一、NEXUS(連結)

- 「你知道嗎！你和總統之間只相隔六個握手寒喧的人」
- 1960年美國心理學家Stanley Milgram (米爾格蘭)，曾做過一個實驗，隨機在內布斯加州及堪薩斯州隨機選出一些人，寄信給它們，在信中麻煩她們把信轉寄給他在波斯嘲的朋友，但沒有給地址。為了轉這封信他請她們只能把信寄給她們認識的某個朋友，很令人訝異的是這些信並每有經過上百次的轉寄，而是至轉寄了大約六次
- 想想看為什麼病毒的傳播這麼快

二、網路要如何管理

- 組態管理
- 效能管理
- 障礙管理
- 安全管理

1.組態管理－I

校園網路IP分配表

名稱	骨幹對應IP	WAN1_IP	WAN2_IP	WAN3_IP
頻寬管理	192.168.0.254	61.220.100.210 61.220.100.211 61.220.100.212 61.220.100.213 61.220.100.214 61.220.100.215	211.78.105.32 211.78.105.33 211.78.105.34 211.78.105.35 211.78.105.36 211.78.105.37	163.22.154.9 163.22.154.10 163.22.154.11 163.22.154.12 163.22.154.13 ：
		Gateway	Gateway	Gateway
		61.220.100.209	211.78.105.31	163.22.154.254
名稱	骨幹對應IP	Gateway	起始IP	終止IP
backboard		192.168.0.254	192.168.0.1	192.168.0.253
名稱	骨幹對應IP	WAN1對應IP	WAN2對應IP	WAN3對應IP
DNS-(TANet)	192.168.0.1			163.22.154.1
DNS-(HiNet)	192.168.0.2	61.220.100.210		
WWW、Mail	192.168.0.3	61.220.100.211		163.22.154.2
WebMail	192.168.0.4	61.220.100.212		163.22.154.3
Library	192.168.0.5			163.22.154.4
VODServer(StreamingServer)	192.168.0.6			163.22.154.5
StudentSystem	192.168.0.7	61.220.100.213		163.22.154.6
NAS	192.168.0.8			163.22.154.9
Ups	192.168.0.20			163.22.154.10
3COM-4950-Switch-1	192.168.0.21			
Intel-無線電AP-1	192.168.0.22			

組態管理－II

SubNet IP 分配表

名稱	WAN		LAN			
	骨幹對應IP	Gateway	起始IP	終止IP	位置	Gateway
行政子網段	192.168.0.24	192.168.0.254	192.168.1.1	192.168.1.180		192.168.1.254
			192.168.1.190	192.168.1.250	dhcp	
教師子網段	192.168.0.24	192.168.0.254	192.168.2.1	192.168.2.180		192.168.2.254
			192.168.2.190	192.168.2.250	dhcp	
學生子網段	192.168.0.24	192.168.0.254	192.168.3.1	192.168.3.180		192.168.3.254
			192.168.3.190	192.168.3.250	dhcp	
電腦教室三	192.168.0.104	192.168.0.254	192.168.4.1	192.168.4.150		192.168.4.254
			192.168.4.151	192.168.4.200	dhcp	
電腦教室二	192.168.0.105	192.168.0.254	192.168.5.1	192.168.5.150		192.168.5.254
			192.168.5.151	192.168.5.200	dhcp	
電腦教室一	192.168.0.106	192.168.0.254	192.168.6.1	192.168.6.253		192.168.6.254
中興樓4樓控制室	192.168.0.107	192.168.0.254	192.168.7.1	192.168.7.253		192.168.7.254
VOD視訊子網段	192.168.0.24	192.168.0.254	192.168.8.1	192.168.8.200		192.168.8.254
圖書室	192.168.0.24	192.168.0.254	192.168.9.1	192.168.9.50		192.168.9.254
			192.168.9.60	192.168.9.100	dhcp	
校區無線電網路	192.168.0.24	192.168.0.254	192.168.10.1	192.168.10.99		192.168.10.254
			192.168.10.100	192.168.10.253	dhcp	

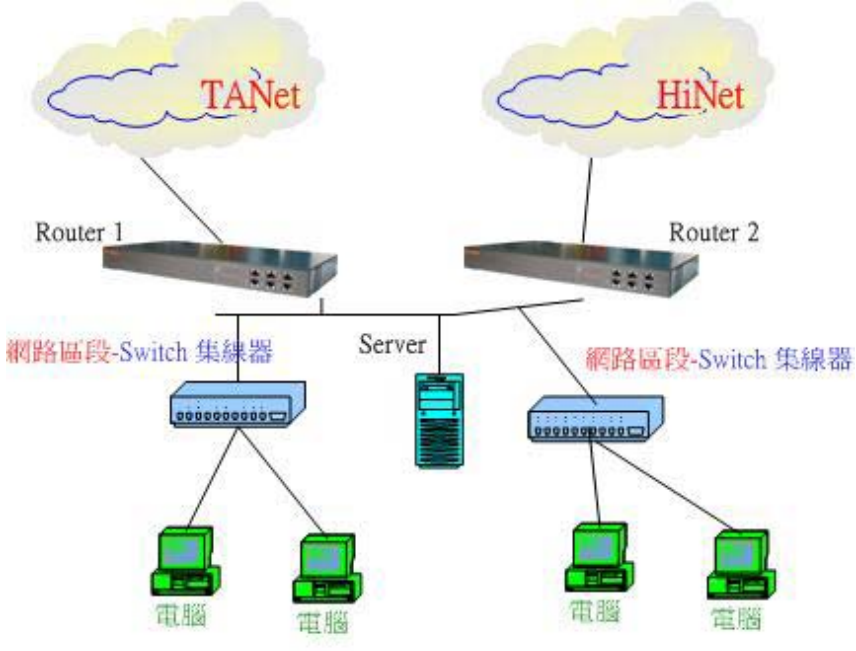
組態管理－III

校內電腦配置暨分布狀況

放置區域	CPU型號	RAM大小	配備	網卡1Mac Adress	IP分配	網卡2Mac Adress	IP分配	V-Lan No
教務處 1	486-DX4	64MB	1.2GHD	464653540600	192.168.1.1			1
教務處 3	P4-2.4G	256MB	Zip,DVD,40GHD	000c7ed50b8f	192.168.1.3			1
教務處 5	P4-2.4G	256MB	Zip,DVD,40GHD	000c7ee3ad34	192.168.1.5			1
訓導處 1	P4-2.4G	256MB	Zip,DVD,40GHD	000c7ed50b94	192.168.1.6			1
訓導處 4	P4-2.4G	256MB	Zip,DVD,40GHD	000c7ee3ac4a	192.168.1.9			1
健康中心	P4-2.4G	256MB	Zip,DVD,40GHD	000c7ee3ad2c	192.168.1.10			1
輔導室 2	P4-2.4G	256MB	Zip,DVD,40GHD	000c7ed50ab0	192.168.1.12			1
輔導室 4	P4-2.4G	256MB	Zip,DVD,40GHD	000c7ee3ad38	192.168.1.14			1
會計室 1	K6-300M	128MB	Zip,DVD,40GHD	000c7ee3acab	192.168.1.15			1
會計室 2	P4-2.4G	256MB	Zip,CD,4GHD	004007e66120	192.168.1.16			1
人事室 1	K6-300M	128MB	Zip,CD,4GHD	000c7ee3ad40	192.168.1.17			1
人事室 2	P4-2.4G	256MB	Zip,DVD,40GHD	0050ca04e4f1	192.168.1.18			1
校長室	P4-2.4G	256MB	Zip,DVD,40GHD	000cced50c41	192.168.1.19			1
總務處 1	P4-2.4G	256MB	Zip,DVD,40GHD	000c7ee3ace3	192.168.1.20			1
總務處 3	P4-2.4G	256MB	Zip,DVD,40GHD	000c7ed50b93	192.168.1.22	000d833bd821	192.168.1.25	1
總務處 5	P4-2.4G	256MB	Zip,DVD,40GHD	000d71051e3b	192.168.1.24	000d833bd820	192.168.1.26	1
導1 一樓	P4-2.4G	256MB	Zip,DVD,40GHD	000c7ee3ac32	192.168.2.1			2
導1 一樓	P4-2.4G	256MB	Zip,DVD,40GHD	000c7ed50b6a	192.168.2.2			2
導1 二樓	P4-2.4G	256MB	Zip,DVD,40GHD	000c7ee3ac5f	192.168.2.3			2
導1 二樓	P4-2.4G	256MB	Zip,DVD,40GHD	000c7ee3ac80	192.168.2.4			2
導1 三樓	P4-2.4G	256MB	Zip,DVD,40GHD	000c7ee3abe2	192.168.2.5			2
導1 三樓	P4-2.4G	256MB	Zip,DVD,40GHD	000c7ee3ad35	192.168.2.6			2
導2 一樓	P4-2.4G	256MB	Zip,DVD,40GHD	000c7ed50c6a	192.168.2.7			2

