目錄

第三章　網際網路的服務與應用

第四章 「 網路安全 」

前言

研究目的：ITE 證照為經濟部工業局所推廣之資訊人員專業級證照，與日本官方相互採認，為國際級證書，剛好我們唸的是資訊管理系，多少都有學到一些關於網路通訊方面的資訊，抱著比人想多學習想多吸收東西、多一份經驗想法，加上對以後未來的出路會比較順利，因此我們作了這次的專題研究。

第一章「區域網路」

1-6 Internet History and Definition

1-1.1

Internet 之起源可追溯到 1968 年，美國國防部高級研究計畫署，為維持電腦與通訊系統免於戰爭的破壞，所進行的一項計畫叫做 ARPA(Advanced Research ProjectAgency ；高級研究專案組織)計劃。簡單的說，就是透過電腦與電話網路的連結，再與全球個個國家的系統相連，形成一個全球最大的網際網路系統。IInternet 原只用在學術研究及教育方面，之後由於許多線上服務公司相繼連上 Internet 及學生自學校畢業後把使用 Internet 的習慣帶到企業界，製造了 Internet 商業服務的市場。網際網路定義了傳輸控制通訊協定(Transmission Control Protocol)及網際網路通訊協定(Internet Protocol)。TCP/IP 通訊協定與各種網路技術互相獨立，透過定義 IP 架在不同網路上的介面，各種網路不管是區域網路或是廣域網路，主要透過與 IP 的介面都可成為網際網路的子網路。因此利用 TCP/IP 的 IP 與實際網路的介面，Internet 的實際連線由於其提供的一致性服務，使用者看到的只有一個網路。

網路之規模分類

1.區域網路（ LAN；Local Area Network ）

指覆蓋局部區域（如辦公室或樓層）的電腦網路。按照網路覆蓋的區域（距離）不同，其他的網路型式還包括個人網、城域網、廣域網等，提供電腦間快速、短距離的資料通訊。

2.都會網路（ MAN；Metropolitan Area Network ）

指大型的計算機網路(介於 LAN 和 WAN 之間能傳輸語音與資料的公用網路)，這些網路通常涵蓋一個大學校園或一座城市。

3.廣域網路（ WAN；Wide Area Network ）

指一個很大地理範圍的由許多區域網組成的網路，提供長距離的通訊、傳輸速率比較。

相關試題

1.(A)網際網路的網路層通訊協定是?

(A)IP

(B)AP

(C)GP

(D)HP

2.(A)WWW 是何者縮寫?

(A)World Wide Web

(B)World Web Wide

(C)Web World Wide

(D)Wide Web World

3.(B)TCP/IP 網路的前身為何?

(A)AppleNet

(B)ARPANET

(C)HiNet

(D)BioNet

1-2.1 DHCP

(Dynamic Host Configuration Protocol, RFC 1531, RFC 1541, 1993)

早期在規劃網際網路時認為四個位元組所能夠表達的機器數目非常的大，共可表示 2^{32} 台機器，因此又依據這四個位元組強制將位址分配給不同的網路區段，第一個位元組固定的話是所謂的 class A 網路，前兩個位元組固定的話是所謂的 class B 網路，前三個位元組固定的話是所謂的 class C 網路，如此分類後各個網路自行掌管其內網路位址的分配。可是近幾年來幾乎所有的個人電腦都具有網路連線的能力了，因此網路的位址立刻顯得不足，尤其是大部分的個人電腦常常只有在少數的工作時間使用網際網路，如果給它固定的一個 IP 位址的話似乎顯得有些浪費，因此發展出動態的指定 IP 位址的 DHCP 協定，如此大部分的個人電腦只有在開機、且連上網路時才動態地指定一個 IP 位址，解決了 IP 位址不足的問題。ISP 提供給一般用戶使用撥號網路連上網際網路時就是動態地指定 IP 位址給每一台電腦。

1-2.2

廣播（Broadcast）：在通訊網路上，一個工作站對於網路上（廣域網路或是區域網路）其他所有電腦所發出的訊息。

1-2.3

路由器（Router)：兩個網路要做連線的設備，例如區域網路與廣域網路連接，為用來決定資料傳遞的路徑設備。

1-2.4

閘道器(Gateway)：閘道器運作屬於高階通信協定，其功能就好比翻譯員，用來解決不同網路間的連接問題；而閘道器則可連接完全不同的網路架構。

區域網路的連接類型

接的類型可分為四種：匯流排式網路結構、星狀網路結構、環狀網路結構或混合式網路結構。

(一) 匯流排式網路結構

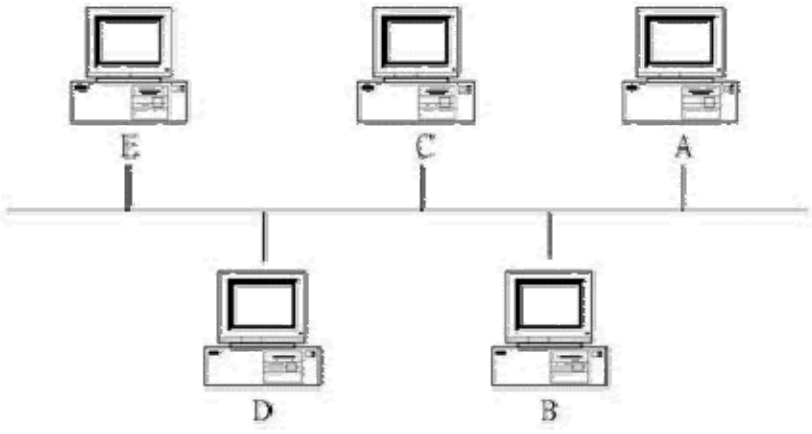


圖 1-2　匯流排式網路

匯流排架構具有廣播的特性，任何一部電腦都可以將資料傳送到網路上，其訊號會往二邊傳遞，並且流入網路上的每一部電腦，達成資料傳輸目標。

當匯流排網路上有任何一部電腦壞掉了，都不會影響到其它電腦間的通訊，所以匯流排架構是目前使用最多的區域網路架構。匯流排架構最脆弱之處就是主幹線。由於只有一條電纜線，所以當電纜線發生損壞或斷線時，則會造成整個網路的癱瘓。

（二）星狀網路結構

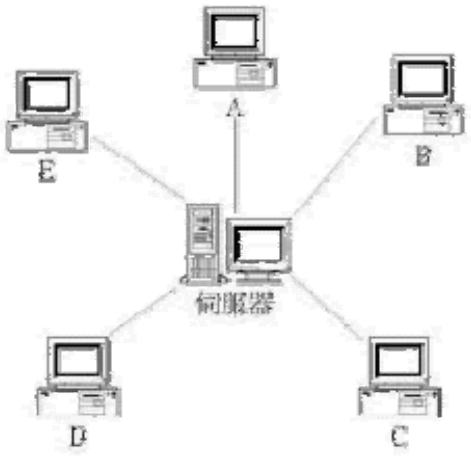


圖 1-2.1　星狀網路結構

這種方式又稱為「放射狀」，使用一部電腦扮演中央控制主機，也就是網路伺服器，所有的電腦都直接和中央控制主機連接。任何資

料的傳送都必須透過中央控制主機。由伺服器總管整個網路的運作，此種結構的施工配線費用高。一般的區域網路加上集線器之後，便可視為星狀網路。星狀網路結構的另一項特性是：網路內所有要傳送的資料都要透過中央的集線器做傳遞。這種排法有種壞處，一旦中央控制主機發生故障，整個網路就癱瘓了

(三) 環狀網路結構

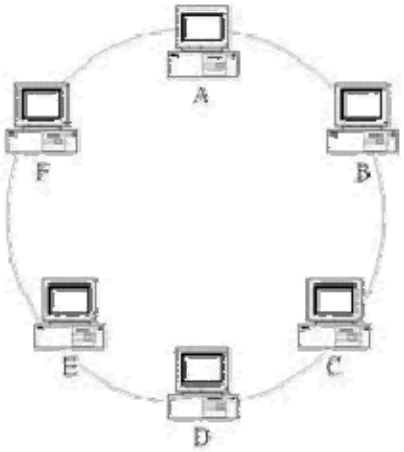


圖 1-2.2 環狀網路結構

環狀架構中，連接所有電腦的主幹線電纜形成一個環狀迴路。事實上這個環狀迴路是由許多段「點對點」的電纜線所組合而成。

環狀網路最脆弱之處也是主幹線電纜。當電纜線受損斷裂時，會導致整個網路或部份網路的損毀。例如：如果上圖中Ｃ－Ｄ之間的電纜線斷裂，那麼整個網路就變成是一個由Ｃ=>Ｂ=>Ａ=>Ｆ=>Ｅ=>Ｄ所組成的單向傳輸網路。

（四）樹狀結構

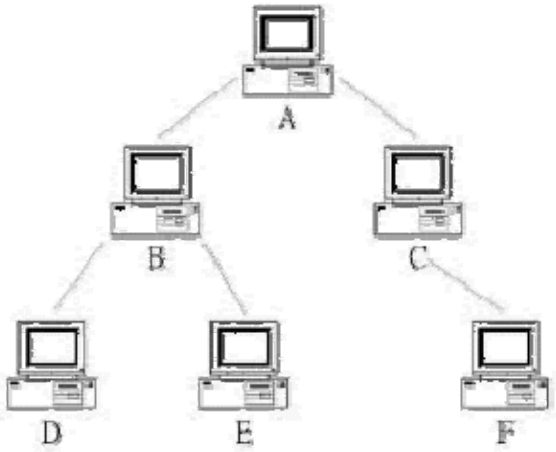


圖 1-2.3 樹狀結構

在傳輸方式上，樹狀架構可以說是匯流排架構的另一種形式。樹狀架構中的任何二部電腦之間都只有一條傳輸線連接，當資料進入任何一個節點後，會向所有的分支傳遞（除了訊號進入的分支）。因此樹狀架也具有廣播傳送的特性。

當樹狀架構某二點間的電纜線故障時，會將此樹狀網路分為二個較小的樹狀網路，而這二個樹狀網路是無法互通的。另外當某一部電腦發生故障，也會造成網路的損毀。

(四)網狀結構

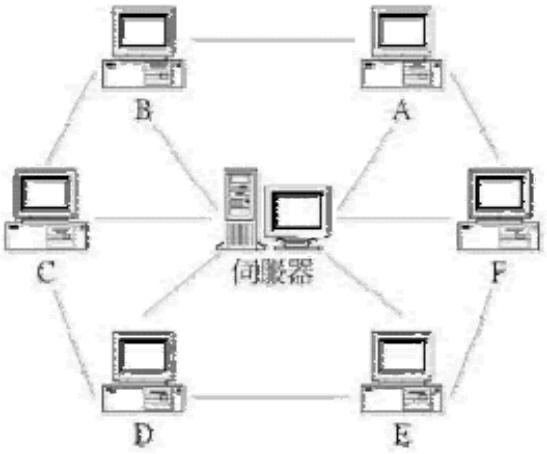


圖 1-2.3 網狀結構

網狀架構是網路架構中安全性最高的一種。二部電腦之間存著不只一條的通路，即使某一條電纜線損毀，也可以利用其他的通路來傳送資料。網狀網構可以設置一部中央控制主機來管理網路上的資源，也可以不設。

對於資料量很大，而且傳送作業不可中斷的環境，網狀架構是很好的選擇。不過網狀網路的架設成本要比其他網路架構來的高，而且施工也比較困難，是需要注意的一點。

相關試題

1.(D)Internet 上使用何者進行動態定址?

(A)Mac address

(B)IP address

(C)IPX address

(D)DHCP

2.(C)VLAN 的標準定義於下列何者?

(A)IEEE802.3

(B)IEEE802.1p

(C)IEEE802.1q

(D)IEEE802.11g

3.(D)集線器(Hub)可提供下列哪一項功能?

