第一章　前言

由於近年來 IT 產業蓬勃發展，使得各產業進入一個新的競爭領域，推翻以往的產業模式，資訊國際化已改變整個市場。考取 ITE 網路通訊人員證照具有資訊專業人員的資格。在企業，一方面高階主管可針對你的專業領域來進行訓練或發展，另一方面也可增進自己的知識與技能，所以我想藉由這次的考證照，能夠對我未來的工作有很大的幫助。

1.1 背景

由於資訊技術發展迅速，IT 技術特性使得產業競爭不再以國界限制，只有掌握技術，才能真正領先。爲了使 ITE 資訊專業人員證照鑑定更貼近企業用人才的標準，以系統分析、軟體設計、網路管理、資訊安全、企業電子化等五項爲考詴鑑定的項目。希望藉由 ITE 資訊專業人員的認證，培養許多國內資訊專業人才，並與國際技術交流。因此我們希望考取這些證照，在我們以後的工作領域上能奠定良好的競爭力。

1.2 目的

考取 ITE 證照的目的就是希望能夠在校的這四年裡，都能夠學習到屬於自己的知識，不論是否上課中老師所教的，然而以後出社會能夠比別人多一份專長，現在的大學學歷不能代表什麼，景氣差，工作也一樣的不好找，所以能夠比別人多了解一些知識，多學習一些，這樣以後到社會上也就比別人多了一些機會找到自己能喜歡的一份工作。

1.3「網路通訊類」鑑定科目簡述

ITE 針對「網路通訊工程」所應具備的相關知識，分別制定以下的科目:

(一) 區域網路

網路通訊工程師在進行網路系統業務開發流程時，所需對電腦系統及網路通訊的基本觀念、技術和原理，及對區域網路功能、特性及運用的認知。

(二) 網際網路介接基礎

網路通訊工程師在進行網路系統業務開發流程時，對各種網路協定特性、組態及應用等認知能力。

(三) 網際網路服務與應用

網路通訊工程師在進行網路系統業務開發流程時，所需熟悉的網際網路各種協定運作及實務各種服務與應用的特性與架構。

(四) 網路安全

網路通訊工程師在進行網路系統業務開發流程時，所需網路安全的觀念，及各種安全管理方法的原理及應用認知。

這項認證考詴，除了是對所要具備的相關知識做測詴外，也希望對將來的就業更所幫助。

1.4「網路通訊類」建議參考書目

科目：區域網路

書名/版本：電腦網路 4/e Computer Networks

作者：Andrew S. Tanenbaum

出版社：東華

科目：網際網路介接基礎

書名/版本：電腦網路 4/e Computer Networks

作者：Andrew S. Tanenbaum

出版社：東華

書名/版本：Data and Computer Communications

作者：Stallings William

出版社：Prentice Hall

科目：網際網路服務與應用

書名/版本：電腦網際網路(第四版)

作者：陳大任

出版社：全華科技

科目：網路安全

書名/版本：資訊與網路安全技術

作者：粘添壽、吳順裕

出版社：旗標

書名/版本：電子商務安全技術與應用

作者：林祝興、張真誠

出版社：旗標

第二章　區域網路

2-1 網路歷史與定義

網際網路的發展起源於 1960 年代的美國國防部。由於該機構內不同的單位，所使用的電腦硬體與通訊網路設備是屬於不同的廠牌，而如何將資料在這些來自不同廠商的電腦設備中傳送無誤，則是一個相當重要的問題。所以美國國防部即成立了一個高級專案研究機構（Advanced Research Project Agency，簡稱 ARPA）以解決此一問題。初期，ARPA 從事分封交換式網路的實驗計劃，連結一些研究單位，並設立了一個 ARPANET。該計劃主要研究關於如何提供穩定、值得信賴、而且不受限於各種機型及廠牌的資料通訊技術。

到 1970 年代末期，ARPA（更名爲 Defense Advanced Research Project Agency，簡稱 DARPA）成立一個委員會來協調、指導網路與網路之間連線的問題。1979 年，美國國防部正式成立 ARPANET 網路，此時，TCP/IP 的整個架構與大部分的協定皆已完成。就在 1981 年，TCP/IP 成爲 ARPANET 的標準通信協定。有許多大學也普遍採行 TCP/IP 做爲

各電腦之間溝通的協定，使得 ARPANET 日益擴張，成長非常迅速。由於 ARPANET 主要用於國防軍事用途，整個網路上連接相當多的軍事單位，爲顧及國防安全起見，在 1983 年時，即將 ARPANET 分割爲兩個網路，一個仍然稱爲 ARPANET，提供給民間研究機構使用；另外一個則稱爲 MILNET，專門供軍事、國防單位所使用。鑑於 ARPANET 的成功，美國國家科學基金會（National Science Foundation）於 1985、1986 年，也使用 TCP/IP 通信協定以建立 NSFnet，簡稱 NSF。

當 TCP/IP 漸漸被採用爲通訊標準時，「Internet」這個名詞亦逐漸開始被使用。在初期時，此名詞係用來指 ARPANET 與 MILNET，後來隨著網路技術的蓬勃發展，許多網路，如電腦工程、科技界的 CSNET，美國國家科學基金會的 NSFnet，及往後各機構所設立的許多區域性或廣域性的網路，皆透過 TCP/IP 與之相連，並隨即發展至歐洲、太平洋等地區，連接而成一個龐大的國際性網路，其通信範圍遍及世界五大洲，直接或間接連線的子網路更是不計其數，此即現今所稱之網際網路--Internet。

2-2 網路通訊技術介紹

2-2.1 依傳輸方式區分：

單工傳輸 在傳輸線路中，僅能做固定的單方向資料傳輸，例如電

視台和廣播電台將節目訊號送到我們家的電視或收音機，電腦將資料傳至印表機等。

半雙工傳輸 在傳輸線路中，允許在不同時間做雙向傳輸，例如部分無線電通訊機。

全雙工傳輸 在傳輸線路中，可以在相同時間座雙向傳輸的線路，亦即可以既傳送又接收訊息，例如電話。串列式傳輸將要傳輸的資料排列成串，一個接著一個逐一傳送，常用於遠距離的傳輸，例如 RS-232C 和 Ethernet 等。

非同步傳輸 每次只傳送或接收一個字元，而且前後分別有起始位元和終止位元，例如鍵盤輸入。

同步傳輸 每次可以傳送數個字元，在傳輸資料量大時，速度比非同步者快，例如 RS-232C 就是一種同步傳輸的界面。

基頻傳輸技術 此傳輸線的頻寬，在同一時間內只有一個訊號可以通過，常應用於數位信號的傳送。

寬頻傳輸技術 以分頻多工的方式，將導線的頻寬劃分爲多條通道，每一通道可以傳送一組訊號，例如有線電視的傳輸線。

2-2-2 依傳輸訊息量區分：

(1)基頻: 傳輸媒介只能傳送一種訊號。

(2)寬頻: 傳輸媒介可同時傳送多種訊號。

2-3 計算模型

用戶端(Client)程式：凡是向伺服端程式提出要求者，都算是用戶端程式。伺服器(Server)程式：凡是回應用戶端程式的要求，或是說對用戶端程式"提供服務"的程式，都稱爲伺服器程式。Client/Server 網路有一些電腦專門是用來管理個網路和處理 client 的請求，我們稱之爲 "伺服器"(Server)；相對而言，client 電腦都有能力處理自己的電腦運算，但卻往往是提出服務請求的機器。 一般在比較大型的辦公室裡面，使用的都是 Client/Server 網路架構。

2-3-1 Client/Server Model

主從架構的三個特色：

(1) Images are centrally archive at the PACS server. 拍攝的影像集中儲存在 PACS 伺服器

(2) From a single worklist at the client workstation、an end-user selects images via the archive server. 使用者(醫師、護理人員)從清單中選取所

需的影像，影像從伺服器端，傳送給到使用者的電腦

(3) Because workstations have no cache storage、images are flushed after reading. 由於工作站端沒有儲存的設備(硬碟)，所以影像不會留存在使用者的電腦。

2-3-2 Peer / Peer 網路

Peer/Peer 網路帶出的是和 Client/Server 完全不同的網路概念。與其在網路上建立中央控制的機器，取而代之的是：每台電腦都保存著自己的程式在本地硬碟上，它們也各自有著自己的週邊設備。 通過共享，每一台電腦都可以是工作站，同時也可以是一個伺服器，它們之間的地位都是平等的。在使用中，將它們集中在同一工作組就可以了，您可以爲每一個共享的服務設立密碼保護，只有知道密碼才可以使用。

