中山科學研究院委託合作研究

國防科技學術合作研究計畫成果報告

國防資訊建設中網路架構設計之探討

A Study on Network Architecture Design of Defense Information Infrastructure

計畫類別：☑個別型計畫　　□整合型計畫

計畫編號：NSC90-2623-7-009-019

執行期間：90 年 1 月 1 日至 90 年 6 月 30 日

計畫主持人：羅濟群

協同主持人：唐　震

執行單位：國立交通大學資訊管理研究所

中　華　民　國　90　年　6　月　15　日

目錄

表次

圖次

中山科學研究院委託合作研究

國防科技學術合作計畫專案

國防資訊建設中網路架構設計之探討*

A Study on Network Architecture Design of the Defense Information Infrastructure(DII)

摘要 本研究以國軍網路管理需求予以展開，作爲提供國防資訊建設中網路架構設計之參考依據，研究過程中針對廣域網路相關標準、可取得之學術單位網路架構、Fault 與 Configuration 兩個主要網路管理議題做出學理分析，另外，爲使研究具實務性質，首先，針對市場上所可取得的網路管理工具提出分析結果，其次，與區網中心之實際負責技術主管訪談網路管理之實務經驗，最後，以個案模擬方式，分析所取得的網路流量資料，其中所具有的實際意義。

Abstract: This research we based on the requirements of military for network management, the results could be the reference of network architecture design on Defense Information Infrastructure as well. We study the WAN standards, network architecture on several academic campus, which we can reach, and fault/configuration management analyst. In addition to focus on the practical issues, firstly we pay attention to the tools currently for network management. Secondary, we have an interview with an experienced manager in charged of a large district of networking range. At last, we supply a case study to simulate the practical network environment and analysis meaning of network data flow.
Keywords: DII、Network Management

1. 序論

1.1 研究背景與動機

1992 年 12 月美國國防部認爲新的戰爭型態，需要新方式來處理及傳送資訊，於 1994 年 11 月發行第一版的國防資訊基礎建設計劃(DII Master Plan)，並於 1998 年 3 月發佈第七版。其最主要的精神在於整合(integration)分散於美國國防部(DOD)內的各個資訊管理計劃(Information Management Programs)，其主要目的是：(1)改善國防資訊的交換效率、(2)加強使用電腦、通訊、資訊管理的功能，以便更能有效率的完成國防任務、(3)有效地減少資訊科技對操作人員的負擔、(4).操作人員僅需要些許的通訊與電腦技術，就可以使用、分享、交換廣泛的資訊。DII 是一個結合通訊網路、電腦、軟體、資料環境、應用軟體、武器系統介面、資料、安全防制，以及能滿足使用者對資訊的處理與傳遞的需求的資訊網。換言之，對國防部的使用者，特別是作戰人員，國防資訊基礎建設(DII)

*中山科學研究院委託合作研究計畫

須能提供無缺失的、安全的資訊以協助決策與達成任務。爲因應資訊科技之衝擊，面對未來資訊作戰環境，現代化國防必須對資訊網路整合技術進行研發，以達成各系統間之整合需求，滿足網路之透通、各系統間裝備「互換性」、資料之「互通性」及「資訊安全」，進而提高系統整體之「存活性」、「維持性」、「擴充性」及降低「維護成本」。以下爲計畫執行說明:網路建設爲 DII 之最基儲之設施,所有資訊須透過其進行傳送。網路設計時須考慮頻寬、服務品質(Qos)、流量控制、壅塞控制(Congestion Control)、斷線備援及資訊安全等需求。實際運作時須執行型態管理(Configuration Management)、容錯管理(Fault Management)、安全管理(Security Management)、性能管理(Performance Management)及帳戶管理(Account Management)等。大型廣域式網路設計常採用階層式架構設計,其類似於電話網路,其優點包括易於網路管理及訊息繞送。一般網路分析須依據真實網路連線進行以下數種分析(1) LAN-LAN (2) LAN-WAN (3) WAN-WAN (4) LAN-WAN-LAN ,網路之間透過橋接器(Bridge)、多協定路由器(Multi-Protocol Router)及傳輸閘道(Transport Gateway)或應用閘道(Application Gateway)連接。針對大型網路分析考量以階層式架構進行分析，網路以叢集(Cluster)、地域(Zone)及群組(Group)加以組成,但建立此網路模式及分析架構須耗費時日,故本研究以台灣學術網路之某一區網中心作爲資料取得與分析的對象，預期在後續研究設計與研究過程中完成及滿足研究需求。

1.2 研究目的

本研究以不影響區網中心的運作與路之安全顧慮下，取得網路流量資料，提供符號表示之網路模式，針對下述之各項分析完成研究目的：

a. 點對點流量分析：本研究將在考量線路容量限制下進行點對點之流量分析；並於研究過程中給予相關的網路管理工具剖析，藉此提供網路需求單位，當在系統設計時欲製定網路流量規格(Specification)確保傳送時速率的參考。
b. 網路壅塞分析:在考量網路整體頻寬及已使用頻道限制下進行網路之壅塞分析以預測可能發生之閉塞(Choke)情況及其採用之方法，本研究將以個案訪談方式，針對區網的實際負責之高階主管技術進行深度訪談，以實際的訪談內容提供網路管理單位，據以建立網路壅塞管理之政策(Policy)，以確保網路整體之交通量。
c. 網路繞送路徑分析及最佳控制點選擇：就學理上，當規劃以靜態分析法(最短路徑法 Shortest Path Method及洪氾法 Flooding)，應考量線路容量限制，爾後，再利用動態分析法(距離向量繞送Distance Vector Routing 及鏈結狀態繞送Link State Routing) 進

行最佳控制點選擇分析，針對此以研究項目，本研究將以文獻探討方式呈現，就理論上的最佳結果，提供網路管理單位參考。

d. 斷線備援路徑選擇：路由器利用鏈結狀態繞送法之5個步驟進行斷線備援路徑選擇，分別是：(S1)以HELLO封包打聽運用之鄰居路由器、(S2)計算其到鄰居路由器之成本及時間、(S3)建立一個此路徑之資訊封包、(S4)將此資訊封包送給其它路由器、(S5)計算到其它路由器之最短路徑法。同上所述，本研究將以文獻探討方式呈現，就理論上的最佳結果，提供網路管理單位參考。

整體網路系統評估除欲達成上述之研究目的，本研究將以網路管理工具軟體進行資料蒐集分析，例如：MRTG、HP Open View、Microsoft SMS 等，當相關資源許可時，配合網路分析儀的硬體設備以驗證分析結果及調整相關參數藉以符合網路真實運作的情境。

1.3 研究步驟

本計畫的實施步驟如下：

a. 蒐集並研究美軍及各重要標準組織所制訂的共同作業環境中網路管理相關標準(X.25、TCP/IP、ATM、SMDS、SONET)，期能對目前的概況及未來的發展趨勢有一通盤瞭解。

b. 針對欲執行國軍共同作業環境系統之節點、地區性網路架構分析時，在網路管理軟硬體工具的選取上提供分析的準則或可行方案的建議。

c. 在無安全顧慮下，以網路模擬的方式，模式網路流量分析之方法，執行網路最佳控制點選擇及備援分析。在固定容量限制及給予線上流量，以文獻探討方式分析各種演算法以執行各種網路架構下之點對點之流量，例外，針對區訪負責人進行深度訪談，藉以瞭解實務上，網路壅塞所發生的原因及解決對策。

d. 對上述各種研究項目完成一份綜合性分析報告，以期有助於國軍共同作業環境之網路系統管理及問題分析之參考。

2. 文獻探討

2.1 網路相關標準

2.1.1 X.25

X.25 是在 1974 年由 CCITT (國際電報暨電話諮詢委員會) 所制定的低速分封交換 (packet switching) 網路標準。X.25 是一種連接導向的通訊協定(在傳送資料之前必須先建立傳送路徑，點對點通訊)，定義了使用者終端機和數位通訊設備之間資料交換的程序，這個協定利用分封不定長度的資料包 (datagram) 來傳送資料，目前廣泛用於如 Internet 的廣域網路之中。典型的 X.25 分封交換網路如圖 2.1 所示。

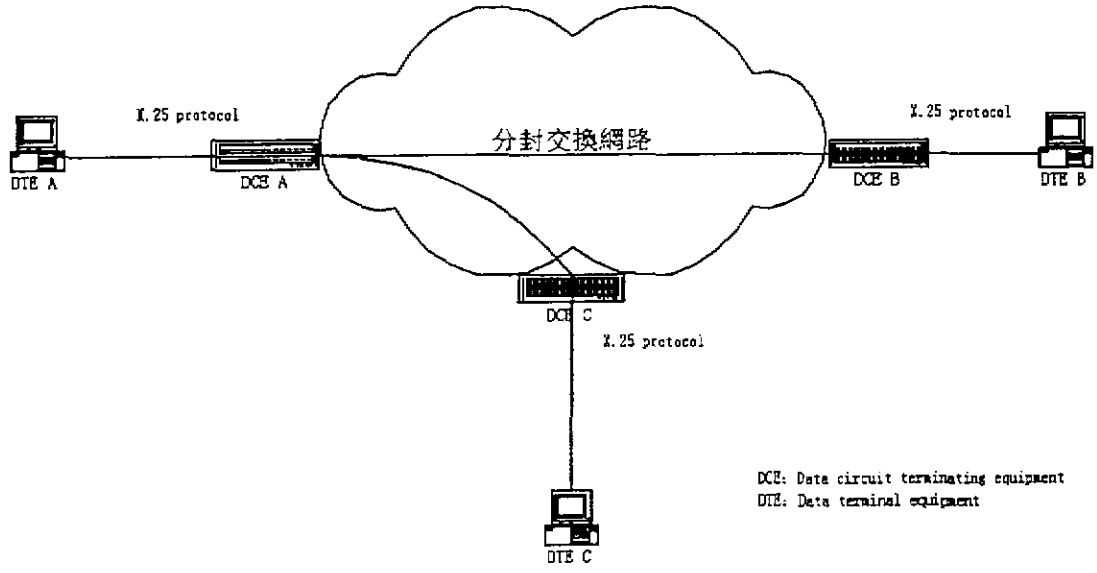


圖 2-1：典型的 X.25 分封交換網路

X.25 通訊協定可分爲三個層級，如圖 2-2 所示。'

