修 平 技 術 學 院

資 訊 管 理 系

實 務 專 題 報 告 審 定 書

本 系 日 間 部 四 技

組長：BF94034 簡孝瑜

組員：BF94018 吳政訓

BF94144 許育誠

所 提 報 告 經濟部資訊專業人員鑑定 網路通訊類

經 本 委 員 會 評 審 通 過 。

口 試 委 員 ：

_____

指 導 老 師 ：

_____

中 華 民 國 九 十 八 年 五 月

目　　錄

第一章　前言

1.1 研究動機 ：

針對這一次的專題，我們是想說我們剛好是讀資管這一科的，而且在平常上課裡，老師們所交的內容也差不多都跟 ITE 有關，所以我們就想說做這個專題應該對我們來說會比較容易上手，而且在加上我們這一組本身就抱著一定要考過 ITE 拿到這張證照的野心，所以才針對 ITE 這方面來做我們的專題報告。

1.2 研究目的 ：

我們的研究目的，也就是希望能在校的這四年裡面，不管是不是上課中老師所教的等等的，都能夠學習到屬於我們自己的知識，然後以後出了社會能夠比別人多一份專長，現在大學生滿街跑，景氣差，工作也非常的不好找，所以能夠比別人多了解一些知識，多學習一些，這樣以後出了社會也就更容易的比別人多一些機會找到自己能夠喜歡的一份工作。

第二章 區域網路

2.1 常見的網路型式

網路可分成三大類：區域網路(Local Area Networks, LANs)、都會網路(Metropolitan Area Networks, MANs)以及廣域網路(Wide Area Networks, WANs)。

區域網路(LAN)

區域網路(Local Area Network, LAN)是將位置比較近的電腦，用一種能讓他們彼此通訊的方式(纜線、紅外線連線、或小型無線電發射機)所連接的網路。

都會網路(MAN)

設計用來跨越整個城市,此種網路的目標是要達到所謂區域網路與區域網路間及設備與設備間的資源共享機能。

例如，中華電信的數位用戶迴路存取多工網路(Digital Subscriber Line Access Multiplexer, DSLAM)。

廣域網路(WAN)

能夠讓數據、語音、影像和視訊等資料在寬廣的地理區內做長距離的傳輸，所涵蓋的範圍可能包括一個國家、一個洲，甚至於全世界。如中華電信的非同步傳輸模式(Asynchronous Transfer Mode, ATM)

互連網路

當兩個以上的網路連結在一起就形成一個互連網路(Internetwork, or internet)，常見的互連網裝置有路由器(Router)和閘道器(Gateway)。

2.2 主從式架構

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。

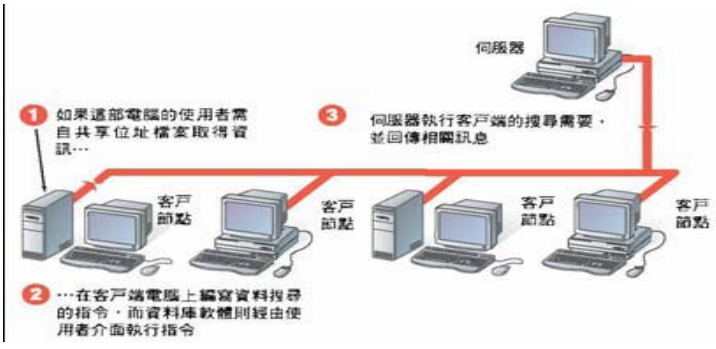
伺服器(Server)程式：

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，都稱為伺服器程式。

2.2.1 主從式網路

客戶/伺服器網路(Client/Server 網路)是伺服器網路架構中的一個應用類型。個人電腦與中央伺服器分享處理與儲存負載。這種架構下的每部電腦與伺服器都需要特殊的軟體，但它並不需採用任何特定類型的網路。客戶/伺服器軟體可用在區域網路或廣域網路上

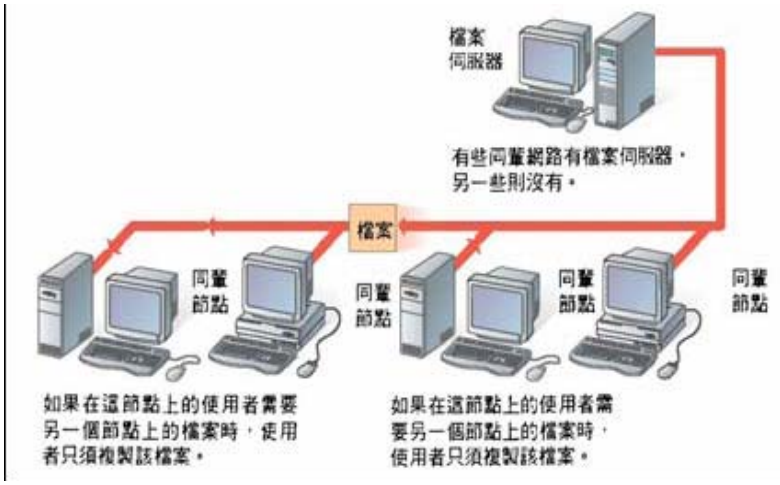
主從式網路(圖)



2.2.2 peer-to-peer 網路

同級間網路(Peer-to-Peer Network)中，網路上的所有節點彼此都有相等的關係，並且全都有類似的軟體，用來支援共享資源。

在一個傳統的同級間網路中,每個節點都至少可以存取其它節點上的一些資訊,如果它們設定正確，多用戶作業軟體都可讓使用者存取硬碟上的檔案，並使用附屬於網路上其它電腦的印表機。



2.3 OSI Reference Model

2.3.1 Layer 1 實體層 Physical Layer

在這個層級當中主要定義了最基礎的網路硬體標準，包括各種網路線、各種無線連線方式，各種設備規範、 以及各種接頭的規則，還有傳輸訊號的電壓等等，反正與硬體有關的標準大多都在這個層級當中定義的！

2.3.2 Layer 2 資料連接層 Data-Link Layer

由於傳送資料的網路媒體是以是電子訊號進行傳送,所以我們的資料要使用這樣的訊號傳送時， 就需要制訂各種網路型態的訊框（frame）了，才能確保資料可以在不同的網路媒體進行傳送的動作。 所以，在這一層當中就制訂了 frame 的格式以及通過網路的方式。包括訊框的資料格式、錯誤控制、流量控制、檢查資料傳輸錯誤的方法等等，都在這裡控制。 既然與訊框有關，當然這個層級就與前面提到的 MAC 有很強烈的相關性囉！

2.3.3 Layer 3 網路層 Network Layer

這一層是我們最感興趣的囉～因為我們提及的 IP（Internet Protocol）就是在這一層定義的， 同時也定義出電腦之間的連線建立、終止與維持等，資料封包（packet）的傳輸路徑選擇等等， 因此這個層級當中最重要的除了 IP 之外，就是封包能否到達目的地的路由（route）概念了！ 此外，這一個網路層可以涵蓋實體層與資料連結層，通常我們不需要設定硬體與相關 MAC 的資料，就是因為網路層已經（有點類似）隱藏了底下兩層，讓我們只要設定好 IP 就能夠上網吶！

2.3.4 Layer 4 傳送層 Transport Layer

這一個分層定義了發送端與接收端的連線技術(如 TCP 技術)，同時包括該技術的封包格式，資料封包的傳送、流程的控制、傳輸過程的偵測檢查與復原重新傳送等等， 以確保各個資料封包可以正確無誤的到達目的端。

2.3.5 Layer 5 會談層 Session Layer

在這個層級當中主要定義了兩個位址之間的連線通道之連接與掛斷,此外，亦可建立應用程式之對談、 提供其他加強型服務如網路管理、簽到簽退、對談之控制等等。如果說傳送層是在判斷資料封包是否可以正確的到達目標， 那麼會談層則是在確定網路服務建立連線的確認。

2.3.6 Layer 6 表現層 Presentation Layer

我們在應用程式上面所製作出來的資料格式不一定符合網路傳輸的標準編碼格式的！ 所以，在這個層級當中，主要的動作就是：將來自本地端應用程式的資料格式轉換(或者是重新編碼)成為網路的標準格式，然後再交給底下傳送層等的協定來進行處理。所以，在這個層級上面主要定義的是網路服務(或程式)之間的資料格式的轉換， 包括資料的加解密也是在這個分層上面處理。

2.3.7 Layer 7 應用層 Application Layer

完全與程式有關的囉，包括定義出檔案的讀取、複製、開啟、關閉等等，常見的程式包括有瀏覽器、資料庫處理系統與電子郵件系統等等。

2.4 雙絞線標準

1．CAT-1：目前未被 TIA/EIA 承認。以往用在傳統電話網路（POTS）、ISDN 及門鐘的線路.

2．CAT-2：目前未被 TIA/EIA 承認。以往常用在 4 Mbit/s 的令牌環網路。

3．CAT-3：目前以 TIA/EIA-568-B 所界定及承認。並提供 16MHz 的頻寬。曾經常用在 10Mbps 乙太網路。

4．CAT-4：目前未被 TIA/EIA 承認。提供 20MHz 的頻寬。以往常用在 16 Mbit/s 的令牌環網路。

5．CAT-5：目前以 TIA/EIA-568-A 所界定及承認。並提供 100MHz 的頻寬。目前常用在快速乙太網（100 Mbit/s）中。

6．CAT-6：目前以 TIA/EIA-568-B 所界定及承認。提供 250MHz 的頻寬，比 CAT-5 與 CAT-5e 高出一倍半。

7．CAT-6A：將來使用在萬兆乙太網（10 Gbit/s）中。

2.4.1 屏蔽雙絞線 (Shielded Twisted Pair STP)

屏蔽雙絞線 (Shielded Twisted Pair STP)，是一種銅質線材。此種線為兩條一對地互相纏繞並包裝在絕緣管套中。雙絞線外的金屬網(通常是銅質)可以屏蔽傳輸線使之不受外部電磁場干擾，同時作為接地之用。但這種額外的保護結構降低了屏蔽雙絞線的彈性。這種線常用在乙太網中。 屏蔽雙絞線額外的保護結構提高了此種線材的單位價格。

2.4.2 網路線介紹

1. EIA/TIA-568A 網路線接腳（白綠 綠 白橙 藍 白藍 橙 白棕 棕）
2. EIA/TIA-568B 網路線接腳（白橙 橙 白綠 藍 白藍 綠 白棕 棕）

T568A 接線

接頭	雙絞線組	線	顏色
1	3	1	綠白
2	3	2	綠
3	2	1	橙白
4	1	2	藍
5	1	1	藍白
6	2	2	橙
7	4	1	棕白
8	4	2	棕

T568B 接線

雙絞線組	線	顏色
2	1	橙白
2	2	橙
3	1	綠白
1	2	藍
1	1	藍白
3	2	綠
4	1	棕白
4	2	棕

2.4.3 網路傳輸媒介

1.有線傳輸媒介:

(1)同軸電纜(coaxial cable): 內層使用銅線作為傳輸線路，外層以塑膠包裝，兩者之間使用絕緣材料加以隔開。其優點為成本低、安裝及擴充容易， 缺點則是可靠性差、網路維護困難。短距離的同軸電纜一般也會用在家用影音器材，或是用在業餘無線電設備中。此外，也曾經被廣泛使用在乙太網的連接，直至被雙絞線（CAT-5 線）所取代。