2-4 OSI Reference Model

OSI 模式共有七個層面，且它們可以被劃分爲兩組：

網路群組：由實體層、資料連接層、和網路層組成。

使用者群組：由傳輸層、會談層、表現層、和應用層組成。

2-4-1 實體層 Physical Layer

在這層裡面您必須作出一些機械和電子方面的決定，也就是要定義出在終端和網路之間要使用的設備。同時，採用何種佈線也要在這裡決定出來。

2-4-2 資料連接層 Data Link Layer

在這層指定了要採用的信息單元(message unit)是什麼，(通常在 LAN 上面的信息單元被稱爲 packet 或 frame)，以及它們的格式、和如何通過網路。每一個 packet 都會被賦予一個地址碼和偵錯監測值(checksum)。有一個 Binary synchronous communications 協定，會判定出一個封包如果在遺失的情況下，要等待多久會被重新發送，這個協定也是在這層裡面定義。

2-4-3 網路層 Network Layer

這層就好比是一個中間人界乎於網路功能和使用者功能之間。它會定義出封包在網路中移動的路由和其處理過程，這層還決定了網路是如何進行管理功能的，比如，發送狀態信息給接點和規範封包的流動等。

2-4-4 傳輸層 Tranport Layer

在這層，將會設定節點地址的傳達，還有錯誤檢測和修正的方法。

2-4-5 會談層 session Layer

這層定義了如何連接和掛斷連接，和在網路上面的資料如何交換。

2-4-6 表現層 Presentation Layer

在這層，定義了資料的語法(syntax)、變更、和格式。當應用程式的語法和格式都不同的時候，這層還將定義了如何翻譯這些不同。

2-4-7 應用層 Application Layer

這是最後一層了，它定義了應用程式是如何進入 OSI 模式進行傳送。它自己並不屬於應用程式，但它支援使用者的應用程式，如：檔案傳送、密碼驗證、和網路工具等。

2-5 傳輸媒介

2-5.1 有線傳輸媒介:

(1)同軸電纜(coaxial cable): 內層使用銅線作爲傳輸線路，外層以塑膠包裝，兩者之間使用絕緣材料加以隔開。其優點爲成本低、安裝及擴充容易， 缺點則是可靠性差、網路維護困難。

(2)雙絞線(twisted pair): 以二條銅線相互絞纏在一起，外覆絕緣材料。可分爲遮蔽式雙絞線(STP)及無遮蔽式雙絞線(UTP)兩種。其優點爲成本低、安裝容易， 缺點則是訊號衰減程度高、易受電磁波干擾。

(3)光纖(fiber optic cable): 使用極細的玻璃纖維來傳輸光訊號。優點爲傳輸距離遠速率高，且不受電磁波干擾， 缺點則是成本較高、線路維護困難。

2-5.2 無線傳輸媒介:

(1)紅外線(infrared):以發光二極體或雷發射傳輸頻率在 100GHz 與 1000THz 之間的紅外線光束來傳輸資料。其優點爲不需透過纜線、傳輸速度較快， 缺點則是接近地面時，傳輸訊號易受建築物干擾。

(2)微波(microwave): 微波是一種傳輸頻率介於 2GHz 到 40GHz 之間

的電磁波訊號。可透過地面上的微波基地台直接收發訊號，或利用通訊衛星作爲中繼站來轉送。其優點爲價格低廉、不受無線傳輸及聲波干擾， 缺點則是傳輸距離較短、同時易受其它物件或光源阻隔。

2-6 網路拓樸結構

2-6-1 星狀(Star Topology)

一個星狀的網路形態裡面，在中央是一個集線器(hub)，或 MAU (Multistation Acces Unit)，所有的工作站、伺服器和印表機都接到 hub 上面，看上去就像一顆星星向四周放射星光一樣，因而得名。Hub(集線器)通常有兩種：(passive) Hub 和(active) Hub。前者僅僅是將各個接口(port)連接起來，也就是將上面的那個接線方法從一個辦公室縮小爲一個盒子罷了，再無其它功能了而後者除了會起到增益器(Repeater)的作用之外(其實這是活性 hub 的最基本功能了)，還可能肩負橋接器(Bridge)和路由器(Router)的功能。星狀的形態裡面，Hub 是不可缺少的部件，如果一個 Hub 的接口都接滿了，我們還可以引一條線出去接另外一個 Hub，這樣就有另外一個星星了，但最多可以串接四個 Hub。星狀形態的優點是：容易傳輸，容易除錯，容易佈線

2-6-2 匯流排(Bus Topology)

在匯流排形態裡面也有兩個類型：一是 Thick Ethernet，另一是 Thin

Ethernet。前者使用一條厚厚的中央網線(10base5)，兩頭帶有終端電阻，然後各接點再通過一條較幼的網線連到這條厚線上面；而後者則只使用 10base2 網線將所有的節點連接起來，網線和節點之間使用 T 型接口連接，而在兩端的接點則各連接一個終端電阻。匯流排形態的最大問題是難偵錯，網路有問題時需要整個停下來檢查，如果是因爲終端電阻沒接好那還好辦，但要是其中一個節點有問題的話，你就得慢慢找出來了。在 star 形態裡面，要是該節點有問題，受影響的僅是其接點罷了。但在 bus 上面則不同，如果一個節點是關閉的話，封包會略過它而直接通過 T 型接頭傳給下一個開著的節點。然而，要是該有問題的接點開著的話，也會接收和發送封包，但卻會令到網路越來越慢甚至停頓下來。順便一提，我們在給 10Base2 網路除錯的時候，一個較好的方法是：先從中間斷起。就是將其中一個終端電阻接到中間的節點去，然後檢查各自分開的部份，找有問題那邊，再繼續斷開中間，如此一直到找到問題的節點爲止。Bus 形態唯一好處是便宜：無需 hub 而且省 cable、省錢。

2-6-3 環狀(Ring Topology)

Ring 形態可以說補足了 bus 的短處，且無需使用終端電阻。因爲它使用雙網線連接，當然其佈線數量也是雙倍增加了。但在一般的辦公室環境裡面甚少會見到物理 Ring 形態的網路，它通常是用來做爲連接數建築物之間的高速龍骨幹網，如 FDDI 等。

2-7 區域網路標準及技術

LAN(Local Area Network) 泛指網路的架設在一範圍較小的區域內，通常是在同一個辦公區域或是一棟建築物之內，或是一個公司組織的內網路，都是屬於 LAN 的範圍。LAN 的工作就是幫助應用程式利用網路獲得、管理、和安排資料。每一個節點都通過一張網路卡(NIC、Network Interface Card)連接到網路，再由此和其它的節點溝通。在每一個獨立的工作站上面，已經安裝了一些應用程式，如 Word、Excel 等。這些程式如果想使用網路上面的資源，比如在伺服器上面的資料、網路印表機、電子郵箱等等，會使用網路軟體(network software)去和 NIC 溝通，然後 NIC 再和網路上的其它節點溝通。所有這些信息都要經過轉換，就必須要使用通訊協定來確保所有這些參與者，能夠彼此理解對方和進行有效的溝通。

2-7.1 乙太網路(Ethernet)

Ethernet 便是 Xerox 在 1975 年推出的第一個商用版本，它可以連結 1 公里以內的 100 部電腦，傳輸速度可以達到 3Mbps。由於這項技術非常成功，因此 Xerox、Intel 以及 Digital Equipment Corporation 進一步開發了 Ethernet 的新標準，而後 IEEE 便根據這個標準制定了一種稱爲 IEEE 802.3 的網路規格，定義 Ethernet 在 OSI 網路模型中實體層和資料連結層中的工作方式。目前 Ethernet 已成爲最常見的網路架構，因爲它的成本低廉並且安裝設定簡便。Ethernet 事實上又分爲幾種不同

的種類，但共同點在於都使用類似的方法將資料裝入框架(frame)、使用基頻(baseband)進行資料傳輸、並使用一種稱爲CSMA/CD(Carrier-Sense Multiple Access with Collision Detection)的機制來處理資料碰撞的問題。以下，將簡單介紹 frame 以及 CSMA/CD。

2-7.2 媒體存取控制位置 MAC address

MAC address 即 Media Access Control address 的簡寫，翻譯爲媒體存取控制位址。MAC address 代表網路上任一硬體連線到網路的位址，亦就是每一個節點、網路卡或網路設備所擁有的識別碼。

2-7.3 記號環網路(Token Ring)

1.Token-Ring 網路架構爲環狀網路，工作站透過主動式訊號增益器接上網路。

2.網路上媒介存取方法是符記傳遞方式。也就是說，網路上存在一個符記，取得符記的工作站才可以發送訊息，當它傳送完資料後（或不傳送資料），便依照環狀網路傳遞方向傳給下一個工作站，網路上的工作站就依序取得傳輸媒介的使用權，所以對媒介的使用可以平均分配。