(A)過濾廣播(Broadcast)封包

(B)負責路由(routing)選徑

(C)記載 IP address 與 MAC address 的對應

(D)傳送 0 與 1 的訊號資料

1-3Computing Model (Centralized,Distributed,Cooperative Computing)&Network Services Model(Clients,Services,peers)

1-3.1

主從式架構 (Client - Server)

在 Intranet 架構中，最能夠發揮出其效率的是多階式的主從式架構。傳統主從式架構是以 2 階(2-tier)或 3 階(3-tier)的主從式應用方式，這種的主從式應用在目前已被廣泛的使用在大型的資料庫中。如圖 1-3

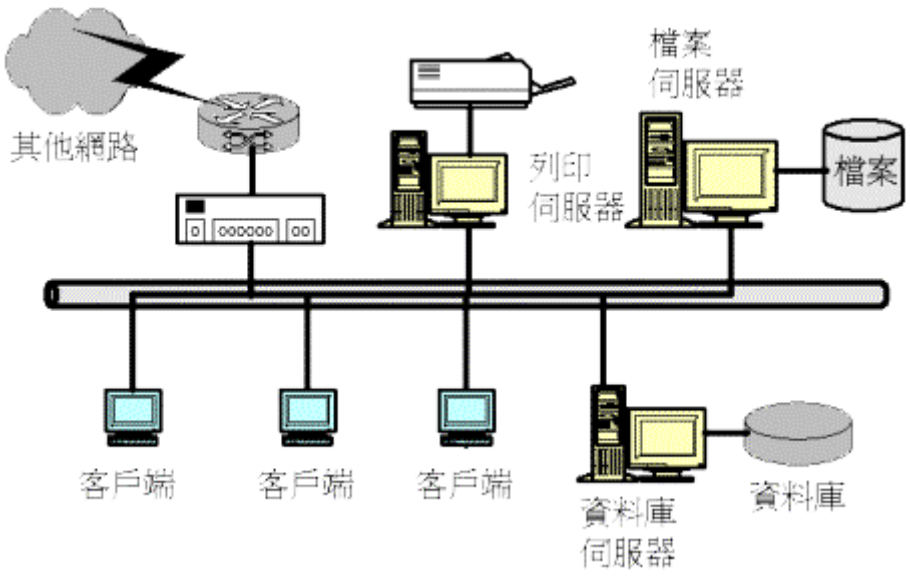


圖 1-3 主從式架構

1-3.2

對等式架構（ Peer-to-Peer ）

對等式網路中沒有主要的伺服器，而是由對等端以群組的方式組成，對等端之間能彼此分享資源。以下四項是對等式之特點。

1.網路連線架構簡單，成本低

2.使用者可以自行控制管理共享的資源

3.資源分享的過程會增加資源提供者電腦的負荷量

4.適用於小型網路系統

相關試題

1.(A)對一般的企業環境而言，以下何者不是採用 Client-Server 架構的理由？

(A)集中管理

(B)降低風險

(C)降低成本

(D)資源分享

2.(A)下列何者不屬於 Client-Server 網路架構?

(A)以網路芳鄰相互溝通的電腦

(B)mainframe 主機及它所有的終端機

(C)WWW 主機及連線上網的電腦

(D)PDC 及登入網域之用戶電腦

3.(A)網路芳鄰屬於下列何種結構?

(A)Peer-to-Peer

(B)Client-Server

(C)master-slave

(D)parent-son

1-4OSI Reference Model

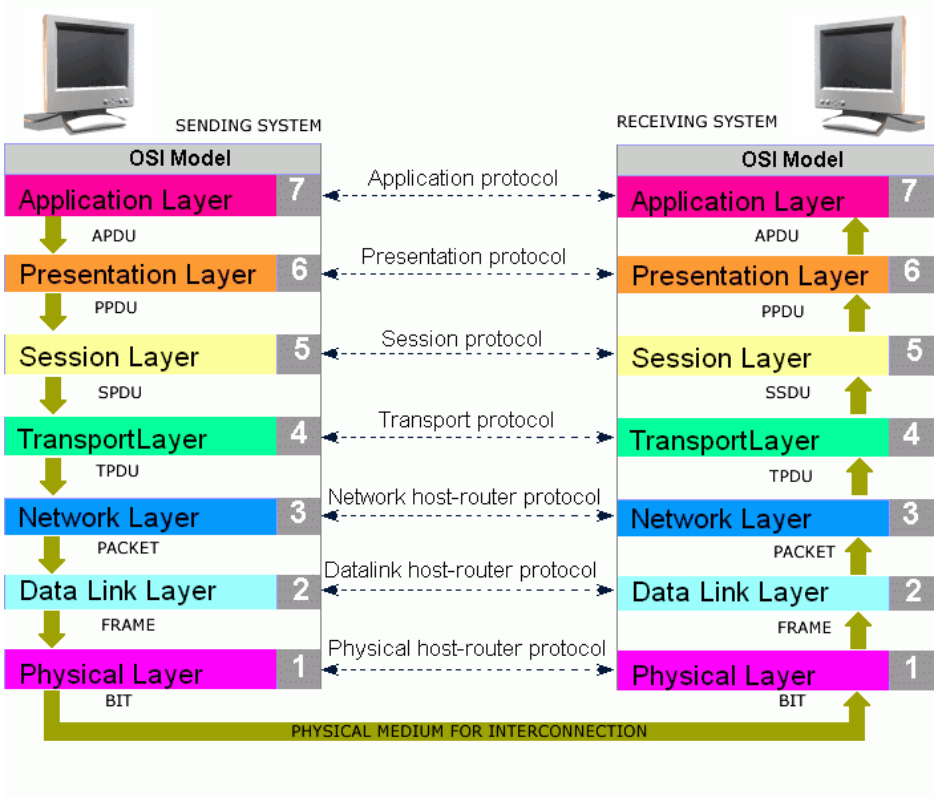


圖 1-4　OSI Model

1-4.1 第一層：實體層(Physical Layer)

是計算機網路 OSI 模型中最低的一層。實體層規定:為傳輸數據所需要的物理鏈路建立、維持、拆除，而提供具有機械的，電子的，功能的和規範的特性。簡單的說，實體層確保原始的數據可在各種物理媒體上傳輸。

1-4.2 第二層：資料連接層(Data Link Layer)

位於實體層與網路層之間，它是 OSI 中比較重要的一層，它會在 frame 尾端置放檢查碼(parity, sum, CRC) 以檢查實質內容，將物理層提供的可能出錯的物理連接改造成邏輯上無差錯的資料鏈路，並對物理層的原始資料進行資料封裝。

資料連結層中的資料封裝是指：封裝的資料信息中，包含了地址段和資料段等。地址段含有點對點(point-to-point)發送節點和接收節點的地址（如 MAC)，控制段用來表示數格連接幀的類型，資料段包含實際要傳輸的資料。

1-4.3 第三層：網路層(Network Layer)

網路層是 OSI 模型中的第三層。網路層提供路由和尋址的功能，使兩終端系統能夠互連且決定最佳路徑，並具有一定的擁塞控制和流量控制的能力。TCP/IP 協議體系中的網路層功能由 IP 協議規定和實現，故又稱 IP 層。

網路層通常都有如下的這些功能：

1.如果封包不是屬于同一個網路的時候，會將之交由 router 處理。

2.控制數據流量，當 router 的緩衝區飽和的時候，會通知數據傳輸設備使用其它路徑或暫停發送封包。

3.MAC 地址和網路地址(如 IP 地址、IPX 地址)之間的解釋和轉換。

1-4.4 第四層：傳送層(Transport Layer)

傳輸層(Transport Layer)是 OSI 中最重要, 最關鍵的一層,是唯一負責總體的數據傳輸和數據控制的一層.傳輸層提供端到端(end-to-end)的交換數據的機制，檢查封包編號與次序。傳輸層對其上三層如會談層等，提供可靠的傳輸服務,對網路層提供可靠的目的地站點信息。

主要功能

1. 為端到端連接提供可靠的傳輸服務.
2. 為端到端連接提供流量控制,差錯控制,服務質量(Quality of Service,QoS)等管理服務

1-4.5 第五層：會談層(Session Layer)

會談層，位於 OSI 模型的第 5 層,主要為兩個會話層實體進行會談（Session），而進行的對話連接的管理服務。

主要功能

1.程式以電腦名稱註冊成為網路上唯一的地址。

2.間建立、監測、和結束虛擬電路(Virtual Circuit)。

3.電腦之間的信息同步,監測資料溝通狀態,並對錯誤信息做出處理。

1-4.6 第六層：表現層(Presentation Layer)

表現層則是主要負責在不同機器之間進行編碼轉換。當應用程式產生資料要進行傳送的時候,表現層會將之換成網路的標準編碼格式再交由下層協定處理; 然後當資料抵達目的地,表現層也會將網路的編碼換成對方應用程式所需的格式。

1-4.7 第七層：應用層(Application Layer)

是七層 OSI 模型的第七層。應用層直接和應用程序介面並提供常見的網路應用服務。應用層也向表示層發出請求。

相關試題

1.(D)TCP 相當於 ISO OSI 七層模型的哪一層?

(A) 資料連接層(Data Link Layer)

(B) 會談層(Session Layer)

(C) 網路層(Network Layer)

(D) 傳送層(Transport Layer)

2.(D)在資料連接層(Data Link Layer)中傳送與接收資料的單位是?

(A) Bits

(B) TCP packets

(C) IP packets

(D) Ethernet frames

3.(C)OSI Reference Model 各層(Layer)定義使用範圍，何者為是?

(A) 實體層(Physical Layer):應用程式介面

(B) 資料連接層(Data Link Layer):資料安全加密

(C) 網路層(Network Layer):路由選擇

(D) 傳送層(Transport Layer):子網路運作

1-5Transmission Model

1-5.1 雙絞線 (Twist pair)

雙絞線依其組成方式又可分為無遮蔽式雙絞線 (Unshieled Twisted Pair)及遮蔽式雙絞線(Shieled Twisted Pair)；遮蔽式雙絞線，顧名思義就是對絞線多了一層金屬遮蔽物，外帶多加了一條接地銅線，因此可想而知遮蔽式雙絞線有較好的防止雜訊電磁波干擾能力，但是價格較為昂貴 ，安裝上也比較困難。

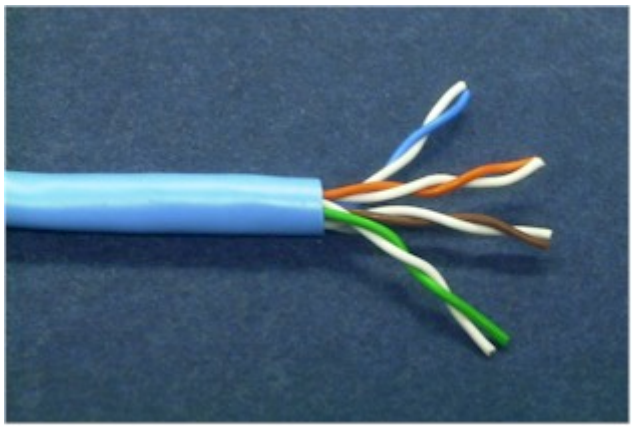


圖 1-5　無遮蔽式雙絞線

1-5.2 同軸電纜

同軸電纜又可分為細同軸電纜及粗同軸電纜，細同軸電纜由內而外分成中央銅線、塑膠絕緣體、導體網、 外皮等四層，如圖 1-5.2 所圖示：

1-5.3 細同軸電纜

細同軸電纜使用的導線為 RG-58A/U，網路拓樸（Topology）都屬於 Bus，因此 Cable 的兩端需要 50 歐姆終端電阻（Terminator），終端電阻的目的是用來終止電器信號，以免產生反射信號而干擾正常信號傳遞。　　細同軸電纜使用的接頭是 BNC 接頭，可分成鍍金針頭、金屬套頭與金屬套管 3 個部份；工作站的連接是透過 T 型接頭連接 。