長距離的同軸電纜常用在電台或電視台的網路上使用。儘使有高科技的器材取代，如：光纖、T1/E1、人造衛星等。但由於同軸電纜相對便宜，也一早已鋪設好，因而沿用至今。

(2)雙絞線(twisted pair): 以二條銅線相互絞纏在一起，外覆絕緣材料。可分為遮蔽式雙絞線(STP)及無遮蔽式雙絞線(UTP)兩種。其優點為成本低、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): 光纖常被電話公司用於傳遞電話、網際網路，或是有線電視的訊號，有時候利用一條光纖就可以同時傳遞上述的所有訊號。與傳統的銅線相比，光纖的訊號衰減（attenuation）與遭受干擾（interference）的情形都改善很多，特別是長距離以及大量傳輸的使用場合中，光纖的優勢更為明顯。然而，在城市之間利用光纖的通訊基礎建設（infrastructure）通常施工難度以及材料成本難以

控制，完工後的系統維運複雜度與成本也居高不下。因此，早期光纖通訊系統多半應用在長途的通訊需求中，這樣才能讓光纖的優勢徹底發揮，並且抑制住不斷增加的成本。

從 2000 年光通訊（optical communication）市場崩潰後，光纖通訊的成本也不斷下探，目前已經和銅纜為骨幹的通訊系統不相上下。

對於光纖通訊產業而言，1990 年光放大器（optical amplifier）正式進入商業市場的應用後，很多超長距離的光纖通訊才得以真正實現，例如越洋的海底電纜。到了 2002 年時，越洋海底電纜的總長已經超過 250000 公里，每秒能攜帶的資料量超過 2.56Tb，而且根據電信業者的統計，這些數據從 2002 年後仍然不斷的大幅成長中。

同軸電纜

雙絞線

光纖

2.4.4 無線傳輸分類

IEEE 802.11b

IEEE 802.11b 是無線區域網的一個標準。其載波的頻率為 2.4GHz，可提供 1、2、5.5 及 11Mbit/s 的多重傳送速度。它有時也被錯誤地標為 Wi-Fi。實際上 Wi-Fi 是無線區域網聯盟（WLANA）的一個商標，該商標

僅保障使用該商標的商品互相之間可以合作,與標準本身實際上沒有關係。[在 2.4-GHz 的 ISM 頻段共有 14 個頻寬為 22MHz 的頻道可供使用。IEEE 802.11b 的後繼標準是 IEEE 802.11g，其傳送速度為 54Mbit/s。

IEEE 802.11g

IEEE 802.11g 在 2003 年 7 月被通過。其載波的頻率為 2.4GHz（跟 802.11b 相同)，原始傳送速度為 54Mbit/s，淨傳輸速度約為 24.7Mbit/s(跟 802.11a 相同)。802.11g 的設備向下與 802.11b 兼容。其後有些無線路由器廠商因應市場需要而在 IEEE 802.11g 的標準上另行開發新標準，並將理論傳輸速度提升至 108Mbit/s 或 125Mbit/s。

IEEE 802.11i

IEEE 802.11i 是 IEEE 為了彌補 802.11 脆弱的安全加密功能（WEP, Wired Equivalent Privacy）而制定的修正案，于 2004 年 7 月完成。其中定義了基於 AES 的全新加密協議 CCMP（CTR with CBC-MAC Protocol)，以及向前兼容 RC4 的加密協議 TKIP（Temporal Key Integrity Protocol)。

無線網路中的安全問題從暴露到最終解決經歷了相當的時間,而各大廠通信晶片商顯然無法接受在這期間什麼都不出售，所以迫不及待的 Wi-Fi 廠商採用 802.11i 的草案 3 為藍圖設計了一系列通信設備，隨後稱之為支持 WPA（Wi-Fi Protected Access）的；之後稱將支持 802.11i

最終版協議的通信設備稱為支持 WPA2（Wi-Fi Protected Access 2）的。

IEEE 802.11n

IEEE 802.11n，是 2004 年 1 月時 IEEE 宣布組成一個新的單位來發展的新的 802.11 標準，在目前仍然處於草案階段。傳輸速度估計將達 540Mbit/s，因此需要在物理層產生更高速度的傳輸率，此項新標準應該要比 802.11b 快上 50 倍，而比 802.11g 快上 10 倍左右。802.11n 也將會比目前的無線網路傳送到更遠的距離。

2.5 Network Topolgies

2.5.1 匯流排網路:

在匯流排架構中，所有電腦都經由一條主幹線連結起來。由於其拓樸形狀就像是在公車上乘客都拉著鐵杆上的吊環站立一樣，所以就被稱為 Bus（巴士)架構。

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。

2.5.2 環狀網路

在環狀架構中，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。資料在環狀架構中傳送，必須依照一定的方向，全部順時針方向或全部逆時針方向。由於迴路的特性，資料在迴路中傳送也具有廣播的性質，每一部電腦都可以接收到資料。

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。所以為了提升環狀網路的容錯能力及增加網路的傳輸效率，高速環狀網路都設計成「雙環狀網路」。二條環狀迴路分別以順時針與逆時針方向傳輸資料。

2.5.3 星狀網路

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。

由於任何通訊都要經過中央控制主機，因此星狀架構具有較佳的管理特性。不過一旦中央控制主機發生故障，整個網路就癱瘓了。另外，二個星狀架構網路可以藉著連接二部中央控制主機來達成網路與網路之間的資料傳輸。

2.6 網路設備

1.傳輸設備

第一層設備：

(1)訊號再生器(Repeater)

(2)集線器 (Hub)

第二層設備：

(1)橋接器 (Bridge)

(2)第二層交換器 (Layer-2)

第三層設備：

(1)路由器 (Router)

(2)第三層交換器(Layer-3)

2.運作原理

第一層設備：

(1)訊號準位回覆

(2)不作編碼檢查

第二層設備

(1)區域網路設備

(2)檢查第二層標頭資料後轉送

第三層設備：

(1)廣域網路設備

(2)檢查第二三層標頭資料後轉送

2.6.1 HUB(集線器)

Hub 集線器最主要的功能便是匯集所有區域網路中的電腦，使各分枝電腦可連接到網路主幹上，一般來說，只具備基本功能的集線器在傳輸品質上較不穩定，因為當區域網路內部在作資料的流動傳輸時，會影響到其它電腦連接到主幹網路上的傳輸速率，相對的，當越多人同時透過 Hub 上網時，各自的傳輸都會被拖累。目前市面上的集線器多以

10Mbps/100Mbps雙速集線器為主流,採用UTP埠,也就是只要使用RJ-45的線插上即可，此種集線器可自動偵測使用者是以10或100Mbps速度上網，因為價格上和容易升級的優勢，所以市場接受度很高；而較好的集線器還可當網路管理設備，即透過集線器中SNMP網管功能，能讓網管人員透過遠端控制軟體得知網路故障所在。

為了解決以往集線器會互相干擾的情況，於是發展出交換式集線器（Switch Hub)。交換式集線器提供多點式橋接的設備，而且因為埠點的交錯形式,所以交換式集線器可允許多人同時資料交流，又不影響彼此的傳輸品質。以往集線器的干擾情況來自於電腦作資料傳輸時，資料會從主幹線平均分配到接到Hub上的每一台電腦,也就是說即使電腦在未開機狀態，一樣會有資料的傳送動作，如此頻寬便被分蝕掉了。但是使用交換式集線器時便可避免這樣的情形,因為交換式集線器中的每個埠是交錯獨立的，也就是假設8台電腦所使用的集線器中，只有一台在使用，這樣子的話此台電腦便可獨享大頻寬,所以共用集線器的使用者使用網路資源相當頻繁時，交換式集線器便是比較好的選擇。

集線器和交換器的比較

較常被用來使用在網路管理上的設備除了集線器外，便是「交換器」。交換器在價格上通常會比集線器貴，但相對的功能上也比集線器好。一般來說，集線器僅支援半雙工，也就是頻寬得共享，而且集線器的封包

流向路徑是以廣播方式傳迭到所有埠，會有干擾碰撞現象，而交換器則支援全雙工，當執行全雙工時，每埠甚至可獨享 200Mbps 的頻寬，而且沒有封包碰撞的憂慮，在擴充方面，交換器也比集線器高。

2.6.2 Bridge 橋接器

1.它是以一條線連接所有電腦，就像是電池串聯一樣....優點是成本低，缺點是只要一端壞掉，維修、找尋錯誤就很麻煩，而且一次只可以一台電腦傳訊。

2.透過一台 Hub or Switch 來做轉接的功能，在家庭用戶或其他地方是很常見的一種方式，優點是一條線壞掉不會影響整段網路，缺點是....要是 Hub or Switch 壞掉呢。

3.環狀拓樸是將所有的電腦都串聯成一個環，將 A 電腦的傳送端接 B 電腦的接收端，B 的傳送端則接 C 的接收端...以此類推。優點是它有一定的傳輸效率，缺點則跟匯流排一樣，一台當機全部接著當機。

4.混合實體拓樸，就是上面三種混合起來使用常見的有：星狀匯流排、星狀環等，星狀匯流排就是在一個區域內的電腦為星狀拓樸，跟另外一個區域的電腦用匯流排拓樸，假設 A 跟 B 兩區，A 跟 B 自己區域內採用星狀，那 AB 兩區連線就使用匯流排。只是缺點是 AB 中間連線有一台壞掉，可能就會影響兩區傳輸。

2.7 ARP

ARP 協議（Address Resolution Protocol），或稱地址解析協議。ARP 協議的基本功能就是通過目標設備的 IP 地址，查詢目標設備的 MAC 地址，以保證通信的順利進行。他是 IPv4 中網路層必不可少的協議，不過在 IPv6 中已不再適用，並被 icmp v6 所替代。

在每台安裝有 TCP/IP 協議的電腦或 route 裡都有一個 ARP 緩存表，表裡的 IP 地址與 MAC 地址是一對應的，如表甲所示。

主機名稱	IP 地址	MAC 地址
A	192.168.38.10	00-AA-00-62-D2-02
B	192.168.38.11	00-BB-00-62-C2-02
C	192.168.38.12	00-CC-00-62-C2-02
D	192.168.38.13	00-DD-00-62-C2-02
E	192.168.38.14	00-EE-00-62-C2-02
...	...	