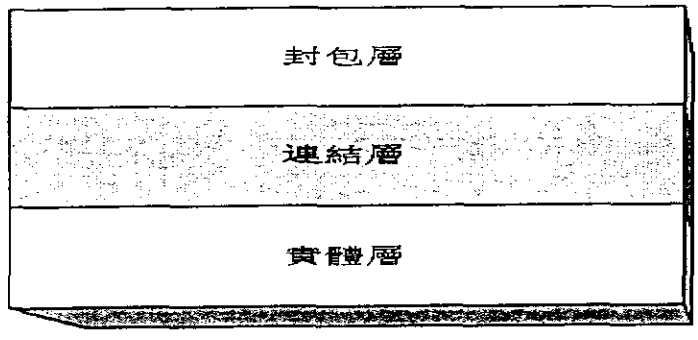
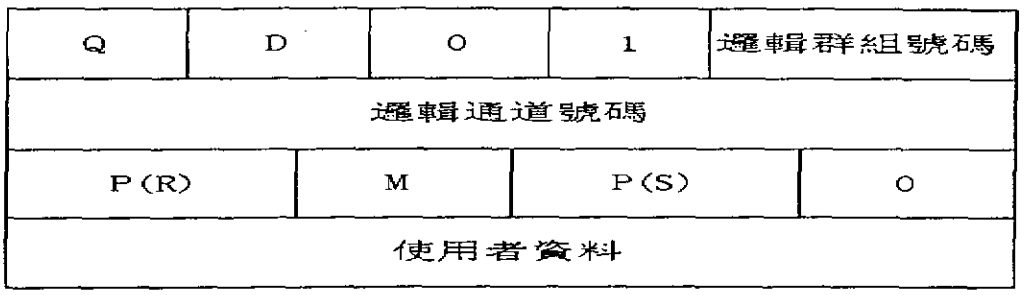
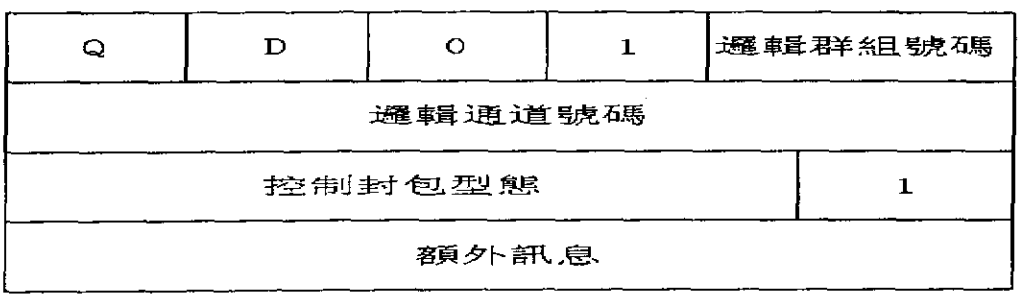


圖 2-2：X.25 協定架構的層次

a. 封包層(Packet level)：X.25 的封包有兩種，一爲資料封包，另一爲控制封包，如圖 2-3 所示。封包的標頭一共 24bits，包括虛擬線路號碼、流量控制 P(S)及錯誤控制 P(R)等訊號。封包使用虛擬線路服務方式傳送，並在傳送資訊後將虛擬線路清除。



(a)



(b)

圖 2-3：X.25 的封包格式：(a)資料封包(b)控制封包

b. 連結層(Link Level or frame level)：連結層採用 LAPB(Link Access Procedure Balanced)協定，它的功能爲連線之建立、提供一正確無誤的資料傳輸以及控制連線上之資料流量，除了單點對單點(Point-to-Point)連線功能之外，也可同時處理多條連線(Multilink)。

c. 實體層(Physical level)：實體層的通訊協定大都以 X.21 作爲標準規格。X.21 利用 ISO 4903 標準，定義了 15 腳接頭的機械結構，而 X.26 與 X.27 定義了電氣特性，X.24 定義了八種利用 X.21 的交換線路。綜合而言，X.21 規定了終端設備與通訊設備之界面。

若以 OSI 七層協定而言，X.25 涵蓋最下面三層，即實體層(Physical Layer)、資料鏈接層(Data Link Layer)與網路層(Network Layer)，但不完全相同。OSI 七層協定與 X.25 的關係比較如圖 2-4 所示。

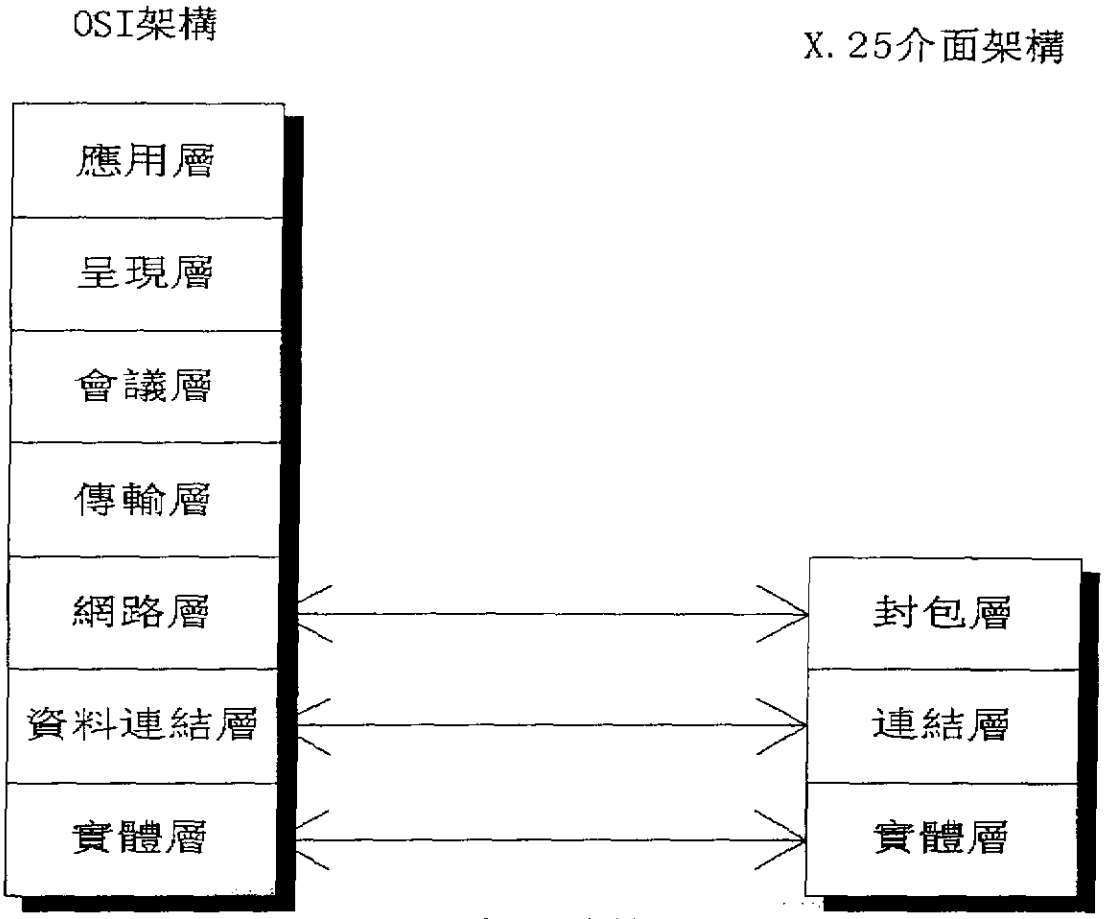


圖 2-4：OSI 與 X.25 架構比較關係圖

2.1.2 TCP/IP

TCP/IP 起源於 1960 年代，美國國防部及學術界有感於電腦主機之間資料無法即時交換，因此成立一個專案計畫及組織來推動電腦之間資料傳送的技術發展，稱爲 Laboratory's DARAPA contract 與 ARPA/IPTO（Advance Research Projects Agency of the Department of Defense（DoD） Information Processing Techniques） 。1978 年，TCP/IP 被建議爲電腦資料交換的良好模式，1983 年，TCP/IP 成爲 ARPANET 上唯一的通訊規範。而以 ARPANET 擴展而成的 Internet 目前已成爲全世界最大的電腦網路系統。

2.1.2.1 TCP/IP 協定的層級架構

TCP/IP 通訊協定群組包含了一系列的通訊協定及應用，提供各式不同之電腦硬體平台、通訊介質及作業系統以一個共通之方式交換資訊。TCP/IP 通訊協定可以分爲以下四層：

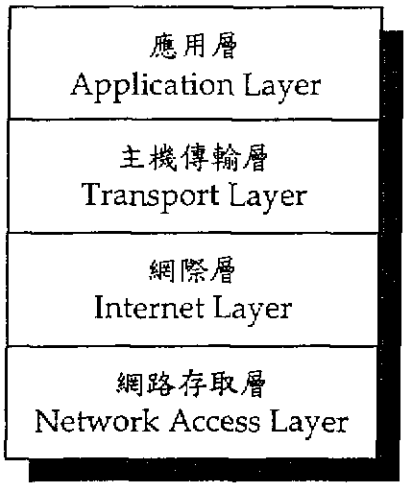


圖 2-5：TCP/IP 協定架構的層次

a. 應用層（Application Layer）：應用程式間溝通的協定，如簡易電子郵件傳送（SMTP, Simple Mail Transfer Protocol）、檔案傳輸協定（FTP, File Transfer Protocol）、網路終端機模擬協定（TELNET）等。
b. 主機傳輸層（Transport Layer）：提供端點間的資料傳送服務，如傳輸控制協定（TCP, Transmission Control Protocol）、使用者資料協定（UDP, User Datagram Protocol）等，負責傳送資料，並且確定資料已被送達並接收。
c. 網際層（Internet Layer）：負責提供基本的封包傳送功能，讓每一塊資料封包都能夠到達目的端主機（但不檢查是否被正確接收），如網際協定（IP, Internet Protocol）。
d. 網路存取層（Network Access Layer）：實質網路媒體的管理協定，定義如何使用實際網路（如 Ethernet, Serial Line 等）來傳送資料。

