳本	<code>/etc/init.d/network restart</code>



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 localhost.localdomain`

- ☞ `route -n` \rightarrow `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`



Linux 防火牆

■ 本機防火牆

☞ 透過 TCP Wrappers

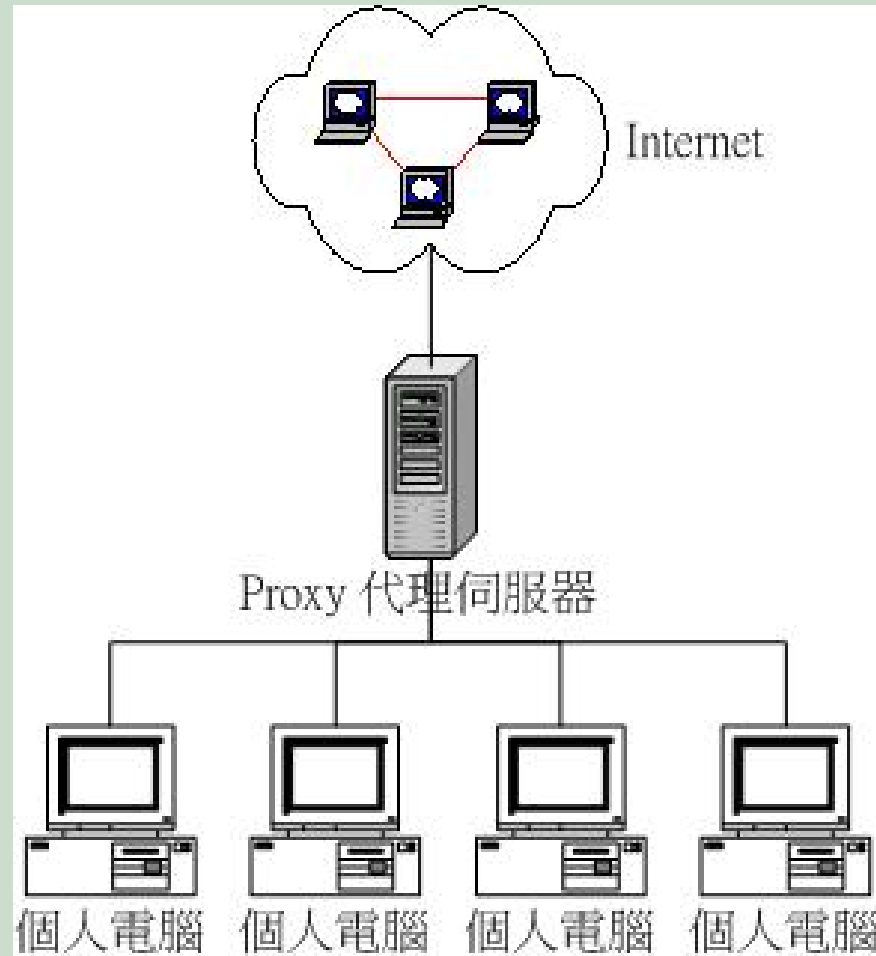
- `/etc/hosts.allow` → 規範可通過的用戶端
- `/etc/hosts.deny` → 規範被抵擋的用戶端