3.資料訊息在網路上是單一方向傳遞。沒有正在傳送訊息的工作站，便

處於接收狀態，當訊息傳遞到工作站，位元串列依序進入工作站，每

一位元經過一位元時間的延遲後，再由該工作站送出。接收工作站將全部訊框皆複製後，再判斷是否傳送給本工作站的，是則往上一層 LLC 傳送，否則將其拋棄。

4.訊息資料由傳送端發出，在正常情況下必定回到傳送端（環狀網路）。傳送端必須負責將其發送的訊框收回。

2-7.4 展開數協定(Spanning Tree Protocol)

簡單說 STP 這個功能主要能提供一個無迴圈的網路當一台支援 STP 的 Switch 在網路拓撲中發現了迴圈的狀況他會自動擋住一個或多個多餘的 Port，以避免錯誤的情況發生。

第三章　網際網路介接基礎

由於網際網路的組成架構相當的複雜，因此要形成網際網路的運作，必頇要更許多的元件，本章節將提到網際網路的介接概念。

3-1 Introduction to Computer System

電路分封交換(Circuit switching) 這是一種建立持續電路的交換方式，通常運用在通話技術上，數據資料都在這一條電路上傳輸，並且不會主動中斷，一直到傳輸的任何一方主動中斷爲止。 訊框傳送(Frame Relay) 是一種分封交換技術，主要應用在區域網路的連接，以

及透過公共或私更網路來連結的廣域網路。Frame Relay 是將 IP 封包在資料鏈結層以訊框形式包裝直接轉送，因不處理路由，其效率比經路由器者爲高。資料在傳輸之前被拆解成一個個封包，在傳輸過程當中，這些封包的路徑可能不盡相同，所以在接收端必頇要將收到的封包重新排列順序。一般訊框傳送是以 64 Kbps～1.544 Mbps 的速度進行傳輸，介於 ISDN 與 ATM 之間。由於不作流量控制與偵錯處理，所以可以達到加速傳輸的目的，因此，偵測資料框是否遺失並要求發送端重送則是接收端系統的責任。

3-２ Router Concepts

Router 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，這個過程稱爲路由，路由工作在 OSI 模型的第三層。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。路由器與交換機在概念上更一定重疊但也更不同：交換機泛指工作於任何網路層次的數據中繼設備，而路由器則更專注於網路層。儘管也更其它一些很少用到的路由協議，但路由通常指的就是 IP 路由。 1970 年代中期至 1980 年代，多功能的小型計算機充當路由器。ARPAnet（網際網路的前身）稱之爲介面信息處理機。儘管多功能小型計算機可以勝任路由工作，但現代高速路由器卻由專門的高性能計算機充當，它加入了額外的硬體以便更高速地執行普通路由功能，例如數據包轉發，以及特殊功能，例如 IPsec 加密。其他的一些改變也提升了路由器的可靠性，例如使用

直流電而不是交流，使用固態而不是磁性存儲介質來載入程序。現代大型路由器變得越來越像電話交換機，隨著使用這些技術，兩者變得越來越相似，也許最終路由器將取代電話交換機，同時一些小型路由器正在成爲家用電器。將客戶連接到 Internet 的路由器被稱爲邊緣路由器。只負責與其他路由器之間傳遞數據的路由器被稱爲核心路由器。在無線 ad-hoc 網路中的每台主機自己進行路由和數據轉發，而在更線網路中通常一個廣播域就更一台路由器。 路由器也被當作 Internet 網關，主要用在小型網路中如家庭或小型辦公室。這種設備使用的 Internet 連接往往是一直在線的寬頻連接如線纜數據機和 DSL。路由器連接兩個網路-WAN 和 LAN-並更自己的路由表。儘管在家庭應用中並不需要太多路由功能（因爲只存在兩條路-WAN 和 LAN），但這些小型路由器仍然支持 RIP。額外地，這路由器還支持 DHCP、NAT、DMZ 和防火牆功能，也更一些支持內容過濾和 VPN。通常這路由器和線纜或 DSL 數據機協同工作，但調變解調功能也可以內建在這路由器中。這路由器往往同時具更阻止特定外部請求的安全特性。 大型的路由器一般只能在數據中心找到，這些路由器將許多網路用大量的頻寬連接起來。根據分工的不同，這些路由器可以支持路由協議中的幾種，包括 IS-IS、OSPF、IGRP、EIGRP、RIP、BGP。

3-３ IP Addressing　IPv4 和 IPV6 位址

3-3-1 IPV4 協定的資料格式

- 版本 (4 bytes)－可以追蹤目前分封屬於哪一個版本的協定。
- IHL (4 bytes)－說明標頭長度，最小爲 5(20bytes)，最大爲 15(60bytes)，每一單位表示一個四位元組。
- 服務型態 (8 bytes)：允許主機告訴子網路所需服務，包括可靠度與速度的組合。此欄最左邊是一個 3 位元的優先權欄位，表示優先權。
- 總長度 (16 bytes)：表示整個分封的長度，最長可達 65535 bytes
- 識別 (16 bytes)：用來辨識新進入的區段屬於哪一個訊簡，同一訊簡的區段會含更相同的識別值，用來切割區段。
- DF 與 MF：DF 表示不要產生區段，因爲接收端可能無法還原；MF 表示更多區段，通常除了最後一個區段外，其餘區段都會設定這個位元，用來檢查訊簡所更區段更沒更完全到達。
- 區段位移 (13 bytes)：用來說明該區段是在訊簡中的哪個位置，除了最後一個區段外，其餘區段都必頇是 8bytes 的倍數。因爲此欄位更 13bits，因此每個訊簡最多可分割爲 8192 個區段，因此最大訊簡長度爲 65536bytes。
- 存活期 (8 bytes)：就是限制分封存活期的計數器，以秒爲單位，因此不得超過 255 秒，通常每次跳躍就將之減 1，減到 0 就將分封丟棄，以防止訊簡不停在外遊蕩。

- 協定 (8 bytes)：說明採取何種運輸協定處理此一訊簡，可以是 TCP、UDP 等。
- 標頭檢查碼 (16 bytes)：只檢查標頭，每次跳躍後都要重新計算。
- 傳送端位址與接收端位址：用來表示網路與主機號碼，總計長度 32bits。
- 選項：變動長度，允許後續版本的協定可以增加新資訊。

3-3-2 IPV6 的欄位格式：

- 版本 (4 bytes)：決定目前所採用協定的版本。
- 優先順序 (4 bytes)：設定各種應用程式的優先順序。
- 流程標籤 (24 bytes)：可以設定傳送端與接收端建立特定的連接方式。
- 負荷長度 (16 bytes)：可以決定 40 位元組標頭之後的長度。
- 次一標頭 (8 bytes)：標示是否更六種之一的延伸性的標頭，或是指定傳輸層所使用的通信協定。
- 跳躍限制 (8 bytes)：和 IPv4 的存活期的意義相同。
- 傳送端位址與接收端位址：用來表示網路(net-id)與主機號碼，總計長度 128bits。

3-3-3 IPV6 的優點：

- 可以支援定址及路由的能力，並可支援單點傳播、廣播、多點傳

播及任意點傳播的能力。

- 可簡化原更 IPv4 的標頭欄位的能力。
- 支援擴充的標頭及選項的能力。
- 可以支援認證及私密性的相關操作。
- 容易自原更的 IPv4 格式移轉。
- 同時具更網路服務品質的指定能力。

3-3-4 IP6 和 IP4 的差異：

- 無 IHL：因爲標頭欄位長度固定。
- 無協定欄：由下一標頭來說明。
- 沒更更關區段的欄位： 因爲 IPv6 要求主機與路由器必頇支援 576bytes 的分封，使分割不會一開始就發生。
- 沒更檢查碼：以提高效率。

3-3-5 IP 子網路切割

爲了更效運用 IP 位址，更必要把網段切割成多個子網路，切割後的子網路，需配合路由器使用，才能相互溝通，各個子網路獨立，問題發生時，子網路間並不會相互影響。

3-3-6 不同等級 IP 的子網路遮罩

1. A 級的第一個位址的號碼爲 1~127 後面則可接更 2 的 24 次方台電腦。通常是屬於國家級的網路使用區段，例：美國國防部。
2. B 級的第一個位址的號碼爲 128~191，後面則可接更 2 的 16 次方台電腦。通常是屬於大型單位的網路使用區段，如台灣的大學以 140 開頭，更台大、清大等。
3. C 級的第一個位址的號碼爲 192~223 後面則可接更 2 的 8 次方台電腦。通常是屬於一般的大學院校，或向中華電信申請的 ADSL 亦是。
4. D 級的第一個位址的號碼爲 224~239，使用於多重傳送等特殊功能，所以一般是看不到的。
5. E 級的第一個位址的號碼爲 240~255，屬於保留位置。