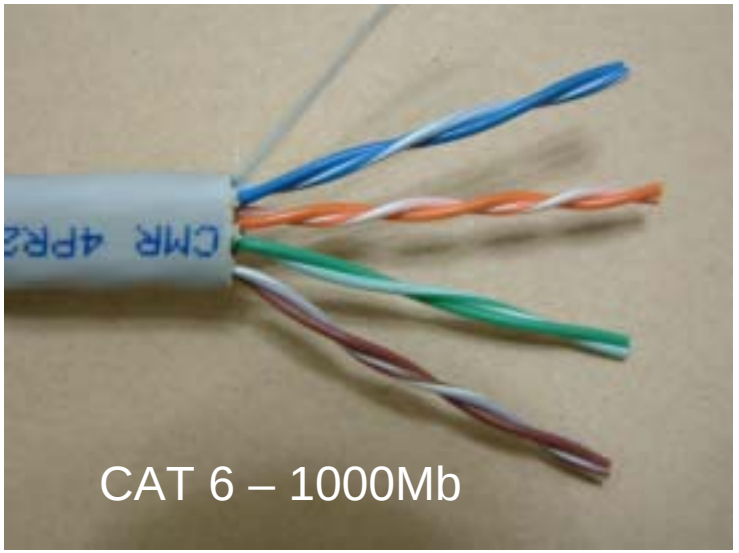
2.網路效能規劃(架構拓普)

簡單型

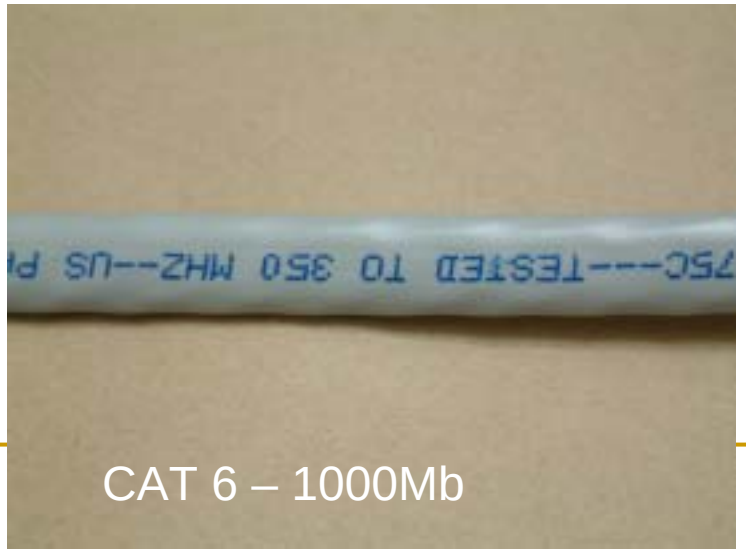


複雜型

網路效能規劃 — 硬體設備(線材)

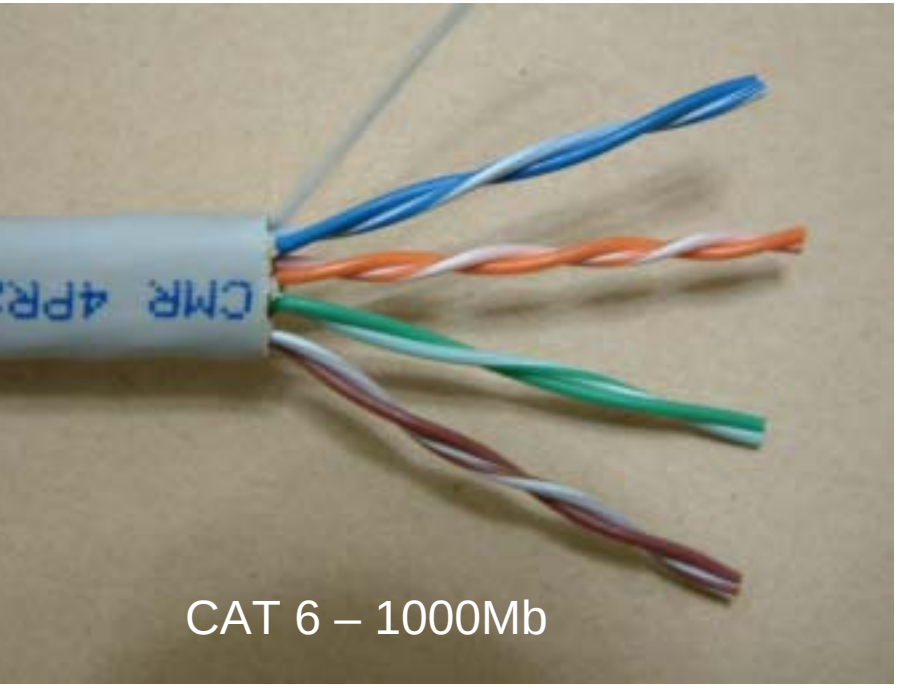

CAT 6 – 1000Mb

CAT 5e – 1000Mb

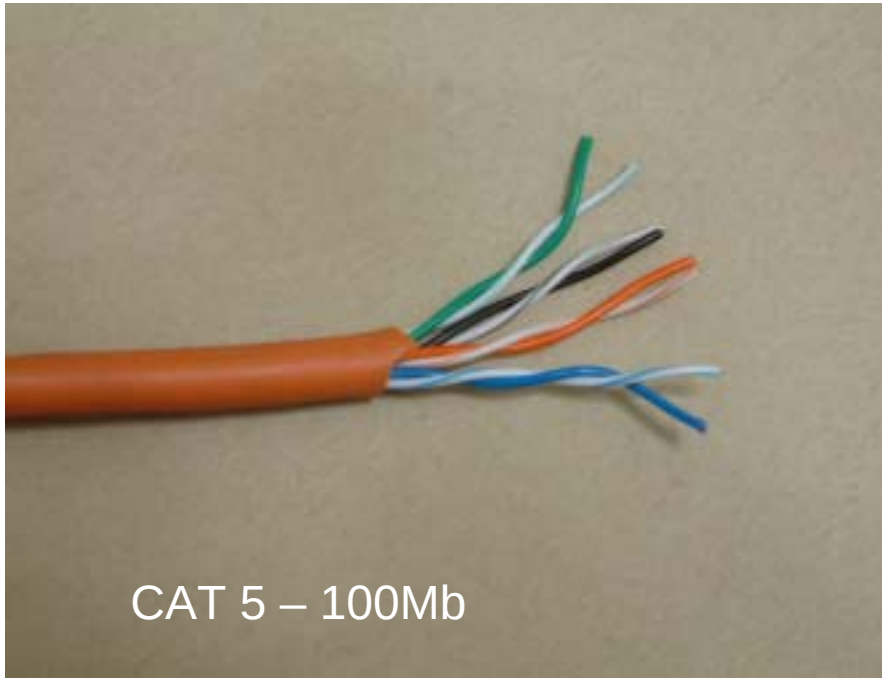

CAT 6 – 1000Mb

CAT 5 – 100Mb

網路效能規劃 — 硬體設備(線材)