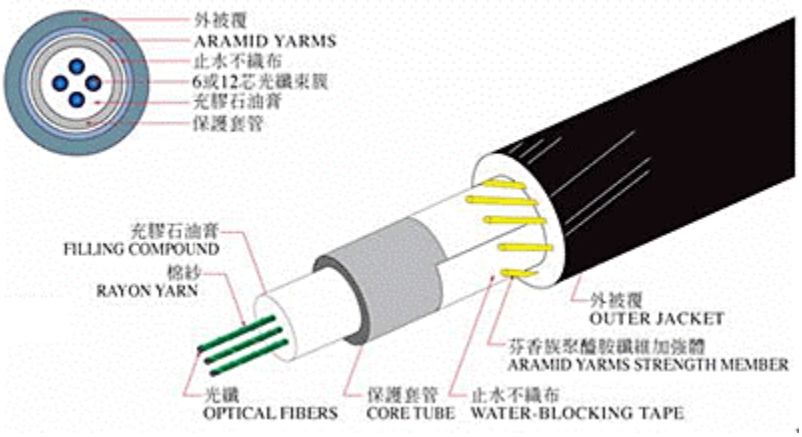
粗同軸電纜構造，由內而外可分為中央銅線、塑膠絕緣體、鋁箔、導體網、鋁箔、導體網、外皮等七層，如圖 1-5.3 所圖示，從外觀上看來，是很明顯的黃色纜線，它所使用的終端 電阻稱為 N 型終端電阻。

1-5.4 粗同軸電纜

粗同軸電纜使用的導線是 RG-11，也是使用 Bus 網路拓樸， 因此纜線的兩端同樣需要 50 歐姆終端電阻。粗同軸電纜連接須使用 TAP 掛上同軸電纜，TAP 除了一端用探針連上纜線，另一端則連上收發器(Tranceiver)，收發器則透過 AUI 纜線連上具有 AUI(Attachment Unit Interface) 接頭的網路卡，其中 AUI 纜線最長不可超過 50 公尺。

光纖纜線

光纖 (Fiber Optic) 纜線以基本構造由內而外分別是 Core、Cladding 以及保護外皮所組成；它的 Core 組成成分可能是塑膠(Plastic)或玻璃 (Glass)，不過傳播光波距離上，玻璃比塑膠好；Cladding 是強化包材一般是使用玻璃。不同於電子媒介，光纖使用光作為傳輸媒介，因此光纖必須要使用光源，光源可以是發光二極體(Light Emitting Diode)或雷射二極體 (Laser Diode)，傳送方式是靠不斷的反射來達到另一端。如圖 1-5.3 所圖示：



1-5.5　光纖纜線

表 1-5.4 雙絞線、同軸電纜、光纖比較

	細同軸電纜	粗同軸電纜	雙絞線	光纖
最大長度	185M	500M	100M	2~5KM
網路規格	10Base-2	10Base-5	10Base-T/ 100Base-TX	10Base-FL/ 100Base-FX/ 1000Base-SX/ 1000Base-LX
可連接節點數	30	100	2	2
網路拓樸	Bus	Bus	Star	Star
連接接頭	BNC	AUI	RJ-45	ST/SC
優點	安裝容易、支援頻寬較高	傳遞距離長、支援頻寬較高、安裝容易、	價格低廉、安裝容易、	體積小、重量輕、安全性高、距離遠、頻帶寬
缺點	維護不易、易遭竊聽	安裝較困難	易受干擾	價格高

相關試題

1.(C)下列何種傳輸媒介最容易受到雜訊干擾：

(A) coaxial cable

(B) STP

(C) UTP

(D) fiber

2.(B)光波透過光纖傳輸，其能量若損失四倍，訊號衰減的 db 數大約為？

(A) 3db

(B) 6db

(C) 12db

(D) 24db

3.(D)雙絞線終將一對線材互相交錯纏繞的原因是?

(A) 美觀

(B) 節省空間

(C) 加強訊號強度

(D) 減少雜訊干擾

第二章　網際網路介接基礎

2-1Introduction to Computer System(計算機系統)

首先先說計算機系統是什麼意思,所謂的計算機系統通常指的就是我們常用的有視窗介面的windows或者是Linux兩者最大的區別就是計算機系統一定有使用者介面不管是windows的視窗介面或Linux的純文字介面可是嵌入式系統就不一定有使用者介面了。

2-1.1circuit switching

電路交換(circuit switching)所謂的電路交換就是以電路聯接為目的的交換方式是電路交換方式。 電話網中就是採用電路交換方式。 我們可以打一次電話來體驗這種交換方式。 打電話時，首先是摘下話機撥號。 撥號完畢，交換機就知道了要和誰通話，並為雙方建立連接，等一方掛機後，交換機就把雙方的線路斷開，為雙方各自開始一次新的通話做好準備。 因此，我們可以體會到，電路交換的動作，就是在通信時建立(即聯接)電路，通信完畢時拆除(即斷開)電路。 至於在通信過程中雙方傳送資訊的內容，與交換系統無關。

舉例來說：我們假設有 A、B 兩個城市，每個城市都有一部交換機並有一千個用戶，兩個交換機之間用 100 條中繼線連接著。 那麼，如果我們說：在 A 城的兩個用戶之間建立一條電路，我們指的是把兩條用戶線路通過 A 城的交換機聯接起來。 但當我們說：在 A 城的一個用戶和 B 城的一個用戶之間建立一條電路時，我們指的就是由 A 城的用戶線路經 A 城交換機聯接到 A、B 城之間的一條中繼線路，在經 B 城交換機聯接到 B 城的用戶線路上。 由於經濟上的原因，中繼線路總是大大少於用戶線路，並且為所有用戶所共用。 那麼，當我們佔用了一條中繼線路以後，即使我們不傳送資訊，別人也不能使用，這就是電路交換最主要的缺點。

在電話通信中，由於講話雙方總是一個在說，一個在聽，因此電路空閒時間佔大約 50%。

相關試題

下列何者使用 circuit switching 之技術?(C)
(A)X.25
(B)Frame Relay
(C)PSTN
(D)Internet

2-1.2 Subnet Mask

子網路遮罩(Subnet Mask)也稱為網路遮罩(Network Mask)。子網路事實上就是網路上的分支。它藉由決定哪一部份 IP 位址組成子網路，以及哪一部份 IP ... 主機與閘道器都會使用子網路遮罩來識別網路及子網路號碼所使用的位元。

GateLock 提供的子網路遮罩為 255.255.255.0。前三個數字為 255，表示網路的 IP 位址。最後一個數字應在 1 至 254 之間，可用來識別網路上的主機。因此當使用子網路，IP 位址會劃分為子網路號碼及主機號碼。主機與閘道器都會使用子網路遮罩來識別網路及子網路號碼所使用的位元。

相關試題：
下列哪一個是 class B IP 網路的子網罩(subnet mask)：(D)
(A)255.0.0.0
(B)255.126.0.0
(C)255.252.0.0
(D)255.255.0.0

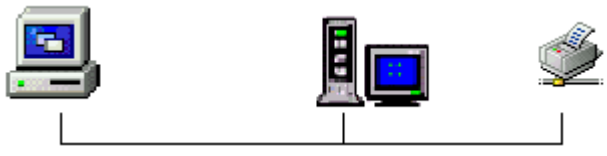
2-1.3 Client Server

客戶端伺服器(Client Server)一般在比較大型的辦公室裡面，使用的都是 Client/Server 網路架構。

相對於 Peer/Peer 網路，Client/Server 網路可以提供更好的集中管理和控制，同時在擴展能力上也比較強，(雖然 P/P 網路也容易擴展，但如果超過 50 台電腦就不那麼好玩了)。或許 C/S 網路最討好的地方是能夠提供嚴謹和更充份的網路安全服務，而避免了沒有經過批准的連線。

大多數 C/S 網路使用者必須先輸入使用者名稱(ID)和密碼(password)才能連接網路，ID 和 password 永遠是一對的。當使用者繼續嘗試使用到網路服務(如檔案，程式)的時候，不同的 ID 所擁有的權限是不同的，比如：有些只能讀取，有些則可以修改，有些甚至可以刪除和建立。

再到程式的使用，也可以在設定上是否需要密碼，如果有設定需要，可以使用相同的網路密碼，也可以使用不同的 ID 和密碼，端看程式的設計。離開了 ID 和密碼，您將使用不到任何的網路資源。雖然在 P/P 網路上面也有密碼，但其設定和管理上面則比 C/S 鬆散得多。



Client / Server Network 圖４－１・３

相關試題：

使用瀏覽器來存取網頁伺服器上的資料，這種資料存取的架構，稱為?(A)

(A)Clinet-Server 架構

(B)Master-Slave 架構

(C)Cooperation 架構

(D)Load Share 架構

2-2 Router Concepts

路由器概念(Router Concepts) Router 路由器 路由器是用來將網路的資訊在電腦之間傳送的基本設備，路由器的工作在於 OSI 模式第三層（網路層），用來決定資料傳遞的路徑的設備。

我們使用的 IP 協定就是藉由路由器將不同的 IP 位址連接在一起。網路上的資料分成一段一段的封包 packet，而這些封包要指向何處便是由路由器來決定的，路由器會根據資料的目的地，指示正確的方向，計算評估最便捷有效率的路徑來傳輸資料，也就是說路由器要為封包做最佳化的工作，找出最適當的路徑。

一個路由器無法全程服務，而是由數個路由器來服務。也就是說，每個路由器所負責的是一段路徑的傳送，而這段傳送的路徑和方式，都可以由路由器就視當時的條件決定，假設決定的路徑發生狀況，路由器還會重新決定新的方向，讓資料迅速傳到目的地。

路由器的功能和作用 路由器的基本功能是，把資料傳送到正確的網路，包 括：

1. IP 資料報的轉發，包括資料報的尋徑和傳送。
2. 子網隔離，抑制廣播風暴。
3. 維護路由表，並與其他路由器交換路由資訊，這是 IP 轉發的基礎。
4. IP 資料報的差錯處理及簡單的擁塞控制。
5. 實現對 IP 資料報的過濾和記帳。

相關試題：

一般而言，路由表(routing table)中不會出現何種資訊：(B)

(A)Next hop address

(B)MAC address

(C)Network address

(D)Metrics

下列哪些是構成 Router 主要的元件？(ACD)

(A)作業系統

(B)大容量硬碟

(C)網路介面

(D)CPU 與 RAM

2-3 IP Addressing(IP 位址)

IP→Internet Protocol 網際網路通信協定，主要規範網際網路路由交換的定址部份。

IP address→網際網路位址，在網際網路上每台電腦都需要有一個個別而不重複的位址才能正確的傳遞資訊，就如同門牌號碼一般，這樣寄信的時候才知道寄到哪裡，回信也才知道回給誰。IP 位址是由 32bit 的二進位數所組成，例如：11000000 10101000 10101110000111111，為了方便一般人使用，一般以換算成四組十進位數值表示。

2-3.1 TTL(Time to Live)

1.TTL 欄位：用來限制封包在網路上存活期的計數器，以秒為單位計數，最大為 255 秒。封包傳送跨越節點時必須遞減此欄位之值，當計數為 0 時，封包會被丟棄，並傳回一警告封包給來源端主機。其作法使用 actual time 或 hop count.。

2.使用 actual time 計算有實際困難，因為封包經過（router）時若停留在 queue 內太久時則必須減去許多秒，試想 router 要處理網路的封包何其多，對於有類別封包及 packet scheduling、設備執行速度快慢時，那對絕對是一大問題，況且在 Internet 上的 router 執行封包轉送速度不一。搞不好經過幾個 router 就時間消耗 TTL 被減至 0 而丟棄。另一個問題還要設定統一的 global timer 來計時，這實計上要執行亦有困難。