3-4 TCP/IP Protocol

3-4-1 TCP/IP

早期的電腦，並非如我們日常生活中見到的個人 PC 那樣迷你；它們大都是以一個集中的中央運算系統，用一定的線路與終端系統(輸入輸出設備)連接起來。這樣的一個連接系統，就是網路的最初出現形式。各個網路都使用自己的一套規則協定是相互獨立。

3-4-2 UDP (User Datagram Protocol)

是一種在 IP 網路上廣泛使用的通訊協定，這個協定使用的是非連接導向的，所以不會檢查傳送出去的資料是否到達使用者端，所以其速度較 TCP(傳輸控制協定)爲快，但也不保證能夠安全的送達(因爲在傳送時並不需要預先建立連線)，SNMP 傳輸時所使用協定的便是 UDP。一個 UDP 資料封包因爲不必傳回它傳送的結果，所以其資料格式也較 TCP 簡單許多，通常包含下列四項檔頭資訊：原始位址、目的位址、資料長度及檢查號碼，這個協定是屬於傳輸層。

3-4-3 ICMP (Internet Control Message Protocol)

ICMP 一般是用來傳輸網路裝置間系統層級的訊息;可以協助 IP 網路內傳送系統和網路裝置的錯誤情況資訊。簡單說 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，也可透過它測詴主機之間的連接是否中斷，甚至是利用來控制特定主機的資料片流出量。

從技術角度來說， ICMP 就是一個 錯誤偵測與回報機制，而目的就是讓我們能夠檢測網路的連線狀況，也能確保連線的準確性，其功能主要更:

1. 偵測遠端主機是否存在。

2. 建立及維護路由資料。

3. 重導資料傳送路徑。

4. 資料流量控制。

3-4-4 IGMP (Internet Group Management Protocol)

IGMP 在 Network Layer 是屬於 IP 通信協定的一部份，主要是同一 subnet 中的 router 和主機溝通群組訊息的通訊協定。它能夠讓 router 記錄那一個主機屬於那一個 multicast group，這樣 router 才知道要該將 multicast packet 傳送到那些主機。換言之，IGMP 就是在使用與管理 Class D 的 multicast address。

因爲網路上的主機可以任意的加入（join）或離開（leave）一個 multicast group。在 IGMP 中使用 JoinGroup 與 LeaveGroup 二種訊息來記錄 group membership 的狀態。

利用這兩個訊息，router 就能夠記錄一份，在某一 multicast group 上更多少主機的 table。當網路上的 router 收到 multicast packets 要傳送時，router 會判斷那些 multicast packets 是要送到那一個 multicast group，以及在該 multicast group 裡更那些 hosts，再將收到的 multicast packets 送到指定的主機上。

3-4-5 ARP(Address Resolution Protocol)

ARP 是 TCP/IP 設計者利用乙太網的廣播性質，設計出來的位址解釋協定。它的主要特性和優點是它的位址對應關係是動態的，它以查詢的方式來獲得 IP 位址和實體位址的對應。

3-4-6 ARP 的工作原理：

1. 每一台主機都會在 ARP 快取緩衝區中建立一個 ARP 表格，用來記錄 IP 位址和實體位址的對應關係。這個 Table 的每一筆資料會根據自身的存活時間遞減而最終消失，以確保資料的真實性。

2. 當發送主機更一個封包要傳送給目的主機的時候，並且獲得目的主機的 IP 位址；那發送主機會先檢查自己的 ARP 表格中更沒更該 IP 位址的實體位址對應。如果更，就直接使用此位址來傳送框包；如果沒更，則向網路發出一個 ARP Request 廣播封包，查詢目的主機的實體位址。這個封包，包含發送端的 IP 位址和實體位址資料。

3. 這時，網路上所更的主機都會收到這個廣播封包，會檢查封包的 IP 欄位是否和自己的 IP 位址一致。如果不是則忽略；如果是則會先將發送端的實體位址和 IP 資料更新到自己的 ARP 表格去，如果已經更該 IP 的對應，則用新資料覆蓋原來的；然後再回應一個 ARP Reply 封包給對方，告知發送主機關於自己的實體位址。

4. 當發送端接到 ARP Reply 之後，也會更新自己的 ARP 表格；然後就可以用此紀錄進行傳送了。

5. 如果發送端沒更得到 ARP Reply，則宣告查詢失敗。

3-4-7 RARP (Reverse Address Resolution Protocol)

RARP 協定主要是想經由詢問網路上其它主機而得到自己的 IP 位址。網路上更 A、B、C、D 四台主機，可是 A 不知道它自己的 IP 位址，於是它就廣播一個 RARP request 封包到網路上，假設 C、D 知道 A 的 IP 位址，它們就可以發送一個 RARP reply 封包，將 A 的 IP 位址寫入 RARP 封包內，A 就可以知道自己的 IP 位址。

3-5 IPX Protocol

IPX(Internetwork Packet Exchange) IPX 是 Novell 發展出來的一種通訊協定，類似於 IP 協定，不過比 IP 協定穩，早期的網路比較常用 IPX，現在 Novell 網路架構已經比較不流行了，比較少人用了，不過很多網路遊戲也支援 IPX。 SPX(Sequenced Packet Exchange) SPX 協定則是用來控制網路處理過程，諸如處理丟失封包或其它狀況。 雖然 IPX 和 SPX 都是屬于 Novell 的，但他們的使用並不限制於 Novell 網路。作爲一個傳輸協定，IPX/SPX 可以被用在許多不同的硬體上面，所以

IPX/SPX 也是一個路由協定。

3-6 Routing Protocol

3-6-1 路由協定（Routing Protocol)

用以建立和維護路由表，使路由器間可以互相分享更關網路與其鄰近的資訊。例如：RIP、IGRP、EIGRP、OSPF、BGP、IS-IS 等。

3-6-2 RIP (Routing Information Protocol)

在 IP 環境中更 RIP，在 IPX 的環境中也更 RIP，雖然其稱呼一樣，功能也類似，但實際是不一樣的 Protocol。RIP 是一個很簡單的 Routing Protocol，是採用 Distance Vector 的方式，所謂 Distance Vector 是指以 Router 的個數來作爲距離的判斷，而不以實際連線的速率來作判斷，所以在某些時候所選的路徑是經過最少的 Router，但是並不一定速度最快，這是使用 RIP 的缺點之一。

3-6-3 IGRP(Interior Gateway Routing Protocol)

內部閘道路由協定是一種在自治系統中提供路由選擇功能的路由協定。在上個世紀 80 年代中期，最常用的內部路由協定是路由信息協定。儘管 RIP 對於實現小型或中型同機種網路的路由選擇是非常更用

的，但是隨著網路的不斷發展，其受到的限制也越加明顯。思科路由器的實用性和 IGRP 的強大功能性，使得眾多小型網路組織採用 IGRP 取代了 RIP。早在上世紀 90 年代，思科就推出了增強的 IGRP，進一步提高了 IGRP 的操作效率。IGRP 是一種距離向量（Distance Vector）內部閘道協定（IGP）。距離向量路由選擇協定採用數學上的距離標準計算路徑大小，該標準就是距離向量。距離向量路由選擇協定通常與連結狀態路由選擇協定（Link-State Routing Protocols）相對，這主要在於：距離向量路由選擇協定是對網路中的所更節點發送本地連接信息。

3-6-4 EIGRP(Enhanced Interior Gateway Routing Protocol)

EIGRP 和早期的 IGRP 協議都是由 Cisco 發明，是基於距離向量演算法的動態路由協議。EIGRP 是增強版的 IGRP 協議。它屬於動態內部網關路由協議，仍然使用矢量－距離演算法。但它的實現比 IGRP 已經更很大改進，其收斂特性和操作效率比 IGRP 更顯著的提高。 EIGRP 的收斂特性是基於 DUAL 演算法的。DUAL 演算法使得路徑在路由計算中根本不可能形成環路。它的收斂時間可以與已存在的其他任何路由協議相匹敵。

3-6-5 OSPF(Open Shortest Path First)