相對於 OSI 七層協定而言，TCP/IP 的應用層範圍涵蓋了 OSI 架構的應用層、表現層和會期層的功能；傳輸層和網路層則與 OSI 架構一一對應；至於網路存取層則包含了 OSI 架構的資料連結層與實體層。OSI 七層協定與 TCP/IP 協定的對應關係比較如圖 2-6 所示。

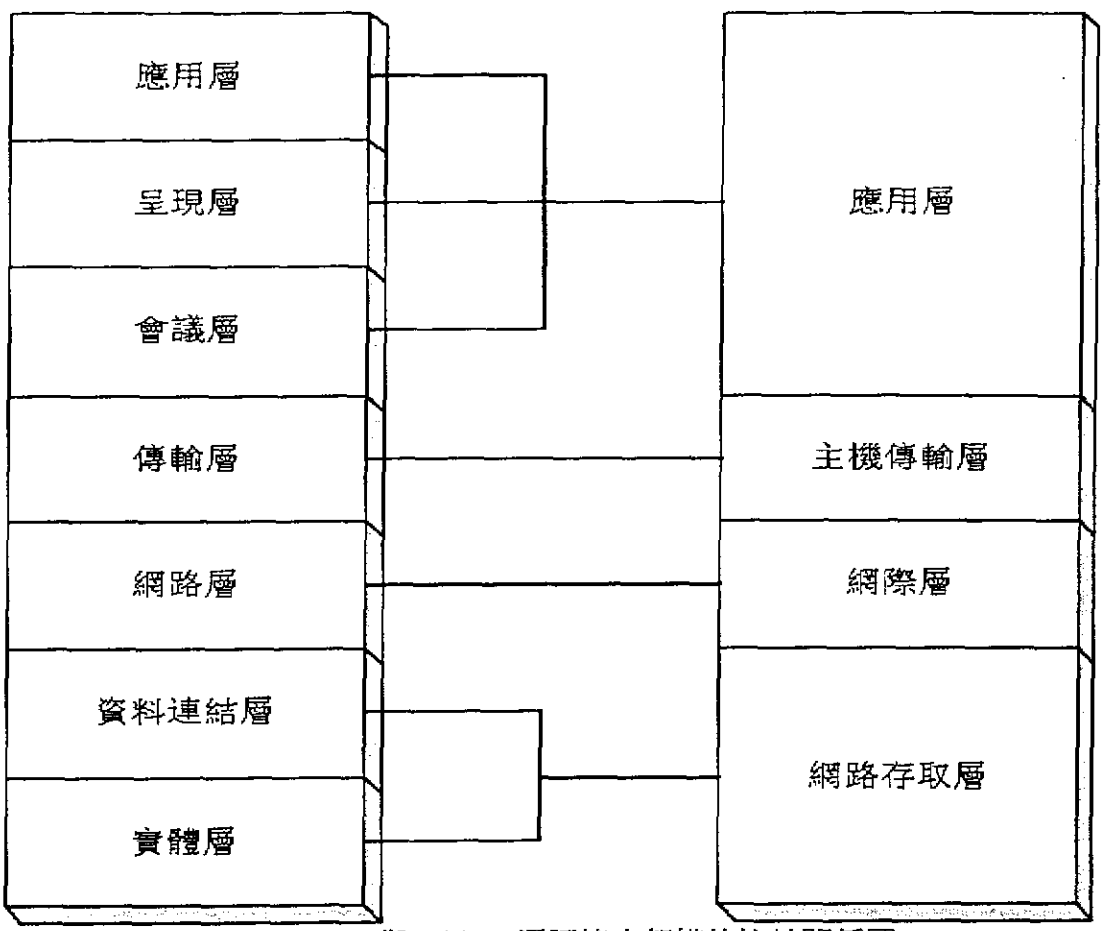


圖 2-6：OSI 與 TCP/IP 通訊協定架構的比較關係圖

2.1.2.2 功能與用途

TCP/IP 通訊協定群組包含了一系列的通訊協定及應用，提供各式不同之電腦硬體平台、通訊介質及作業系統以一個共通之方式交換資訊。以下是各通訊協定與應用的介紹。

a. Internet Protocol (IP)

說明：Internet 通訊協定。

功能：提供資料封包傳送基本服務，包括封包格式及定址。

用途：TCP/IP 資料封包傳送。

b. Internet Control Message Protocol (ICMP)

說明：Internet 訊息控制通訊協定。

功能：爲輔助 IP 之低信賴度，提供錯誤及訊息處理。

用途：訊息和狀態傳送及自我測試。

c. Internet Group Multicast Protocol (IGMP)

說明：Internet 群體多重傳送通訊協定。

功能：提供有效率之封包多目的位址之傳送。

用途：傳送封包至多目的位址時。

d. User Datagram Protocol (UDP)

說明：使用者資料流通訊協定。

功能：提供資料流的傳送服務，不保證資料之信賴度。

用途：交易型態（Transaction type）之資料流傳送。

應用：細瑣檔案傳輸通訊協定 （Trivial File Transfer Protocol, TFTP）、領域名稱伺服器（Domain Name Server, DNS）、遠程啓動通訊協定（Bootstrap Protocol, BOOTP）。

e. Transmission Control Protocol (TCP)

說明：傳輸控制通訊協定。

功能：提供資料傳送信賴度保證之服務。

用途：資料信賴度高之應用服務。

應用：遠程登錄終端模擬（TELNET）、檔案傳輸通訊協定（File Transfer Protocol, FTP）、SMTP。

f. Exterior/Border Gateway Protocols (EGP/BGP)

說明：外部閘道通訊協定。

功能：閘道之可送達網路位址報告。

用途：獨立系統之間（Between Autonomous systems）之閘道路徑選擇。

應用：Router、Gateway。

g. Interior Gateway Protocols ((Routing Information Protocol, RIP; Open Short Path First, OSPF)

說明：內部閘道通訊協定。

功能：閘道之路徑選擇資訊交換。

用途：獨立系統之內（Within Autonomous system）之閘道路徑選擇。

應用： Router、Gateway。

h. Electronic Mail

功能：用戶訊息交換。

i. File Transfer and Access (FTP, TFTP, NFS)

說明：檔案傳輸與存取。

功能：不同主機之間之檔案交換。

j. Remote Terminal Access （TELNET, RLOGIN）

說明：遠端終端機存取。

功能：遠端主機之終端機模擬。

用途：遠程登錄。

k. Internet Management (SNMP)

說明：Internet 網路管理。

功能：提供網路狀態資料及控制。

用途：網路監測管理。

l. Transaction Application (DNS, BOOTP)

說明：交易型態應用服務。

功能：提供單筆資料交換作業。

用途：清楚並明確之需求可以單筆作業完成之交易（Transaction）。

m. Interconnect with other network systems (TP-TCP, SLIP, PPP)

說明：異質網路資料交換相關通訊協定。

功能：提供異質網路或通訊協定資料交換之規定。

用途：異質網路系統之資料交換。

2.1.3 ATM

非同步傳輸模式(Asynchronous Transfer Mode, ATM)網路是一種交換連結導向的高速網路技術，它原先設計的目的是用來取代現行廣域網路的傳輸技術，只要是數位式的資訊就以高速的方式將訊息作點對點(peer to peer)的傳送，而不管這資料是聲音、影像、或者單純的文字資料。由於 ATM 網路資料長度固定，可藉由硬體來完成交換與多工(Multiplexing)的處理，處理速度極快。更重要的是此種技術亦能應用區域網路上，充分支援語音、影像與視訊等多媒體訊息的傳輸。典型的 ATM 拓樸如圖 2-7 所示。

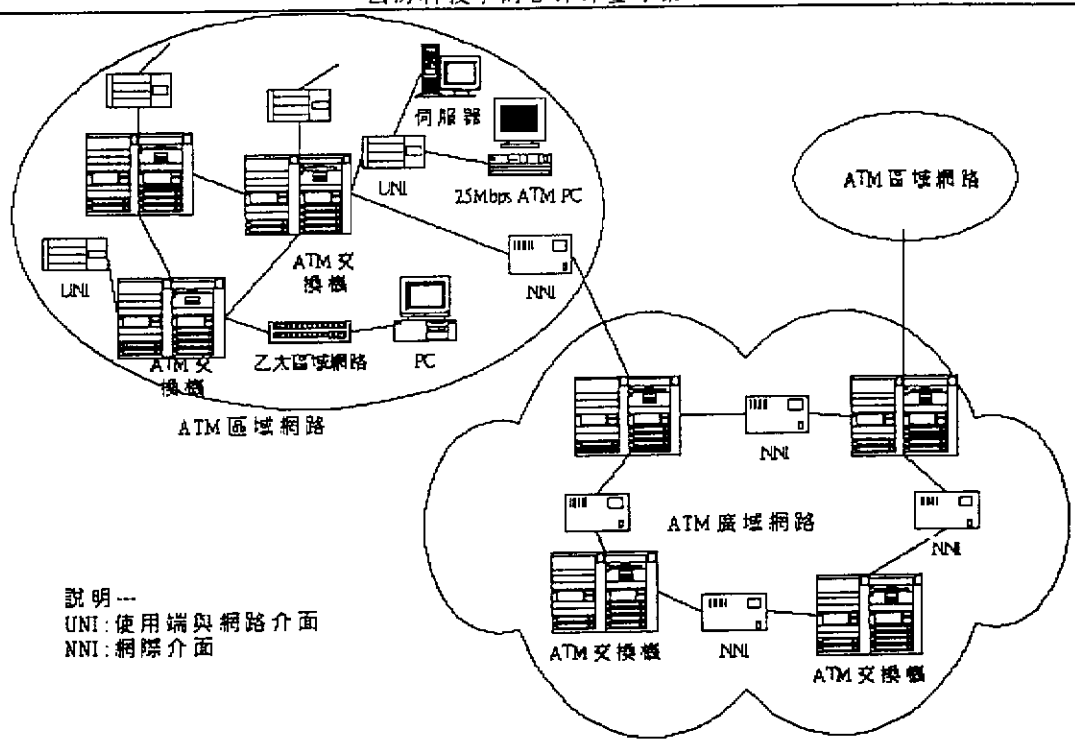


圖 2-7：典型的 ATM 網路拓樸

2.1.3.1 ATM 網路架構

ATM 網路採用固定大小 cell 封包(53 Bytes)的策略，使得 Switch 硬體設計更簡易、處理速度更快速，並可提供各類資訊網路 QoS 要求，滿足聲音、影像應用要求的低延遲、低延遲變化率的服務特性。此外，ATM 網路可使用的傳輸介質極廣，從 UTP、TP、同軸電纜、單模光纖至多模光纖等，彈性極大。