3. 因為使用實際時間來計算有其問題，故目前 TTL 都使用 hop 為單位，TTL field 可使用 8 個 bit 來表示 hop 數。每當封包經過一個路由器，其存活時間就會減一，當其存活時間是 0 時，主機便丟棄封包，並傳送一個 ICMP 封包給來源端主機。

相關試題：

TTL(Time to Liev)的主要用處何在：(C)

(A)避免行程路由迴路

(B)加速封包在網路傳送的速度

(C)避免封包在路由迴路內無止境地傳送

(D)偵測錯誤封包

2-3.2 IP 位址的分類

IP 可以分成五個種類為：

Class A

Class B

Class C

Class D

Class E

類別 A IP 位址

類別 A IP 位址的最左邊位元固定為 '0'，後接 7 個網路位元及 24 個主機位元。由於有 7 個網路位元 'ONNNNNNN'，故可提供 2^7 = 128 個網路系統，該位元組的十進位則介於 0 ~ 127 之間，其中 0 和 127 兩個網域做特殊用途使用。

除了 '0.0.0.0' 和 '127.0.0.0' 兩個網域外，類別 A IP 位址另外保留網域 '10.0.0.0'，提供給企業內網路（Intranet）IP 位址設定。由於 Intranet 彼此間獨立的網路架構，故分別使用 '10.0.0.0' 網域並不會互相衝突。若 Intranet 要與外部的 Internet 連繫，必須透過「網路位址轉譯（Network Address Translation，NAT)」路由器提供一個可辨識使用的 IP 位址與外界溝通。由於各個 Intranet 均可提供以 '10.0.0.0' 為網域的所有主機位址，故可改善 IP 位址不足的現象。

由上述可知，原本 128 個網路系統，扣掉 0、10、127 三個特殊網域，故實際上可用的網域為 1 ~ 9、11 ~ 126 共 125 個網域。

類別 A IP 位址的 24 個主機位元則可提供 2^24 個主機位址，各位元組的十進位值介於 0 ~ 255 之間，其中將所有主機位元設為 '0'，用十進位將 IP 位址表示成 'N.0.0.0' 為網域位址；將所有主機位元設為 '1'， 用十進位將 IP 位址表示成 'N.255.255.255' 為廣播位址。故個主機位址扣掉網域位址和廣播位址，實際上可用的主機位址為 2^24 -2 = 16,777,214 個。

從上述得知類別 A IP 位址可提供 125 個網域，而各網域可用（ 2^24－2)個主機位址，故 A 類位址共可提供約 125 × 16,777,214

= 2,097,151,750 個 IP 位址。類別 A IP 位址已分配給早期參與 Internet 的組織機構使用，所以現在沒有空的類別 A IP 位址以供申請。

類別 A IP 位址保留 '127.0.0.1' 用來進行「迴路回測（Loopback Testing)」，主要是透過本身主機將訊息送回本身主機，以檢查主機的 TCP / IP 的設定是否正確，所使用的指令為 'ping 127.0.0.1'，若 TCP / IP 設定不完整會出現錯誤訊息。

類別 B IP 位址

類別 B IP 位址的最左邊兩個位元固定為 '10'，後接 14 個網路位元及 16 個主機位元。IP 位址的左邊第一個網路位元組 '10NNNNNN' 可提供 2^6 個組合，該位元組的十進位值介於 128 ~ 191 之間，而第二個網路位元組 'NNNNNNNN' 則可提供 2^8 個組合，十進位值介於 0 ~ 255 之間; 另外，類別 B IP 位址保留 '172.16.0.0 ~ 172.31.255.255' 網域作為企業內網路（Intranet）使用。由此二個網路位元組即可提供 2^14 -8 = 16,376 個網路系統（網域)。

類別 B IP 位址的 16 個主機位元則可提供 2^16 個主機位址，各位元組的十進位值介於 0 ~ 255 之間，同樣將所有主機位元設為 '0'，十進位 IP 位址表示法 'N.N.0.0' 為網域位址；將所有主機位址設為 '1'，十進位 IP 位址表示法 'N.N.255.255' 為廣播位址。故個主機位址扣掉網域位址和廣播位址，實際上可用的主機位址有 2^16 - 2 = 65,534 個。類別 B IP 位址也已發送完畢，所以現在沒有空的類別 B IP 位址以供申請。

由上述可知，類別 B IP 位址可提供 2^14 個網域，而各網域可用 65,534 個主機位址，故類別 B IP 位址共可提供約 16,376 × 65,534 = 1,073,184,784 個 IP 位址。

類別 C IP 位址

類別 C IP 位址的最左邊三個位元固定為 '110'，後接 21 個網

路位元及 8 個主機位元。IP 位址左邊第一個網路位元組 '110NNNNN' 可提供 2^5 = 32 個組合，該位元組的十進位值介於 192 ~ 223 之間，而第二、三個網路位元組 'NNNNNNNN' 則分別可提供 2^8 = 256 個組合，十進位值介於 0 ~ 255 之間，此三個網路位元組可提供 2^21 = 2,097,152 個網路系統（網域）。

類別 C IP 位址的 8 個主機位元則提供 2^8 = 256 個主機位址，該主機位元組的十進位值介於 0 ~ 255 之間，同樣將所有主機位元設為 '0'，十進位表示法 'N.N.N.0' 為網域位址；將所有主機位元設為 '1'，十進位表示法 'N.N.N.255' 為廣播位址。故 256 個主機位址扣掉網域位址和廣播位址，實際上可用主機位址有 254 個。

另外，類別 C IP 位址保留 '192.168.0.0' 網域作為企業內網路（Intranet）使用。由此可知 C 類位址可提供 2,097,152 - 1 = 2,097,151 個網域，而各網域可用 254 個主機位址，故 C 類位址共可提供約 2,097,151 × 254 = 532,676,354 個 IP 位址。

類別 D IP 位址

類別 D IP 位址的最左邊四個位元固定為 '1110'，後接 28 個群播設定位元。IP 位址的左邊第一群播位元組 '1110MMMM' 可提供 2^4 個組合，十進位介於 224 ~ 239 之間，其他三個群播位元組則分別提供 2^8 個組合，十進位值介於 0 ~ 255 之間，故類別 D IP 位址共可提供 2^28 = 268,435,456 個群播 IP 位址。多點傳送操作並沒有區分網路位元與主機位元。

所謂「多點傳送（Muticasting）」，或稱「群播」，是指一電腦主機可透過「多點傳送路由器（MRouter；Muticasting Router）」同時對多部主機傳送相同的資料。使用單點傳送（1 對 1）將相同資料送到三台主機，需要傳送三次才能完成；而多點傳送（1 對多）只需傳送一次即可，故多點傳送可以降低在網路上的資訊傳送量。欲進行多點傳送的群組必須擁有一個類別 D IP 位址方可彼此連繫。

在類別 D IP 位址中，224.0.0.0 ~ 224.0.0.255（224.0.0.0/24）是保留給區域子網路（local subnet）之用，其封包不會被路由器傳

送出去，不論其 TTL 為何；而 IP 位址在 224.0.1.0 ~ 238.255.255.255 是為多點傳送正常使用；IP 位址在 239.0.0.0 ~ 239.255.255.255（239.0.0.0/8）則是保留給管理用途。

Microsoft 支援類別 D IP 位址，作為應用程式多點傳送資料至 Internet 上可多點傳送的主機。

類別 E IP 位址

類別 E IP 位址最左邊四個位元固定為 '1111'，後接 28 個保留位元。IP 位址的左邊第一個保留位元組 '1111RRRR' 之十進位值介 240 ~ 255 之間，類別 E IP 位址和類別 D IP 位址一樣，沒有網路位元和主機位元，共可提供 2^28 = 268,435,456 個 IP 位址。類別 E IP 位址是保留給實驗網路所使用。

相關試題：

IP位址總共分成哪幾種Class(分類)?(C)

(A)Class A,B

(B)Class A,B,C,D

(C)Class A,B,C,D,E

(D)Class A,B,C

2-3.3 IPv4 與 IPv6 有什麼不同

1. 位址空間

IPv4=32 bits（共有 2 的 32 次方個 IP 組合）

IPv6=128 bits（共有 2 的 128 次方個 IP 組合）

2. 封包傳送類型

IPv4 有 Unicast, Multicast 及 Broadcast

IPv6 有 Unicast, Multicast 及 Anycast

3. 位址表示法

IPv4 用 10 進位，例如：168.95.1.1

IPv6 用 16 進位，例如：2003:4a01:5b02:6c03:7d04:8e05:9f06:005a

4. 專有名詞

IPv4 用 Network ID，Host ID 與 Subnet Mask

IPv6 用 Prefix, Interface ID 與 Prefix-length

5. 設定方式

IPv4 只有手動設定與自動取得兩種

IPv6 則有完全手動設定，EUI-64 手動設定，Stateless 自動取得與 Stateful 自動取得四種

6. RFC Link-local 位址

IPv4=169.254.0.0/16，且必須為無法自動取得 IP 時才會出現

IPv6=FE80::/10，且每一張介面一定都會有

7. RFC Loopback 位址

IPv4=127.0.0.0/8（共 16777214 個 IP 代表自己）

IPv6=::1（只用一個 IP 代表自己）

以上為最基本的差別

要注意 IPv6 是一個全新設計的協定

並不是 IPv4 的改良版哦

相關試題：

採用 IPv6 比 IPv4 的優點有哪些？(AC)

(A)可以分配的 IP 位址較大

(B)可以重複使用相同的 IP 網段在 Internet 上

(C)本身具備有 IP Mobility(漫遊)的設計

(D)IPv6 可以提供 64Bit 長度的位址空間

2-4 TCP/IP Protocol(TCP/IP 通訊協定)

TCP/IP 協定，包含了一系列構成網際網路基礎的網路協定。這些協定最早發源於美國國防部的 ARPA 網項目。TCP/IP 字面上代表了兩個協定：TCP（傳輸控制協定）和 IP（網際協定）。

2-4.1 UDP(用戶數據報協議)

用戶數據報協議（User Datagram Protocol, UDP）是一個簡單的面向數據報的傳輸層協議，IETF RFC 768 是 UDP 的正式規範。

在 TCP/IP 模型中，UDP 為網路層以下和應用層以上提供了一個簡單的介面。UDP 只提供數據的不可靠傳遞，它一旦把應用程序發給網路層的數據發送出去，就不保留數據備份（所以 UDP 有時候也被認為是不可靠的數據報協議）。UDP 在 IP 數據報的頭部僅僅加入了復用和數據校驗（欄位）。

UDP 首部欄位由 4 個部分組成，其中兩個是可選的。各 16bit 的來源埠和目的埠用來標記發送和接受的應用進程。因為 UDP 不需要應答，所以來源埠是可選的，如果來源埠不用，那麼置為零。在目的埠後面是長度固定的以位元組為單位的長度域，用來指定 UDP 數據報包括數據部分的長度,長度最小值為 8byte。首部剩下地 16bit 是用來對首部和數據部分一起做校驗和（Checksum）的，這部分是可選的，但在實際應用中一般都使用這一功能。

但是絕大多數 UDP 應用都不需要可靠機制，甚至可能因為引入可靠機制而降低性能。流媒體、實時多媒體遊戲和 IP 電話 (VoIP)就是典型的 UDP 應用。如果某個應用需要很高的可靠性，那麼可以用傳輸控制協議來代替 UDP。

由於缺乏擁塞控制(congestion control)，而導致的擁塞崩潰效應。換句話說，因為 UDP 發送者不能夠檢測擁塞，所以像使用包隊列和丟棄技術的路由器這樣的網路基本設備往往就成為降低 UDP 過大通信量的有效工具。這些應用包括域名系統(DNS)、簡單網路管理協議(SNMP)、動態主機配置協議(DHCP)、路由信息協議(RIP)和某些影音串流服務等等。