以主機 A（192.168.38.10）向主機 B（192.168.38.11）發送數據為例。當發送數據時，主機 A 會在自己的 ARP 緩存表中尋找是否有目標 IP 地址。如果找到了，也就知道了目標 MAC 地址為(00-BB-00-62-C2-02)，直接把目標 MAC 地址寫入幀裡面發送就可以了;如果在 ARP 緩存表中沒

有找到相對應的 IP 地址，主機 A 就會在網路上發送一個廣播(ARP request)，目標 MAC 地址是「FF.FF.FF.FF.FF.FF」，這表示向同一網段內的所有主機發出這樣的詢問：「192.168.38.11 的 MAC 地址是什麼？」網路上其他主機並不響應 ARP 詢問，只有主機 B 接收到這個幀時，才向主機 A 做出這樣的回應(ARP response)：「192.168.38.11 的 MAC 地址是(00-BB-00-62-C2-02)」。這樣，主機 A 就知道了主機 B 的 MAC 地址，它就可以向主機 B 發送信息了。同時它還更新了自己的 ARP 緩存表，下次再向主機 B 發送信息時，直接從 ARP 緩存表裡查找就可以了。ARP 緩存表採用了老化機制，在一段時間內如果表中的某一行沒有使用，就會被刪除，這樣可以大大減少 ARP 緩存表的長度，加快查詢速度。

第三章　網際網路介接基礎

3-1 Introduction to Computer System

3.1.1 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為止。PSTN(Public Switched Telephone Network)使用銅線來傳輸類比聲音的電話系統就是使用這種技術。

3.1.2 PSTN (Public Switched Telephone Network)

也就是以傳統銅線作為傳遞媒介的電信局,這是一種傳統過時的電話網路(Network),設備複雜而且維修不易,頻寬(Bandwidth)窄,且時常會有許多雜音及停頓,自然就不能如光纖網路那般提供許多附加服務。

3.1.3 DNS (Domain Name System)

DNS 的全稱是 Domain Name System, 當您連上一個網址, 在 URL 打上: www.hotmail.com 的時候, 可以說就是使用了 DNS 的服務了。但如果您知道這個 www.hotmail.com 的 IP 地址, 直接輸入 209.185.243.135 也同樣可以到達這個網址。其實, 電腦使用的只是 IP 地址而已(最終也是 0 和 1 啦), 這個 www.hotmail.com 只是讓人們容易記憶而設的。因為我們人類, 對一些比較有意義的文字比記憶那些毫無頭緒的號碼,往往容易得多。DNS 的作用就是為我們在文字和 IP 之間擔當了翻譯, 而免除了強記號碼的痛苦。

3.1.4 OSI 七層協定

OSI 七層協定		
OSI	說明	例子
應用層 Application	提供雙方應用程式存取 OSI 環境的方法。	Ftp,Email, Telnet
表現層 Presentation	提供雙方應用程式之間資料格式的轉換。	字元碼轉換,加密
會議層 Session	提供雙方應用程式之間的溝通方式和規則。 含有溝通、群組、還原三個主要服務。	全/半雙工
傳輸層 Transport	提供雙方資料交換規則及品質最佳化。	TCP
網路層 Network	提供雙方透過網路的定址方法、傳送路徑。 在點對點傳輸中，由於資料連結層已提供管理之功能，因此用不到此層。	IP
資料連結層 Data link	提供網路層及實體層間之管理、錯誤偵測&控制。	MAC
實體層 Physical	提供雙方系統間實體介面、傳送位元的規則。	Ethernet

3.1.5 SSID服務組識別碼

"服務組 (Service Set)" 指的是提供無線網路功能的一組設備，例如您的 Access Point 和一堆無線網卡，就可以算是一個無線網路服務組。您可以為每一個無線網路服務組其定義一個識別代號，這個代號就是 "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。

相關試題

1.下列何者使用 circuit switching 之技術？(C)

(A)X.25

(B)Frame Relay

(C)PSTN

(D)Internet

2. 一般電腦要上網，需要哪些必要步驟？(複選) (ADB)

(A 安裝網路卡

(B)安裝網路卡驅動程式

(C)設定 BookMarks

(D)設定 TCP/IP，閘道器與 DNS 伺服器

3.針對 MSN 和 Yahoo Messenger 作日密來發送即時訊息是屬於 OSI

7Layer 的哪一層？(A)

(A) Presentation

(B) Network

(C) Application

(D) Data link

4.如果安裝了無線網路卡，但是無法上網，可能是什麼原因？(複選)(BD)

(A)無線網路卡沒有設定固定 IP，只能抓到動態 IP

(B)無線網路卡沒有設定正碇的 SSID

(C)安裝的 CPU 不夠快

(D)無線網路卡的加密設定和 AP 不一致

3-2 Router Concepts

3.2.1 Router 路由器

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。

3.2.2 BGP (Border Gateway Protocol)

BGP 全名為 Border Gateway Protocol, 是路由協定(Routing Protocol)的一種, 一般使用在路由不同自主系統(Autonomous System)之間或之內, BGP 是為 TCP／IP 互聯網設計的外部網關協議，用於多個自治域之間。它既不是基於純粹的鏈路狀態演算法，也不是基於純粹的距離向量演算法。它的主要功能是與其他自治域的 BGP 交換網路可達資訊。為了滿足 Internet 日益擴大的需要，BGP 還在不斷地發展。在最新的 BGp4 中，還可以將相似路由合併為一條路由。

相關試題

1.下列哪些是構成 Router 主要的元件？(複選)(A B C)

(A)作業系統

(B)大容量硬碟

(C)網路介面

(D)CPU 與 RAM

2.Route 的網路作業系統，通常存放在哪裡，具有較高的可靠性？(A)

(A)Flash Memory

(B)Hard Disk

(C)DRAM

(D)SRAM

3.除了硬體故障以外，通常造成 Router 無法轉送封包的主要原因有哪些？(複選)(B C D)

(A)記憶體使用量過高

(B)CPU 負載過高

(C)介面流量滿載

(D)病毒攻擊造成 Router 當機

4. BGP (Border Gateway Protocol)：(複選)(B C)

(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

3-3 IP Addressing

3.3.1 IP Addressing

IP 就等於是你上網的那台電腦的地址，網路世界和真實社會有點很類似，都需要一個門牌號碼，方便對方把各種訊息，傳遞到你的位置，或反過來發信號，送到你想發送的位置。這個「位置」就是所謂的 IP（Internet Protocol，網際網路協定），也稱為「IP Address」（IP 位址）。也就是說，不管是要連上網路，或是傳送信件，都必須知道對方的 IP 位址才能與該台電腦溝通。

動態 IP

動態 IP，就是你每次上線時系統都會給你一組不同的 IP 號碼讓你使用網路資源 。

固定 IP

固定 IP，例如，你如果向中華電信申請一個商業型態的 ADSL 專線，那他會給你一個固定的實體 IP ，這個實體 IP 就被稱為『固定 IP 』了。

虛擬 IP

虛擬 IP：IP 位址為 xxx.xxx.xxx.xxx 的型態，其中， xxx 為 1-255 間的整數，但近來上網人數成長速度太快，實體的 IP 已經有點不夠使

用了,但在最初規劃 IP 時就已經預留了三個網段的 IP 做為內部網域的虛擬 IP 之用。但是虛擬 IP 的電腦並不能直接連上 Internet 喔。

3.3.2 IP6 和 IP4 的差異。

有關 IPV6 和 IPV4 的差異則概略說明如下：

(一) 無 IHL：因為標頭欄位長度固定。

(二) 無協定欄：由下一標頭欄說明。

(三) 沒有有關區段的欄位： 因為 IPv6 要求主機與路由器必須支援 576bytes 的分封，使分割不會一開始就發生。

(四) 沒有檢查碼：以提高效率。

IPV4 協定的資料格式固定至少 20bytes，最多可達 60bytes。主要包含下列欄位：

(一) 版本(Version)(4)：可以追蹤目前分封屬於哪一個版本的協定。

(二) IHL(Internet Header Length)(4)：說明標頭長度，最小為 5(20bytes)，最大為 15(60bytes)，每一單位表示一個四位元組。

(三) 服務型態(Type of Service)(8)：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。

(四) 總長度(Total Length)(16)：表示整個分封的長度，最長可達 65535 bytes

(五) 識別(Identification)(16):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有相同的識別值，用來切割區段。

(六) DF(Don't Fragment)與 MF(More Fragment)：DF 表示不要產生區段，因為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，用來檢查訊簡所有區段有沒有完全到達。

(七)區段位移(Fragment Offset)(13)：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，其餘區段都必須是 8bytes 的倍數。因為此欄位有 13bits，因此每個訊簡最多可分割為 8192 個區段，因此最大訊簡長度為 65536bytes。

(八)存活期(Time to Live)(8)：就是限制分封存活期的計數器，以秒為單位，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。

(九)協定(Protocol)(8)：說明採取何種運輸協定處理此一訊簡，可以是 TCP、UDP 等。

(十)標頭檢查碼(Header Checksum)(16)：只檢查標頭，每次跳躍後都要重新計算。

(十一)傳送端位址與接收端位址(Source Address & Destination Address)：用來表示網路(net-id)與主機號碼(host-id)，總計長度

32bits。

(十二)選項(Option)：變動長度，允許後續版本的協定可以增加新資訊。

Total Length:32bits

Version	IHL	Type of Service	Total Length			
Identification				DF	MF	Fragment Offset
Time to Live		Protocol	Header Checksum			
Source Address						
Destination Address						
Options						

※IPV6 的欄位格式：

(一)版本(Version)(4)：決定目前所採用協定的版本。

(二)優先順序(Priority)(4)：設定各種應用程式的優先順序。

(三)流程標籤(Flow Label)(24)：可以設定傳送端與接收端建立特定的連接方式。

(四)負荷長度(Payload Length)(16):可以決定 40 位元組標頭(header)之後的長度。

(五)次一標頭(Next Header)(8)：標示是否有六種之一的延伸性的標頭(extension header)，或是指定傳輸層所使用的通信協定。

(六)跳躍限制(Hop Limit)(8)：和 IPv4 的存活期的意義相同。

(七)傳送端位址與接收端位址(Source Address & Destination Address)：用來表示網路(net-id)與主機號碼(host-id)，總計長度 128bits。

Total Length: 32bits

Version	Priority	Flow Label		
Payload Length			Next Header	Hop Limit
Source Address (128 bit)				
Destination Address (128 bit)				

※IPV6 的優點：

(一)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。

(二)可簡化原有 IPv4 的標頭欄位的能力。

(三)支援擴充的標頭及選項的能力。

(四)可以支援認證及私密性的相關操作。

(五)容易自原有的 IPv4 格式移轉。

(六)同時具有網路服務品質的指定能力。

3.3.3 Multicast

Multicast 的目的在於協助處理以少量頻寬傳送超載的資料，並減輕相關網路設備的負載。即在網路上的任意一位使用者，同時傳送資料給多位使用者時，並非以一人一份的方式傳送，而是考慮以降低重覆程度的方式來傳送。舉例來說，如果一份資料約為 200kb，同時送給 10 位使用者，則傳送端的使用者機器便需有 2Mb 的上傳頻寬才能完成此一任務。這樣的頻寬需求對於目前國內的網路環境而言仍有相當程度的不便，此時便需運用 Multicast 的技術來解決這樣的問題。

3.3.4 IP 的等級

IP ADDRESS 能分配的數量為:A~E 五個等級

1. CLASS A : 127 個網路, 每個網路有 16 個百萬的主機.

2. CLASS B : 16000 個網路, 每個網路有 65000 個主機

3. CLASS C : 2 個百萬網路, 每個網路有 254 個主機.使用這個方式分配導致很多可用位址被浪費, 新版的 IPV6 打算使用 CIDR 編碼方式來取代

4.Class D 和 Class E 為保留區域。

相關試題

1.實際可用的 A 等級 IP 網路的總數為(D)

(A)256

(B)254

(C)128

(D)126

2.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

3.Internet 的 IP 日益缺乏,如何正確設計才能使得 IP 使用效率提高？(複選)(A B)

(A)減少 subnet 切割所浪費的 network/broadcast 位址

(B)使用 PrivateIP 分配給一般 PC，再使用 NAT 轉成 Public IP

(C)將使用的 IP 都切成點對點的 30bit 子網段

(D)將好幾個 Class C 的 IP 合伴成一個大網段來使用

4.一般在 Internet 上所使用的 IP 位址是屬於哪幾種 ClASS 的 IP？(C)