CAT 6 – 1000Mb



CAT 5 – 100Mb

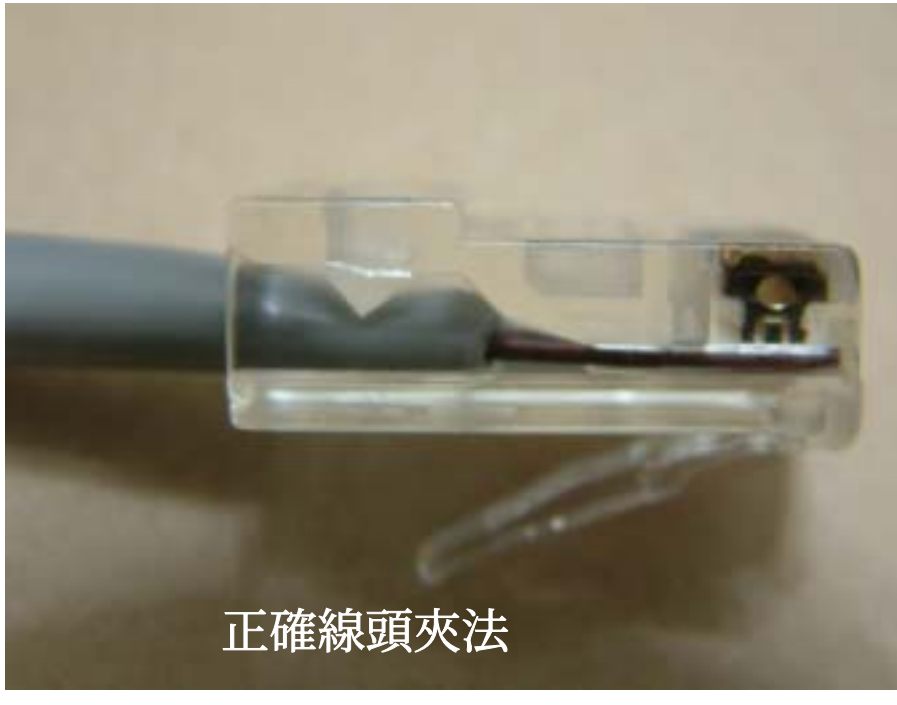
網路效能規劃 — 硬體設備(線材)

CAT 5 – 多股線

CAT 5 – 單心線

網路效能規劃 — 硬體設備(線材)

外包覆皮鬆脫

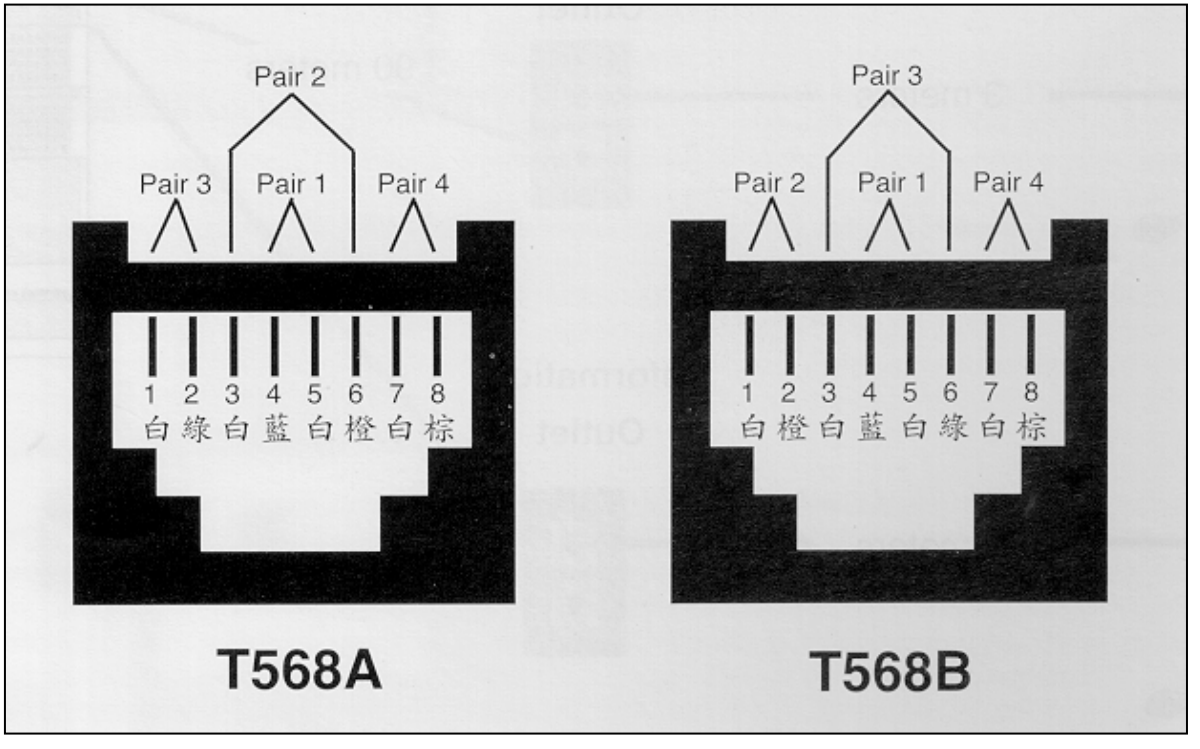


正確線頭夾法

網路效能規劃 — 硬體設備(線材)

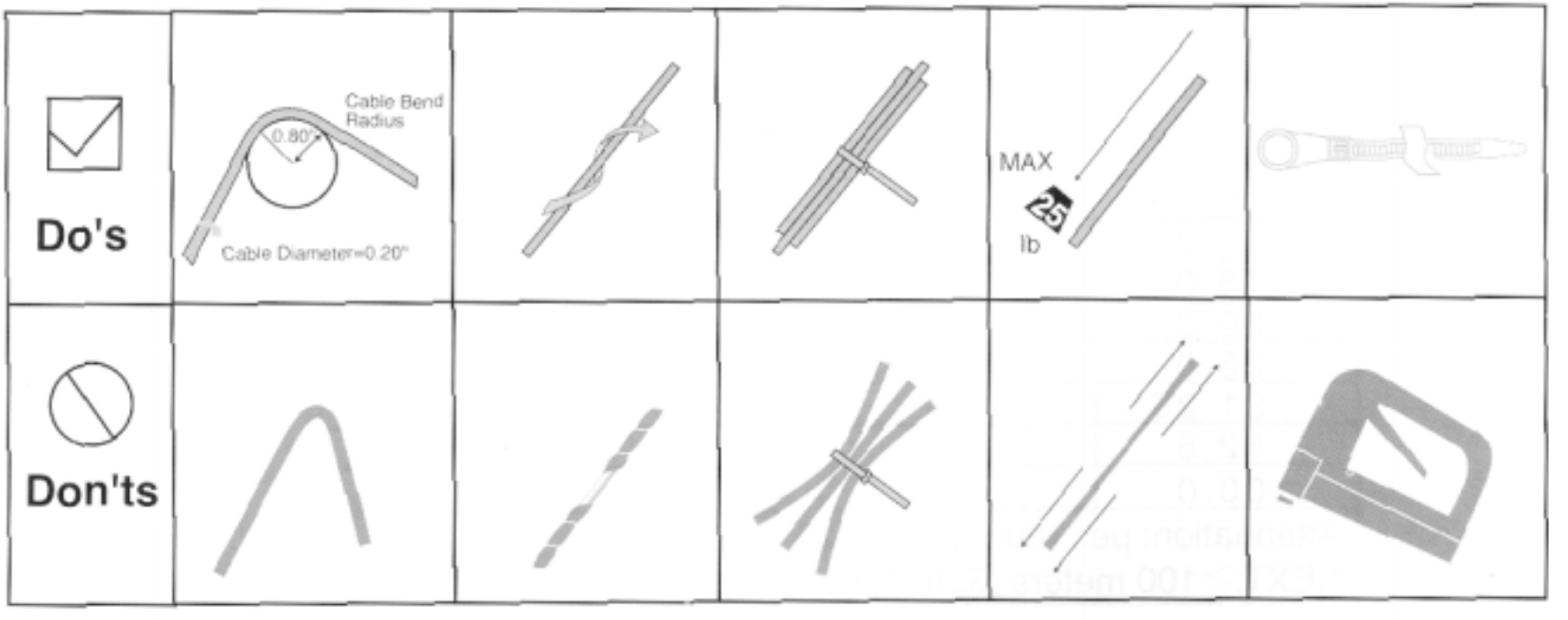
網路效能規劃 — 硬體設備(線材)