相關試題：

指出使用 UDP 服務的應用協定有哪些：(複選) (B、C)

(A)HTTP

(B)RTP

(C)SNMP

(D)BGP

2-4.2 SSH(Secure Shell)

SSH 為 Secure Shell 的縮寫，由 IETF 的網路工作小組（Network Working Group）所制定；SSH 為建立在應用層和傳輸層基礎上的安全協議。

傳統的網路服務程序，如 FTP、POP 和 Telnet 其本質上都是不安全的；因為它們在網路上用明文傳送數據、用戶帳號和用戶口令，很容易受到中間人（man-in-the-middle）攻擊方式的攻擊。就是存在另一個人或者一台機器冒充真正的伺服器接收用戶傳給伺服器的數據，然後再冒充用戶把數據傳給真正的伺服器，透過 SSH 可以對所有傳輸的數據進行加密，也能夠防止 DNS 欺騙和 IP 欺騙。

SSH 協議框架中最主要的部分是三個協議：

1.傳輸層協議（The Transport Layer Protocol）：傳輸層協議提供伺服器認證，數據機密性，信息完整性等的支持。

2.用戶認證協議（The User Authentication Protocol）：用戶認證協議為伺服器提供客戶端的身份鑒別。

3.連接協議（The Connection Protocol）：連接協議將加密的信息隧道復用成若干個邏輯通道，提供給更高層的應用協議使用。

相關試題：

SSH 是使用 TCP 什麼 PORT 呢？(C)

(A)211

(B)161

(C)22

(D)25

2-5 IPX Protocol(IPX 通訊協定)

由 Novell 公司提出的運行於 OSI 模型第三層的協議。具有可路由的特性。IPX 的地址分為網路地址和主機地址，網路地址由管理員分配，主機地址為 MAC 地址。由於 IP 協議的廣泛使用，IPX 的應用逐漸減少。

相關試題：

IPX 是由哪家公司所推出的網路協定？(B)

(A)Microsoft

(B)Novell

(C)IBM

(D)Cisco

2-6 Routing Protocol(路由器通訊協定)

路由器是一種計算機網路設備，它能將數據包通過一個個網路傳送至目的地，這個過程稱為路由。

功能：路由器就是連接兩個以上網路線路的設備。由於位於兩個或更多個網路的交匯處，從而可在它們之間傳遞分組（一種數據的組織形式）。路由器與交換機(Switch)在概念上有一定重疊但也有不同：交換機泛指工作與任何網路層次的數據中繼設備（儘管多指網橋），而路由器則更專注於網路層。

2-6.1 BGP(邊界網關協議英文：Border Gateway Protocol)

邊界網關協議是網際網路的核心路由協議。它通過維護路由表來實現自治系統（AS）之間的可達性，屬於路徑向量協議。BGP 不使用傳統域內路由協議的距離度量，而是基於路徑、網路策略和規則集來決定路由。

自從 1994 年以來，BGP 版本 4 在網際網路上廣泛使用，更早的版本都已經廢棄。版本 4 的主要改進在於支持無類型域間路由（CIDR）並使用路由聚類來減小路由表的尺寸。

相關式題：

BGP (Border Gateway Protocol)：(B、C)(複選)

(A)是 IRP(interior router protocol)。

(B)是 ERP(exterior router protocol)。

(C)運作於 TCP 之上。

(D)運作於 IP 之上。

2-6.2 IGRP(Interior Gateway Routing Protocol, IGRP)

內部網關路由協議是一種相似於內部路由協議(Interior gateway protocol, IGP)的一種動態距離向量路由協議 Distance-Vector Routing Protocol 以自治系統 （Autonomous System, AS）的方式提供路由選擇路由協議(Routing Protocol),由思科(Cisco)私有的協議於上世紀的 80 年代中葉發展出來，透過用戶配置，如廷遲，頻寬、可靠性及負載量等於各路由器進行的路由管理。

相關試題：

IGRP 利用下列何種資訊來計算最佳路徑：(D)

(A)Reliability,Delay,Cost,Hop,count

(B)Cost,Reliability,Delay,Bandwidth

(C)Loading,Cost,Reliability,Delay

(D)Bandwidth,Delay,Reliability,Loading

第三章 網際網路的服務與應用

3-1 Introduction to System Development and Operation

3-1.1 TANET

TANet 將全台灣共分為數個區域，每個區域分別成立一個以國立大學計算機中心為主要成員的區域網路中心，負責該區所有相關事宜。

3.2 Internet Services 「FTP、Mail、DNS」

3-2.1 FTP

檔案傳輸協定(FTP)主要用來傳輸檔案所使用的協定，目前學術網路上所提供的網路資源當中，最常使用的項目之一。

明白來說 FTP 就是用來的規範電腦之間傳輸檔案的共同協定(也就是規則)，因此兩部不同的電腦之間傳遞檔案時，雖然檔案格式或本身電腦系統不同，但透過 FTP 協定就可以很容易讓兩部電腦檔案傳送順利進行。

3-2.2 POP3

POP 即為 Post Office Protocol 的簡稱，是一種電子郵局傳輸協議，而 POP3 是它的第三個版本，是規定了怎樣將個人計算機連接到 Internet 的郵件服務器和下載電子郵件的電子協議。它是 Internet 電子郵件的第一個離線協議標準。簡單點說，POP3 就是一個簡單而實用的郵件信息傳輸協議。

3-2.3 SNMP

簡易網路管理協定(SNMP)為 Simple Network Management Protocol 的簡稱，也是網際網路的標準之一，它讓網路上不同的設備，產生具有共通標準，且可供網路管理的資料。這些資料，可進一步由網管應用程式來讀取或是進行監控。也就是說，只要網路設備上

擁有 SNMP 代理者（Agent）之機制，我們就可以使用網路管理軟體，透過這些代理者，檢視或監控其設備上的相關網管資訊。

當網路的建設愈來愈多時，就會發現到，當網路出問題時，你光要找出那一個裝置發生故障，就得花費相當大的時間、人力成本。這時如果有一套網路設備的管理系統的話，你就可以很快的得知是那一台那一部份出了問題。

而 SNMP 就是一種這方面的一種簡易型協定，有支援 SNMP 的設備，你就可以透過一台具有支援 SNMP 的管理軟體去取得那些設備的狀態、警告、使用情況。

3-2.4 TFTP「Trivial File Transfer Protocol」

簡單文件傳輸傳輸協定，TCP/IP 傳輸協定族中的一個用來在客戶端機與伺服器之間進行簡單文件傳輸的傳輸協定，提供不複雜、預先配置不大的文件傳輸服務。TFTP 承載在 UDP 上，提供不可靠的資料流傳輸服務，不提供存取授權與認證機制，使用超時重傳方式來保證資料的到達。與 FTP 相比，TFTP 的大小要小的多。現在最普遍使用的是第二版 TFTP。

一、等級 0 (TP0)－簡單等級(Simple Class)：

具備最基本的運送連接功能，其流量控制、連接釋放有賴於網路層的協助，且並不提供緊急資料的處理。

二、等級 1(TP1)－基本錯誤回復等級(Basic Error Recovery Class)：

除具備等級 0 的功能之外，並能根據網路層的錯誤回報或連接釋放，作一些簡單的錯誤回復。若網路層提供緊急資料傳送的功能，等級 1 亦可讓使用者有傳送緊急資料的選擇。

三、等級 2 (TP2)－多工等級(Multiplexing Class)：

提供多工的功能，數條運送連接的資料可以經由一條網路連接傳送。並具備擴充性編號(Extended Numbering)，使用較大的接收窗(Receive Window)來進行資料量的控制和錯誤回復。

四、等級 3(TP3)－錯誤回復多工等級(Error Recovery and

Multiplexing Class)：

為等級 1 與等級 2 功能的總合。

五、等級 4(TP4)－錯誤偵測和回復等級(Error Detection and Recovery Class)：

為功能最強的一個等級，除了具備等級 3 所有的功能外，並能偵測出資料的流失、重複、失序等狀況，而做回復的工作。

3-2.5 NNTP

「新聞信件傳輸協定」

它不是一個單獨的軟件包，而是一個 Internet 標準。它基一個系統引導連接-通常是通過 TCP-與一個網絡上任何位置的一個客戶。以及一個在磁盤上保留 netnews 的一個 服務器。流向連接允許客戶和服務器內部討論文章傳送而沒有延遲，保証復制文件數量少。加上 Internet 的高傳輸率，使一個新聞傳輸比以前的 UUCP 網絡 快得多。而幾年前，一個文章到達 Usenet 角落需要兩周 以上的時間。而現在只要兩天。在 Internet 本身，可能只是幾分鐘。

許多命令允許用戶恢復，發送和郵遞文章。發送和郵遞之間的區別是者有不完整的標題信息。文章恢復 可能被新聞傳送客戶或則新聞發送者使用。這使 NNTP 成為一個很好的工具用來提供新聞在本地網絡上訪 問許多客戶而不需要使用在 NFS 上必須的歪曲。

NNTP 還提供一個文章和一個新聞傳送的積極的方法。通俗稱為推和拉。推基本上與 C-news ihave/sendme protocol 相同。客戶使用‘‘IHAVE’’命令提供一個文章到服務器，服務器

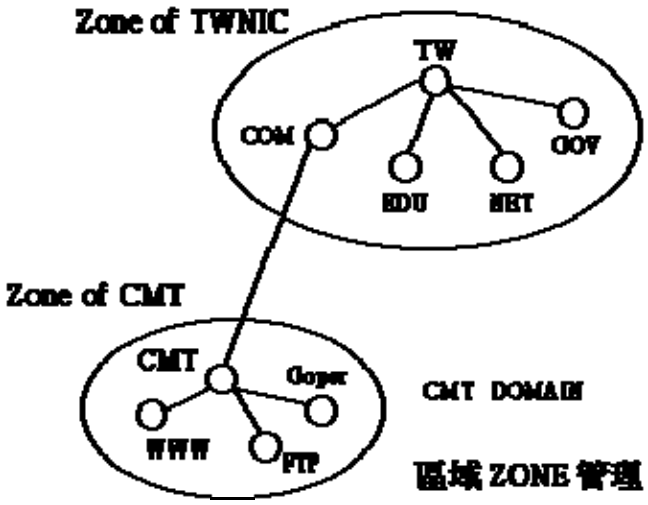
返回一個代碼指出它是否已經擁有了文章，或者它是否需要。如果這樣，客戶發送文章，在一個分開的行上 由一個單獨的點結尾。NNTP 的一個全面的問題是它允許知情者使用假發件人指定插入文章到新聞流。

3-2.6 DNS 「Domain Name System」

網域名稱系統,其主要的目的是用來解釋網際網路上的電腦主機名稱與 IP 位址之間的關係，進而能正確的在網際網路上找到該主機並傳送正確的訊息。其實 DNS 在 Internet 的發展上是很重要的一環，在 Internet 的應用上,我們最常看到它的地方除了網路設定裡的 DNS 設定，其實我們用瀏覽器開啟網址，寄發 E-mail 都和 Domain Name 及 DNS 系統息息相關，網路上的位址是用 IP 來定址的，而如何從 Domain Name 看出正確的位址，就得靠 DNS 系統的運作。

DNS 的架構

DNS 網域名稱的架構是採分散式處理的模式來分類，從根網域出發，分類出不同的分類網域環境,在每一個網域下又可再建立該網域的主機名稱，主機名稱下又可在延伸另一個子網域，整個樹狀結構我們稱為網域名稱空間(Domain Name Space)。



3-3 Internet Caching Technology

3-3.1 ICP

(網際網路內容提供者)指的是在網際網路上提供各種服務內容的廠商。如 Yahoo 雅虎、AOL 美國線上等，都是屬於 ICP 的一種。任何人只要有網路的空間放置網頁，都可以成為 ICP。而 ICP 的收入大都來自廣告收入。