(A)Class D,E

(B)Class G,H

(C)Class A,B,C

(D)Class D

5.採用 IPv6 比 IPv4 的優點有哪些？(複選)(A C)

(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

3-4TCP/IP Protocol

3.4.1 TCP/IP(Transmission Control Protocol/Internet Protocol)

早期的電腦,並非如我們日常生活中見到的個人 PC 那樣細小; 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, 可以說是相互獨立的。

在 1969 年, 為美蘇冷戰期間, 美國政府機構試圖發展出一套機制, 用來連接各個離散的網路系統, 以應付戰爭危機的需求。這個計劃, 就是由美國國防部委託 Advanced Research Project Agency 發展的 ARPANET 網路系統, 研究當部份電腦網路遭到工具而癱瘓後, 是否能夠透過其他未癱瘓的線路來傳送資料。

3.4.2 UDP (User Datagram Protocol)

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) 為快，但也不保證能夠安全的送達(因為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。

3.4.3 ICMP(Internet Control Message Protocol)

ICMP 網際網路控制訊息協定

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(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，也可透過它測試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"，其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，其功能主要有:

偵測遠端主機是否存在。

建立及維護路由資料。

重導資料傳送路徑。

資料流量控制。

3.4.4 MAC address（網路實際位址）

每一張網路卡在工廠出廠時，都會分配到一個獨一無二的號碼，此號碼即為 MAC address。它的功用就好像我們的身份證號碼一樣，除了用來辨別每張網路卡外，它也讓網路上的資料，能正確地找到傳送或接收的地方，所以也稱網路卡實際位址。

相關試題

1.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.TCP/IP 中，用來傳遞錯誤或控制信息的協定為：(B)

(A)IGMP

(B)ICMP

(C)HMP

(D)ISO-IP

3.TCP 和 IP 對應到 OSI 7 Layer 是分別屬於哪二層？(C)

(A)Session、Network

(B)Network、Transport

(C)Transport、Network

(D)Application、Network

4.TCP/IP 的通訊定中包含哪些 Layer？(複選)(A B C)

(A)Application

(B)Transport

(C)Internet

(D)Data Link

5.IPv6 位址的長度為？(D)

(A)32bit

(B)48bit

(C)64bit

(D)128bit

3-5 IPX Protocol

3.5.1 IPX(Internet Packet Xxchange)

IPX 是一種通訊協定被發展出來應用在允許一台機器的應用程式和另一台透過網路溝通。這種通訊協定的使用最常被應用在網路遊戲上，諸

如很有名的 WAR2、doomlike game、DIABLO 等，但是它被應用最多的就是在 Novell 的網路流通上。而也有一個跟它非常相近的通訊協定稱為 SPX。而兩者之間的唯一不同點就是，當你要傳一堆資料封包到另外一台電腦而使用 IPX 通訊協定時,對方電腦收到封包的順序會跟你傳封包的順序一模一樣。但如果是 SPX 通訊協定的話，這點就不能擔保了，這點對即時性的資料就會發生沒辦法處理判定的問題了。

3.5.2 RIP(Routing Information Protocol)

RIP 是 Routing Information Protocol 的簡稱,在 IP 環境中有 RIP，在 IPX 的環境中也有 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 Distance Vector 的方式，所謂 Distance Vector 是指以 Router 的個數來作為距離的判斷，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。

3.5.3 RIP 的優缺點

RIP 的最大優點是設定及部署極為簡單。RIP 的最大缺點是不能應用於大型或超大型的網路。RIP 路由器所使用的最大躍點數是 15。如果網路有 16 或以上的躍點則會無法連線。隨著網路的大小逐漸增長，每個

RIP 路由器所進行的定期宣告可能導致流量過高。RIP 的另一缺點是它的復原時間太長。當網路拓樸變更時，RIP 路由器可能需要幾分鐘才會重新設定成新的網路拓樸。儘管網路會自行重新設定，可能會形成導致資料遺失或無法投遞的路由迴圈。

3.5.4 OSPF(Open Shortest Path First)

OSPF 路由協議是一種典型的鏈路狀態（Link-state）的路由協議，一般用於同一個路由域內。在這裡，路由域是指一個自治系統(Autonomous System)，即 AS，它是指一組通過統一的路由政策或路由協議互相交換路由信息的網路。在這個 AS 中，所有的 OSPF 路由器都維護一個相同的描述這個 AS 結構的資料庫，該資料庫中存放的是路由域中相應鏈路的狀態信息，OSPF 路由器正是通過這個資料庫計算出其 OSPF 路由表的。

3.5.5 RIP 與 OSPF 的差別

OSPF 跟 RIP 最大的不同處在於說它不是兩個鄰近路由器之間彼此交換，而是對整體網路廣播，而路由器收集這些訊息建構 Routing Table。另一個不同處在於路由器以距離參數(Distance metric)取代單純的經過節點數，以連結狀況更新距離參數，然後用動態規劃(Dynamic Programming)的演算法算出最短路徑。

相關試題

1.在透過 IPX 協定作資料傳輸之前，需要先進行什麼動作？(A)

(A)取得 Netware Server 名稱，使用帳號登入

(B)作 DNS 查詢

(C)建立所有檔案的清單

(D)取得伺服器的 IP 位址

2.IPX 是由哪家公司所推出的網路協定？(B)

(A)Microsoft

(B)Novell

(C)IBM

(D)Cisco

3.IPX 協定與 IP 比較，哪些正確？(複選)(B C D)

(A)IPX 和 IP 一樣都可以全世界暢行無阻

(B)IPX 無法像 IP 一樣，連接全世界網路

(C)IPX 廣播封包，往往造成網路麥能低落

(D)IP 協定現今已經取代 IPC 成為 Novell 新版作業系統的預設標準協定

4.下列關於 IPX 的敘述何者錯誤？(D)

(A)每個介面可有多個 Data-Link Encapsulation

(B)每個介面可以有多個 Logical Network

(C)每個 Network 都需要一個單獨的 Encapsulation Type

(D)每個介面最多只能有一個 Logical Network

3-6 LAN/WAN Interfacing Equipment，Devices and Configuration

3.6.1 ATM （Asynchronous Transfer Mode）非同步傳輸模式

ATM 是一種網路通訊協定與技術，這是未來的寬頻網路的標準，是一項資訊互通的世界標準，並不屬於私人公司的技術。

如果要使得多媒體在網路上的傳送更有效率，可由像是多媒體的傳送即可經由多個 ATM 轉接點（Switches）交換技術來完成，這些多媒體服務項目包括隨意視訊、視訊會議與遠距教學、聲音與影像，要有這些結果則頻寬與處理速度的需求必須增強，未來的技術研究是要解決長途的傳送所產生的延遲。

在傳送資料時將資料切割成固定大小的封包（ 53 位元組的 CELLS）傳送到目的地，到達目的地以後，再重組成原來的資料，ATM 可以在同一條網路上同時傳輸資料時不會友任何一種資料格式會佔據頻寬而延遲其他資料格式的傳輸。 ATM 的層次相當於 ISO/OSI 的第一和第二層，系統使用的速率的範圍在 1.5Mbps 到 600Mbps 之間。

3.6.2 ATM 調節層(AAL)

雖然 ATM 層處理所有有關細胞的傳送、接收、及交換的工作，它並不知道這些細胞究竟是從哪一種資料轉換而來,例如是一般檔案資料或具有即時性的聲音、影像、視訊資料。這種作法可以使 ATM 層的工作單純化,提高處理的效率和速度,但也因此需要某一層通訊協定來提供能夠滿足各種應用軟體需求的服務。AAL 層就是這個負責提供各種不同的服務給上層應用軟體的通訊協定。目前在標準中制定的服務有四類，此四類服務分別稱為 AAL1，AAL2，AAL3/4，及 AAL5。

3.6.3 AAL 的四種不同服務

1.AAL1

採接續型連接模式、傳輸速率固定、一般用來傳送語音、視訊等即時性資料。

2.AAL2

採接續型連接模式、傳輸速率為變動、使用變動速率傳送即時性資料，如影像電話。

3.AAL3/4

採接續型連接模式、傳輸速率為變動、不需傳送即時性資料。

5.AAL5

資料格式較簡單、沒有防止訊胞遺失的機制、表頭資訊中包含了一個位

元說明此訊胞是否為最後一個 ATM 訊胞 。

相關試題

1.AAL 的 A 類服務(class A service)主要是提供何種類型的通信：(A)

(A)固定位元率(bit rate)

(B)可變位元率

(C)連結導向(connected-oriented)資料傳輸

(D)非連結式導資料傳輸

2.下列關於資料傳輸單元的敘述，何者正確？(A)

(A)ATM 具備固定長度的單元，長度為 53Bytes

(B)Ethernet 封包有固定的長度，為 1500Bytes

(C)ATM 不具備固定長度的單元，最大長度為 64 Bytes

(D)Ethernet 封包具備有不固定長度，通常最大為 512 Bytes

3.下列哪一種 WAN 技術最具有同時傳輸即時語音、影像與資料服務的能力，並提供良好的 Qos 機制？(B)

(A)Dial-Up

(B)ATM

(C)Frame RELAY

(D)X.25

第四章 「網際網路服務與應用」

4-1 Introduction to System Development and Operation

4.1.1 TANET

台灣學術網路 (Taiwan Academic Network，TANet)

TANet 為台灣學術網路的英文縮寫，全名為 Taiwan Academic Network。成立於 1990 年 7 月，初期連接台灣部份的學術單位與研究機構，為全台灣第一個網際網路系統，初期骨幹頻寬為 9.6kbps。1991 年 12 月以 64Kbps 數據專線，連接美國普林斯頓大學的 JvNCnet，成為台灣的第一條跨國電路。1994 年年初，以 T1 連接架設中的 Hinet，成為台灣第一條 peering，台灣的網際網路正式進入跨網時代。同年 6 月以 10Mbps 的乙太網路連接 SEEDNet，台灣開始了多網系統的網網相連。

4.1.2 ASP 動態伺服器網頁 (Active Server Pages)

由微軟公司開發的伺服器端運行的指令碼平台，它被 Windows 下的 Internet Information Services (IIS)程式所管理。透過 ActiveX server 的技術讓不同的使用者能有不同的畫面，或需要讓他們可以存取伺服器 (server)上的資料時，使用 ASP3.0 中提供了五個內建的物件建立模擬和安全性的動態內容，來協助程式設計師隱藏複雜的溝通機

制，讓程式設計師可以專注在解決問題和應用之上。

4.1.3 CSS 串接樣式表(Cascading Style Sheets)

它是由許多樣式名稱和樣式指定值所組成的字串，我們可以利用設定好的樣式表，指定給某一種 HTML 標籤，或某一群組 HTML 標籤來使用。而被套用的 HTML 標籤，將會依據所套用的 CSS 來顯式它的外觀。

CSS 可說是 JavaScript 物件模型的一個重要部份，因為在 CSS 設定之後，我們還可以利用 JavaScript 重新指定不同的值給元件，而達成動態改變的效果（JavaScript 動態改變的功能 IE 已完全支援，但 NC 只支援極少部份）。

相關試題

1.(A) 下列何種網路系統，禁止商業用途?