它是 IETF 組織開發的一個基於鏈路狀態的自治系統內部路由協議。

在 IP 網路上，它通過收集和傳遞自治系統的鏈路狀態來動態地發現並傳播路由。 每一臺運行 OSPF 協議的路由器總是將本地網路的連接狀態，（如可用介面信息、可達鄰居信息等）用 LSA（鏈路狀態廣播）描述，並廣播到整個自治系統中去。這樣，每台路由器都收到了自治系統中所更路由器生成的LSA，這些LSA的集合組成了LSDB（鏈路狀態資料庫）。由於每一條 LSA 是對一臺路由器周邊網路拓撲的描述，則整個 LSDB 就是對該自治系統網路拓撲的真實反映。

3-7 LAN/WAN Interfacing Equipment，Devices andConfiguration

ATM (Asynchronous Transfer Mode) 是由國際電話電報諮詢委員會所制定具更高速分封及多工交換標準的高速網路傳輸協定，目前爲 ANSI 及 CCITT 認可爲 B-ISDN 寬頻整體服務數位網路的基礎。ATM 乃是整合語音，影像，資料等，並以相當高的速度傳輸。ATM 也是全球資訊高速公路 information superhighway 觀念的主體架構。

ATM 在傳送資料前必頇先建立好通路，而在通訊的傳送和接收方並不需要同步的動作，所以傳輸信號並不需要附帶時序信號，減少傳送和接收方的聯繫工作和關連性。

其傳輸速率由 1.5Mbps 到 2.5Gbps，一般以 155 Mbps 或是 622

Mbps 居多，點與點之間的距離可由 100 公尺到 40 公里，所以同時可以適用於區域網路與廣域網路。

使用前端錯誤更正 FEC 演算法來更正細胞所產生的單位元錯誤，若是一個細胞當中發生了一個位元以上的傳輸錯誤，則 ATM 交換機會將該細胞丟棄，而 ATM 網路當中並沒更重新傳送的機制。

第四章 網際網路服務與應用

4-1 網際網路服務(Internet Services)

4-1-1 全球資訊網(Web)

從 HTML 文件中顯示靜態（static）網頁並且能夠執行一些程序來創建動態（dynamic）網頁的系統軟件，也是大家常說的網站伺服器。blog（如：無名、天空、pchome 新聞台）這是程式需要 web server 底下才可運作。

Web 是圖形化及易於導航的 ： 可以提供將圖形、音頻、視頻資訊集合於一體的特性，也可以從一個連接跳到另一個連接，方便閱覽。Web 與平台無關 ： 訪問 WWW 時，不會有平台限制，只透過軟體瀏覽器實現。Web 是分佈的 ：Web 將資訊都分佈於不同站點上，只需要在瀏覽器中指明站點就行。

4-1-2 檔案傳輸協定(FTP)

FTP 是所謂的「File Transfer 檔案傳輸」，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。

4-1-3 電子信箱(Mail)

隨著網際網路的興起，SMTP(Simple Mail Transfer Protocol， 簡易郵件傳輸協定)便成了網際網路領域裡的頭號電子郵件傳輸協定。

4-1-4 網域名稱伺服器(DNS)

(網域名稱伺服器 Domain Name Server 之縮寫)用來轉換、記錄 Domain Name 與 IP Address 的伺服器，它可以在 Domain Name 與 IP 之間建立關係。IP 網址是由四組數字組成。爲了方便記憶，我們對 IP 位址做了適度的修改：將四組數字轉成文字，稱之爲 Domain Name(網域名稱)。然後在網路上設立 DNS (Domain Name Server)名稱伺服器，將每台電腦輸入欲前往的主機名稱轉換成電腦看得懂的 IP Address。

一般我們在網路上要求連線時，通常都是使用主機網域名稱例如：http://tw.yahoo.com，http://www.microsoft.com 等。但由於電腦只認得 IP 位址，因此必須透過 DNS 以將網域名稱轉換成對應的 IP 位址，才能順利的連線。

4-1-5 網路新聞論壇伺服器(News Server)

新聞群組是一個集合各式主體的大型討論區域｛網路論壇｝，以全世界而言有數萬個群組，每天全球有數百萬使用者使用，因此新聞群組是一個非常適合發表/廣告/詢問/促銷的地方，商機無限。

4-2 網際網路儲存技術 Internet Caching Technology

代理伺服器(proxy)就是幫用戶端去向目的地的機器要求用戶需求的主機，因爲他是你的代理人，所以，當你設定代理伺服器之後，你的所有相關的要求均會經過代理伺服器去搜尋。

4-2-1 代理伺服器優點

快速的存取動作：他最大的優點就是可以提供用戶端較爲快速的瀏覽或者是資料的存取，剛剛的說明來看，你直接向 www.kimo.com.tw 的要求需要經過一個主機的存取動作，甚至是多個主機的存取，那理應更慢才對，爲何會造成較快的情況，仔細的看一下上面的流程，會發

現，當第一個人要求過 www.kimo.com.tw 的資料後，ksproxy.seed.net.tw 就已經保存有這份資料了，所以以後向這部 proxy 要求相同資料的用戶端，將會直接取用這份資料，而不用到 www.kimo.com.tw 去了。故，通常我們設定代理伺服器的時候，一定要找距離我們的機器最近的那一部，否則就沒有達到代理伺服器的功用了。通常快速的存取動作最明顯的大概是連去國外的網站了。

4-2-2 降低網路的負荷

由於我們是項代理伺服器要求資料，如果代理伺服器內剛好有你要的資料，將會直接傳給你，則你的要求將不會到真實的那一個網頁去（除非你在 IE 內按下『重新整理』這個按鈕），而如果沒有你要求的資料，那他也會去捉一份你要的資料給你，並存下來，以後如果有與你相同需要的用戶，那他就可以直接傳送給用戶，如此當可降低網路的負荷！另外，有些企業部門會將不同目標的代理伺服器分開來，達到分流的目的！例如：proxy1 主要爲找尋台灣的網站，proxy2 爲找國外的網站，則你的網域終將可以達到很好的分流效果，網路會比較快速喔！

4-2.3 提供防火牆內部的電腦連上 Internet

這個是一般企業比較常用的情況！由於企業內部害怕被駭客侵入，通常會設立一些比較嚴密的防火牆，然而如此一來公司內部的電腦可能

面臨無法連上 Internet 的窘境，那使用 proxy 讓你的內部電腦可以透過這一架主機的代理服務而取得 Internet 上的資訊，就是一個很好的方法。

4-2.4 多層次的管道

代理伺服器可以提供多重的管道設定，例如，當你需要國內的資料時，代理伺服器將直接去捉取，而需要國外的資料時，才連到上一層的代理伺服器！如此將可達到你的需求（而不用常常在你的 IE 等瀏覽器上更改所需的代理伺服器）

4-3 多頻率解答(Broadband Solution)

4-3.1 ISDN

ISDN 就是 Integrated 整合、 Service 服務、 Digital 數位和 Network 網路的組合。

4-3.2 Network

網路其實就是將彼此分散的用戶以點對點的方式串接起來，而達到人與人之間 相互溝通的目的。爲了滿足不同的溝通形態，各種不同的網路架構因應而生。

4-3.3 Service

網路的目的在於溝通，並且提供各種不同資訊的服務。ISDN 目前所能提供的服 務大致如下 : 語音，文件，數據，影像，音樂，視訊，監控訊號。以上所列舉的服務，透過 ISDN 傳送可以得到優良的服務品質。以技術而言如廣撥、電視、電影等服務均可以架構在 ISDN 電話網路上。不過將來是由電話公司來經營電視或是由電視公司來經營電話是一大爭論。最重要的是如何汰換舊有網路、建構新網路系統以及更新客戶家用 設備。

4-3.4 Digital

事實上電信局機房裡的交換機 (Swithing)，無論是 PSTN 或是 ISDN 均已數位化其主要的差別在於 CPE 與交換機之間的傳輸方式，前者爲數位(Digital)後者爲類比(Analog)。因此在同一雙絞線上傳輸，ISDN 提供了比 PSTN 更高的速度和更多的服務給使用者。數位的方式傳輸的好處：不易受干擾、錯誤率低、便於儲存、運算、傳遞、易於標準化、模組化、易於整合、未來世界的國際標準語言。

4-3.5 Integrated

當網路完全數位化後，自然就可以提供整合性的服務 : Telephone，

Fax，利用電腦傳送 Data，傳送 Video，上 Internet 等可以同時傳送兩種 資料或訊息給相同或不同的使用者(以窄頻 ISDN BRI 爲考量)。不但要把一般的電話網路上的服務數位化，未來也要將廣播、電視數位化，然後 再整合在一起。因此將來看電視的同時也可以接影像電話、收發傳真、透過所謂 的虛擬實境(Virtual Reality)購物。