3-3.2 ICMP

「網際控制訊息協定」ICMP 是與 IP 模組整合在一起的控制訊息協定，它透過 IP 收發 ICMP 訊息，ICMP 被用於報告在傳輸資料片(datagram)的過程中發生的各種狀況，包括資料片的目標不存在、遞送路徑不正確等訊息，也可透過 ICMP 測試主機之間的連接是否中斷，甚至利用 ICMP 控制特定主機的資料片流出量。

與 IP 的上層協定相似，ICMP 既然透過 IP 收發控制訊息，其訊息在經 IP 傳送前，自然也被裹上一層 IP 表頭，ICMP 不做錯誤偵測，因此它與 IP 同樣不可完全被信賴，ICMP 訊息內含錯誤報告或回應，其訊息種類有許多，每種訊息的結構不盡相同，主要結構有 6 種，共同的部份為其前導的三個欄位－訊息型別(Type)、訊息代碼(Code)、及核對合(checksum)，後續部份則視訊息型別而有不同。

3-4 Broadband Solutionx

3-4.1 ISDN 「tegrated Service Digital Network」

整體服務數位網路，它是一種公眾通信網路，適用於全世界，它是以數位方式傳送聲音、文字、影像等資訊， 也是一種同時傳送資料與聲音的標準，簡單地說，就是單一介面，提供多種服務。 ISDN 發展的目標是，快速的傳送多媒體資訊。

3-4.2 ADSL 「Asymmetric Digital Subscriber Line」

非對稱數位用戶迴路，乃利用調變技術，藉由普通電話用的雙絞銅線傳輸,將現有的電話線上加裝 ADSL 數據機,利用 ADSL 寬頻技術，用戶可以在使用電話時，同時以高於 512 Kbps 以上的速率上網或進行資料的傳輸。

ADSL 也可以用來提供在家上班者存取公司內部企業網路的服務，或是提供新式互動式多媒體之應用，用戶上網時並不佔用傳統電話的頻帶，亦即是上網與打電話可同時進行，不會互相干擾，且用戶上網時也不必像傳統數據機或單向 Cable Modem 另需支付電話費用。

ADSL 的 Key Point 在於其上行與下行的頻寬是不對稱的，下傳速率提昇至 1.5Mbps～9Mbps,上傳速率則提昇 64Kbps～到 640Kbps，由於上、下傳速率不等因而稱為非對稱。應用 ADSL 的技術，不需要再增加現有基礎架構設備，只要用戶端加裝 ADSL 數據機，就可以在使用電話時，同時上網或進行資料的傳輸。從網路提供者到用戶家中(謂之下行) 的頻寬是比較高的，這樣的設計一方面是配合現有電話網路頻譜的相容性,另一方面也符合了一般使用網際網路的使用習慣與特性，也就是說使用者接收的資料量遠比其送出的資料量來得多。

3-4.3 HDSL 「High Data Rate DSL」

高速數位用戶迴路，是採用上下行對稱技術傳送 1.544 Mbps 及 T1 速率，初期的市場定位在於企業客戶須採用高速且對稱速率的環境下，必須使用兩對線，且不管距離長短皆固定 T1 速率在傳輸線上及用戶端只用 64Kbps 之頻寬。

因為它可快速將系統架設在現有用戶迴路架構上，大量減少安裝雙絞銅質電話線時間數天之久，其優異操作性能及成本優勢顯示在它現有之銅纜線，附有 T 接頭 (Bridge Tap) 環境的優點，然而它有 3 Miles 的距離限制，需要加裝訊號放大器 (Repeater)，以增加傳送 E1/T1 資料傳送的距離。

HDSL 雖然可以省略中繼器以放大訊號，且使用既有的用戶迴路，省下大筆佈建成本，但是 HDSL 需要使用兩對雙絞線，而使得用戶迴路必須重新拉線，大幅增加電信業者線路佈建費用之支出，此乃為其之一大缺點。

3-4.4 SDSL 「Symmetric Digital Subscriber Line 」

對稱式數位用戶迴路，是一種對稱性的 xDSL 技術，SDSL 技術特性與 HDSL (高速數位用戶迴路)相同，不同的地方在於它只利用一對雙絞線，也是採取雙向對稱傳輸方式，深受企業客戶喜愛。SDSL 傳輸技術上、下行速率皆達 2320 Kbps 的特性，對於家庭客戶而言，網路應用大多以讀取資料為主，網路端下載的資料流量遠比用戶端上傳的資料流量大，較不適用家庭客戶，而有家庭客戶較適用於 ADSL(非對稱數位用戶迴路) 的傳輸技術。

SDSL 傳輸利用一對雙絞線以全雙工 T1 或 E1 方式，而且是 xDSL 技術中最成熟的一種，較適合企業客戶、網頁設計者及 SOHO 族等資料上傳量大之客戶使用，亦是低成本 T1 連線之替代方案。SDSL 傳輸優於 ADSL 的流量，因為 ADSL 為不對稱頻寬，上傳較窄的頻寬無法在

視訊傳輸上發揮效用;又因為 SDSL 是使用專用網路,防火牆也較 ADSL 可以保證資料和通訊的機密，免於駭客入侵。相較於 Cable Modem 為一共享頻寬，速度隨使用人數增加而降低，如用 SDSL 的話，即使在尖峰時間也能保證有最高的傳輸速率。

SDSL 是傳統數據專線的一種替代技術，主要應用於高頻寬視訊會議、遠程教學及專用寬頻網路的建立等。且不受電話交換機的影響，不須占用電話線路之頻寬，更不會因為電信機房之電話交換機當機而上不了網路，同時也不影響原有的通話品質。

3-4.5 VDSL 「Very High Data Rate DSL」

超高速數位用戶迴路，這是目前速度最快的 xDSL 技術，顧名思義較 HDSL (高速數位用戶迴路)為快，主要依據線路長短不同而改變，進行雙向等速的對稱式傳輸。只要利用一條雙絞線，即可擁有 12.9Mbps 到 52.8Mbps 的速度，甚可高達 60Mbps。

VDSL 與 ADSL 一樣，是以銅質電話線傳輸的 xDSL 寬頻解決方案家族成員，但比起 ADSL 離固網機房約 4 公里的距離限制，VDSL 有效傳輸距離只有幾百公尺，是「光纖到府」時代可望實現的寬頻上網解決方案。VDSL 的缺點是傳輸速度與傳輸距離成反比，大多數配線無法達到其品質要求,因此用戶端數百呎以內線路不能使用一般的數位式電路，一定要使用光纖數位電路才行。而且 VDS 的制定目前還沒有一套標準，是故距真正普及應用還需要進一步的努力。

3-5 VOIP 「Voice over IP」

網路電話，廣指凡以 Internet 協定在一數據網路上執行任何通信應用者。凡透過網際網路進行語音通訊的應用方式，都可說是網路電話的一環，網路電話系通過語音壓縮的設備對話音進行壓縮編碼處理，然後把這些語音資料根據相關協定進行打包，經過 IP 網路把資料包傳輸到目的地，再把語音資料包串起來，經過解碼解壓處理後，恢復成原來的語音信號，而每通電話均佔用一特定頻寬，從而達到由 IP 網路傳送話音的目的。

「網路電話」和「傳統電話」於架構上有明顯的不同。傳統電話是透過「公用交換電話網」的電路交換網路來提供聲音；而「網路電話」則是利用閘道(Gateway)技術，將語音封包透過網際網路送出。每一個封包傳送時都經過加密並附有地址及目的地，當封包到達目的地時會經過重組，並再轉換成一般的通話聲音。

網路電話透過網際網路比透過電路交換網路所傳輸的資料多很多。一條傳統電話的語音頻道需要 64Kbps，然而網路電話每一語音頻道依據使用的壓縮技術最多只使用 20-25Kbps 的頻寬，而且可以和其他數據資料共同使用同一條線路，這樣所帶來的好處不僅可降低成本，同時也有效提升在頻寬上傳遞即時語音的應用。

優點

有效節省成本.網內互打免費(包含國際電話），撥打傳統電話與手機可節省話費約 20~80%

整合電信語音與數據網路，有效提高效能比傳統 PSTN 電話的頻寬高出 8 到 10 倍

建置方便，擴充性高，降低維修成本有效利用網路資源安全的溝通及多元化的服務支援多重資料傳送(Voice, Fax, Date, Multimedia)

3-5.1 H.323 通訊協定簡介

H.323 通訊協定是由 International Telecommunications Union (ITU) 所推薦的，做為經由封包交換網路（如網際網路及企業網路）進行多媒體通訊之標準。這些標準界定了各單元間如何建立通話程序、如何交換經壓縮後的音訊及視訊資料、如何建立多方通話、及如何與非 H.323 相容的端點互動。

3-5.2 ISP 介紹

隨著 INTERNET 的蓬勃發展，現行最多人使用的 VoIP 技術 (H.323/Hxxx...)已不能滿足多樣化的通訊方式，且 ITU 在 90 年代初所訂定的 H.323 等技術亦非完全著眼於 INTERNET 環境的使用。故在 90 年代末期時，由 IETF 主導，經過廣泛討論後，發展出新的協定 SIP(RFC 2543(Session Initiation Protocol)，最新的 RFC 是 2361~2367)，其著眼於 Internet 與 PSTN 整合環境的一種技術，並以純文字，類似 HTTP 協定的方式來傳送指令及狀況，以達到協定簡單化、文字化，而不以訊號來判斷之目的。

H.323 和 SIP 比較

通訊協定	H.323	SIP
發展時間	較早	較晚
開發動機	節省電話費	彌補 H.323、MGCP 缺點
技術差異性	H.323 為較老舊的網路電話協定，雖然已升級到第六版,但仍舊建構在舊有的技術之上	SIP 為最新的 VoIP 通訊協定，開發起因為改善舊有技術的瓶頸和缺點
廠商進入門檻	低	較高
語音話質	較差	有品質控管機制來確保話質，較優
對公司原有網路的影響	會將網路速度減慢 50%，且對網路頻寬要求較多	可支援網路環境下各種不同 IP 型態，頻寬要求較小
系統當機時	所有安裝客戶均無法相互通話	客戶通話完全不受影響，一樣繼續保持暢通
容量限制	約僅能支援 300~500 個客戶	無容量限制，可以無上限地擴充
相容性	較難與以後微軟所推的 SIP 新協定相通	可以和 H.323、MGCP 協定相通，無被排擠的窘境

3-6 QOS

VPN 虛擬專用網

被定義為通過一個公用網絡（通常是因特網）建立一個臨時的、安全的連接，是一條穿過混亂的公用網絡的安全、穩定的隧道。虛擬專用網是對企業內部網的擴展。

虛擬專用網可以幫助遠程用戶、公司分支機構、商業伙伴及供應商同公司的內部網建立可信的安全連接，並保証數據的安全傳輸。通過將數據流轉移到低成本的壓網絡上，一個企業的虛擬專用網解決方案將大幅度地減少用戶花費在城域網和遠程網絡連接上的費用。同時，這將簡化網絡的設計和管理，加速連接新的用戶和網站。另外，虛擬專用網還可以保護現有的網絡投資。隨著用戶的商業服務不斷發展，企業的虛擬專用網解決方案可以使用戶將精力集中到自己的生意上，而不是網絡上。虛擬專用網可用不斷增長的移動用戶的全球因特網接入，以實現安全連接；可用實現企業網站之間安全通信的虛擬專用線路，用經濟有效地連接到商業伙伴和用戶的安全外聯網虛擬專用網。