(A)TANet

(B)HiNet

(C)SeedNet

(D)TISNet

2.(C) 關於 ASP（Active Server Pages）的描述何者錯誤?

(A)ASP 是微軟的技術

(B)ASP 是在伺服器端提供動態網頁設計的功能

(C)ASP 只能使用 VBScript 撰寫

(D)Microsoft 的 IIS(Internet Information Services)支援 ASP

3.(AC) 關於 CSS(Cascading Style Sheets)的描述哪些有誤? 複選

(A)CSS 可以配合 HTML 文件使用，但不能配合 XML 文件使用

(B)CSS 可以控制文字的字體和顏色

(C)CSS 可以控制視窗的位置

(D)CSS 可以控制網頁上物件的位置

4.(C) 以下文件類型與使用者的對應何者為非?

(A)管理者手冊→系統管理者

(B)安裝說明→系統管理者

(C)參考手冊→系統分析師

(D)簡介手冊→初學者

5.(B) 以下何者定義了測試過程的相關文件?

(A)IEEE1394

(B)IEEE829

(C)ISO14642

(D)IEEE802.11

4-2 Internet Services(Web、FTP、Mail、DNS and News Server, DHCP)

4.2.1 Web 全球資訊網(Web)

是一個資料空間。在這個空間中：一樣有用的事物，稱為「資源」並且由一個全域「統一資源標識符」(URI)標識。這些資源通過超文本傳輸協議(Hypertext Transfer Protocol)傳送給使用者，而後者通過點擊連結來獲得資源。從另一個觀點來看，全球資訊網是一個透過網路存取的互連超文件(interlinked hypertext document)系統。

4.2.2 FTP 文件傳輸協議 (File Transfer Protocol)

是用在網路上進行文件傳輸的一套標準協議。FTP 是一個 8 位的客戶端-伺服器協議，能操做任何類型的文件而不需要進一步的處理，但是 FTP 有著極高的延時，這意味著，從開始請求到第一次接收需求數據之間的時間，會非常長，並且不時需要進行一些冗長的登陸進程。

4.2.3 (Mail)

SMTP(Simple Mail Transfer Protocol 簡易郵件傳輸協定)，由於網路的興起所以 SMTP 便成了網際網路上的重要傳輸協定。

4.2.4 DNS 網域名稱系統（Domain Name System）

網際網路的一項核心服務，它作為可以將域名和 IP 地址相互映射的一個分散式資料庫，能夠使人更方便的訪問網際網路，而不用去記住能夠被機器直接讀取的 IP 數串。

4.2.5 新聞群組(News Servers)

新聞群組是最先開始受大眾喜歡的網路群組。我們可以在特定主題上交換訊息，所以新聞群組讓每一個群組容易溝通。目前管理新聞群組要管理上游、中游、下游的新聞群組互相傳送信件，以及發送新聞郵件，算是比較有技術性的工作。

4.2.6 DHCP

動態主機設定協定（Dynamic Host Configuration Protocol, DHCP）是一個區域網的網路協議，使用 UDP 協議工作，主要的用途有兩類:給內部相連網站或網路服務供應商自動分配 IP 地址給用戶使用。

給內部相連網站的管理員作為對所有電腦做中央管理的程式。

相關試題

1.(C)在一個較大的可路由網路上，我們使用子網路來分割網段。而為了使所有子網段上的電腦均可以透過一部位於某一子網路上之 DHCP 伺服器來自動取的 IP 位址，我們必須在路由器或其他子網段上的其中一

台電腦啟動何種功能?

(A)DHCP Cilent

(B)DHCP Server

(C)DHCP relay agent

(D)DHCP relay server

2.(C)在 DNS 的資源紀錄中,主機別名可以使用下面哪種紀錄型態建立?

(A)A

(B)PTR

(C)CNAME

(D)RR

3.(C)下列對 DHCP 說明何者錯誤?

(A)DHCP 是 Dynamic Host Configuration Protocol 之縮寫

(B)它的前身是 BOOTP

(C)它只提供一種 IP 定位方式:動態分配

(D)BOOTP 有一個缺點:客戶端的硬體位址與 IP 的對應是靜態的

4.(C)當一個 DHCP 使用者剛加入時應向下列哪一個網址發出它的 DHCP discovery message:

(A)DHCP server IP address

(B)DNS server IP address

(C)255.255.255.255

(D)Mail server IP address

5.(B)外寄郵件伺服器採用何種傳輸協定?

(A)POP3

(B)SMTP

(C)IMAP

(D)SNMP

6.(CD)對於簡易檔案傳輸協定(TFTP)的敘述，以下哪些選項是正確的?(複選)

(A)TFTP 使用的通訊協定是 TCP

(B)TFTP 可以透過瀏覽器程式執行

(C)TFTP 沒有認證的功能，使用者不用輸入登入名稱與密碼

(D)TFTP 可以用於沒有硬碟硬體設備開機啟動

7.(A)目前在世界上最大的網路新聞(News)系統是什麼?

(A)USENET

(B)UUNET

(C)NSNET

(D)WORLDNET

8.(BC)以下有關 DND 解析的敘述有哪些錯誤? 複選

(A)DNS 正解是指由機器名稱對應至 IP 位址

(B)DNS 正解是指由 IP 位址對應至網域名稱

(C)反解網域是以網域名稱為節點標籤

(D)網域名稱空間以網域名稱為節點標籤

9.(AC)下列哪些工具可用於 DNS 名稱解析除錯之用?(複選)

(A)Nslookup

(B)Telnet

(C)Dig

(D)traceroute

10.(D)以下何者不是 DHCP 訊息?

(A)DHCPDISCOVER

(B)DHCPOFFER

(C)DHCPREQUEST

(D)DHCPDROP

4-3 Internet Caching Technology

4.3.1 Cache

快取(Cache 或稱為高速緩存)，其原始意義是指存取速度比一般隨機存取記憶體(RAM)來得快的一種 RAM，一般而言它不像系統

主記憶體那樣使用 DRAM 技術，而是使用昂貴但快速的 SRAM 技術。

4.3.2 Proxy serve

代理伺服器（proxy server）設置的兩個主要目的：加強網路安全及提升網路使用效率。在加強網路安全方面，早期代理伺服器是作為內部網路與外部網路之間的一個通道,所有要連到外部的流量都須經過代理伺服器，因而可利用此特性，在代理伺服器加上管制的機制，進而加強內部網路安全。

4.3.3 Domain Name

域名(Domain Name) 是由一串用點分隔的名字組成的 Internet 上某一台計算機或計算機組的名稱，用於在數據傳輸時標識計算機的電子方位。

相關試題

1.(ABC)下列哪些為網路應用層快取(Cache)的好處?(複選)

(A)節省廣域網路頻寬，降低成本

(B)加快網路下載速度，增進使用者生產力

(C)整合網站過濾，加強安全存取管控

(D)加快交換器封包交換速度

2.(BC)下列哪些為企業常用的網路快取技術?(複選)

(A)High Speed Cache

(B)Transparent Cache

(C)Proxy Cache

(D)Local Cache

3.哪一類型的物件不應該被代理伺服器(proxy server)?

(A)圖片(gif，jpg 等)

(B)可攜式文件(PDF)

(C)網頁廣告

(D)身份識別資訊

4.(D)無法瀏覽奇摩網站與下面哪個事件無關?

(A)奇摩網站伺服器故障

(B)網路名稱伺服器(DNS)故障

(C)代理伺服器(Proxy)故障

(D)軟碟機故障

5.(CD)關於網路名稱伺服器(DNS)功能，以下哪些是錯的?(複選)

(A)將 IP 對應到 Domain Name

(B)將 Domain Name 對應到 IP

(C)儲存使用者認證資料

(D)阻擋不當資訊存取

4-4 Broadband Solution(ISDN、xDSL/CATV/…)

4.4.1 ADSL

非對稱數位用戶線路（ Asymmetric Digital Subscriber Line)是因為上行（從用戶到電信服務提供商方向，如上傳動作）和下行（從電信服務提供商到用戶的方向，如下載動作）頻寬不對稱因此稱為非對稱數位用戶線路。它採用分頻復用技術把普通的電話線分成了電話、上行和下行三個相對獨立的通道，從而避免了相互之間的干擾。

4.4.2 ISDN

整合服務數位網路（Integrated Services Digital Network）是一個數位電話網路國際標準，是一種典型的電路交換網路系統。它透過普通的銅纜以更高的速率和質量傳輸語音和數據。因為 ISDN 是全部數位化的電路，所以它能夠提供穩定的數據服務和連接速度，不像類比線路那樣對干擾比較明顯。在數位線路上更容易展開比類比線路業者更多的業務。例如除了基本的打電話功能之外，還能提供視訊、圖像、遠距教學與數據服務。ISDN 需要一條全數位化的網路用來承載數位信號（只有 0 和 1 這兩種狀態），與普通類比電話最大的區別就在這裡。

4.4.3 CATV

有線電視(CATV) 是一種使用同軸電纜作為介質直接傳送電視，調頻廣播節目到用戶電視的一種系統。同軸電纜有線電視。大體上分為三-四級： 首端寬頻放大器， 將信息放大，輸出到各幹線寬頻放大器。

幹線寬頻放大器，將來自首端寬頻放大器的訊號放大，輸往幹線電纜。

支線寬頻放大器，將來自幹線電纜的訊號放大，輸往分配電纜。

分配放大器，將來自分配電纜的訊號放大，通過訊號分配器輸往用戶。

各級寬頻放大器都必須對高頻和超高頻訊號有均勻的放大率,和很小的訊號交叉干擾。

4.4.4 Cable modem

纜線數據機（Cable Modem）是一種上下行帶寬不對稱的技術，適合提供上網及 VOD 這兩種業務。其中，提供互聯網接入業務可以採用“HFC＋Cable Modem＋以太網/ATM”的方式。局端需要配備一台 HFC 頭端設備，透過 ATM 或快速以太網與互聯網進行互聯，並且完成信號的調制和混合功能。數據信號透過光纖同軸混合網（HFC）傳至用戶家中，Cable Modem 完成信號的解碼、解調等功能，並透過以太網連接埠將數位信號傳送到 PC 機。反過來，Cable Modem 接收 PC 機傳來的上行信號，經過編碼、調制後透過 HFC 傳給頭端設備。

4.4.5 DSL

數位用戶迴路（Digital Subscriber Line），是通過銅線或者本地電話網提供數位連接的一種技術。它的歷史要追溯到 1988 年，貝爾實驗室一位工程師設計了一種方法可以讓數位信號載入到電話線路未使用頻段，這就實現了不影響話音服務的前提下在普通電話線上提供數據通信。但是貝爾的管理層對這個並不熱心, 因為如果用戶安裝兩條線路會帶來更多的利潤。這一狀況直到 1990 年代晚期有線電視公司開始推銷寬頻網際網路訪問時才得到改善。當意識到大多數用戶絕對會放棄安裝兩條電話線訪問網際網路，貝爾公司才搬出他們已經討論了 10 年的 DSL 技術，來爭奪有線電視網路公司的寬頻市場佔有率。

4.4.6 QAM

正交振幅調變（QAM，Quadrature Amplitude Modulation）是一種在兩個正交載波上進行振幅調變的調變方式。這兩個載波通常是相位差為 90 度（$\pi/2$）的正弦波，因此被稱作正交載波。這種調變方式因此而得名。同其它調變方式類似，QAM 通過載波某些參數的變化傳輸信息。在 QAM 中，數據訊號由相互正交的兩個載波的振幅變化表示。

4.4.7 WINS

動態的複寫資料庫服務(WINS，Windows Internet Name Service)，是

由 Microsoft 所發展出來的一種網路名稱轉換服務。它可以將 NetBIOS 電腦名稱轉換為對應的 IP 位址，可讓伺服器電腦能變成 NetBIOS 的名稱伺服器，並且在網路上登錄並解析 WINS 的用戶端電腦名稱，在 TCP/IP 上的 NetBIOS 標準協定中加以說明。

相關試題

1.(A)你的電腦可以在家裡經由電話線連接上 Internet，應用下列哪一種通訊協定?