事實上，ATM 網路歷經多年的發展，目前已被 ITU-T(前身爲 CCITT)列爲寬頻整合服務網路 B-ISDN 的重要標準之一。ATM 網路的使用者至網路間介面(User Network Interface, UNI)可以分成以下兩種，一爲公用 UNI，它定義公共服務的 ATM 網路與用戶擁有的 ATM 交換機之間的介面；另一爲私有的 UNI，它定義使用者工作站與用戶的 ATM 交換機之間的介面。

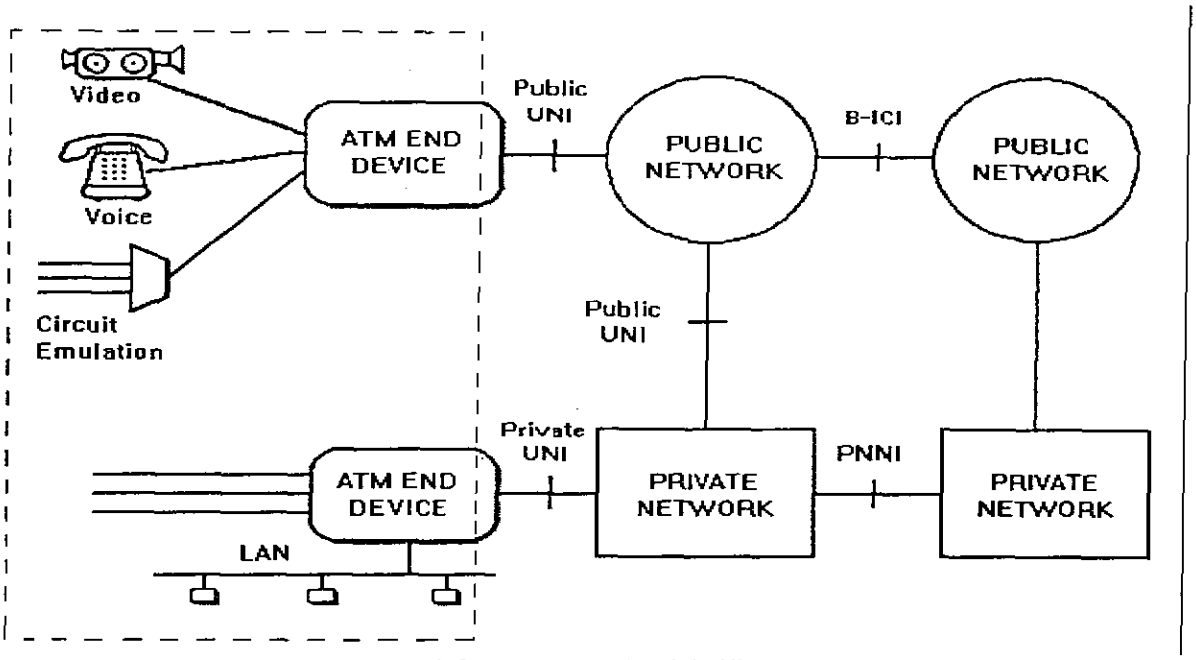


圖 2-8　ATM 網路架構

2.1.3.2　ATM 網路協定的層級架構

ATM 通訊協定的層級架構主要可分成三層，由上而下上分別是 ATM 調適層(ATM Adaptation Layer)、ATM 層(ATM Layer)與實體層(Physical Layer)，如圖 2-9 所示。

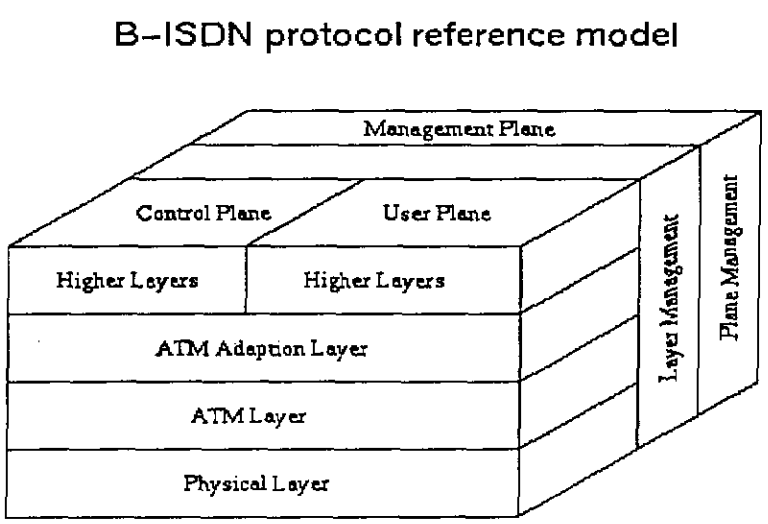


圖 2-9：ATM 網路層級架構

ATM 網路各層功能簡介如下：

2.1.3.2.1 ATM 調適層(ATM Adaptation Layer)

ATM 適應層協定在 ATM 層上提供一個轉換協定，使 ATM 網路能提供高層的服務如音訊，視訊與數據傳送。AAL 可分爲收斂子層(Covergence sublayer-CS)及切割和重組子層(Segmentation and Reassembly sublayer-SAR)，CS 子層又可分成服務指定(Service-specific CS)及共同部份(Common Part CS)。

2.1.3.2.2 ATM 層(ATM Layer)

ATM 層的功能包含有建立 cell 封包的標頭，標頭認證、多工與解多工，VPI 與 VCI 的繞徑轉換，用戶網路的流量控制等。

2.1.3.2.3 實體層(Physical Layer)

實體層提供的功能是在二個連接的 ATM 設備的實際傳輸媒體上傳送 ATM cell 封包。實體層分爲二個子層，分別是實際媒體相關子層(PMD: Physical Medium Dependent)及傳送收斂子層(TC: Transmission Convergence)。TC 子層是負責在實際傳輸媒體上將 cell 封包流量轉換成穩定的位元及位元組流量。PMD 子層則提供 cell 封包中每個位元真正傳送工作。

2.1.4 SMDS

Switched Multimegabit Data Service(SMDS)是一個高速的，封包交換，並以 datagram 爲基礎在公用資料網(PDNs)上使用來通訊溝通的廣域網路技術。SMDS 可以使用以光纖或者以銅軸爲基礎的傳輸媒體，而其速度可以超過數位訊號等級一(DS-1)的傳輸能力至 1.544Mbps 的水準，甚至可超過數位訊號等級三(DS-3)的傳輸能力而達到 44.736Mbps 的水準。除此之外，SMDS 的資料單位的大小亦足夠將整個 IEEE 802.3、IEEE 802.5 與 FDDI 的框架。

2.1.4.1 SMDS 網路元件

SMDS 爲了提供高速的資料傳輸服務，它包含了以下幾個元件。使用者端設備(customer premises equipment, CPE)、傳輸媒介，(subscriber network interface, SNI)，如圖 2-10 所示。CPE 是使用者端的終端設備，它通常是終端機、個人電腦、或者是路由器、數據機、多工器。傳輸媒介通常包含符合目前網路設備規格的高速廣域網路轉換器(switch)。這個規格通常定義了網路運作的方法，本地與遠端傳輸媒介的溝通介面與轉換器互相溝通的介

面。SNI 是 CPE 與傳輸媒介設備之間的溝通介面，它提供了將 SMDS 傳輸網路轉換到使用者端網路的技術與運作方法。

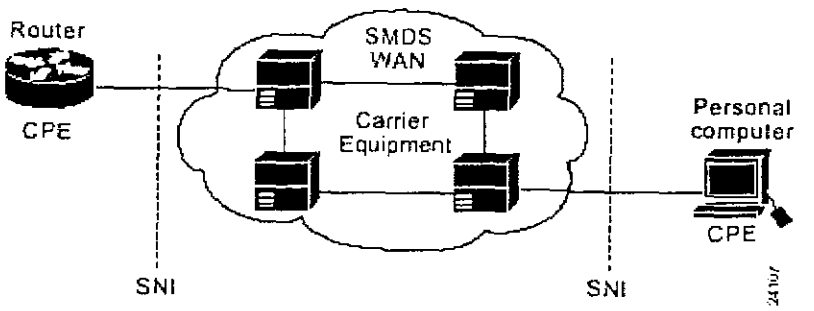


圖 2-10：SMDS 網路元件

2.1.4.2 SMDS Interface Protocol

SMDS Interface Protocol(SIP)是讓上節所述的 CPE 與 SMDS 傳輸媒介設備之間進行溝通的協定。SIP 提供無連接傳輸模式(connectionless)的服務透過 SNI 元件，讓 CPE 能存取 SMDS 的傳輸媒介設備，以上所述之關係如圖 2-11 所示。SIP 是依據 IEEE 802.6 Distributed Queue Dual Bus(DQDB)標準而制定的，這是因爲 DQDB 是一個公開的標準並且符合 SIP 的需求。