4-3.6 xDSL

常見的 xDSL 網路接取技術

(一) IDSL(ISDN Digital Subscriber Loop)技術： 爲 xDSL 技術的一種，採用 ISDN 中 2B1D 的技術，可在一條傳統的兩芯電話線上同時傳送語音及數據資料，兩個 B-Channel 64K 合併後頻寬可達 128Kbps，若有外線語音進入，則自動將其中一個 B-Channel 64K 提供給語音使用，並向下調降數據傳輸爲 64K，待語音離線後再自動回到 128K 的數據頻寬。它的優點包括：

- 採用 2B1Q 的鏈路編碼，最高傳輸距離可達一萬八千呎，不論多大的社區都可接取。
- 價格低廉(目前大都爲固定收費，不限時數上網)。
- 可同時傳送語音及數據資料。
- 爲 xDSL 技術的一種，可以使用 PPP 點對點的傳輸協定，每個用戶皆

可獨享社區內部專屬的頻寬而不會被其他用戶干擾，亦增加網路接取

的安全性。

而其缺點則是頻寬較小，即時影像應用(如 Video On Demand)較受影響。目前國內主要供應商有明碁電通的 iRAC1200 系列 CVD 模組，合勤科技的 Prestige1600 系列 IDSL 模組(但無提供語音的功能)。

(二)MSDSL(Multi-Speed Digital Subscriber Loop)技術：同爲 xDSL 技術的一種，爲 SDSL(Symmetric Digital Subscriber Loop)的改良，有別於 SDSL 及 HDSL2 僅能以固定 2M 的頻寬接取網路，它可針對用戶的實際需求分 128K、256K、384K、512K、 1024K、1536K、1920K、1984K、2048K、2304K 共多達九種不同的頻寬接取網路。其優點包括：

- 爲對稱式(Symmetric)的網路接取方式，上行及下行皆爲同樣的頻寬，非常適合同時需傳送及接收數據資料的商業用途，如即時互動多媒體或公司行號架設網站等。
- 用戶價格可視實際使用頻寬的大小彈性調整。
- 同樣爲 xDSL 技術的一種，可以使用 PPP 點對點的傳輸協定，每個用戶皆可獨享社區內部專屬的頻寬而不會被其他用戶干擾，增加網路接取的安全性。

而其缺點則是無法傳送語音。目前國內尚無針對寬頻網路社區所提供的

相關設備及模組。

(三)ADSL(Asymmetric Digital Subscriber Loop)技術：

同樣爲電信領域中 xDSL 傳輸技術的一種，採用下行與上行分別以不

同的傳輸頻寬接取技術(非對稱)，但隨傳輸距離的長短接取頻寬有512K、64~6M、 2M 之差異。在語音傳送方面，將語音及數據傳輸以分頻方式處理，故可在一條兩芯的電話線上以低頻傳輸語音(4KHz)高頻傳輸數據(25KHz~約 1.1MHz)的方式，同時傳送取語音及數據資料。其優點包括：

- 可以最高達下行 6M、下行 2M 的高速頻寬接取網路。
- 搭配語音分離器(Splitter，將低頻的語音部分分頻開來接至傳統電話公眾網路 PSTN)，可同時傳送語音及數據資料。
- 同樣爲 xSDL 技術的一種，可以使用 PPP 點對點的傳輸協定，每個用戶皆可獨享社區內部專屬的頻寬而不會被其他用戶干擾，亦增加網路接取的安全性。

其缺點則是設備價格昂貴，相對用戶而言，實際使用的成本較其他接取技術高；此外，需有較好的銅線線路品質，才能達到技術理論所述的接取頻寬。目前國內尚無針對寬頻網路社區所提供的相關設備及模組。

(四)VDSL(Very High Data Rate DSL)技術：

中文譯成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)爲快，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。

4-4 網路電話(Voice over IP)

VoIP(Voice over IP)網路電話，是將語音訊號壓縮成數據資料封包後，在 IP 網路基礎上傳送的語音服務，也就是說，透過開放性的網際網路，傳送語音的電信應用服務。利用 Internet 不僅做到了可即時提供語音服務，更可連接至世界各地，讓使用者可以不需再透過傳統的公眾電話網路(PSTN)進行遠距離電話交談。

VoIP 基本之概念就是將原爲類比的聲音訊號以 " 數據封包 "（Data Packet）的型式在 IP 數據網路（IP Network）上做即時傳遞，換句話說，VoIP 系統就是將原爲聲音的類比訊號 數位化後（digitized），透過由網路上各相關通訊協定下，做點對點（ end-to-end ）的即時通訊功能。 VoIP 技術可將資料封包在網路上傳遞過程中所發生的失真、迴音及資料遺失做適當修補功能，使其原音重現。

VoIP 的缺點

有利必有弊，將語音電話改由網路技術傳送存在一些缺點，包括： 初始設置成本：

雖然市場上已有低成本或甚至是零成本方式進行 VoIP 語音傳送，但真的認真考慮使用 VoIP 的企業則需花一大筆投資在 VoIP 設備上(比如 Cisco 的語音閘道器)。

品質問題

雖然 VoIP 的品質已經越來越好了，但大部分的 VoIP 服務和產品都還未能趕上 PSTN 的品質。對於在封包網路(packet network)上傳送語音串流仍舊存在許多挑戰。

相容性問題

有些服務需要發話與受話方都是同一服務商的用戶才行，而有些軟體程式也需要收發話雙方都安裝相同的軟體。然而，有許多其他的服務/程式也可以讓你打電話給任何人，包括從電腦發話到一般的電話上，或甚至是直接以一般電話將封包傳送於 IP 網路上。

4-5 服務品質(QOS)

Quality of Service (QoS)乃是提供穩定、可預測的資料傳送服務，來滿足使用程式的需求。QoS 並不能產生新的頻寬，而是依據應用程式的需求以及網路管理的設定來有效的管理網路頻寬。網際網路的資料流量隨著電子商務、多媒體資訊傳輸、大量檔案下載等應用呈現大幅的

成長。瞬間大量的資料傳輸更影響了企業網路的使用效能。加大頻寬不但非常昂貴，並且不能保證能夠解決網路效能不足的問題。

QoS 的好處

一般的 Traffic Shaping，Queuing，Policy Management 或是 Caching 的產品，或許能夠增加網路的效能，但卻不能保證重要網路應用的穩定運作及反應速度(Consistent response time)。QoS 則能夠將既有的頻寬資源作最佳化的調整，相關機制的完整應用，對網路上的交通做到真正完全的控管。

QoS 的網路架構

在整合型服務路徑上的所有路由器都必須針對每一個資料包流通道記錄其相關參數，且路由器必須要記錄及管理目前的網路資源，以作爲 RSVP 建立通道時的進入許可控制依據。而在分類型服務中，有關進入許可控制部分的機制轉移至帶寬管理者執行，這使得分類型服務的擴充性大爲增加，更適用於骨幹網路。除了單獨使用整合型服務或分類型服務架構之外，也可將兩者混合使用。

整合型服務架構以 RSVP 作爲通道建立的信號規約，若要實現端到端 QoS 網路架構，RSVP 必須能控制分類型服務網域，且在分類型服務網域轉換並建立相關的 QoS 通道參數。以 QoS 架構實現的難易度而言，整合型服務因爲有擴充性的問題，較適合企業網路的應用。對 ISP 而言，短期內要實現 QoS，以分類型服務架構較爲可行。

4-6 串流媒體 (Streaming Media Protocols)

過去要在網路上欣賞影片或音樂這類影音的資料時，需將該檔案完全的下載回電腦中，再透過一些適當的播放程式來觀賞；因這些檔案大多不算小，所以使用者就必需等待較長的下載時間，如果等到下載完了才發現不是自己要的東西，更是白白浪費了那些時間。

因此出現了一種在網路上的多媒體傳播方式，其原理是當伺服器收到用戶端的需求時，將這些影音檔編碼壓縮後，分割成許多的封包(Packet)，送到用戶端將這些封包重組起來呈現在用戶端上，持續的接收資料並播放已接收的部份，就這樣這些資料流不斷的傳送到用戶端上，這樣的技術稱爲串流(Streaming)，而使用這種技術播放的資料就叫做串流媒體(Streaming Media)；藉著串流媒體，使用者不需要將龐大的影音檔案完全下載，就可以做即時的觀賞。簡單的說，串流媒體的原理就是一面下載檔案，一面播放已接收的部分。

這些直接播放的串流媒體，不是以一般的 HTTP 協定輸送，而是經由特定的伺服器作即時廣播，所以它們的位址(URL)並不是以 http:// 爲起始，例如 MicroSoft 是以 mms:// 爲起始，RealWorks 是以 rtsp:// 或 pnm:// 爲起始。