(A)SLIP

(B)POP

(C)FTP

(D)HTTP

2.(B)計時制 ADSL 或 Cable modem 並無固定之實體 IP 位址可用，使用者若想在這種非固定實體 IP 上架設網路，供他人透過公網連線，則採用下列何種協定最為適合?

(A)DHP

(B)DDNS

(c)WINS

(D)NetBIOS

3.(A)Cable modem 下載訊號採用何種調變方式?

(A)QAM

(B)QPSK

(C)PSK

(D)OFDM

4.(B)ISDN 基本數率(Basic Rate)服務適合一般辦公室或個人住家，是由哪種頻道所組成的?

(A)2BRI+D

(B)2B+D

(C)23BRI+D

(D)23B+2D

5.(C)屬於銅質電話線傳輸的 DSL(Digital Subscriber Line)頻寬解決方案成員之一，卻因為有效傳輸速率只有幾百公尺，而需要搭配光纖電路的是以下哪一種 DSL?

(A)SDSL

(B)HDSL

(C)VDSL

(D)VoDSL

6.(AD)有線電視頻寬上網與 ADSL 比較，下列哪些選項是正確的?(複選)

(A)有線電視寬頻上網的資料安全性比較低

(B)ADSL 提供的網路傳輸速率比較快

(C)有線電視寬頻上網的速率是固定的

(D)電話系統通常比有線電視系統可靠

7.(AB)有關 ADSL 數位用戶迴路服務的特性，下列敘述哪些是正確的?(複選)

(A)電話公司提供的速率與提供服務的範圍成反比

(B)ADSL 中的”A”是指 Asymmetric 意思是上下行速路不一致

(C)住戶只要家中有裝電話線，即可以申請任何速率的 ADSL

(D)ADSL 通常上行速率比下行速率高

8.(D)下列有關各種 DSL 技術比較何者錯誤?

(A)HDSL 使用兩對雙絞線，而 SDSL 使用一條雙絞線

(B)SDSL 雙向傳輸可達 2M 以上，較 SDSL 傳輸速率高

(C)CDSL 傳輸速率較 SDSL 高，但有效傳輸距離較 SDSL 短

(D)VDSL 採用兩條雙絞線，因此容錯度及傳輸速率皆較高

4-5 Voice over IP

4.5.1 VoIP

網路電話(Voice over Internet Protocol) 是一種透過網際網路或其他使用 IP 技術的網路，來實現新型的電話通訊。過去 IP 電話主要應用

在大型公司的內聯網內，技術人員可以復用同一個網路提供數據及語音服務，除了簡化管理，更可提高生產力。隨著網際網路日漸普及，以及跨境通訊數量大幅飆升，IP 電話亦被應用在長途電話業務上。而 IP 電話也開始應用於固網通信，其低通話成本、低建設成本、易擴充性及日漸優良化的通話質量等主要特點，被目前國際電信企業看成是傳統電信業務的有力競爭者。

4.5.2 RTCP

實時傳輸控制協議（Real-time Transport Control Protocol）RTCP 為 RTP 媒體流提供通道外控制。RTCP 本身並不傳輸數據，但和 RTP 一起協作將多媒體數據打包和發送。RTCP 定期在流多媒體會話參加者之間傳輸控制數據。RTCP 的主要功能是為 RTP 所提供的服務質量(Quality of Service）提供反饋。RTCP 收集相關媒體連接的統計信息，例如：傳輸位元組數，傳輸分組數，丟失分組數，jitter，單向和雙向網路延遲等等。RTCP 本身不提供數據加密或身份認證

4.5.3 SIP

會話發起協議（Session Initiation Protocol）是一個由 IETF MMUSIC 工作組開發的協議，作為標準被提議用於建立，修改和終止包括視頻，語音，即時通信，在線遊戲和虛擬現實等多種多媒體元素在內的互動式

用戶會話。2000 年 11 月，SIP 被正式批准成為 3GPP 信號協議之一，並成為 IMS 體系結構的一個永久單元。SIP 與 H.323 一樣，是用於 VoIP 最主要的信令協議之一。

4.5.4 AES

高級加密標準（Advanced Encryption Standard）又稱 Rijndael 加密法，是美國聯邦政府採用的一種區塊加密標準。這個標準用來替代原先的 DES，已經被多方分析且廣為全世界所使用。經過五年的甄選流程，高級加密標準由美國國家標準與技術研究院 （NIST）於 2001 年 11 月 26 日發佈於 FIPS PUB 197，並在 2002 年 5 月 26 日成為有效的標準。2006 年，高級加密標準已然成為對稱密鑰加密中最流行的演算法之一。

4.5.5 DES

數據加密標準(Data Encryption Standard))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(FIPS)所選中，隨後既在國際上廣泛流傳開來。這個演算法因為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國家安全局(NSA)的後門而在開始是有爭議的，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 現在已經不視為一種安全的加密演算法，因為它使用的 56 位秘鑰過短，以現代計算能力，24 小時內即可能被破解。也有一些分

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（AES）所取代。

4.5.6 MD5

資訊-摘要演算法 5（Message-Digest Algorithm）用於確保資訊傳輸完整一致。是電腦廣泛使用的雜湊演算法之一，主流程式語言普遍已有MD5 實作。將資料運算為另一固定長度值是雜湊演算法的基礎原理，1992 年 8 月 Ronald L. Rivest 在向 IETF 提交了一份重要檔案，描述了這種演算法的原理，由於這種演算法的公開性和安全性，在 90 年代被廣泛使用在各種程式語言中，用以確保資料傳遞無誤等。MD5 由 MD4、MD3、MD2 改進而來，主要增強演算法複雜度和不可逆性。

4.5.7 ARQ

自動重傳請求（Automatic Repeat-reQuest）是 OSI 模型中數據鏈路層的錯誤糾正協議之一。它包括停止等待 ARQ 協議和連續 ARQ 協議。停止並等待協議的工作原理如下:發送點對接收點發送數據包,然後等待接收點回復 ACK 並且開始計時 在等待過程中,發送點停止發送新的數據包當數據包沒有成功被接收點接收時候,接收點不會發送 ACK 這樣發送點在等待一定時間後,重新發送數據包反覆以上步驟直到收到從接收點發送的 ACK。

相關試題

1.(B)在H.323網路電話系統中,Gatekeeper在收到何種請求(request)時會回應RCF(Registration Confirm)

(A)GRQ(Gatekeeper Request)

(B)RRQ(Registration Request)

(C)LRQ(Location Request)

(D)ARQ(Admission Request)

2.(ABD)下列哪些屬於SIP架構中的組成元件?(複選)

(A)Location Server

(B)Redirect Server

(C)Gatekeeper

(D)Proxy Server

3.(C)下列哪些因素對於VoIP通話品質影響最小?

(A)語音封包遺失

(B)語音封包傳輸延遲

(C)語音封包加密機制

(D)語音封包的傳遞路徑

4.(C)下列有關VoIP安全性的敘述何者正確?

(A)必須在傳輸層進行

(B)必須利用 RTP 進行

(C)必須在實體層及傳輸層進行

(D)在傳輸層或 RTP 進行皆可

5.(D)下列何者對 VoIP 優勢的敘述不正確?

(A)比較低的設備與操作成本

(B)可以整合語音與資料服務

(C)對於寬頻的要求會比較低

(D)聲音品質一定比較好

6.(A)下列哪一個加密防護機制最適合用來保護 VoIP 的語音資料封包?

(A)AES

(B)Blowfish

(C)DES

(D)MD5

7.(ABCD)下列哪些是 SIP 協定中的網路實體?(複選)

(A)呼叫者(call or client)與被呼叫者(callee or server)

(B)代理人伺服器(proxy server)

(C)重新導向伺服器(redirect server)

(D)註冊或位置伺服器(registrar or location server)

8.(D)下列何者不應該是現在 VoIP 服務會面臨的挑戰

(A)服務品質(QoS)

(B)NAT 與防火牆

(C)安全與防護(Security and Protection)

(D)來電顯示

4-6 QoS

4.6.1 QoS

服務質量(Quality of Service)指的是網路滿足給定業務合同的機率，或在許多情況下,非正式地用來指分組在網路中兩點間通過的機率。QoS 是一種控制機制,它提供了針對不同用戶或者不同數據流才用相應不同的優先順序，或者是根據應用程序的要求，保證數據流的性能達到一定的水準。QoS 的保證對於容量有限的網路來說是十分重要的，特別是對於串流多媒體應用，例如 VoIP 和 IPTV 等，因為這些應用常常需要固定的傳輸率，對延時也比較敏感。

4.6.2 SNMP

簡單網路管理協議（Simple Network Management Protocol）構成了互聯網工程工作小組（IETF，Internet Engineering Task Force）定義的 internet 協議簇的一部分。該協議能夠支持網路管理系統，用以監測連接到網路上的設備是否有任何引起管理上關注的情況。它由一組網

路管理的標準組成，包含一個應用層協議(application layer protocol)、資料庫模型（database schema)，和一組資料物件。

4.6.3 FIFO

先進先出（First In, First Out）先進先出法在計算機語言領域裡面是一種排程演算法。它描述了一個佇列所使用的先到先得服務方式：先進入佇列的工作將先被完成，之後進來的則必須稍候。

4.6.4 CBR

固定位元速率（英文 constant bit rate，縮寫 CBR）這是一個用來形容通信服務質量的術語。

當形容編解碼器的時候，CBR 編碼指的是編碼器的輸出碼率（或者解碼器的輸入碼率）應該是固定製。當在一個頻寬受限的通道中進行多媒體通訊的時候 CBR 是非常有用的，因為這時候受限的是最高碼率，CBR 可以更好的易用這樣的通道。但是 CBR 不適合進行存儲，因為 CBR 將導致沒有足夠的碼率對複雜的內容部分進行編碼，同時在簡單的內容部分會浪費一些碼率。

相關試題

1.(D)下列哪一項不是 ATM service class 其中一之?

(A)CBR

(B)ABR

(C)UBR

(D)BBR

2.(A)SNMP 協定主要之通信形式為?

(A)查詢-回應(query-response)

(B)自動為應

(C)叉斷

(D)陷阱(trap)

3.(D)下列何者可以限制資料流量的最高速率?

(A)選擇式回應(SACK)

(B)先進先出(FIFO)

(C)二元搜尋(Binary Search)

(D)漏水桶(Leaky Bucket)

4.(ABD)下列哪些屬於 QoS 的控制方法?(複選)

(A)許可控制(admission control)

(B)封包分類與排程(classification and scheduling)

(C)存取認證(access authentication)

(D)監測與管制(monitoring and poliing)

5.(A)客戶與網路服務供應商(ISP)可以就服務品質簽訂協議書，一般稱

做?