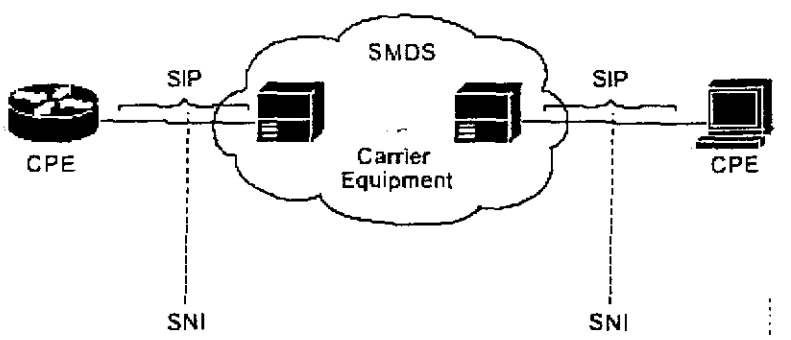


圖 2-11：SIP 與其他元件的關係圖

SIP 的架構總共分爲三層，SIP 第三層與第二層均對應到 OSI 模型的資料連結層，而 SIP 第一層則對應到 OSI 模型的實體層。其關係如圖 2-12 所示。

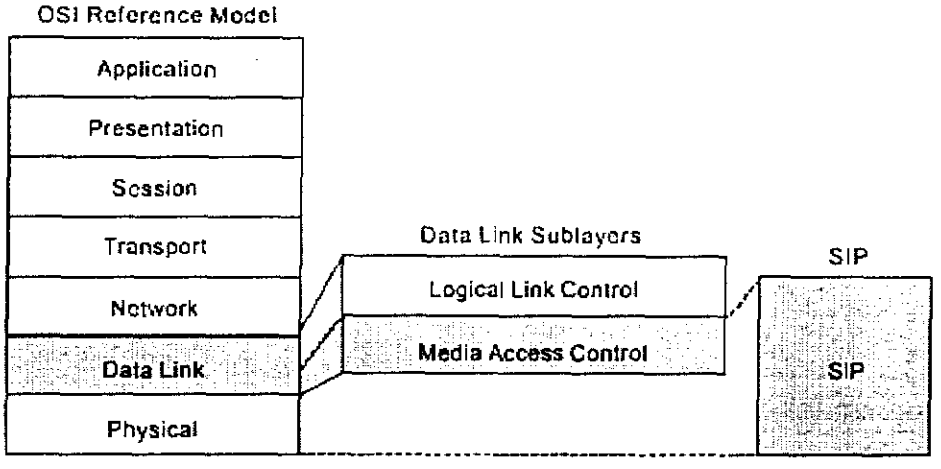


圖 2-12：SIP 與 OSI 模型的對應關係

2.1.5 SONET

自 1980 年代數位電話交換機帶給公眾網路的使用者與經營者莫大好處，而且光纖通信亦獲得大量運用，但由於缺乏統一標準，各廠商均自行推出產品，使得傳統同步數位架構（Plesiochronous Digital Hierarchy；PDH）的推展在網路上發生了一些問題，在此情況下，美國貝爾實驗室提出同步光纖網路（Synchronous Optical Network；SONET）概念，而 CCITT 以此爲版本訂定建議書，因其應用不只限於光纖網路，因此重新命名爲數位同步架構（Synchronous Digital Hierarchy；SDH）；一般而言，我們將 SONET 視爲北美規格，而 SDH 視爲世界標準規格。SONET 以同步數位傳輸方式與 SDH 的傳輸架構相容。

2.1.5.1 SONET 頻道規格

在北美，開始發展時速度爲 51.84Mbps 到 2.1Gbps。未來，將會達到 13Gbps。雖然在歐洲也使用相同的技術，但不採用 SONET 的架構，而是從 155Mbps(SONET STS-3)開始起算，此爲 SDH STM-1。且 SDH 是以 155Mbps 爲單位的。所以，任何 SONET STS 的編號除以 3 即是 SDH STM 的編號，例如，STS-48=STM-16。SONET 與 SDH 的頻道規

格對照表如表 2-1 所示。

表 2-1：SONET 與 SDH 之頻道規格

SONET	LINE RATE (Mbps)	OPTICAL	SDH (ITU-T)
STS-1	51.840	OC-1	
STS-2	103.680	OC-2	
STS-3	155.520	OC-3	STM-1
…	…	…	
STS-6	311.040	OC-6	STM-2
…	…	…	…
STS-*n*	*n**51.840	OC-*n*	STM-(*n*/3)
…	…	…	
STS-256	13271.040	OC-256	

2.2 網路架構模型

2.2.1 台灣學術網路架構

台灣學術網路(Taiwan Academic Network；以下簡稱 TANet)係由各主要國立大學及教育部，於民國 79 年 7 月起，所共同建立的一個全國性教學研究用之電腦網路。它的主要目的是爲了支援全國各級學校及研究機構間之教學研究活動，以相互分享資源並提供合作機會。TANet 具有骨幹(Back bone)和區域(Regional)的網路架構與研究相關資訊應用之基台(Information Infrastructure)。現行 TANet 骨幹之網路通信協定係以 ATM 爲底層，上架以 Internet TCP/IP 系列之協定爲主，區域網路中心或校園內依其需要支援其它多重協定之運作。民國 80 年 12 月教育部電算中心申請 64Kbps 數據專線，連接美國普林斯頓大學 JvNCnet 安裝完成，並可直接連通美國國家科學基金會網路(NSFNET)骨幹，並於 81 年 11 月將專線速率提升至 256Kbps，83 年 10 月提升至 512 Kbps，爲滿足使用之需求，緩和對國外連線速率緩慢之情況，84 年 10 月將速率提升至 T1(1.544Mbps)，85 年 5 月提昇至 2 條 T1，並將進入美國之連接點由東岸 JvNCnet 移至西岸之 GLOBAL-ONE。87 年 11 月擴充國際電路頻寬爲 T3(45Mbps)，其中教育部使用 24Mbps。關於台灣學術網路與國際 Internet 網路的關係如圖 2-13 所示。

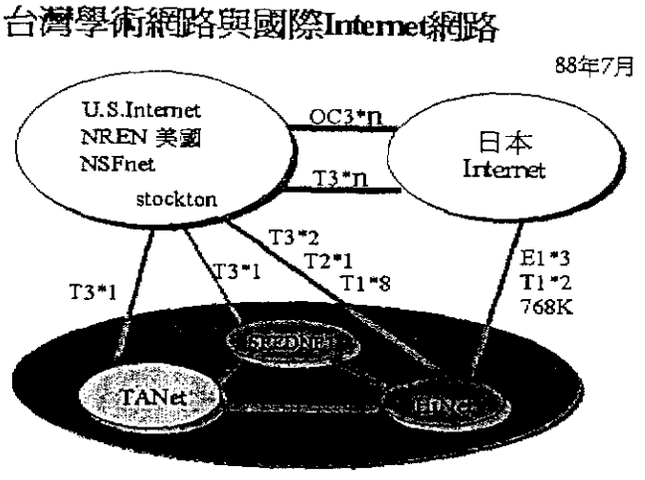


圖 2-13：台灣學術網路與國際 Internet 網路

TANet 國內骨幹網路由北到南，分別爲台北(教育部電算中心、台灣大學、政治大學)、桃園(中央大學)、竹苗(交通大學)、台中(中興大學)、雲嘉(中正大學)、台南(成功大學)、高屏 (中山大學)、花東(花蓮師院、東華大學、台東師院)等區域網路中心，以 ATM 交換器經由高速(T1 至 T3)線路連接，並包含骨幹必要之備援線路，各區域之鄰近學校及研究單位則連至各區域網路中心，其網路專線速度則視連線單位的需要自行決定。關於台灣學術網路骨幹架構圖如圖 2-14 所示。