虛擬專用網至少應能提供如下功能：

.加密數據，以保証通過公網傳輸的信息即使被他人截獲也不會泄露。

．信息認証和身份認証，保証信息的完整性、合法性，並能鑒別用戶的身份。

．提供訪問控制，不同的用戶有不同的訪問權限。

VPN 的分類 根據 VPN 所起的作用，可以將 VPN 分為三類：VPDN、Intranet VPN 和 Extranet VPN。

1. VPDN（Virtual Private Dial Network）

在遠程用戶或移動雇員和公司內部網之間的 VPN，稱為 VPDN。實現過程如下：用戶撥號 NSP（網絡服務提供商）的網絡訪問服務器 NAS（Network Access Server），發出 PPP 連接請求，NAS 收到呼叫，在用戶和 NAS 之間建立 PPP 鏈路，然，NAS 對用戶進行身份驗証，確定是合法用戶，就啟動 VPDN 功能，與公司總部內部連接，訪問其內部資源。

2. Intranet VPN

在公司遠程分支機構的LAN和公司總部LAN之間的VPN。通過Internet這一公共網絡將公司在各地分支機構的LAN連到公司總部的LAN，以便公司內部的資源共享、文件傳遞等，可節省DDN等專線所帶來的高額費用。

3. Extranet VPN

在供應商、商業合作伙伴的LAN和公司的LAN之間的VPN。由不同公司網絡環境的差異性，該產品必須能兼容不同的操作平台和協議。由用戶的多樣性，公司的網絡管理員還應該設置特定的訪問控制表ACL（Access Control List)，根據訪問者的身份、網絡地址等參數來確定他所相應的訪問權限，開放部分資源而非全部資源給外聯網的用戶。

第四章　「 網路安全 」

4-1 Introduction toNetwork Security and standardization

隨著網路的普及，電腦犯罪的手法日漸翻新，也逐漸普遍且複雜化，使資訊安全受到越來越多威脅。資訊安全顧及的是使資訊資產不受到有意或無易地洩漏、破壞、假造，以及未經授權的獲取、使用、修改。然而不管是機關團體的整體資訊安全，或是個人使用上的安全顧慮，通常都是在使用過程中所產生的，因此了解並培養良好的使用習慣是很重要的。

網路通訊安全危機，是透過網路而對電腦造成損害的可能，以下主要分為下列幾種來討論。

駭客

駭客，主要來自英文字「hacker」的翻譯，起初指的是一群熱衷於寫程式的人。這些人認為資訊應該是共享的，因此藉由撰寫一些自由軟體來促進資訊的流通，並將專業分享給他人。因此原先的駭客，指的是一群具有駭客倫理的人。

而今日的「駭客」所帶有的負面意涵，主要是來自「cracker」，稱為破網者，或鬼客。主要指的是一群未經許可便透過網路擅入電腦系統並竊取電腦內部資料的人，他們有著超乎一般人的入侵技巧，從事破壞人或機關團體的網路資訊系統的行為。

病毒

「病毒」一詞最早用來表達此意是在弗雷德·科恩（Fred Cohen）1984 年的論文《電腦病毒實驗》。而病毒一詞廣為人知是得力于科幻小說。一部是 1970 年代中期大衛·傑洛德（David Gerrold）的《When H.A.R.L.I.E. was One》，描述了一個叫「病毒」的程式和與之對戰

的叫「抗體」的程式；另一部是約翰·布魯勒爾（John Brunner）1975年的小說《震蕩波騎士（ShakewaveRider）》，描述了一個叫做「磁帶蠕蟲」、在網路上刪除資料的程式。

1960年代初，美國麻省理工學院的一些青年研究人員，在做完工作後，利用業務時間玩一種他們自己創造的電腦遊戲。做法是某個人編製一段小程式，然後輸入到電腦中運行，並銷毀對方的遊戲程式。而這也可能就是電腦病毒的雛形。

電腦蠕蟲

電腦蠕蟲與電腦病毒相似，是一種能夠自我複製的電腦程式。與電腦病毒不同的是，電腦蠕蟲不需要附在別的程式內，可能不用使用者介入操作也能自我複製或執行。電腦蠕蟲未必會直接破壞被感染的系統，卻幾乎都對網路有害。電腦蠕蟲可能會執行垃圾代碼以發動拒絕服務攻擊，令到計算機的執行效率極大程度降低，從而影響電腦的正常使用。

特洛伊木馬

特洛伊木馬指的是一種後門程式，是駭客用來盜取其他用戶的個人資訊，甚至是遠程控制對方的電腦而加殼製作，然後透過各種手段傳播或者騙取標的用戶執行該程式，以達到盜取密碼等各種資料資料等目的。與病毒相似，木馬程式有很強的隱秘性，隨作業系統啟動而啟動。但不會自我複製，這一點和病毒程式不一樣。

4-2 Network Security threats and Related laws

4-2.1 D O S

阻斷服務(denial of service)攻擊，只要攻擊者企圖阻止網路上某個資源被使用或是傳送給使用者，都屬於阻斷服務攻擊。例如攻擊者剪斷大樓的主要電話線路，或者入侵專用型交換機(PBX)的switch，使得所有對外或對內的連線都中斷。應用在電腦網路上，由於頻寬、記憶體大小和硬體效能，router 或是網路上的 server 只能處理有限的需求，一但達到其上限，合法的流量也會被忽略，攻擊者只要能送給目標特定的大量封包，就可達到阻斷服務攻擊的目。

4-2.2 Internet Protocol Spoofing IPSpoofing

IP 位址欺偽(Internet Protocol Spoofing)是一種攻擊者得知主機位址之後，利用外部封包攻擊主機的方法，由於封包 (Packet) 的來源位址和內部封包一樣，因此主機 (Host) 會認為這是來自內部的封包，因而允許進行鏈結 (Link) ，這種攻擊方法也會被內部破壞者使用。

4-2.3 IDS

入侵偵測系統(Intrusion-detection system)是檢測和響應電腦誤用的學科，其作用包括威懾、檢測、響應、損失情況評估、攻擊預測和起訴支持。入侵檢測技術是為保證電腦系統的安全而設計與配置的一種能夠及時發現並報告系統中未授權或異常現象的技術，是一種用於檢測電腦網絡中違反安全策略行為的技術。進行入侵檢測的軟體與硬體的組合便是入侵檢測系統。

相關試題

1. (A)SSL(Secure sockets Layer) 是再不改變第四層(TCP)以下之通訊協定的情況下， 提供應用程式依個安全的通訊介面(API)，其最大的弱點易受何種攻擊?

(A) 阻絕服務
(B) 資料遭竊取
(C) 系統遭入侵
(D) 病毒攻擊

2.(AB) DOS(Deny of Sever)的攻擊中，下列何者正確?(複選)

(A) 消耗 Sever 的主機資源

(B) TCP Sync flooding 為其中一種

(C) 受害主機遭受網路病毒感染

(D) 受害主機將透過 e-mail 傳播 DoS 病毒

3. (A) 下列何者不是 ITIL(Information Technical Infrastructure Library)的管理機制?

(A) 病毒碼管理
(B) 問題管理
(C) 設定管理
(D) 更變管理

4-3 Information Security Management and Control Concepts

(Security Measures and Control)

電腦程式的防護

由於網際網路的開放性與普及性，造成網路犯罪的情況日亦增多，隨著電腦犯罪技巧及數量的提升，各界對網路安全管理的重視程度也逐漸增加。從各界投入大量的人力及物力來加強資料加密、網路管理、網路認證及安全等研究來看，現今各界對網路的安全管理已達迫切的需求。

一般資訊系統安全上的危險包括：

■天災因素：包括水災、火災、地震等天然因素。

■人為因素：包括人為的疏忽、犯錯、蓄意的破壞、程式設計錯誤、不周全的系統安全設定 等因素。

■環境因素：包括有機器設備的損壞、斷電、老鼠等動物的破壞。

電腦病毒或是駭客是屬於人為因素，在使用的過程中，還是可以透過一些小技巧，來避免電腦安全危機。

1. 隨時安裝電腦系統的修正程式，修補系統與軟體的漏洞，減少駭客或病毒的入侵。

2. 定期更新系統，使系統軟體處在最佳狀態。

3. 擁有安全掃瞄與評估的軟體機制，如掃毒軟體的自動偵測，可以針對可疑的程式動作進行偵察。

4. 定期更新防毒軟體的病毒碼。

5. 加裝個人防火牆。防火牆是一種安裝在個人電腦上的程式，如同在電腦與網路之間築起一道牆，保護電腦降低被攻擊或植入程式的機會。

個人使用的防護

面對電腦通訊危機，個人應該養成安全的使用習慣：

1. 使用密碼管理電腦使用者，並且密碼避免過於簡單或容易猜測。

2. 不要隨便安裝或執行來路不明的程式。如不明來源郵件的附加執行檔。

3. 過濾有害郵件，對於不明來源的郵件先加以過濾。

4. 關閉瀏覽器的任意開啟視窗程式，避免受到不良網站的惡意程式攻擊。

5. 訂定嚴謹的存取規定，如使用者憑證。

資訊安全三要素

機密性

（Confidentiality）是指個人或團體的信息不為其他不應獲得者獲得。在電腦中，許多軟體包括郵件軟體、網路瀏覽器等，都有保密性相關的設定，用以維護用戶資訊的保密性，另外間諜檔案或駭客有可能會造成保密性的問題。

完整性（Integrity）

完整性是信息安全的三個基本要點之一，指在傳輸、存儲信息或數據的過程中，確保信息或數據不被未授權的篡改或在篡改後能夠被迅速發現。在信息安全領域使用過程中，常常和保密性邊界混淆。以普通 RSA 對數值信息加密為例，駭客或惡意用戶在沒有獲得密鑰破解密文的情況下，可以通過對密文進行線性運算，相應改變數值信息的值。例如交易金額為 X 元，通過對密文乘 2，可以使交易金額成為 2X。也稱為可延展性（malleably）。為解決以上問題，通常使用數字簽名或散列函數對密文進行保護。

可用性（Availability）

是一種以使用者為中心的設計概念，可用性設計的重點在於讓產品的設計能夠符合使用者的習慣與需求。以網際網路網站的設計為例，希望讓使用者在瀏覽的過程中不會產生壓力或感到挫折，並能讓使用者在使用網站功能時，能用最少的努力發揮最大的效能。

相關試題

1.（C）關於資訊安全管理的敘述，下列何者是錯的?

(A) 限制使用者登入的來源及時間

(B) 定期備份重要資料

(C) 將全部的資料用相同的金鑰加密

2.（ABC）下列哪些是破壞資訊系統安全的來源?

(A) 網路駭客

(B) 內部員工

(C) 天災

(D) 憑證機構

3.（C）為了讓郵件在傳送過程中不被駭客破壞，可以藉由電子郵件系統內之哪一項功能來達成?

(A) 壓縮

(B) 反駭客

(C) 加密

4.（ABC）資訊安全的三要素?(複選)

(A) Confidentiality(機密性)

(B) Integrity(完整性)

(C) Availability(可用性)

(D)Stability(穩定性)

4-4 System Security Concepts (Access Control)

4-4.1 ＳＳＩＤ

服務組識別碼 (SSID, Service Set Identifier)"。SSID 是由 32 個字元長度的字母、數字或符號所組成。同一個服務組的設備可以使用 SSID 來驗證另外一個網路設備是否為同一個群組。例如您的 Access Point 就可以透過在無線網卡裡組態的 SSID，來判斷是否為同一個群組，如果是相同的 SSID，就允許網卡存取; 如果不是則會禁止存取無線網路。

4-4.2 IPSec

IPsec(縮寫 IP Security)是保護 IP 協議安全通信的標準，它主要對 IP 協議分組進行加密和認證。IPsec 作為一個協議族（即一系列相互關聯的協議）由以下部分組成：(1)保護分組流的協議；(2)用來建立這些安全分組流的密鑰交換協議。前者又分成兩個部分：加密分組流的封裝安全載荷（ESP）及較少使用的認證頭（AH），認證頭提供了對分組流的認證並保證其消息完整性，但不提供保密性。

4-4.3 ＳＳＬ

資料保密協定(Secure Socket Layer) 的縮寫，是一種網際網路上最普遍使用的安全通訊協定，保障網站伺服器及瀏覽器之間的數據資料傳輸的安全性。透過使用這個協定，網路上的數據傳輸會按照認證的種類(40 位元、128 位元) 進行不同程度的加密，更會檢查資料的完整性。除此以外， 透過所謂『金鑰匙』的加密技術及嚴謹的 SSL 認證註冊的程序，SSL 可以驗證伺服器的身分而達到網站瀏覽者向網站身分作出檢查的目的。網站瀏覽者當看到瀏覽器右下角出現『金鑰匙』，瀏覽者可以點選查看伺服器的位置及身分，確認網站是否真實可靠。

相關試題

1. (C) 無線網路連線，第一要確認的是何?