(A)服務等級協議(Service Level Agreement)

(B)服務保證協議(Service Guarantee Agreement)

(C)品質保證協議(Quality Guarantee Agreement)

(D)應用等級協議(Application Level Agreement)

第五章 網路安全與管理

5.1 Introduction to Network Secruity and Standardization

5.1.1 RFC

Request For Comments (RFC)，是一系列以編號排定的文件。文件收集了有關網際網路相關資訊，以及 UNIX 和網際網路社群的軟體文件。目前 RFC 文件是由 Internet Society（ISOC）所贊助發行。

基本的網際網路通訊協定都有在 RFC 文件內詳細說明。RFC 文件還額外加入許多的論題在標準內，例如對於網際網路新開發的協定及發展中所有的記錄。因此幾乎所有的網際網路標準都有收錄在 RFC 文件之中。

5.1.2 IPsec

IPsec 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。目前為止，IKE協議是唯一已經制定的密鑰交換協議。

5.1.3 DDOS

分散式阻斷服務攻擊，亦作分散式拒絕服務攻擊或洪水攻擊，通常簡稱為DDoS，即英語「Distributed Denial of Service」的縮寫。顧名思義，即是利用網路上已被攻陷的電腦作為「喪屍」，向某一特定的目標電腦發動密集式的「拒絕服務」要求，藉以把目標電腦的網路資源及系統資源耗盡，使之無法向真正正常請求的用戶提供服務。駭客通過將一個個「喪屍」或者稱為「肉雞」組成殭屍網路（即Botnet），就可以發動大規模DDOS或SYN洪水網路攻擊，或者將「喪屍」們組到一起進行帶有利益的刷網站流量、Email垃圾郵件群發，癱瘓預定目標受雇攻擊競爭對手等商業活動。

攻擊方式

DDoS攻擊通過大量合法的請求佔用大量網路資源，以達到癱瘓網路的目的。 這種攻擊方式可分為以下幾種：

1.通過使網路過載來干擾甚至阻斷正常的網路通訊。

2.通過向伺服器提交大量請求，使伺服器超負荷。

3.阻斷某一用戶訪問伺服器

4.阻斷某服務與特定系統或個人的通訊

SYN flood

SYN flood 是一種駭客通過向服務端發送虛假的包以欺騙伺服器的做法。具體說，就是將包中的原 IP 地址設置為不存在或不合法的值。伺服器一旦接受到該包便會返回接受請求包,但實際上這個包永遠返回不到來源處的計算機。這種做法使伺服器必需開啟自己的監聽埠不斷等待，也就浪費了系統各方面的資源。

LAND attack

這種攻擊方式與 SYN floods 類似，不過在 LAND attack 攻擊包中的原地址和目標地址都是攻擊對象的 IP。這種攻擊會導致被攻擊的機器無窮迴圈，最終耗盡資源而死機。

ICMP floods

ICMP floods 是通過向未良好設置的路由器發送廣播信息佔用系統資源的做法。

Application level floods

與前面敘說的攻擊方式不同，Application level floods 主要是針對應用軟體層的，也就是高於 OSI 的。它同樣是以大量消耗系統資源為目的,通過向 IIS 這樣的網路服務程序提出無節制的資源申請來迫害正常

的網路服務。

相關試題

1.DDOS 的攻擊模式有哪些特性?(AB)

(A)攻擊具有放大的效果

(B)為階層式的攻擊

(C)受害主機的封包被竊聽

(D)受害主機被入侵

2.IPSec 通訊協定由哪兩種協定所組成?(BD)

(A)IP

(B)AH

(C)SSL

(D)ESP

3.DNS 設定中用來標示郵件寄送順序的紀錄是?(D)

(A)NS

(B)PTR

(C)NXT

(D)MX

5.2 Network Security Threats and Related laws

5.2.1 IDS

入侵檢測系統（Intrusion-detection system，下稱「IDS」）是一種對網路傳輸進行即時監視，在發現可疑傳輸時發出警報或者採取主動反應措施的網路安全設備。它與其他網路安全設備的不同之處便在於，IDS 是一種積極主動的安全防護技術。IDS 最早出現在 1980 年 4 月。該年，James P. Anderson 為美國空軍做了一份題為《Computer Security Threat Monitoring and Surveillance》的技術報告，在其中他提出了 IDS 的概念。1980 年代中期，IDS 逐漸發展成為入侵檢測專家系統（IDES）。1990 年，IDS 分化為基於網路的 IDS 和基於主機的 IDS。後又出現分散式 IDS。目前，IDS 發展迅速，已有人宣稱 IDS 可以完全

5.2.2 SSL

TLS 利用密鑰演算法在網際網路上提供端點身份認證與通訊保密，其基礎是公鑰基礎設施（PKI）。不過在實現的典型例子中，只有網路服務者被可靠身份驗證，而其客戶端則不一定。這是因為公鑰基礎設施普遍商業運營，電子簽名證書要花大錢購買，普通大眾很難買的起證書。協議的設計在某種程度上能夠使客戶端/伺服器應用程序通訊本身預防竊聽、干擾（Tampering）、和消息偽造。

TLS 包含三個基本階段：

1.對等協商支援的密鑰演算法

2.基於公鑰加密交換公鑰、基於 PKI 證書的身份認證

3.基於私鑰加密的數據傳輸保密

在第一階段，客戶端與伺服器協商所用密碼演算法。 當前廣泛實現的演算法選擇如下：

公鑰保密系統：RSA、Diffie-Hellman、DSA 及 Fortezza；

私鑰保密系統：RC2、RC4、IDEA、DES、Triple DES 及 AES；

單向散列函數：MD5 及 SHA。

5.2.3 SKYPE

Skype，是支援語音通訊的即時通訊軟體，由 KaZaA 開發人員所研發，採用 P2P（點對點技術）的技術與其他用戶連接，可以進行高清晰語音聊天，連線雙方網路順暢時，音質可能超過普通電話。

Skype 軟體會在電腦上開啟一個網路連線埠來監聽其他 Skype 用戶的連線呼叫;當其他電腦能順利連線到這部電腦,Skype 稱呼該用戶為 Super node！Super Node 在該 P2P 環境中的腳色，即為提供其他無法被連線的用戶的之間的中繼站，借用諸多 Super Nodes 的些許網路頻寬，協助其他的 Skype 使用者之間能夠順利的互相聯繫。這種行為，在 P2P 環境中，這算是相當常見的手法，也是點對點連線的精髓之一。Skype 是第

一個將此種做法運用到網路語音通話與即時訊息應用層面上。

5.2.4 ITIL

ITIL 是用來管理信息技術（IT）的架構設計，研發和操作的一整套概念和思想 TIL 最初是藉由一套書籍發布。這套書籍的每一本都涵蓋一個信息技術的領域. ITIL 這個名稱和 IT Infrastructure Library 都是英國政府商務辦公室 (OGC)的註冊商標. 藉由為不同的 IT 組織量身定製一些複雜的清單，任務，流程，ITIL 為許多重要的 IT 時間準則給出了詳盡的解釋。

相關試題

1.DOS 的攻擊中下列哪些正確?(AB)

(A)消耗 Server 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

2.程式具有自行複製繁殖能力、破壞資料檔案、干擾 PC 系統的運作稱為?(D)

(A)電腦複製程式

(B)電腦遊戲

(C)電腦程式設計

(D)電腦病毒

3.預防電腦犯罪最應作之事項?(A)

(A)建立資訊安全管制系統

(B)資料備份

(C)維修電腦

(D)和警局連線

5.3. System Security Concepts

5.3.1 IPV4

IPv4，是網際網路協議（Internet Protocol，IP）的第四版，也是第一個被廣泛使用，構成現今網際網路技術的基石的協議。1981 年 Jon Postel 在 RFC791 中定義了 IP。

IPv4 可以運行在各種各樣的底層網路上，比如端對端的串列數據鏈路(PPP 協議和 SLIP 協議），衛星鏈路等等。區域網中最常用的是乙太網。一個用於 IP 包的乙太網數據幀，在 IP 包首部前有一個 14 位元組的乙太網幀首部，在 IP 數據部分後添加了一個 32 位(4 位元組）的 CRC 校驗。

除了 1518 位元組的最大傳輸單元(MTU）限制外，乙太網還有最小傳輸

單元的限制: 總幀長不能小於 64 位元組。如果 IP 包太短，比如 IP 數據部分短於 26 位元組，那麼後面會添 0(Padding) ，這時 IP 首部中的'包長度'指示了真正的包長。

乙太網使用 48 位的地址。每個乙太網網卡都有一個獨一無二的 48 位的硬體地址。所有的位均為 1 的地址是乙太網廣播地址。發送數據的乙太網網卡必須知道數據接送方的乙太網地址才能把數據發給它。

地址解析協議 ARP(Address Resolution Protocol) 用於將 IP 地址轉換成乙太網地址。每台計算機上都有一個 ARP 列表，裡面存儲了乙太網中不同的 IP 地址與乙太網地址的對應關係。如果一台計算機發現某個目標 IP 地址沒有對應的乙太網地址，它會發一個 ARP 請求(Request) 到乙太網中詢問，擁有該 IP 地址的計算機就會發一個 ARP 應答(Reply) 來通知它自己的乙太網地址。

5.3.2 IPV6

IPv6 是網際網路協議的第六版；最初它在 IETF 的 IPng 選取過程中勝出時稱為網際網路下一代網際協議（IPng)，IPv6 是被正式廣泛使用的第二版網際網路協議。

現有標準 IPv4 只支持大概 40 億（232）個網路地址，而 IPv6 支持 2128（約 3.4 ×1038）個，這等價于在地球上每平方英寸有 4.3×1020 地址（6.7×1017 地址/mm2)。(IPv5 不是 IPv4 的繼承，而是實驗性的面向流

的數據流協議，用來對聲音，圖像等提供支持。）

5.3.3 WEP

有線等效加密（Wired Equivalent Privacy），又稱無線加密協議（Wireless Encryption Protocol），簡稱 WEP，是個保護無線網路（Wi-Fi）資料安全的體制。因為無線網路是用無線電把訊息傳播出去，它特別容易被竊聽。WEP 的設計是要提供和傳統有線的區域網路相當的機密性，而依此命名的。不過密碼分析學家已經找出 WEP 好幾個弱點，因此在 2003 年被 Wi-Fi Protected Access（WPA）淘汰，又在 2004 年由完整的 IEEE 802.11i 標準（又稱為 WPA2）所取代。WEP 雖然有些弱點，但也足以嚇阻非專業人士的窺探了。

相關試題

1.以下何者不是 TCP/IP 的特點?(A)

(A)網路不會遭受攻擊

(B)網路的種類無關

(C)容錯力高

(D)資料格外負擔小

2.在 Windows XP 中，要查詢本基電腦在網路上的 TCP/IP 組態設定值，應使用哪一個指令?(A)

(A)Ipconfig

(B)Ping

(C)Traceroute

(D)telnet

5-4 System Security Conepts(Access Control)

5.4.1 EAP

擴展認證協議(EAP),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,而且可以用於有線區域網,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 作為正式的認證機制。 EAP 是一個認證框架,不是一個特殊的認證機制。EAP 提供一些公共的功能,並且允許協商所希望的認證機制。現代的 EAP 方法可以提供一個安全認證機制,並且在用戶和網路接入伺服器之間協商一個安全的 PMK。該 PMK 可以用於使用 TKIP 和 AES 加密的無線會話。

5.4.2 IEEE 802.1X

IEEE 802.1X 是 IEEE 制定關於用戶接入網路的認證標準,它的全稱是「基於埠的網路接入控制」。於 2001 年標準化,之後為了配合無線網路的接入進行修訂改版,於 2004 年完成。

IEEE 802.1X 協議在用戶接入網路(可以是乙太網/802.3 或者 WLAN 網)

之前運行，運行於網路中的數據鏈路層。EAP 協議 RADIUS 協議。

5.4.3 NTP

網路時間協議（Network Time Protocol，NTP）是以封包交換把兩台電腦的時鐘同步化的網路協議。NTP 使用 UDP 埠 123 作為傳輸層。它是用作抵銷可變延遲的影響。NTP 是其中一個最舊的網路協議仍在被使用，NTP 最初由德拉瓦州大學的 Dave Mills 設計，他與一群志願者仍在維護 NTP。

相關試題

1.(C)下列何者 eap 機制，使用者端(client)一定要安裝憑證(x.509)?