RJ-45槽座的腳位與**UTP**線顏色的對應

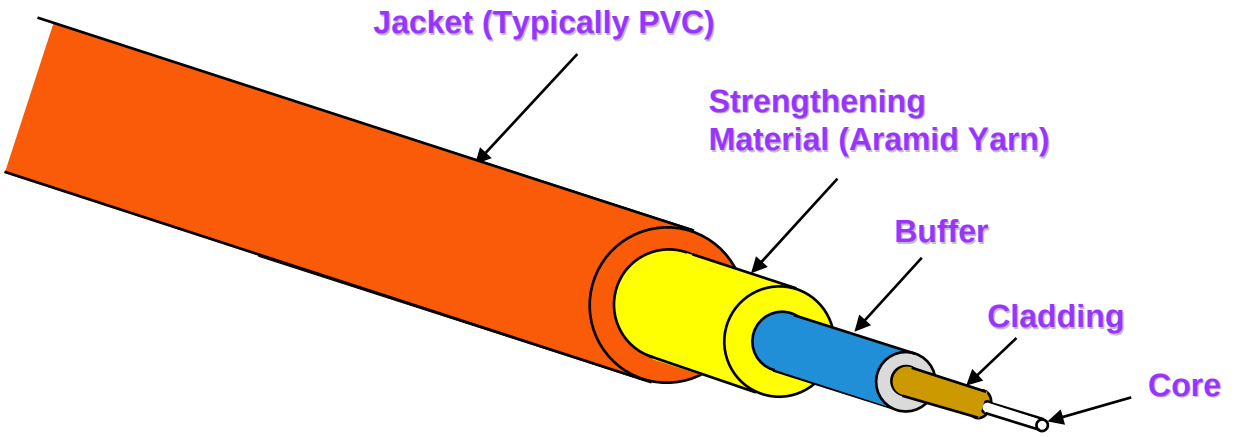


網路效能規劃 — 硬體設備(線材)

■ 安裝應注意事項：



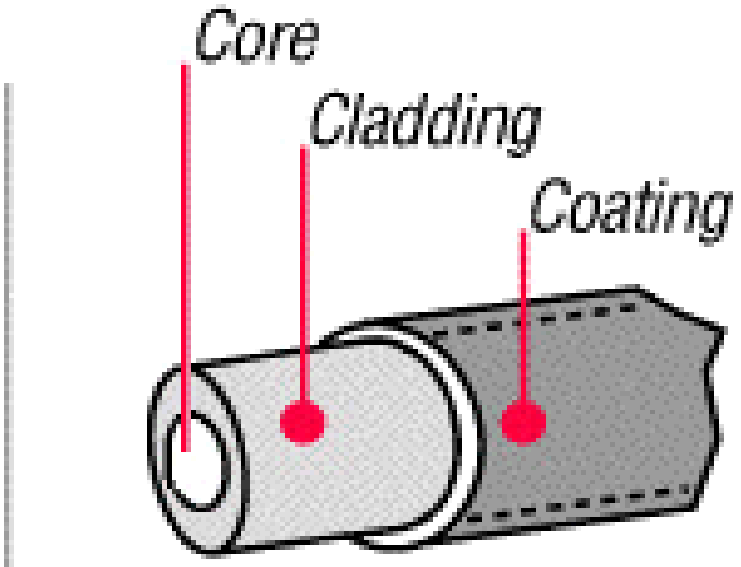
網路效能規劃 — 硬體設備(線材)



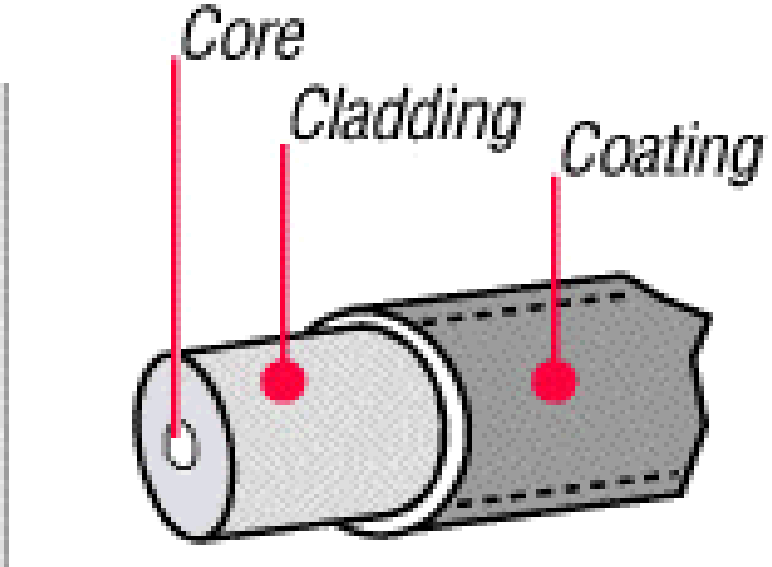
Multimode	Multimode	Singlemode
62.5/125 μm	50/125 μm	10/125 μm
一般使用 100m~230m	使用在 230m~5Km	
以 1000 Base SX設備為準	以 1000 Base SX設備為準	

網路效能規劃 — 硬體設備(線材)

CORE SIZE
Multimode versus Singlemode



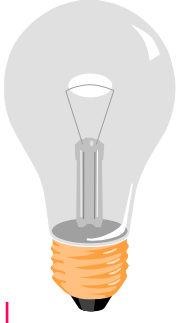
Multimode Fiber (MM)



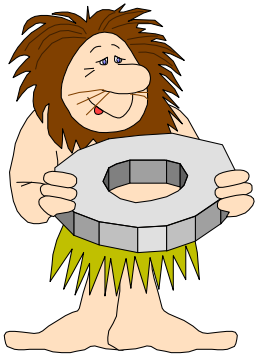
Single-Mode Fiber (SM)

網路效能規劃 — 硬體設備(線材)

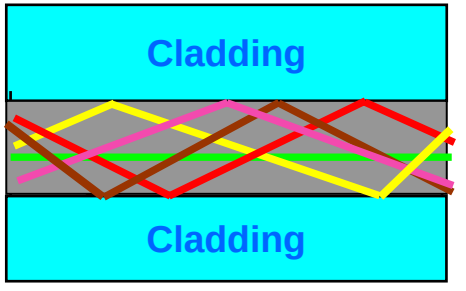
Human Vision



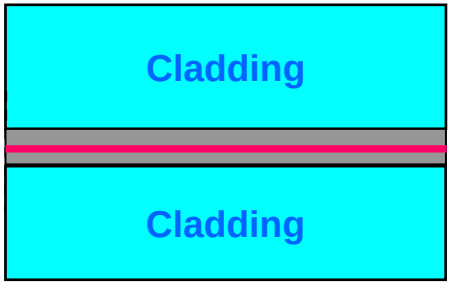
POF



Multi Mode



Single Mode



550*nm* 650*nm* 850*nm* 1300*nm* 1310*nm* 1550*nm*

網路效能規劃 — 硬體設備(網路卡的分類)

從協定標準來分

10/100Base-TX網路卡(最普遍)

1000Base-T網路卡(當紅炸子雞)