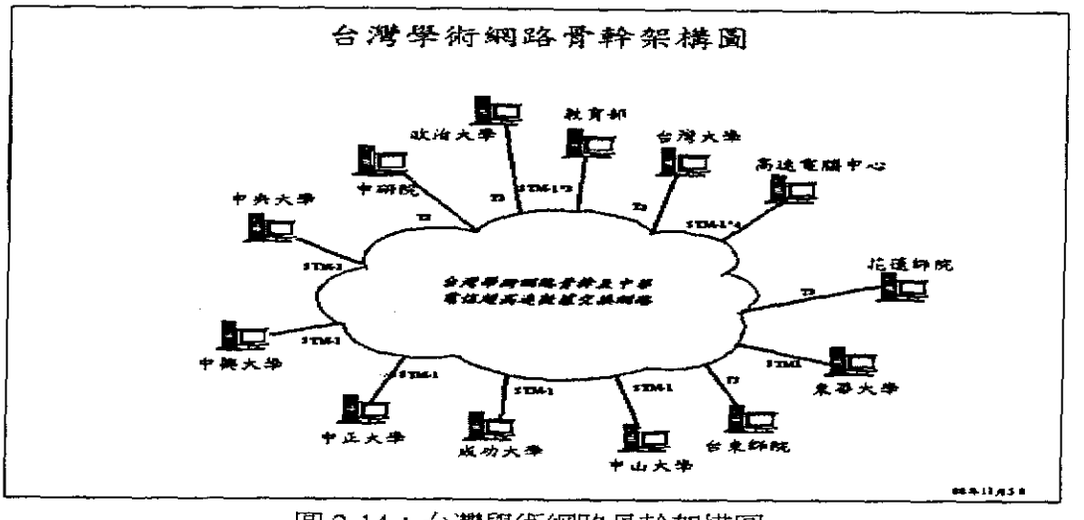


圖 2-14：台灣學術網路骨幹架構圖

2.2.2 台灣大學網路架構

台大校園網路原以高速光纖分散式網路（FDDI）爲主幹，但因網路使用量激增，於 1995 年 7 月開始高速網路 ATM 實驗平台之測試工作，於 1996 年 7 月將部分系統轉移至高速網路 ATM 實驗平台上實地運作。同時亦積極規劃台大高速網路之骨幹架構，並協助網路使用量較大之各系所單位將其既有之 FDDI 網路逐步昇級爲 ATM 網路。「台大校園網路寬頻化」第二期建置工程於 1999 年 7 月完成，並將台大網路環境正式提升邁入高速 ATM 寬頻網路。目前台大校園網路主幹已更換爲 ATM 的寬頻網路環境，網路普及率完成百分之百，涵蓋校總區、法、醫、社會及公衛等學院（包含各系所單位與男女生宿舍）。台大校園網路於 2000 年 11 月開始提供各系所與宿舍以 100MB 的速率連結校園網路，共計 118 個系所與 23 棟男女生宿舍，其餘少數系所與宿舍目前也計畫升級爲 100MB 的傳輸速率。目前台大校園網路的主幹由五台 Cisco 7513 路由器及二台 Cisco LightStream 1010 ATM Switch 所組成。每台 7513 路由器透過 ATM OC-3 (155Mbps) 連接到 LightStream 1010，路由器對外以 155MB 的速率連接，對內則提供各系所 100MB 的傳輸速率。至於 DNS 伺服器、Proxy 伺服器、NEWS 伺服器、蕃薯藤台大分站及和信寬頻皆透過路由器連上中心主幹設備 LightStream 1010，以提供全校教職員學生連線使用。再者，利用中華電信的 ADSL 線路，將所有使用者之流量集中於中華電信，再以一條 DS-3(45Mbps) 專線連接至校內的 LightStream 1010。爲了減輕經由教育部出國的 Proxy 流量，向中華電信租用一條 T1 直接連上 Hinet。醫學院及法學院校區目前也已從原先的 T1 升級爲 ATM OC-3，直接連到總區計資中心的 1010 設備。北區區網的所有連線學校及單位經由 Cabletron SSR8600 連接台大對外 7513 路由器，透過該路由器連接教育部電算中心提供之 LightStream 1010 ATM Switch，提供區網連線學校及單位更穩定的傳輸品質及完善的連線環境。各區網學校及單位透過該連線可直接連接至台灣學術網路（TANET / I1）。關於整個台大校園網路的架構圖如圖 2-15 所示。

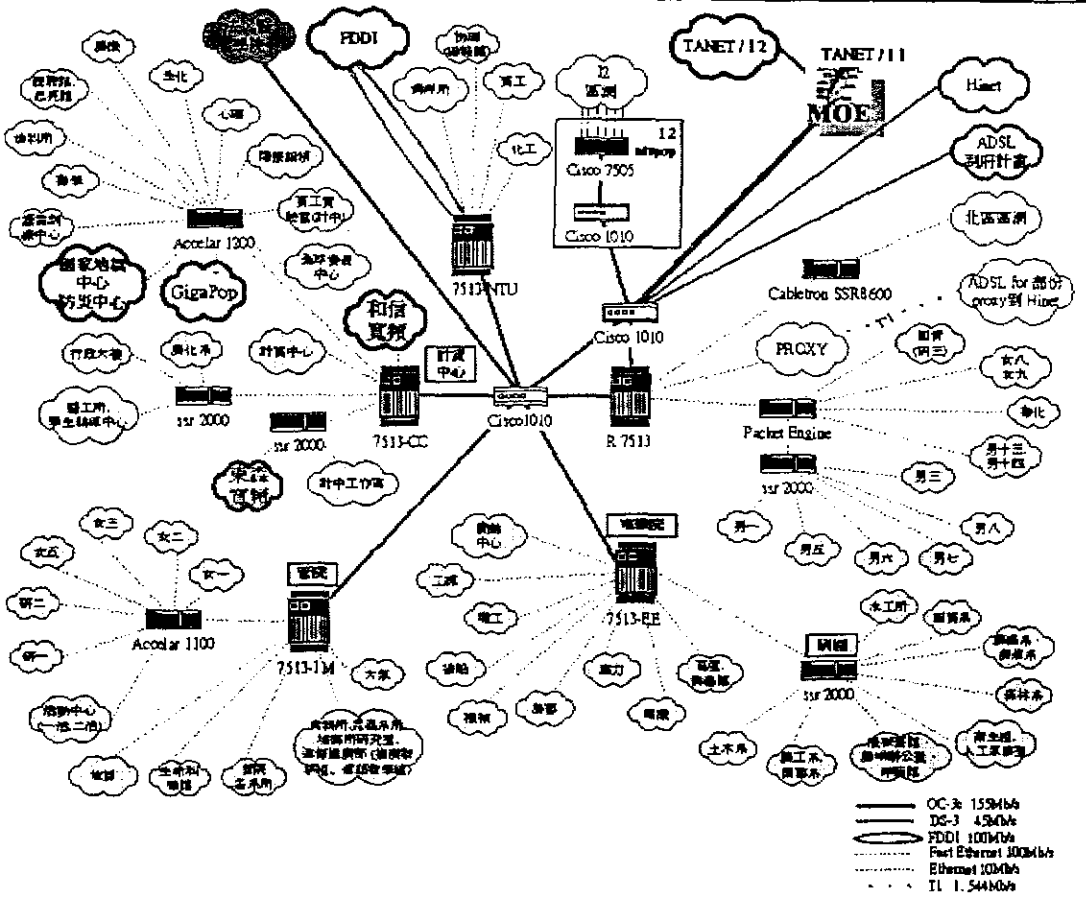


圖 2-15：台大校園網路架構圖

2.2.3 北京大學網路架構

北京大學校園網路的建設共經過三次階段：第一次是 1989 年的「中關村地區網」建設，第二次是 1994 年的「中國教育科研電腦網路示範工程」建設，第三次就是中國教育系統的「211 工程」的實施。「中關村地區網」是由中國國家計委投資，科學院、清華大學和北京大學共同承擔建設，由科學院院網、清華大學校園網和北京大學校園網三個院、校網通過光纜連結而成。透過「中國教育科研電腦網路示範工程」，北京大學成爲 CERNET 華北地區網路主節點之一，負責河北省、天津市的高校及北京市部分高校與 CERNET 的連接。1996 年，北京大學利用「211 工程」實施的機會，著手進行了校園網路更新改造工作。經過一年多的調查研究和思考，北京大學最後把校園網更新改造採用的網路技術定位於：全面採用交換網路技術和虛擬網路技術：主幹網採用高速的 ATM 技術，速率爲 622M，到一些主要樓群的速率爲 155 M（ATM）或 100 M（LAN 交換）；樓內採用 10Base-T 或 100Base-T 交換式乙太網路。

2.2.3.1　北京大學校園網路架構

北京大學校園網由網控中心、主幹網和各樓內的局域網組成。整個校園網採用一個 B Class IP 位址，按現在的設計目標，可以配置 255 個子網，連接 65000 多台電腦。全校共鋪設光纜 30 多公里。計算中心、圖書館和物理大樓三個主節點用單模、多模混合 14 芯光纖連成一個主幹環路。通過光纜將校內教學、科研和行政辦公樓群 50 多棟與校園主幹網相聯；另外位於中關園外的技物樓和位於上地產業開發區的方正研究院均通過 2Mbps 微波與校園主幹網相連。通過 PSTN 電話網與 800 多台家庭電腦撥號聯網。

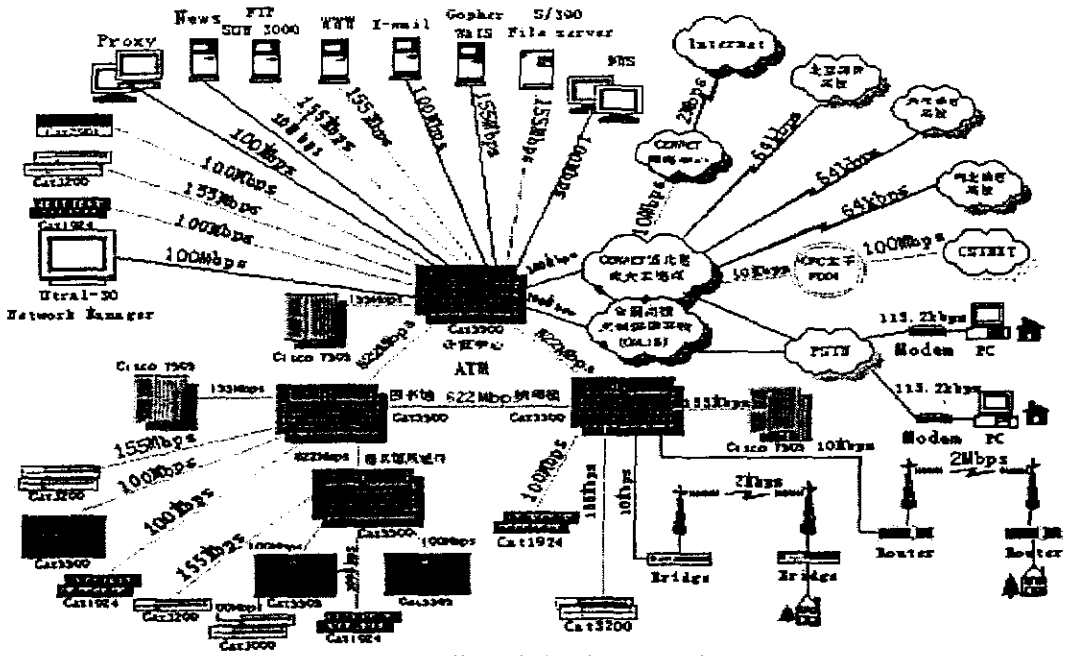


圖 2-16：北京大學校園網邏輯圖

北京大學在計算中心、圖書館和物理大樓三個主節點分別配置了一個主交換機 Catalyst5500 和一個路由器 Cisco7505，主幹網上運行速率爲 ATM 622M。主幹網到校內樓群的連接提供三種速率以供選擇：

a. 10Base-FL（乙太交換） 共 48 個埠；
b. 10Base-TX（乙太交換） 共 24 個埠；
c. 100Base-FL（快速乙太交換） 共 48 個埠；
d. 10/100Base-TX（快速乙太交換）共 60 個埠；
e. 155M/MM （ATM） 共 48 個埠；
f. 155M/UTP （ATM） 共 24 個埠；