傳統影音的檔案格式不一定可以直接在網路上以串流媒體的方式來

傳播，所以一些媒體廠商就開發了自有的格式以符合串流媒體的需求，

目前在網路上可以透過串流形式播放的影音檔案，如：RealNetworks 的 RealVideo (.rm)和 RealAudio (.ra)、MicroSoft 的 Windows Media Video (.wmv)、Windows Media Audio (.wma)和 Active Streaming Format (.asf)、Apple 的 Quicktime (.mov)等。

串流媒體將網路科技融入了生活中，讓使用者更爲便利，應用的範圍很廣泛，如：即時的股市行情、遠距教學、E-Learning、線上影音多媒體(MTV、KTV、線上廣播、電視節目)…等。

第五章 網路安全

在當今，由於網路發展迅速，網路帶給人們許多的便利，但也造成了不少重要資料外洩，進而成爲駭客攻擊的目標，所以本章節將詳細介紹網路安全。

5-1 Introduction to Network Security

5-1-1 網路安全的隱憂

網路攻擊技術日新月異，攻擊工具易於取得，界面淺顯易懂，不需高深技巧，即可進行攻擊。網路攻擊已不侷限於入侵動作，許多攻擊行

爲旨在阻斷網站之服務能力(破壞服務之更效性)。目前的網路設備安全性不足。路由器之封包過濾功能僅能檢視封包第三層資訊。各式防火牆(封包過濾型，電路階層代理型，應用階層代理型)對私更網路資源防護層級各更不同，防毒軟體逐漸無法辨識網路攻擊，因此資訊安全漸漸被大家所重視。

5-1-2 資訊安全的三要素(CIA)

(一)機密性(Confidentiality) 任何資訊儲存在本局的資訊系統中、資訊系統在處理中或在傳輸線上均要維持其機密性

(二)完整性(Integrity) 任何資料儲存在本局的資訊系統中、資訊系統在處理中或在傳輸線上均要保護，以防不當竄改及資訊系統在運作中被不當的操縱或入侵。

(三)可用性(Availability) 確保資訊與系統持續運轉無誤，當合法使用者要求使用資訊系統時(例如：收送電子郵件、OA 應用系統等)。

5-1-3 資訊安全威脅的攻擊型態

(一)密碼破解(Cryptanalysis)

1. 密文攻擊法：蒐集許多密文，再從中分析並推論出明文的意義。
2. 已知明文攻擊法：假設攻擊者知道一些明文和密文以及其對應關係，從中解出金鑰。
3. 選擇明文攻擊法：破密者將所選擇的明文送給密碼系統加密，破

密者再根據密文-明文配對進行解密。

4. 選擇密文攻擊法：破密者將所選擇的密文送給密碼系統解密，但解出來的明文可能不具更任何意義，之後破密者再根據此密文-明文對進行攻擊。

(二)暴力攻擊法(Brute-Force Attacks) 如果攻擊者諸圖使用所更可能的排列組合來破解密文訊息，那麼這種破解將被稱爲暴力攻擊法。

(三)資源竊取(Resource Theft)

(四)阻斷服務攻擊(Denial of Service) DoS 攻擊並不以篡改或竊取主機資料爲目的，而是癱瘓系統主機使之無法正常運作。換言之，由於一般網路系統的系統資源（例如記憶體、磁碟空間以及網路頻寬等）皆更限，因此駭客可以根據部分網路系統或者相關通信協定等之設計或實作上的漏洞，在一段期間內透過傳送大量且密集的封包至特定網站，使該網站無法立即處理這些封包而導致癱瘓，進而造成網路用戶無法連上該網站而被阻絕在外。

5-1-4 電腦病毒

電腦病毒是一段很小的電腦程式，它是一種會不斷「自我複製」及「感染」的程式，在傳統的 DOS 環境下，通常它會寄存在可執行的檔案之中，或者是軟、硬碟的開機磁區啓動部份，隨著被感染程式由作業

系統載入記憶體而同時執行，病毒因此獲得系統控制權；但在視窗系統中出現的文件巨集病毒則是附著在文件檔中，且其感染之對象亦限於文件檔。

5-1-5 惡意程式

(一)寄生蟲（Worms） 寄生蟲屬於電腦病毒的一種，此型的病毒不會攻擊其他程式，它只會不停的複製自己。再利用網路傳播到其他伺服器，最後所更的伺服器將忙著複製、傳播病毒，沒空服務其他合法的使用者。

(二)暗門程式（Trapdoor） 暗門程式指的是程式或伺服器中未公開的秘密通口，利用暗門程式可以自由進出系統，而不被別人發現。 若電腦系統的管理者發現了漏洞，將漏洞補好了，駭客仍可利用早就安插好的暗門程式，繼續入侵此系統。

(三)木馬（Trojan Horse） 特洛依木馬指的是類似電腦病毒的指令組合，暗藏在普通程式中，藉著普通程式的執行，偷偷的作自己的事。特洛依木馬程式會記載該使用者做了哪些動作，當然包括使用者所按下的密碼。

(四)邏輯炸彈（Logical Bomb） 邏輯炸彈屬於特洛依木馬的一種，它需隱藏在其他的程式中，當某個被預先設定的條件吻合時，它便會啓動。

如被公司開除的員工因心中不滿，離職前便在公司電腦裡擺置了一個邏輯炸彈，若干時日以後，炸彈啓動，自動將電腦中的資料全數銷毀。

5-2 BS7799&VPN

BS7799 是資訊安全管理體系，由英國標準協會發佈。用意是現代企業對資訊的依賴越來越大，沒更各種資訊的支援，企業就不能發展。事實上，資訊已成爲現代企業的一種重要資產，成爲企業成功的關鍵所在。這種資產，更需要加以妥善保護。否則，可能由於人員的原因、競爭對手原因和自然災害等原因，在一瞬間被毀滅、消失、損壞、盜竊、貶值、轉移，給企業帶來致命的打擊。

BS7799 的主要條文內容：

1. 安全方針：爲資訊安全提供管理指導和支援。
2. 安全組織：在公司內管理資訊安全。
3. 資產分類與管理：對公司的資產採取適當的保護措施。
4. 人員安全：減少人爲錯誤、偷竊、欺詐或濫用設施的風險。
5. 實體和環境安全：防止對商業場所及資訊未經授權的取得、損壞及干擾。
6. 通訊與動作管理：確保資訊處理設施正確和安全運行。
7. 接觸管制：管制對資訊的接觸。
8. 體系的建立和維持：確保將安全納入資訊體系。
9. 商業活動連續性管理：防止商業活動的中斷，並保護關鍵的業務

過程免受重大故障或災難的影響。

10. 符合法律：避免違反任何刑法和民法、法律法規或合同義務以及任何安全要求。

VPN(Virtual Private Network)

VPN 是私人網路在公共網路的延伸，透過公共網路的連線使用 VPN，可以用類似點對點通道協定連結的方式來傳送資料。對於使用者來說，就好像使用私人連線來傳送資料。 優點：可以在全世界快樂、經濟且安全地建立通訊連結，不需專用的私人網路，就能夠設定高層級安全性。不適用於：

1. 當任何價格的效能是主要的考慮因素時。
2. 當大多數通訊是同步進行時，如聲音影像。
3. 當使用到與 TCP/IP 不相容的非一般性協定的應用程式時。

運作方式：在 VPN 中，連線的兩端都連結到 Internet。此連線可以採用幾種常用方式，如普通電話線或某種專線等。VPN 使用通道協定將資訊封包封裝到一個額外的標頭中發送，取代原始節點所產生的資訊封包，這個標頭將提供路由資訊，使得被封裝的資料能跨越中間的 Internet 線路。基於隱私權，該資料經過加密，如果資訊封包被攔截，則需要金鑰來解密。

5-3 System Security Concepts (Access Control)

EAP (Extensible Authentication Protocol)

擴展認證協議，是一個普遍使用的認證機制，它常被用於無線網路或點到點的連接中。EAP 不僅可以用於無線區域網，而且可以用於更線區域網，但它在無線區域網中使用的更頻繁。最近，WPA 和 WPA2 標準已經正式採納了 5 類 EAP 作爲正式的認證機制。

EAP 是一個認證框架，不是一個特殊的認證機制。EAP 提供一些公共的 73

功能，並且允許協商所希望的認證機制。這些機制被叫做 EAP 方法，現在大約更 40 種不同的方法。

5-4 Communication Encryption and Authentication Concepts

雜湊函數

安全的雜湊函數在設計時必頇滿足兩個要求：其一是尋找兩個輸入得到相同的輸出值在計算上是不可行的，這就是我們通常所說的抗碰撞的；其二是找一個輸入，能得到給定的輸出在計算上是不可行的，即不可從結果推導出它的初始狀態。現在使用的重要計算機安全協議，如 SSL，PGP 都用雜湊函數來進行簽名，一旦找到兩個文件可以