1000Base-SX網路卡(逐漸被1000Base-T取代) (短距離mutimode 100m~500m)
1000Base-LX網路卡(非常稀有) (長距離mutimode 500m~5km)
10GBe網路卡(稀有到極點)

10Base-2/10Base-5/10Base-T/100Base-FX網路卡(青春已逝)

網路效能規劃 ── 硬體設備(網路卡的分類)

從傳輸媒介來分

雙絞線網路卡

常見的接頭型式為RJ-45

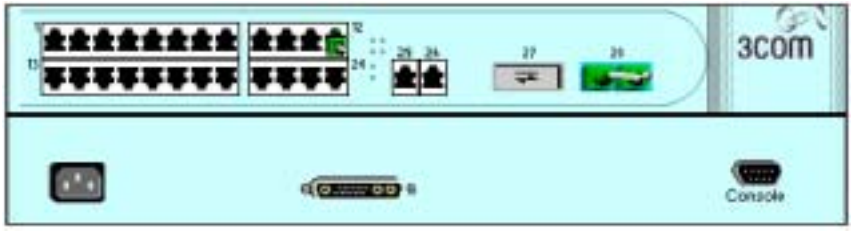
光纖網路卡

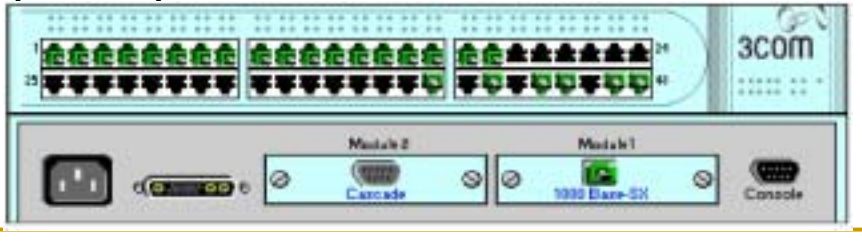
常見的接頭型式有SC(短距離)/ MT-RJ / LC(長距離)

※對於光纖網路來說了解網路卡的接頭型式很重要
※否則拿不正確的光纖跳接線是接不上去的

網路效能規劃 — 硬體設備(交換器)

- HUB
- Switch
- Layer 2 Switch (無網管)
- Layer 2 Switch (有網管)
- Layer 2 + Layer 4 Switch (有網管)
- Layer 3 Switch (又稱Router Switch 有網管)
- Layer 4 Switch (?)
- Layer 7 Switch (????)





網路效能規劃－硬體設備

- 怪機絲－Internet On Power

- DWDM－未來之星
  - 分波多工(Wave Division Multiplexing；WDM) －利用不同的光波波長，將多個光纖訊號合併在單一的光纖中傳送的一種光纖傳輸技術
  - DWDM一詞則常被用來描述那些可以在單一光纖線路上，支援許多通道(通常是十六個以上)的系統

3.障礙管理管理

- 首先要先思考“慢”的定義
- 這句話雖然看起來很無趣其實卻很有趣
- 然後找出為何會慢的原因
- 是網路設備效能不行
- 還是架構錯誤
- 還是頻寬不足
- 還是伺服器網卡連線塞車
- 還是佈線太差
- 還是伺服器負載太重
- 還是 .....等等的問題

- 對症下藥才能立竿見影

— ZMAN

障礙管理－ I (PC端)

PC端的錯誤-1：網路卡跟PC的連接

- 網路卡插好沒
- I/O ADDRESS,IRQ相衝
- 驅動程式
- 接頭(port)連接正確？
- 線材良好？
- 網管跳線沒？
- port故障？
- 設備故障？

障礙管理— II (網路錯誤無法連線)

- 設備故障？
- DNS Server
- 設定錯誤/盜用IP
- 惡意攻擊

障礙管理— III (校園網路部分的連線不正常)

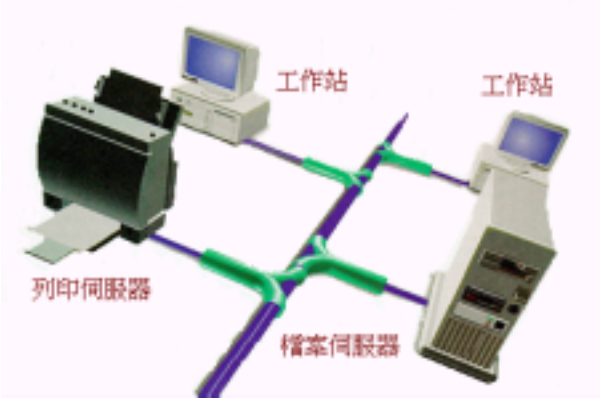
- DNS (Ping、Nslookup)
- Router (Ping、Traceroute)
- Web server (Ping、Traceroute)
- Proxy server (Ping、Traceroute)

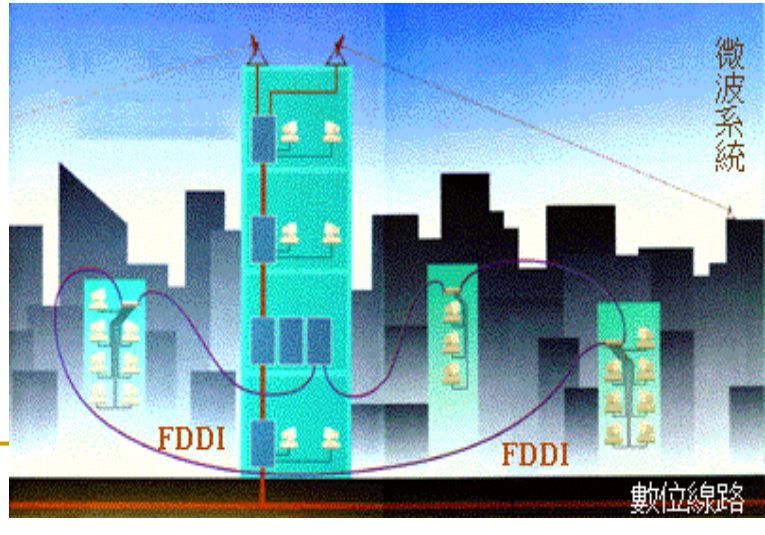
障礙管理— IV (校園網路之外的部分)

- Router (ping、Traceroute)

4.網路通訊的基本概念

- **WAN**
  - 網際網路
- **LAN**
  - 區域網路
- **MAN**
  - 都會型區域網路 －TANet 2





網路通訊的基本概念－I

- **Layer 2**
  - OSI標準將通訊分為7層(Layer)，包括 Physical，Logic，Network，Transport，Session，Present及Application等，每層各司其職，最高層的應用程式(如WWW / HTTP)逐層透過解析與封包，
  - 由第一層(如Ethernet)之傳輸媒介載送信號傳至接收端；值得注意的是TCP/IP的通信協定與各種應用程式通常省略了第五及第六二層，故只有五層。
  - 而Layer 2 Switch顧名思義，即是在區域網路通訊傳輸中僅以第二層(MAC層)的資訊來作為傳輸與資料交換之依據，通常此類交換器先以學習的方式(Learning) 在每一個port 紀錄該區段的MAC Address再根據MAC層封包中的目的地位址(Destination Address，DA)傳送該封包至目的地的port (或區段)，其他port (或區段)將不會收到該封包，若目的地位址仍然在該(或區段)，則封包將不會被傳送。
  - Layer 2 的Switch由於只判斷第二層的資訊故其處理效能佳，且其有效隔絕區段間非往來封包(及獨享頻寬)，大大提昇網路的傳輸效能，且因技術與ASIC晶片的功能日益強化，目前較高檔的Layer 2 Switch 每個port 均可達到Wiring Speed 的傳輸率(Ethernet 為14880pps，Fast Ethernet 為148800pps)。