北京大學的網路設備配置如以下所示：

網路管理系統：硬體平臺爲 SUN Ultra 30 一台，軟體平臺爲 HP Openview；硬體平臺爲 IBM RS/6000-41T 一台，軟體平臺爲 IBM Netview；

網路計費系統其硬體平臺爲 IBM RS/6000-390 一台；

網路服務器：DNS 伺服器－SUN 20 一台，SUN Ultra 1 一台；

FTP 伺服器－SUN 3000 一台；

WWW 伺服器、NEWS 伺服器－SUN 1000E 一台；

MAIL 伺服器－SUN 3000 一台，SUN 450 一台，SUN 1000E 一台；

PROXY 伺服器－SUN Ultra 30 一台，PC Pentium II 一台；

文件伺服器－IBM S/390 一台；

北京大學透過光纜以 100 Mbps FDDI 與中關村地區（NCFC）網路中心及清華大學校園網路中心相連；透過光纜以 10 Mbps 與 CERNET 網路中心相連；並分別透過 NCFC 的專線和 CERNET 的專線與 Internet 相聯。關於整個北京大學校園網路的邏輯圖如圖 2-16 所示。

2.2.4 清華大學網路架構

民國 77 年，清大參與新竹區大園光纖網路系統(FMAN)實驗計畫，並透過教育部連結上國際學術網路(BITNET)。並於民國 79 年開始建構全校性光纖網路系統，將全校各系所單位以光纖銜接，進而連接上台灣學術網路(TANET)及全球網際網路(Internet)。民國 80 年，清大校園光纖網路提升爲 100 Mbits 的 FDDI 光纖主幹系統，並建置完成全校性校園電子佈告欄系統(NetNews system)及 Domain Name system，提供完整之網際網路服務機制。民國 82 年，完成「學生宿舍區 FDDI 光纖網路系統」，將學生之宿舍網路與校園銜接。民國 83 年，以「紅外線無線通訊系統」隔空連接至國家高速電腦中心，作爲清華大學與交通大學校際光纖網路備援系統。民國 84 年，完成全國校園第一套校園光纖網路使用量計費系統。民國 85 年，以高速頻寬之 ATM Switch 連接上 TANET ，提供校際之同步遠距教學服務。民國 87 年，以 ATM Switch OC12 622 Mbits 連接至交通大學與國家高速電腦中心，協同建構新竹區高速光纖網路中心。民國 88 年，連接上 TANET/I2 研究網路，同年銜接上國家實驗網路(NBEN)。民國 89 年，進行校園光纖網路升級計畫，更新爲超高速交換式主幹網路。關於整個清大校園網路的架構圖如圖 2-17 所示。

國立清華大學超高速交換式校園主幹網路架構圖

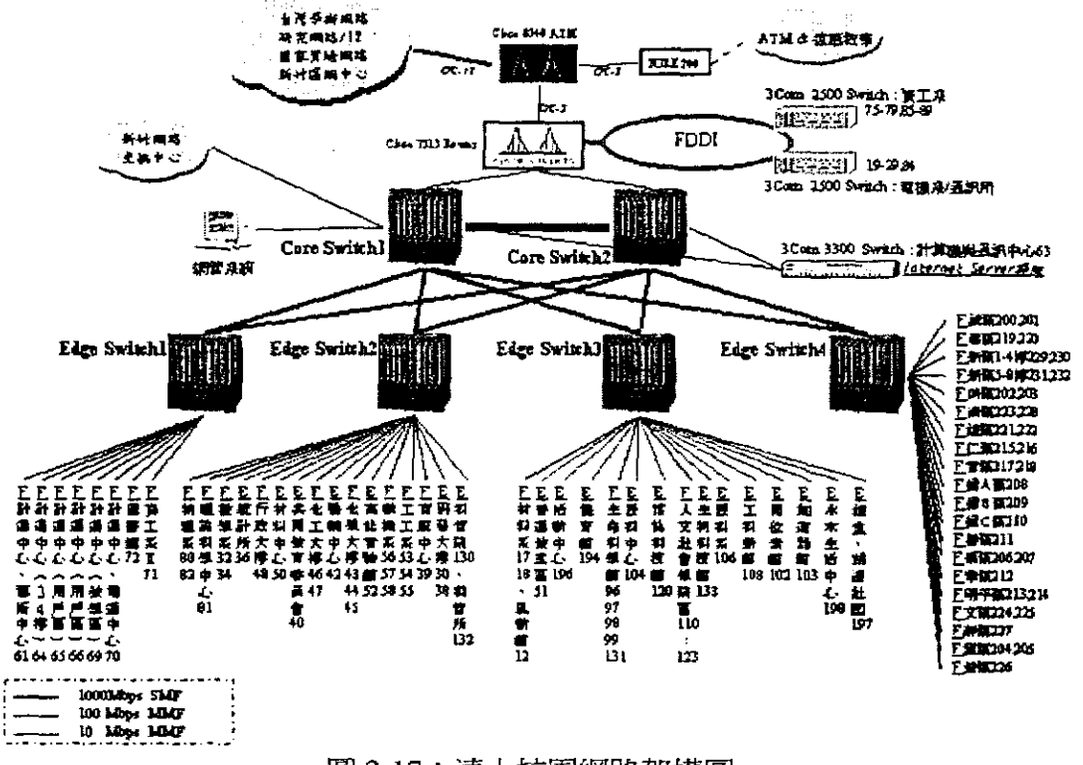


圖 2-17：清大校園網路架構圖

2.2.5 中央大學網路架構

中央大學利用校園光纖網路的建設，校內各樓館間直接互通，各系所皆有分散式計算環境的建置；校外和台灣學術網路連接，藉由與國科會高速電腦中心間的高速連線使用該中心的各種計算資源。中央大學目前計有多個 Netware 及 NT 網路檔案資料庫系統，對外電話撥接線路計有 155 線，所有的線號均具有大型 terminal/slip/ppp 的功能。關於中央大學校園網路的架構圖如圖 2-18 所示。

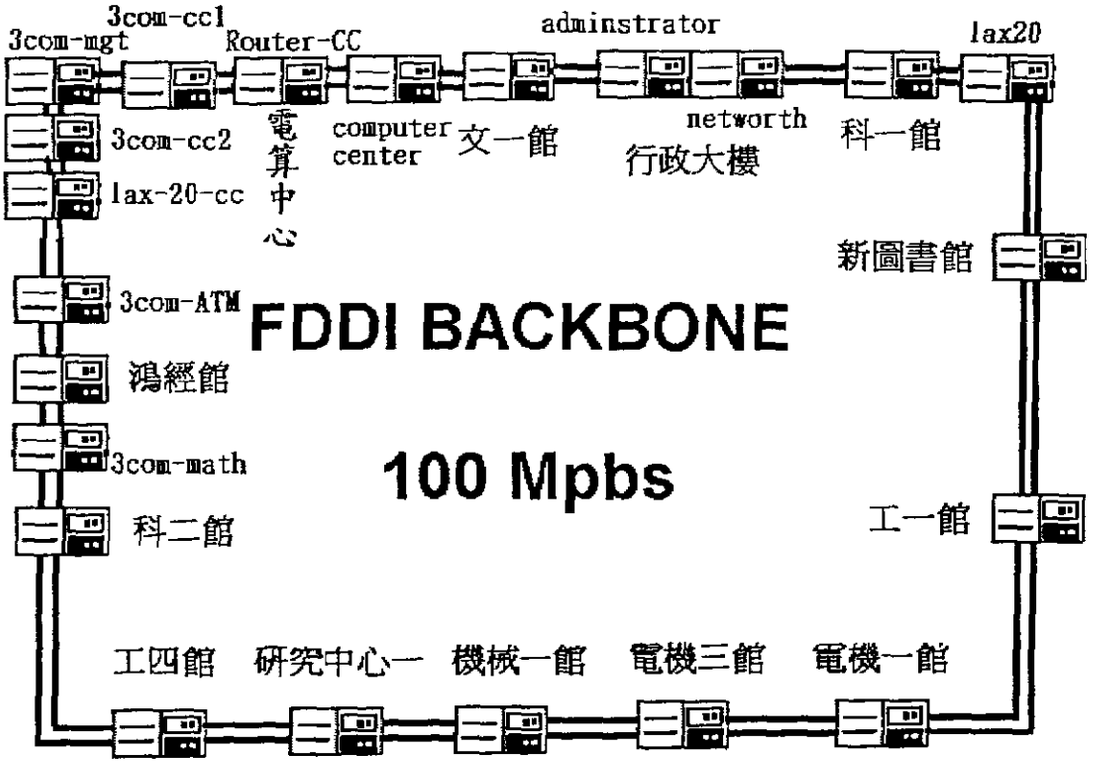


圖 2-18：中央大學網路架構圖

2.2.6 交通大學網路架構

交大新竹校園網路目前以光纖銜接兩校區，目前正計畫向四家固網承租台北新竹長途光纖，銜接台北新竹校區，使交大校園能夠藉助光纖網路之助跨越地理限制。交大新竹校區館舍幾乎均有光纖網路，各館舍佈放有 12 蕊多磨光纖連往十二個集中點，資訊館、木工房、綜合一館、管理二館、工三館資科系、工三館資工系、工四館、工五館、圖資大樓、電子資訊大樓、豪微米、竹銘館，上述十二個館舍再以單模加多模光纖連往資訊館與木工房集中。校內網路以 3com 9000 router 十二顆，以 400 個 fast ethernet layer 3 routing port 銜接各館舍，十二顆 router 以單模光纖以兩路 giga Ethernet layer 2 分別銜接到資訊館與木工房的兩顆 3com 9000 router。校內網路採分層管理，宿舍網路由計中規劃，學生社團管理，各系所研究單位，館舍對外網路由計中規劃管理，館舍內部網路由系所自行規劃管理，行政單位館內館外網路均由計中規劃管理。交大校內網路 IP 原採固定制 netmask 255.255.255.0，由於所剩 IP 不多，從去年中期開始陸續改用 netmask 255.25.255.224。校內 router routing 爲避免遭受網路攻擊，改採封閉系統，不接收也不傳