(A) Computer Name
(B) Network Name
(C) SSID
(D) Domain Name

2. (A) 當存取某些特定伺服器(如 FTP Server)時，常會利用反查功能來確定存取者具有合法的 IP 地址，請問反查功能是利用下列服務所提供?

(A) DNS
(B) POP3
(C) SMTP
(D) NTP

4-5 Communication Encryption and Authentication Concepts

4-5.1 D E S

資料加密標準 Data Encryption Standard (DES)是由美國國防部於 80 年代制定的資料加密標準。它是一種區塊加密方法，它將欲加密的信息分割成 64 位元的區塊，用 56 位元的密鑰加密。由於密鑰長度不長，再加上電腦運算速度愈來愈快，利用窮舉法破解密鑰已非遙不可及的事，美國政府已規定從 1998 年 11 月起，不得再使用 DES 加密技術。

4-5.2 I D E A

演算法 International Data Encryption Algorithm IDEA 是設在瑞士蘇黎士的 ETH 發展的資料加密方法，已在美國與大部分歐洲國家取得專利，專利權歸 Ascom-Tech 所有。

它是一種區塊加密方法，採用 128 位元密鑰加密，一般認為其安全性很高。若是非商業用途，不需付費；若欲取得商業使用執照，可連繫 Ascom-Tech。

4-5.3 A E S

加密標準 Advanced Encryption Standard 是一種比 DES 碼還要先進的加密標準，由美國國家技術標準和技術研究所在 1997 年 9 月開始對外昭告 AES 標準後，經由 15 種加密標準中初步選出 5 種，並

將於 2001 年選出最後規格。

AES 的數字碼長達 128 位元（bit ）、192 位元以及 256 位元，而 DES 碼只有 56 位元，因此在嚴謹度上自然比 DES 要高出許多。

4-5.4 Ad Hoc Mode

Ad-Hoc 網路:是一個點對點建立起之網路連結,不需要無線存取器(AP,或稱橋接器)，透過個別電腦間無線連結，建構出一個群組網路，以達到資源共享(印表機 、檔案、網際網路等）。

4-5.5 R S A

RSA 加密演算法是一種非對稱加密演算法。在公鑰加密標準和電子商業中 RSA 被廣泛使用。RSA 是 1977 年由羅納德·李維斯特（Ron Rivest）、阿迪·薩莫爾（Adi Shamir）和倫納德·阿德曼（Leonard Adleman）一起提出的。當時他們三人都在麻省理工學院工作。RSA 就是他們三人姓氏開頭字母拼在一起組成的。

RSA 演算法的可靠性基於分解極大的整數是很困難的。假如有人找到一種很快的分解因子的演算法的話,那麼用 RSA 加密的信息的可靠性就肯定會極度下降。但找到這樣的演算法的可能性是非常小的。今天只有短的 RSA 鑰匙才可能被強力方式解破。到 2008 年為止，世界上還沒有任何可靠的攻擊 RSA 演算法的方式。只要其鑰匙的長度足夠長，用 RSA 加密的信息實際上是不能被解破的。

相關試題

1.（A）在無線網路中 可以做到 peer- to-peer 連線兒不需要使用 AP，此模式稱為?

(A) Ad Hoc Mode

(B) Peer Mode

(C) Infrastructure Mode

(D) Network Mode

2.（AD）下列哪些演算法可以達到資料一制性?

(A) RSA

(B) AES

(C) DES

(D) MD5

4-6 Network Address Translation(NAT) & Virtual Private Network(VPN)

4-6.1 NAT

網路地址轉換（Network Address Translation 或簡稱 NAT，也叫做網路掩蔽或者 IP 掩蔽）是一種在 IP 數據包通過路由器或防火牆時重寫源 IP 地址或/和目的 IP 地址的技術。這種技術被普遍使用在有多台主機但只通過一個公有 IP 地址訪問網際網路的私有網路中。根據規範，路由器是不能這樣工作的，但它的確是一個方便並得到了廣泛應用的技術。當然，NAT 也讓主機之間的通信變得複雜，導致通信效率的降低。

4-6.2 V P N

虛擬私人網路，又稱為虛擬專用網路（Virtual Private Network，簡稱 VPN），是一種常用於連接中、大型企業或團體與團體間的私人網路的通訊方法。虛擬私人網路的訊息透過公用的網路架構(例如：網際網路)來傳送內聯網的網路訊息。。虛擬私人網路利用已加密的通道協議(Tunneling Protocol)來達到保密、傳送端認證、訊息準確性等私人訊息安全效果。若使用得法，這種技術可以用不安全的網路(例如：網際網路)來傳送可靠、安全的訊息。需要注意的是，加密訊息與否是可以控制的。沒有加密的虛擬私人網路訊息依然有被竊取的危險。

相關試題

1. (B) 下列哪一種技術不是運用來建立 VPN

(A) L2F

(B) Proxy

(C) IPSec

(D)PPTP

2. (B) 下列有關網路位址轉換(NAT)說明，何者有誤?

(A) 可分成靜態和動態轉換兩種

(B) 動態 IP 轉換時必須更要 IP 表頭(Header)以及調整封包的部份 payload 內容

(C) 可以隱藏內部 IP 位址並可和虛擬私有網路(VPN)技術搭配一起使用

3. (B) NAT 適合縮寫:

(A) Network Adaptive Transfer

(B) Network Address Translation

(C) National Address Toward

4. (A) NAT (Network Address Translation)的用途為何?

(A) 私有 IP 位址與合法 IP 位子轉換

(B)路由

(C)防毒

(D)網域名稱與 IP 位址轉換

4-7 Firewalls

防火牆

防火牆(英文：firewall)是一項協助確保資訊安全的裝置，其會依照特定的規則，允許或是限制資料通過。防火牆可能是一台專屬的硬體或是架設在一般硬體上的一套軟體。防火牆最基本的功能就是控制在電腦網路中，不同信任程度區域間傳送的資料流。例如網際網路是不可信任的區域，而內部網路是高度信任的區域。以避免安全策略中禁止的一些通信，與建築中的防火牆功能相似。它有控制資訊基本的任務在不同信任的區域。 典型信任的區域包括網際網路(一個沒有信任的區域) 和一個內部網路(一個高信任的區域)。 最終目標是提供受控連通性在不同水平的信任區域通過安全政策的執行和連通性模型之間根據最少特權原則。

防火牆類型

網路層防火牆

網路層防火牆可視為一種 IP 封包過濾器，運作在底層的 TCP/IP 協定堆疊上。我們可以以列舉的方式，只允許符合特定規則的封包通過，其餘的一概禁止穿越防火牆。這些規則通常可以經由管理員定義或修改，不過某些防火牆設備可能只能套用內建的規則。我們也能以另一種較寬鬆的角度來制定防火牆規則，只要封包不符合任何一項「否定規則」就予以放行。現在的作業系統及網路設備大多已內建防火牆功能。

應用層防火牆

應用層防火牆是在 TCP/IP 堆疊的「應用層」上運作，您使用瀏覽器時所產生的資料流或是使用 FTP 時的資料流都是屬於這一層。

應用層防火牆可以攔截進出某應用程式的所有封包，並且封鎖其他的封包(通常是直接將封包丟棄)。理論上，這一類的防火牆可以完全阻絕外部的資料流進到受保護的機器裡。

防火牆藉由監測所有的封包並找出不符規則的內容，可以防範電腦蠕蟲或是木馬程式的快速蔓延。不過就實作而言，這個方法既煩且雜(軟體有千千百百種啊)，所以大部分的防火牆都不會考慮以這種方法設計。

相關試題

1.（A）下列有關防火牆之敘述何者錯誤?

(A) 防火牆可以防止病毒入侵

(B) 防火牆無法防止內賊對內的侵害，根據經驗，許多入侵或犯罪行為都是自己人或熟之內部網路佈局的人做的

(C) 防火牆基本上只管制封包的流向，他無法偵測出外界假造的封包，任何人皆可製造假的來源住址的封包

(D) 防火牆無法確保連線的可信度，一旦連線涉及外界公共網路，及有可能被竊聽貨劫奪，除非連線另行加密保護

2.（B）用來加強兩個網路間的存取控制策略的網路安全系統是?

(A) 存取控制系統

(B) 防火牆

(C) 加密處理

(D) RADIUS 伺服器

3.（B）下列有關封包過濾是防火牆的說明，何者有誤?

(A) 依據封包到達時的介面來過濾封包

(B) 可依據傳送的資料內容過濾封包

(C) 存取規則的設定較 proxy firewall

4-8 Technology Trend

展向來是持續不斷的，由安全工具的角度來看，除了傳統的端點防毒軟體之外，匣道端的整合安全設備，無疑地在過去幾年，已為許多企業節省了寶貴的管理時間與成本。

這的確是網路安全業界的一項突破性進展。基於整合集中化控管的發展趨勢，我們可以預見未來會有愈來愈多相關的功能，能夠彼此互通整合地統一管理，例如支援虛擬化與網路加速這兩大領域，讓網路除了得以淨化之外，也得以優化和虛擬化管理。

若從網路安全的發展來看，未來網路安全更將進一步走向「安全的網路」，意即網路本身就是安全的。任何資料或流量在進入網路前，就已經過檢查、掃瞄或受到監控，網路安全的保護將先由使用者最初的接入點－網路服務供應商 ISP，或由資料存取的第一站－Portal 入口網站來提供。這些趨勢現在就看得到，未來，也將更加普及。

相關試題

1.(A) 好的區域網路管理是指?

(A)解決網路上的問題
(B)產生網路上的問題
(C) 技術要很高超
(D) 功能超炫

2.(A) 下列何者為資料安全首要考慮的項目?

(A) 檔案機密等級分類
(B) 程式之變更管理
(C) 消防設備
(D) 門禁管制

結論

在大學畢業以前，未曾想過有那麼一天能擁有一本屬於自己撰寫的專題，也不敢想像這篇文章該如何落筆，從不善於彙整資料及文筆遣詞不順，到如何應用適當的文字敘述，也在製作 ITE 專題過程中，遭遇到許多的困難及阻礙，但我們依舊克服了重圍，完成專題的製作。

感謝蔡篤校老師的指導，在研究過程中老師引導我們做專題的方向及概念，並協助規劃來一一做修正，適時地督促我們完成該注意的地方與修辭，每當研究專題報告的同時，免不了疑慮及看法，但是，老師總是微笑認真的幫我們排解，讓我們的畢業專題能更加的順利。

最後也感謝組員間的努力和配合，相信組員一定有把大學中所學的學以致用，也在未來的就職領域中如期的發展，相信藉此的友誼會更加堅定及長存，對於未來的窘境也都能勇敢的面對。

參考文獻

(1).維基百科 - 維基百科,自由的百科全書

(2).http://tw.knowledge.yahoo.com/question/question?qid=1305090207339

(3).http://tw.knowledge.yahoo.com/question/question?qid=1607041904 04http://tw.knowledge.yahoo.com/question/question?qid=13051007072369

(4).http://mtaiwan.tainan.gov.tw/faq_1.htm

(5).http://tw.knowledge.yahoo.com/question/question?qid=100503190162

(6).http://tw.knowledge.yahoo.com/question/question?qid=1007120610635 5