(A)EAP-MD5

(B)EAP-TTLS

(C)EAP-TLS

(D)EAP-PEAP

2.(C)802.1x 使用下列何種協定?

(A)SCP

(B)HTTP

(C)EAP

(D)RTP

3.(A)當存取某些特定伺服器(如 FTP Server)時，常會利用反查功能

來確定存取具有合法的 ip 地址，請問此反查功能是利用下列服務所提供?

(A)DNS

(B)POP3

(C)SMTP

(D)NTP

4.(AB)封包式過濾技術(packet filtering)是基於哪些資訊來過濾?(複選)

(A)協定種類

(B)連線阜號(port)

(C)供應商

(D)資料內容

5.(D)DdoS 攻擊破壞了網路安全的哪項特性?

(A)CRC

(B)ABC

(C)ISO

(D)OSI

5-5 Communication Eneryption and Authentiction Concepts

5.5.1 IDS

侵檢測系統（Intrusion-detection system，下稱「IDS」）是一種對網路傳輸進行即時監視，在發現可疑傳輸時發出警報或者採取主動反應措施的網路安全設備。它與其他網路安全設備的不同之處便在於，IDS 是一種積極主動的安全防護技術。IDS 最早出現在 1980 年 4 月。該年，James P. Anderson 為美國空軍做了一份題為《Computer Security Threat Monitoring and Surveillance》的技術報告，在其中他提出了 IDS 的概念。1980 年代中期，IDS 逐漸發展成為入侵檢測專家系統（IDES)。1990 年，IDS 分化為基於網路的 IDS 和基於主機的 IDS。後又出現分散式 IDS。目前，IDS 發展迅速，已有人宣稱 IDS 可以完全取代防火牆。

5.5.2 OFDM

正交分頻多工（Orthogonal frequency-division multiplexing）有時又稱為分離複頻變調技術（discrete multitone modulation，DMT)正交分頻多工技術可以視為多載波傳輸的一個特例，具備高速率資料傳輸的能力，加上能有效對抗頻率選擇性衰減通道，而逐漸獲得重視與採用。

OFDM 優點:

1.有效減少多路徑(multipath)及頻率選擇性通道造成接收端錯誤率上升的影響

2.接收端可利用簡單的 one-tap equalization 補償通道傳輸的失真

3.頻寬使用效率上升

OFDM 缺點:

1.傳送與接收端需要精確的同步

2.對於都普勒效應頻率飄移的敏感

3.峰值對平均功率(PAPR)的比例高

5.5.3 TDM

分時多工（TDM）是一種數字或者模擬的多路復用技術。使用這種技術，兩個以上的信號或數據流可以同時在一條通信線路上傳輸，其表現為同一通信通道的子通道。但在物理上來看，信號還是輪流佔用物理通道的。時間域被分成周期循環的一些小段，每段時間長度是固定的，每個時段用來傳輸一個子通道。例如子通道 1 的採樣，可能是位元組或者是數據塊，使用時間段 1，子通道 2 使用時間段 2，等等。一個 TDM 的幀包含了一個子通道的一個時間段，當最後一個子通道傳輸完畢，這樣的過程將會再重複來傳輸新的幀，也就是下個信號片段。

5.5.4 Hash Function

雜湊函數(Hash Function) 是一種從任何一種資料中建立小的數字「指紋」的方法。該函數將資料打亂混合，重新建立一個叫做雜湊值的指紋。雜湊值通常用來代表一個短的隨機字母和數字組成的字串。好的雜湊函數在輸入域中很少出現雜湊衝突。在雜湊表和資料處理中，不抑制衝突來區別資料，會使得資料庫記錄更難找到。

5.5.5 RSA

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。1973 年，在英國政府通訊總部工作的數學家在一個內部文件中提出了一個相應的演算法，但他的發現被列入機密，一直到 1997 年才被發表。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。1983 年麻省理工學院在美國為 RSA 演算法申請了專利。這個專利 2000 年 9 月 21 日失效。由於該演算法在申請專利前就已經被發表了，在世界上大多數其它地區這個專利權不被承認。

相關試題

1.(AD)下列哪些演算法可以達到資料一致性(Intergrity)?（複選）

(A)RSA

(B)AES

(C)DES

(D)MD5

2.(ABD)下列有關雜湊函數(Hash Function)特性的描述，哪些正確?

(A)雜湊函數是一單向的數學函數

(B) 雜湊函數是一單向的數學函數

(C)雜湊函數的輸出可以是任何長度的訊息摘要

(D)對於任何的輸入訊息，雜湊函數可以輕易的算出其相對應的訊息摘要

3.(B)802.11a 實體層使用何調變技術?

(A)Direct Sequence Spread Spectrum(DSSS)

(B)Orthogonal Frequency Division Multiplexing(OFDM)

(C)Frequency Hopping Spread Spectrum(FHSS)

(D)Time Division Multiplexing(TDM)

4.(B)解決非授權存取網路的最佳法為?

(A)防火牆

(B)使用者認證

(C)QoS

(D)IDS

5.(A)Triole DES 的加解密順序(E:表示加密，D:表示解密)，只有兩把 KEY:

(A)EDE

(B)DDE

(C)EED

(D)DED

5-6 Network Addres Translation(NAT)&Virtual Private Network(VPN)

5.6.1 PPP

點對點協議(Point-to-Point Protocal)，通常用在兩節點間建立直接的連接。它主要用於利用電話線來連接兩台計算機，現在也有用在寬頻(broadband)計算機連接上。很多網際網路服務提供商(ISP)使用 PPP 給用戶提供接入服務。PPP 作為數據鏈路層 layer 2 協議既支持用於同

步鏈路連接，也支持非同步鏈路連接。PPP 協議被設計成可以配合多種網路層協議工作，並被設計用於代替數據鏈路層的非標準協議 SLIP。PPP 協議是在原來的 HDLC 規範之後設計的。所以 PPP 協議的設計者把很多直到那時在廣域網數據鏈路層協議中都沒有考慮的額外的特性都包含進來了。

5.6.2 VPN

虛擬私人網路(Virtual Private Network)，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。

5.6.3 WiMAX

WiMAX （Worldwide Interoperability for Microwave Access），是一項基於標準的技術，主要用在城市型區域網路(MAN)。由 WiMAX 論壇（WiMAX Forum）提出並於 2001 年 6 月成形。它可提供最後一公里無線寬頻接入，作為電纜和 DSL 之外的選擇。它在 IEEE 802.16 標準的

多個版本和選項中做出唯一的選擇，以保證不同廠商產品的互操作性。在 802.16 物理層的三個變體中，WiMAX 選擇了 802.16-2004 版的 256 carrier OFDM[1]，能夠藉由較寬的頻帶以及較遠的傳輸距離，協助電信業者與 ISP 業者建置無線網路的最後一哩，與主要以短距離區域傳輸為目的之 IEEE 802.11 通訊協定有著相當大的同。WiMAX 能提供許多種應用服務，包括最後一哩無線寬頻接入、熱點（hotspot）、細胞式回程線路以及作為商業用途在企業間的高速連線。通過 WiMAX 一致性測試的產品都能夠對彼此建立無線連接並傳送網際網路封包數據。在概念上類似 WiFi，但 WiMAX 改善了性能，並允許使用更大傳送距離。

相關試題

1.(D)以下哪一項不是虛擬私有網路(VPN)必備的基本技術?

(A)穿隧技術(Tunneling)

(B)加解密技術(Encryption&Decryption)

(C)使用者與設備身份認證技術(Authentication)

(D)網路位址轉換(Network Address Translation)

2.(A)下列何者不是 VPN 技術?

(A)Proxy

(B)PPTP

(C)Ipsec

(D)SSLVPN

3.(A)NAT 環境一般都使用 private network address，請問 private network address 是定義在?

(A)RFC 1918

(B)RFC 2003

(C)RFC 2139

(D)RFC 2683

4.(D)下列何者是 Application VPN?

(A)ATM

(B)IPSec

(C)L2TP

(D)SSLVPN

5.(A)下列何者不是 VPN 技術?

(A)Proxy

(B)PPTP

(C)IPSec

(D)SSLVPN

6.(A)下列哪一種隧道協定能夠支援 IPX、NetBEUI 和 IP 協定的 VPN?

(A)PPTP

(B)L2LP

(C)L2F

(D)IPTP

7.(A)IPSec VPN 可支援何種通訊協定?

(A)IP

(B)IPC

(C)NETBEUI

(D)DECNET

8.(AB)IPSec VPN 可使用哪些 HASH 機制?(複選)

(A)MD5

(B)SHA1

(C)3DES

(D)AES

第六章　　結論

這次的專題本來是要做理論上的,但是聽到資訊科老師說可以用證照抵專題，大家紛紛討論要去考看看，可分為四大類別，區域網路、網際網路介面基礎、網際網路服務與應用、網路安全，區域網路主要是電腦系統及網路通訊的基本觀念、技術和原理，和區域網路的功能，網際網路介面基礎主要是網路協定特性及應用認知能力,網路服務與應用主要熟悉網路各種協定運作,網路安全主要時工程師在網路系統上各種安全管理方法。

第一版本的書雖然來的難一點，課本佔的比率只有 50%，只有幾個人考過…到了 97 年又換了一本課本，這次真的來的比較簡單，題目也變少了，不像之前的 100 多題的題庫，每個人都考的不錯，只要有看最少還可以考的不錯的成績，我們這組也在十二月前都考到証照了，希望這張證照對以後可以很多的用途才好呀。

參考文獻

http://www.tsshs.tpc.edu.tw/networking/chap4.htm

http://www.csie.ntu.edu.tw/~b6506066/Micro2/netbeui.htm

http://zh.wikipedia.org/wiki/%E5%B1%8F%E8%94%BD%E5%8F%8C%E7%BB%9E%E7%BA%BF

http://cai.cis.scu.edu.tw/C21/ch08/powerpoint/4_8-3.pdf

http://teacher.ksvs.kh.edu.tw/~t165/net.htm

http://zh.wikipedia.org/w/index.php?title=%E9%A6%96%E9%A1%B5&variant=zh-hant