網路通訊的基本概念－II

- **Layer 3**
  - Layer 3 Switch 又稱為IP Switch 或Switch Router,
  - 意即其工作於第三層網路層的通信協定(如IP)，並藉由解析第三層表頭(Header)將封包傳至目的地，有別於傳統的路由器以軟體的方式來執行路由運算與傳送，Layer 3 Switch是以硬體的方式(通常由專屬ASIC構成)來加速路由運算與封包傳送率並結合Layer 2 的彈性設定，因此其效能通常可達每秒數百萬封包(Million packet per second)的傳送率。
  - **傳統路由器通常可處理Multiprotocal 多重協定路由運算**(如IP，IPX AppleTalk，DEC Net...etc)但**Layer 3 Switch 通常只處理IP 及IPX為簡化設計**，降低路由運算與軟體的複雜性以提昇效能，並配合網路協定發展的單純化(**多重協定簡化至IP一種協定**)趨勢所致。
  - 由於**Layer 2 的Switch 並無法有效的阻絕廣播域**(Broadcast Domain)如ARP (Address Resolution Protocol)及Win95/98 中大量使用的NetBEUI協定均大量使用廣播封包，因此就算Layer 2 Switch 以VLAN (Virtual LAN)的方式(虛擬網路)將經常要通訊的群組構成一廣播域(Broadcast Domain)來試圖降低broadcast封包對網路層的影響，但仍無法完全避免廣播風暴問題(同一個VLAN間仍會產生廣播風暴)，再加上現今網路(尤其是Campus內部間流量及對外的Internet/Intranet流量)已不是80/20規則(80%流量在本地，20%是外地)，而是漸漸成為20/80規則，且加上Client/Server 及Distributor Server之運用，因此單靠Layer 2 Switch或傳統Router路由器便無法符合對效能(傳統路由器變成瓶頸)及Intranet上對安全顧忌(Layer 2 Broadcast Domain，對因廣播而使資訊傳送被盜取的安全疑慮)之要求，因此Layer 3 Switch便大量興起。
  - **如同傳統路由器(Router)，Layer 3 Switch的每一個連接埠(port)都是一個子網路(Subnet)**，而一個子網路就單獨是一個Broadcast Domain廣播域，因此每一個port的廣播封包並不會流竄到另一個port，其僅負責傳送要跨越子網路的封包(Routing Forward)，並以目的地的IP位址(目的地子網路的網路號碼)來決定封包要轉送至哪一個port，並以Routing Protocol(如RIP或OSPF)來交換Routing Table並學習網路拓蹼，其通常存放於Layer 3 Switch的Routing Forward Data-Base(FDB)，並以硬體及Route Cache的方式來加速IP table lookup並予以定址與更新(目前大多以ASICIC來執行)，因此才得以提昇運算效能達成Wiring Speed Forward之目的。
  - **Layer 3 Switch通常提供較大頻寬的交換核心(Switch Fabric)以提供較大的容量(Port Capacity)與較高的交換效能**，近來各廠家並不斷附以**Layer 3 Switch更強大的支援能力，如Class of Service(服務等級優先權)，Quality of Service(服務品質保證)，Policy Management(策略分級品質與頻寬管制與管理)，Multicast Routing(群組廣播路由傳送)等功能**，以符合網路環境的快速變化與應用。

網路通訊的基本概念－III

- **Layer 4**
  - 在OSI 的Layer 4傳輸層(Transport Layer)之中有所謂的連接埠(Port), 應用程式必需獨佔一個連接埠,當主機收到IP封包之後，就可以藉由連接埠編號,判斷此封包要送給那一個應用程式處理。Layer 4交換器通常內含高效能的ASIC晶片,能檢測分析封包至少前80位元組的資料,利用對傳輸層內的TCP或UDP埠號的辨識,就可以判斷封包內是包含那一種應用協定(HTTP,SNTP,FTP),然後將資料正確的送往更上層的應用軟體去做處理。 Layer 4交換器功能含蓋相當廣泛
  - QoS(Quality of Service)
  - LAN-Based Prioritization-IEEE802.1p/Q
  - 分類型服務(Differentiated Services; DiffServ)

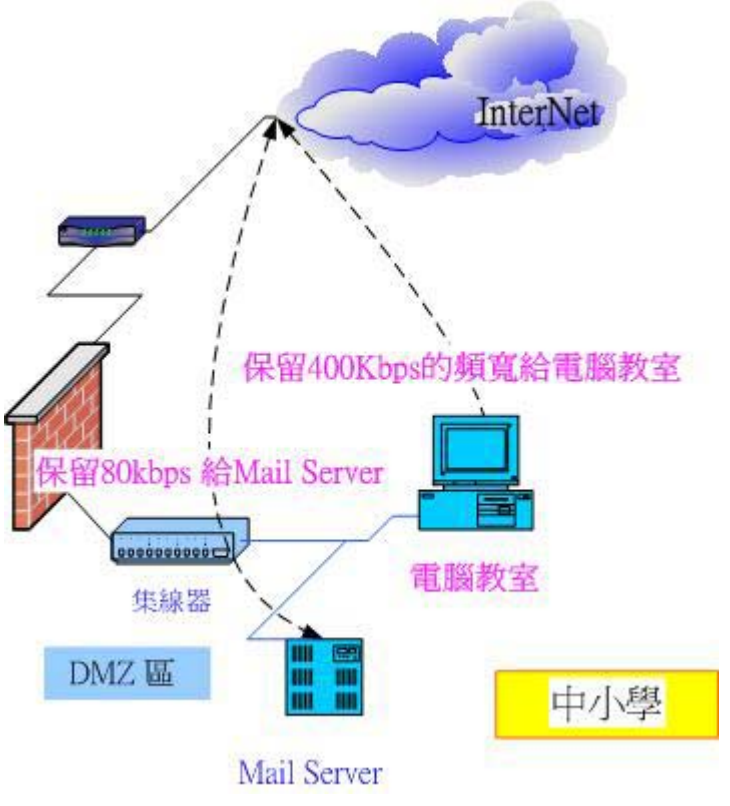
網路通訊的基本概念－IV

QoS

- Wire-Speed Traffic Classification
  能夠根據使用者設定的策略做資料的分類，及時的將資料傳送出去。
- Tranparent / Non-single point failure
  設備的引進使用，應不影響的一般使用者及網路上其他設備的設定(即是對使用者為Transparent)，以減少所需的設定至最低。同時，如果因任何原因而當機時，系統應自動變成如同一條網路線，雖然頻寬管理的功能喪失了，但不會影響總體網路的運作效能。
- Traffic Management / Bandwidth and Latency Policy Setting
  頻寬管理機制，共有TCP Rate Shaping、Class-based Queuing、Fail Allocation of Bandwidth及Packet-size Optimization等四種；完整的架構出最佳化的頻寬控管功能：
- TCP Rate Shaping：
  TCP Rate Shaping為一專為TCP/IP交通設計的管理法則，它會告知資料傳送者適時的減少資料傳輸量，來使得TCP資料流(TCP Flow)傳送更加平順，以便達到將TCP交通的瞬間巨量(Burst)情形降至最低。這些突如其來的巨量交通會造成路由器的交通阻塞，嚴重影響到一些無法接受傳輸延遲的網路應用(Latency-Sensitive Application)。 TCP Rate Shaping對低速的專線並無法有效的達到準確的頻寬管理。TCP Rate Shaping 只能控制TCP的交通，對於Non-TCP 的交通則無法管理；而根據統計。
- Class-based Queuing (CBQ)
  Class-based Queuing(CBQ)乃依據不同的Class等級提供不同的Traffic Queuing，它可補足TCP Rate Shaping只能管理TCP交通的問題，支援TCP及Non-TCP的交通管理，並且能管控到網路交通的封包階層(Packet Level)，故能更有效的控制低速頻寬的傳輸。
- Policy-Smart Web Caching
  Web Caching功能能夠有效的降低HTTP交通的高頻寬需求，以提供更多的頻寬資源給予”Mission Critical”及”Latency-Sensitive”的應用，藉以在有限的頻寬中提供使用者最快的服務。而且，Web Caching可以依據每一個策略(Policy)可以設定為”Enable Caching”或是”Disable Caching”。QoSWorks 的 Caching 功能乃是”Transparent Caching”，完全不需更改路由器、使用者電腦或是交換器的設計。