☞ 透過核心支援的 Netfilter

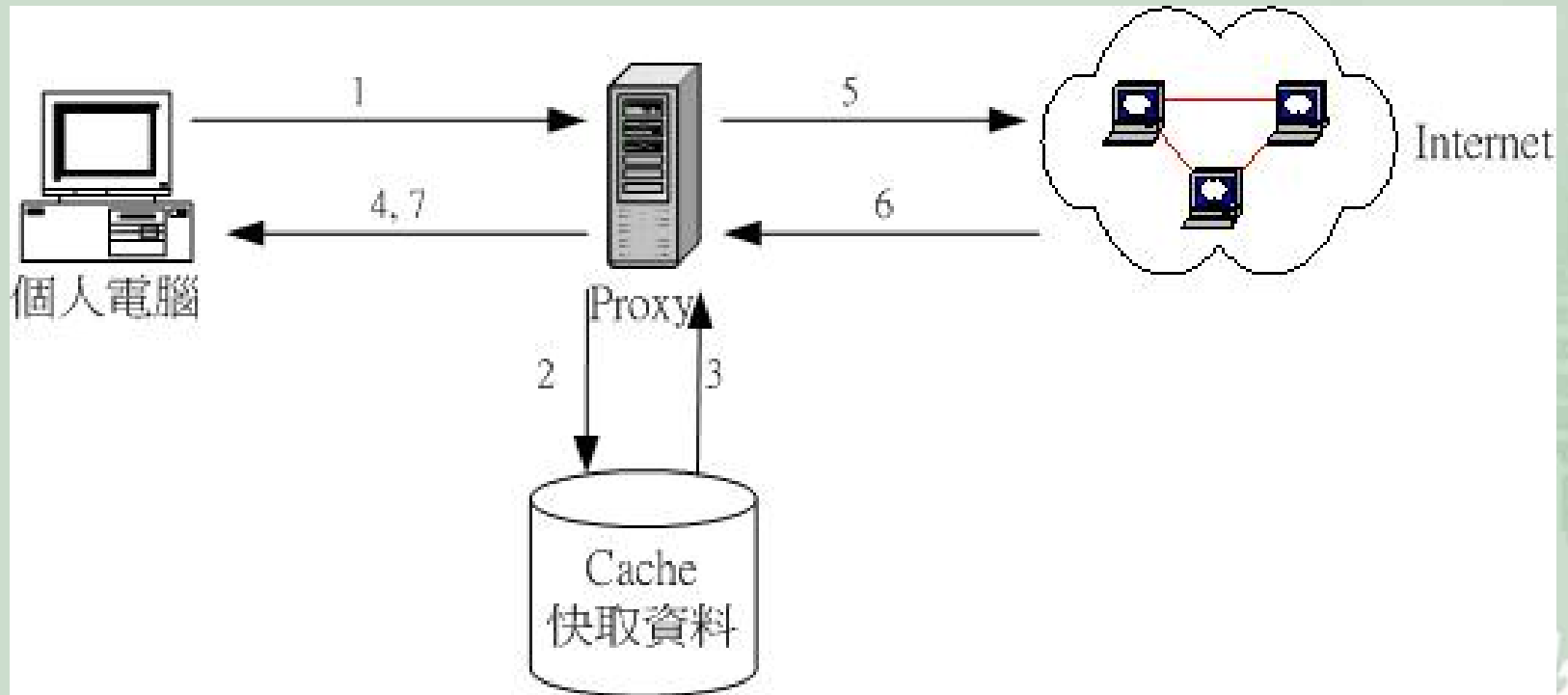
- 指令為 `iptables`
- 核心支援，需載入記憶體中
- 規則設定檔在 `/etc/sysconfig/iptables`



Linux Proxy 功能



Linux Proxy 功能





精選範例

- 下列哪些正確描述網路協定？（複選）**ABC**
 - ☞ (A) 網路協定就是網路之間溝通、交流的橋樑
 - ☞ (B) TCP/IP協定是Internet的標準協定
 - ☞ (C) Internet Protocol，主要用於負責IP定址、路由選擇和IP資料包的分割和組裝
 - ☞ (D) Internet Protocol Version 6為現行通用的Internet Protocol

- 下列何者為 Linux 作業系統 Kernel 的一部份?(複選) **CD**
 - ☞ (A) X Window
 - ☞ (B) bash
 - ☞ (C) 硬體驅動程式
 - ☞ (D) TCP/IP



- 以下何者最適用來描述星狀拓樸？單選 D
 - ❧ (A) LAN拓樸是資料從網路工作站透過單一的同軸電纜線送出，並由所有其他工作站接收
 - ❧ (B) 使用一個主幹節點呈分枝狀連接到其他節點的LAN拓樸
 - ❧ (C) 以線性鏈結的方式將網路中央節點連接到一個共用中央交換器的LAN拓樸
 - ❧ 中央節點以纜線呈放射狀連接到其他節點的LAN拓樸

- 哪一個區域網路(LAN)標準是指定乙太網路資料鏈結層中的實體層和媒體存取控制(MAC)的實作方式？單選 A
 - ❧ (A) IEEE 802.3
 - ❧ (B) IEEE 802.5
 - ❧ (C) EIA/TIA-568B
 - ❧ (D) EIA/TIA-569



- 哪一項最適合用來說明CSMA/CD的碰撞？單選 A
 - ☞ (A) 當兩個不同設備所傳來的訊框同時到達實體媒體時，會產生撞擊而損壞
 - ☞ (B) 兩個節點在同一時間傳送，其中一個資料封包具有高優先權，以覆蓋掉較低優先權的封包
 - ☞ (C) 兩個資料的傳輸路徑在網路媒體上交叉而互相損壞
 - ☞ (D) 因為網路媒體上的能量尖峰脈衝而導致資料傳輸損壞

- 乙太網路規格終將封包的間隔時間規定至少要持續多少bit time才能傳送資料？單選 A
 - ☞ (A) 96
 - ☞ (B) 80
 - ☞ (C) 120
 - ☞ (D) 200



- OSI七層模型中，哪些層和TCP/IP連結層對應？複選ABA
 - ☞ (A) 實體層
 - ☞ (B) 資料連結層
 - ☞ (C) 網路層
 - ☞ (D) 傳輸層

- 關於乙太網路 MAC 的傳輸方法敘述哪些正確？複選 AD
 - ☞ (A) 同一網路上的每一網卡都能接收到封包
 - ☞ (B) 若封包目的 MAC 位址和自己的 MAC不同，亦將該封包收下處理
 - ☞ (C) 若封包大小比 46bytes小或比1518bytes大，就予以丟棄
 - ☞ (D) 若發生碰撞(collision)時，則各主機隨機等待一時間後，再重新送出資料