產生相同的壓縮值，就可以僞造簽名，給網絡安全領域帶來巨大隱患。MD5 就是這樣一個在國內外更著廣泛的應用的雜湊函數算法，它曾一度被認爲是非常安全的。

PGP(Pretty Good Privacy) 此方法結合傳統對稱式與公開金鑰密碼演算法，應用下列技術提供電子郵件安全服務。

1. 隱密性：採用 CBC 模式的 IDEA 加密演算法將要傳送的資料加密，在此 IDEA 金鑰長度是 128 位元。

2. 金鑰管理：應用 RSA 長度 384、512 或 1024 位元的金鑰管理技術，來對隨機選取的交談金鑰（Session Key）加密。

3. 訊息真確性及數位簽章：PGP 使用 RSA 與 MD5 作爲判斷訊息真確與鑑別安全的演算法。

4. 壓縮：訊息在加密前先用 ZIP 2.0 壓縮，可減少資料量和明文資料的重複性（Redundancies），以提高破密的困難度。

DES (Data Encryption Standard)

數據加密標準是一種加密演算法，1976 年被美國聯邦政府的聯邦信息處理標準所選中，隨後既在國際上廣泛流傳開來。這個演算法因爲包含一些機密設計元素，相關的短密鑰長度以及被懷疑內含美國國家安全局的後門而在開始是更爭議的，DES 因此收到強烈的學院派式的審查，並以此推動了現代的分組密碼及其密碼分析。

DES 屬於區塊加密法，而區塊加密法就是對一定大小的明文或密文來做加密或解密動作，Secret Key 長度爲 56 位元， 對長度爲 64 位元的區塊作加密，重複加密處理 16 回合， 每一回合之加密處理，使用 48bits 的子鑰匙。

DES 現在已經不視爲一種安全的加密演算法，因爲它使用的 56 位密鑰過短，以現代計算能力，24 小時內即可能被破解。也更一些分析報告提出了該演算法的理論上的弱點，雖然實際情況未必出現。該標準在最近已經被高級加密標準所取代。

IPSec(Internet Protocol Security)

以 IP Packet 爲單位對信息進行暗號化的方式，來對傳輸途中的信息包進行加密或者防止遭到篡改的一種協議。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 作爲一個協議族（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及較少使用的認證頭，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。目前爲止，IKE 協議是唯一已經制定的密鑰交換協議。

5-5 Network Address Translation (NAT)

NAT(Network Address Transfer)

網路位址轉譯器，主要是用來簡化及保存 IP 位址，它可以讓原本無法上網，而且無法使用內部 IP 位址的主機可以成功的連接 Internet，而且它也就是將要傳送出去的封包進行 IP 轉換的動作，使用 NAT 可以大大減少 IP 位址的需求，因爲基本上整個內部網路都可憑藉 NAT 上的一個外部 IP 來連接 Internet。

NAT 解決了 IPv4 地址短缺的問題，爲一種減少對 IP 需求的機制。若接取設備更支援 NAT，則可作到多台主機使用一組 IP，即 IP sharing。這樣可以減少對 IP 位址的需求。NAT 除了帶來方便和代價之外，對全雙工連接支持的缺少在一些情況下可以看作是一個更好處的特徵而不是一個限制。在一定程度上，NAT 依賴於本地網路上的一臺機器來初始化和路由器另一邊的主機的任何連接，它可以阻止外部網路上的主機的惡意活動。這樣就可以阻止網路蠕蟲病毒來提高本地系統的可靠性，阻擋惡意瀏覽來提高本地系統的私密性。很多具更 NAT 功能的防火牆都是使用這種功能來提供核心保護的。

NAT 的特性是存在兩種地址轉換方式。一種是經常被簡記爲 "NAT"的網路地址轉換，這種方式支持埠的映射並允許多台主機共享一個公用 IP 地址。另一種也可以稱作 NAT、「基本 NAT」或「靜態

NAT」，但在技術上更簡單一點，僅支持地址轉換，不支持埠映射，這就需要對每一個當前連接都要對應一個 IP 地址。寬頻路由器通常使用這種方式來允許一臺指定的電腦去接收所更的外部連接，甚至當路由器本身只更一個可用外部 IP 時也如此，這台路由器更時也被標記爲 DMZ 主機。

支持埠轉換的 NAT 又可以分爲兩類：源地址轉換和目的地址轉換 NAT 。前一種情形下發起連接的電腦的 IP 地址將會被重寫，後一種情況下被連接電腦的 IP 地址將被重寫。實際上，以上兩種方式通常會一起使用以支持雙向通信。

5-6 Firewalls

在電腦運算領域中，防火牆是一項協助確保資訊安全的裝置，會依照特定的規則，允許或是限制傳輸的資料通過。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訊，與建築中的防火牆功能相似。它更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(一個沒更信任的區域) 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忉的信任區域

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。

5-7 Future Trend

無線網路

所謂無線網路，就是利用無線電波來作爲資料的傳遞，它與更線網路的用途完全相似，兩者最大不同的地方在於傳輸資料的媒介不同，一個使用無線電波另一個使用實體線路。由於它是無線電波來作爲資料傳遞，因此在硬體架設或使用之機動性均比更線網路要方便許多，但安裝驅動程式及相關設定，則稍微麻煩一些。

無線網路目前已漸朝公共無線區域發展，各種無線區域網路的通訊協定亦蓬勃發展中，國內大學校園更是無法置身於外。爲因應各大學交流日益頻繁，學生或教職員至外校交流、研究、會議時，通常無法便利地使用當地的網路與外界通訊，因此校園內實更必要建置無線區域網路，以提供跨校區網路漫遊需要，以方便校際網路使用。

DWDM (Dense Wavelength-Division Multiplexer) 高密度多工分波器，它用於光纖通訊中，將一個波長分成許多個波長的技術，使每條光纖能搭載的傳輸訊號倍增，達到光纖的更效使用及降低增加頻寬所需的成本，目前在光通訊界常用的 DWDM，大多是在 1530～1565nm(主要是 1550nm)的波段中，分出 32 個或更多的波長。

PSTN (Professional Security Training Network) 公用交換電話網路是傳統的電路切換網路，主要是用於即時語音通訊上。在進行呼叫時，先關掉撥號關閉，並建立與其他人的電路。PSTN 會將電路指定給呼叫，直到掛斷電話爲止，這樣可以保證服務品質。不管雙方正在通話或是無聲的，都可繼續使用同一電路直到掛斷爲止。

第六章 結論與心得

我們這組專題做的是 ITE 網路通訊的報告，一開始要考試的時候，我們的參考資料只有考古題，就是要反反覆覆的一直看，當然不知道的東西還是要了解內容對自己比較有幫助，有些資料其實都是以前上課的內容、老師所講過的東西，所以上課還是要認真的聽老師上課，不然到考試了，都覺得題目很眼熟，可是不見得會知道答案會是什麼。還有一些課外題就真的很難，除了一些有關電腦的常識之外，還有比較新的網路知識。對於這次的考試，其實一開始的信心不大，總覺得很難考，有時候遇到不會的題目真是要靠運氣，考試有的類別也沒一次就考過，不過有努力過還是會有收穫的，當全部科目都考過時，就有種成就感。雖然這只是一張證照，對未來要上班的地方不一定會有用，但是有了第一章證照的開始，我想會再有動力想考考下一張證照的。

參考文獻

〔1〕http://tw.knowledge.yahoo.com/question/question?qid=1004122203054

〔2〕. http://zh.wikipedia.org/zh-tw/OSI%E6%A8%A1%E5%9E%8B

〔3〕. http://entry.hit.edu.tw/~bd92009/page1.htm

〔4〕. http://zh.wikipedia.org/zh-tw/%E5%85%89%E7%BA%96

〔5〕. http://www.tsnien.idv.tw/Aid/Token_Ring.htm

〔6〕. http://cyber.cs.ntou.edu.tw/~bunny/cybersafe.htm

〔7〕. http://www.msservermag.com.tw/technicwords/020523.aspx

〔8〕.

http://tw.knowledge.yahoo.com/question/question?qid=1508030605311

〔9〕.

http://tw.knowledge.yahoo.com/question/question?qid=1306052708071

〔10〕.

http://tw.knowledge.yahoo.com/question/question?qid=1206110804567