網路通訊的基本概念－以QoS建立頻寬管理機制

- 視訊會議、VOD等多媒體服務對於網路頻寬都有最高優先權。
- 否則VOD播放斷斷續續、影音間斷會是相當難過，反而浪費時間，但是如果全部保留給他使用又稍微浪費。
- 使用QoS頻寬管理機制，確保最高使用權，但是當這些多媒體服務不用時，頻寬自動釋放。



- **Firewall**
  - 防火牆的兩種基本型態
  - Dual-Home Gateway
    這一類的防火牆是在單一主機上架設兩個網路介面。這樣的架構，防止了網際網路上的封包直接傳入企業內部網路中。因此網際網路上的電腦和企業內部網路上的電腦彼此不能互通，除非透過防火牆的中介。
    - Dual-Home gateway 最大的缺點：在於它將網路上直接的IP交通給封鎖了。因此跨網路的主從式應用程式便無法使用，要解決這樣的不便，必須要在Dual-Home gateway上執行proxy才行。Proxy 等於是主從架構中的一個居間的媒介，伺服程式與用戶端都藉著與proxy的溝通來完成工作。目前對proxy的要求是〝透明化〞，讓使用者在操作的過程中，完全不會查覺到proxy的存在。
  - Screened-Host Gateway
    控制主機運作的原理，對於router的管控。一般router都設定為僅對控制主機的某些服務開放外部直接通訊。更進一步，router 可以僅對外部網路的某些特定主機開放通訊。大部份的系統監管者對router都設定為對內部網路的所有主機開放對外通訊，在這樣的情況，完全不需要架設 proxy程式。
    - 前面我們曾經提到，對於router我們可以開放某些特定的通訊。要注意的是，在開放的同時，我們等於也對網路駭客下了邀請函。對於類似World Wide Web 等這類新服務，或許還留有許多安全上的漏洞。如果開放內部的網路主機直接對外提供 www 的服務，或許你已經在FireWall的銅牆鐵壁上，大開方便之門。
      Screened Host Gateway 其控制主機僅有一個網路介面，並且需要router來協助完成工作。關於 router 的設定，必須能擋住所有通往內部網路的通訊，僅留下Screened Host可與外界直接溝通。與Dual-Home gateway 不同的是 Screened Host gateway並不強制經手所有的通訊。藉由router的設定，可以在firewall上開放某些特定的通訊。

- **Firewall**
  - 安全等級
    - **LEVEL D1－所有等級中最低的一級**
    - **LEVEL C1－別稱鑑別式安全保護系統，是一般UNIX所通用的安全系統**
    - **LEVEL C2**－C2在C1的缺點中作了一些改進。在C2的環境中，除了權限的設定外，系統管理者可針對特定的使用者開放特定的檔案存取權。更進一步，在系統上所有的活動都必須受到監管。通常都會有一個監管程式來紀錄系統上所有的活動。在C2的環境中，系統管理不再依賴系統監管者一人。藉由授權的方式，系統管理者可以開放特定的權限給某個使用者。讓他來執行系統管理的工作。
    - **LEVEL B1－標記式安全保護**，這是第一個支援多層安全的等級，像密件、機密還有極機密等。在這個強制性安全系統的管制下，物件【如：檔案】的擁有者是不可以任意更改物件的存取權限。
    - **LEVEL B2**－又稱**結構化保護**，在這個系統中，所有的系統都必須作上標記。每一種設備【如：磁碟機、磁帶機、終端機等】都有多層安全標記。這是第一個等級考慮到不同安全等級的物件互相溝通時的安全問題。
    - **LEVEL B3**－別稱**安全區域等級**。在這個等級中，所有硬體的安裝都必須有安全上的考量。例如：記憶體的管理、硬體上必須作到能夠未授權的存取。在這個等級中，終端機的連結也必須透過可信賴的途徑。

三、網路安全

1. 網路攻擊的種類－I

- 搗蛋、破壞型
  - 電腦病毒 (Virus，具 感染/繁殖)
    - 程式無法使用，檔案遭刪除，硬碟遭格式化
    - 網路蠕蟲(Worm，具 感染/繁殖 傳染)
      - 消耗甚至癱瘓主機及網路設備的運作
        - 思坎(Sircam): E-mail 病毒
        - 紅色警戒(Code Red)→娜妲(Nimda): 利用Microsoft IIS
        - 1988, 9/2, Internet Worm: 利用fingerd
    - 網路細菌 Bacteria、兔子 Rabbit
      - 大量繁殖→阻斷服務(DoS/DDoS) 攻擊-癱瘓服務型
    - 攻擊程式
      - 郵件炸彈(Mail Bomb)，耗盡使用者信箱空間，癱瘓伺服器

網路攻擊的種類 — II

- 竊取、偷窺型
  - 後門程式：跳過授權程序
  - 木馬程式：偽裝精良的陷井程式
  - 監聽掃瞄：Traffic Dump, Scanner
- 直搗黃龍型
  - 利用程式的錯誤(Bug)，直接獲取進階權限
- 攻擊跳板
  - 網路編織法攻擊 Network Weaving
  - 連接延申攻擊 Connection Laundering
- 野心大膽子小
  - 祕密通道程式：用隱密的程式，讓自己也可以藏龍！☺
- 怎麼會這樣型
  - 作者自己也控制不了，一下子就爆發成大災難的