- ICMP封包的type欄位有各種不同的類型，試問 ping 指令發出的 ICMP 封包類型 (type) ？單選 D
 - ☞ (A) 0
 - ☞ (B) 3
 - ☞ (C) 5
 - ☞ (D) 8

- 網路主機欲透過 TCP/IP 進行通訊，至少需要有哪些設定？複選 ABC (因為尚未談到主機名稱)
 - ☞ (A) IP 位址
 - ☞ (B) Netmask
 - ☞ (C) Gateway Address
 - ☞ (D) DNS server address



- 下列對 ARP (Address Resolution Protocol) 的敘述何者正確？複選 AD
 - ☞ (A) 由 OSI 第三層的定址找出第二層的定址
 - ☞ (B) 由 OSI 第二層的定址找出第三層的定址
 - ☞ (C) 屬於 OSI 第三層的通訊協定
 - ☞ (D) 屬於 OSI 第二層的通訊協定

- TCP 的 three-way shake 中，各封包所舉的旗標依序為？單選 C
 - ☞ (A) SYN → RCV/ACK → ACK
 - ☞ (B) SYN → SYN/ACK → SYN/ACK
 - ☞ (C) SYN → SYN/ACK → ACK
 - ☞ (D) SYN → RCV/ACK → SYN/ACK



- 請問下列哪些為 private IP address ? 複選 ABC
 - ☞ (A) 192.168.255.33
 - ☞ (B) 172.23.10.240
 - ☞ (C) 10.255.1.132
 - ☞ (D) 172.32.223.12

- 關於連接埠(port)的敘述何者正確 ? 複選 AD
 - ☞ (A) 屬於 OSI 七層的傳輸層
 - ☞ (B) 通常用戶端的來源連接埠是小於 1024
 - ☞ (C) 屬於 OSI 七層的網路層
 - ☞ (D) 通常用戶端的來源連接埠是大於 1024



- 下列的哪些IP區段是INTERNET不分配的IP，是保留給企業組織私用的IP？複選 ACD
 - ☞ (A) 10.0.0.0-10.255.255.255
 - ☞ (B) 127.0.0.0-127.255.255.255
 - ☞ (C) 172.16.0.0-172.31.255.255
 - ☞ (D) 192.168.0.0-192.168.255.255

- 一部電腦IP為61.62.0.71遮罩為255.255.255.128，請問該區段的『Network IP』為何？單選 A
 - ☞ (A) 61.62.0.0
 - ☞ (B) 61.62.1.0
 - ☞ (C) 61.62.0.255
 - ☞ (D) 61.62.0.128



- 下列何者可以查詢 DNS Client 的內容 (Red Hat 系統) ? C
 - ☞ (A) cat /etc/hosts
 - ☞ (B) cat /etc/sysconfig/network
 - ☞ (C) cat /etc/resolv.conf
 - ☞ (D) cat /etc/sysconfig/network-scripts/ifcfg-eth0

- 下列那個IP是B等級的私有IP ?
 - ☞ (A) 10.10.168.xxx
 - ☞ (B) 170.16.125.xxx
 - ☞ (C) 172.16.32.xxx
 - ☞ (D) 192.168.1.xxx



- 那個指令可以用來測試網路狀況？複選 AC
 - ☞ (A) ping
 - ☞ (B) host
 - ☞ (C) traceroute
 - ☞ (D) nslookup

- 請問 MAC 位址的表示方式？ C
 - ☞ (A) 四組，每組八個二進位的數字組成，組與組之間用小數點隔開
 - ☞ (B) 四組十進位的數字組成，數字間用一個小數點分開
 - ☞ (C) 六個十六進位的數字組成
 - ☞ (D) 十二個十六進位的數字組成



- 關於 TCP/IP 的描述下列何者正確？ 複選 AB
 - ☞ (A) 封包在接收時如果發生遺失或者是損毀，Transport Layer會要求對方重送
 - ☞ (B) HTTP、SMTP都是屬於Application Layer的通訊協定
 - ☞ (C) 使用TCP的通訊協定進行資料傳輸比 UDP 快
 - ☞ (D) 封包大小(packet size)越小資料的傳輸效率將越好

- 請問 Linux 用什麼指令來顯示 IP 位址？ C
 - ☞ (A) ipconfig
 - ☞ (B) ipcfg
 - ☞ (C) ifconfig
 - ☞ (D) netconfig



- 下列指令哪些可以查詢路由資訊？複選 AB
 - ☞ (A) route
 - ☞ (B) netstat
 - ☞ (C) ifconfig
 - ☞ (D) iptables

- 關於 Proxy server 的描述何者有誤？ C
 - ☞ (A) 可用來提高網路的安全性
 - ☞ (B) 可提供網頁快取功能
 - ☞ (C) 只能使用在 HTTP 通訊協定上
 - ☞ (D) 可拿來當作防火牆



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>