2.擬定安全計畫－I

- 注意目前的威脅有哪些
- 利用子網路分散威脅
- 確認使用者身份
- 評估應用程式的安全性
  - 移除不必要的軟體
  - 隨時更新軟體

2.擬定安全計畫－II

- 安全監控
  - 找出搗蛋者

這種屬於other型的流量所佔的比例偏高，該主機很可疑

2.擬定安全計畫 — III

- 存取控制
  - 對有管理權的網路存取IP或Domain作嚴格控制

這台主機僅local端的機器有權要求所有的服務

僅此網段的機器有可使用Telnet 23 port,其餘不行

僅local端所有的subnet網段可使用這個特殊需求的 port,其餘不行

僅local端所有的subnet網段可使用ICMP需求的port,其餘不行

第一步先把所有的服務關閉再開啟可使用的資源

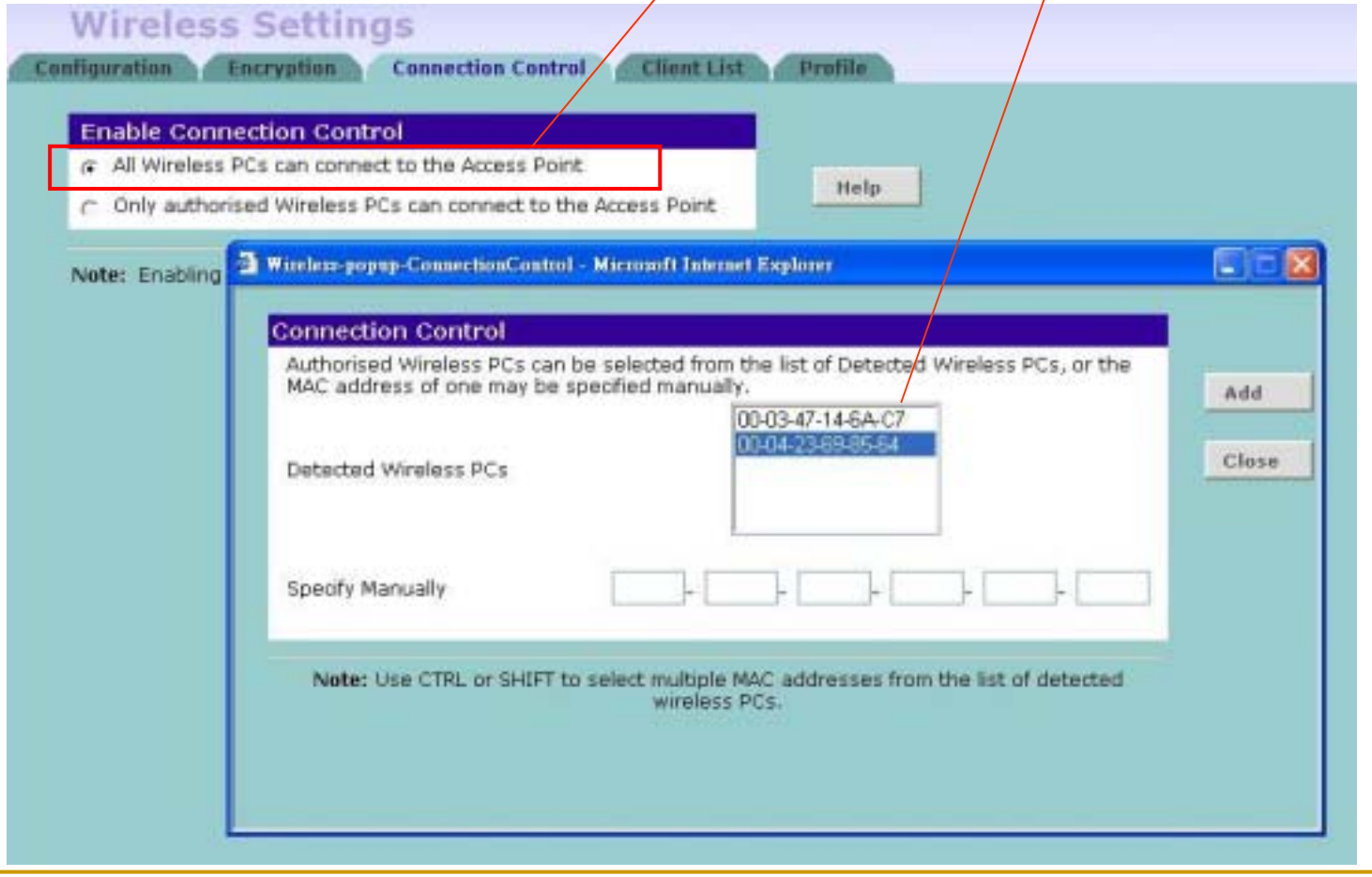
Service/Firewall

Rules

E	When	Source	Destination	Service	Action	L
☑	All-Time	LAN	192.168.1.23	Any	Accept	☐
☑	All-Time	LAN	Any Address	FTP (21)	Accept	☑
☑	All-Time	Any Address	192.xx.xx.xx	SSH (22)	Accept	☑
☑	All-Time	Any Address	192.168.1.0/255.255.255.0	TELNET (23)	Accept	☑
☑	All-Time	Any Address	Any Address	SMTP (25)	Accept	☑
☑	All-Time	Any Address	Any Address	DNS (53)	Accept	☑
☑	All-Time	Any Address	Any Address	HTTP (80)	Accept	☑
☑	All-Time	Any Address	Any Address	POP3 (110)	Accept	☑
☑	All-Time	Any Address	Any Address	TCP@3128	Accept	☑
☑	All-Time	LAN	192.168.2.252	TCP@3306	Accept	☑
☑	All-Time	LAN	Any Address	TCP@443	Accept	☑
☑	All-Time	LAN	Any Address	ICMP	Accept	☑
☑	All-Time	Any Address	Any Address	Any	Deny	☑
☑	All-Time	Any Address	Any Address	Any	Accept	☐

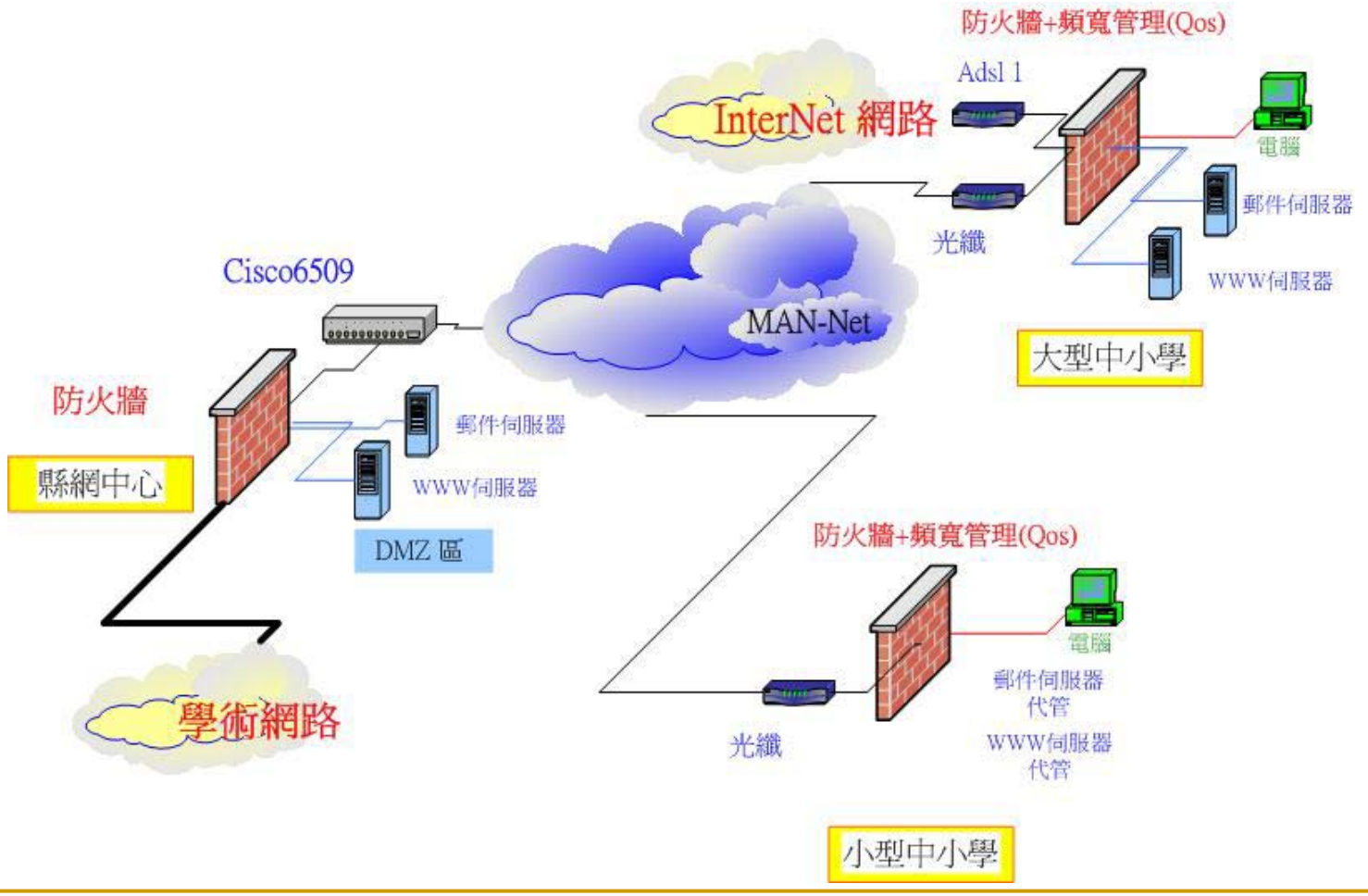
2.擬定安全計畫 — IV

- 存取控制
  - Wireless 的存取控制



四、展望

未來南投縣網安全計畫


防火牆+頻寬管理(Qos)
Adsl 1
InterNet 網路
電腦
郵件伺服器
光纖
WWW伺服器
Cisco6509
MAN-Net
大型中小學
防火牆
郵件伺服器
縣網中心
WWW伺服器
DMZ 區
防火牆+頻寬管理(Qos)
電腦
郵件伺服器
代管
光纖
WWW伺服器
代管
學術網路
小型中小學