送 routing。 交大校內網路瓶頸在用戶端與學校對外兩點，網路規劃重點在積極開拓連外來源，鼓勵系所切割現有網路以提高效率。校內網路對外有多重出口。透過 cisco 6000 router 以雙回路 giga Ethernet 銜接 3com 9000 兩顆核心 3com 9000 router，銜接新竹網路交換中心。透過資訊館以 fast Ethernet 銜接 TANet2 新竹維運中心之 cisco 7500。透過資訊館以 fast Ethernet 銜接國家實驗網路新竹 giga pop NT500BH router。以 giga Ethernet 與清華大學 extrem 校內網路銜接。以 fast Ethernet 與國家高速電腦中心 cisco 6000 內部網路銜接。以 fast Ethernet 與 HiNet 銜接。透過 giga Ethernet 與 15 個其他 ISP 直接連線，其中以光纖連線的佔一半左右。以 ATM 155M 連接新竹縣、新竹市、苗栗縣教育網路中心。以 gaga Ethernet 連往新竹八個學術單位。以 T1 1536K 連往 30 個左右學術單位。關於交通大學校園網路架構示意圖如圖 2-19 所示。

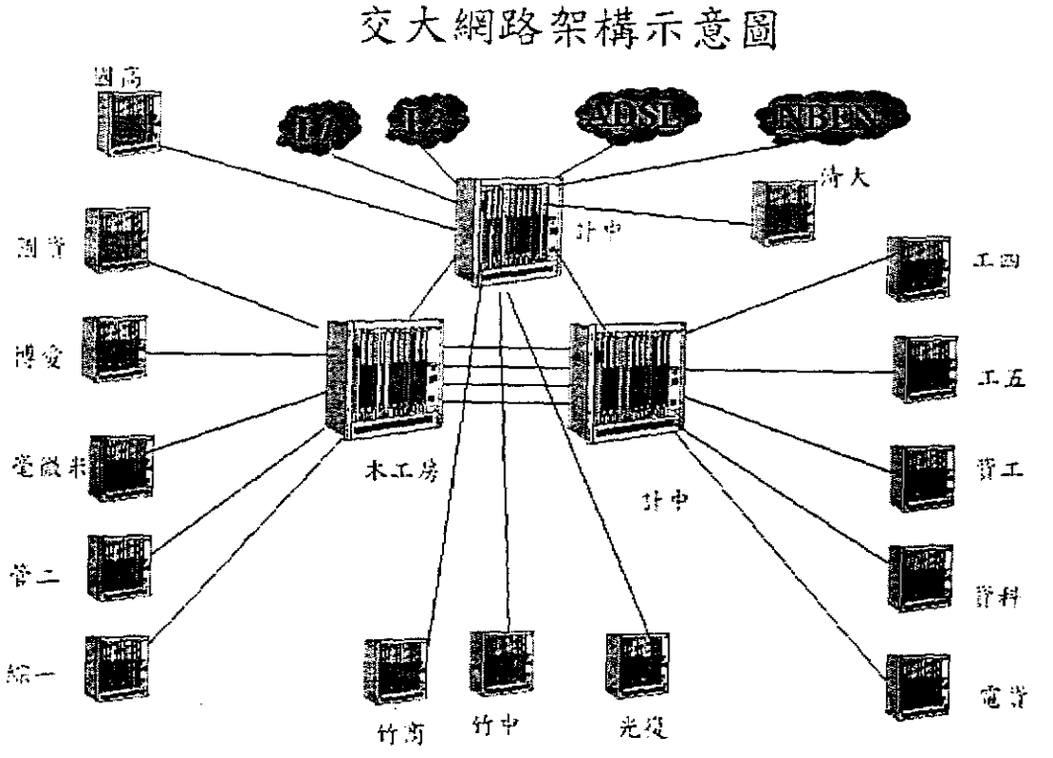


圖 2-19：交通大學網路架構圖

2.3 網路流量分析

只要有網路的存在，流量分析這個議題必須考量。有這正確的測量結果，不只可以監測整個網路的狀況，也可以比較容易地評估網路的效能。

2.3.1. 流量測量與分析的需求

維持網路正常的運作是網路管理者最主要的工作之一。誰是網路上的最大流量者，有任何不常用的應用程式佔用太多資源嗎？有哪些損壞的硬體正影響整個網路呢？正確的網路資訊可以幫助網路管理者完成他的任務。

一般而言，對於流量分析，我們可以考量以下幾點：

a. 監控網路的狀態並適時除錯。

b. 調整與計劃網路的架構。

c. 追蹤、探討與審查任何的異常事件。

2.3.2 流量測量與分析的方法

2.3.2.1 以監視爲基礎的系統(Surveillance Based Systems)

在以往的網路環境下，流量的量測分析都是透過乙太網路的監聽程式(sniffer, nnstatm, tcpdump)，利用乙太網路廣播(broadcast)的特性，在相同的子網路上架設工作站，即可監聽每一個傳遞的封包，隨後可以做進一步的分析處理。圖 2-20 展示了傳統的流量統計架構。

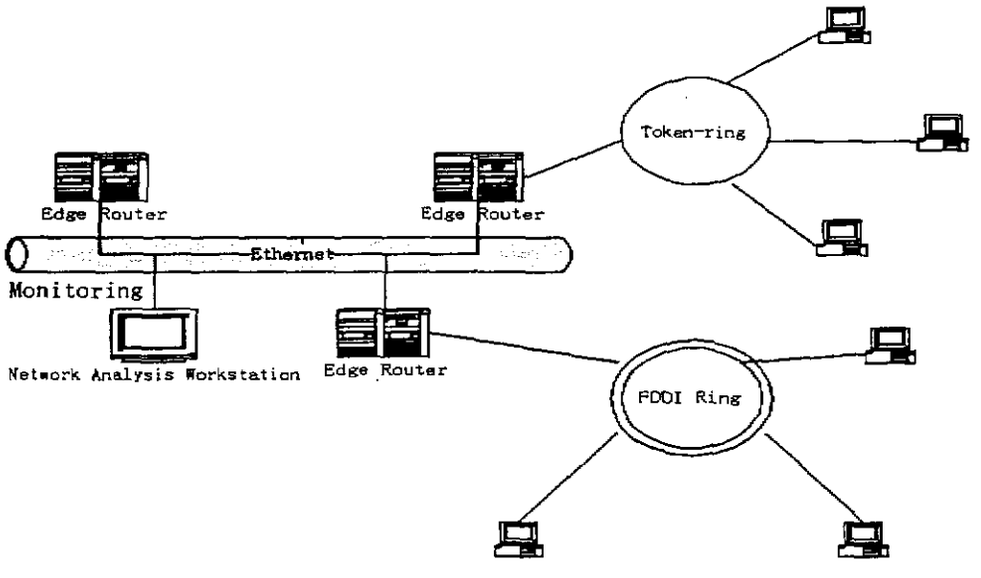


圖 2-20：傳統的 Ethernet 流量統計

然而在現今的網路架構下，這種網路監測方式會受到許多的限制，其中包括以下幾點：

a. 網路卡的接收能力：要監測網路流量，網路卡必須啓動 promiscuous 模式，然而一旦無限制接收封包，首先面臨的就是卡上面的 buffer 與系統 bus 是否可以接收大量湧入的封包資料，以 tcpdump 爲例，在網路負載超過 40%的情況下，開始會有 1%的 packet loss 情況。
b. 無法運作於 Switching Device 的環境下：現在的網路架構，傾向設置 switching device，以有效舒緩 collision 的困擾。但是 sniffer 在這個架構下除非 switching device 有提供 monitor port，否則將無法完全接收所有網路上的流量封包，因此將失去網路監控的作用。
c. 只適合運作於區域網路的環境：由於監測系統是利用完全監聽的概念，所以可以在區域網路的環境架構下正常運作，但是對於廣域網路的專線模式，例如 ATM、HDLC、PPP 等協定，一般來說，sniffer 將無從下手。

2.3.2.2 以 SNMP 爲基礎的系統

現在的網路設備通常都有提供 SNMP(Simple Network Management Protocol)的功能，而網路管理者則可以透過 SNMP 讀取 MIB(Management Information Base)以進行網路流量的動作。

2.3.2.3 SNMP 概述

SNMP 是由 IETF 所發展出來的一項簡單的網路管理協定。這項協定可以當作是一種可以提供以及轉換網路元件之間的管理信息的一種機制。SNMP 爲應用層協定，它可以收集、交換網路裝置間的網管資訊，例如各裝置的資料傳輸率、例外事件等。圖 2-21 爲一個 SNMP 簡單網路管理協定架構圖。

爲了能夠監督所有的網路裝置，SNMP 採用的管理方式爲集中式的管理方法(SNMP 第二版已將分散式管理的觀念納入其架構中)，透過一個網路管理者(SNMP Manager)監督所有的網路裝置，每一個被管的網路裝置必須有一個代管器(SNMP Agent)與網路管理者溝通訊息，如果所要管理的裝置本身沒有代管器，那麼這個裝置便需要一個 Proxy Agent。Proxy Agent 同網路管理者之間的溝通方法，與一般代管器同網路管理者之間的溝通方法並無差別，差別僅在於所交換的資訊，Proxy Agent 是設計來讀取本身不具備代管器裝置的相關網路訊息，再利用這些訊息與網路管理者溝通，而不論是代管器或 Proxy Agent，都可以硬體或軟體的方式存在，不受限制。

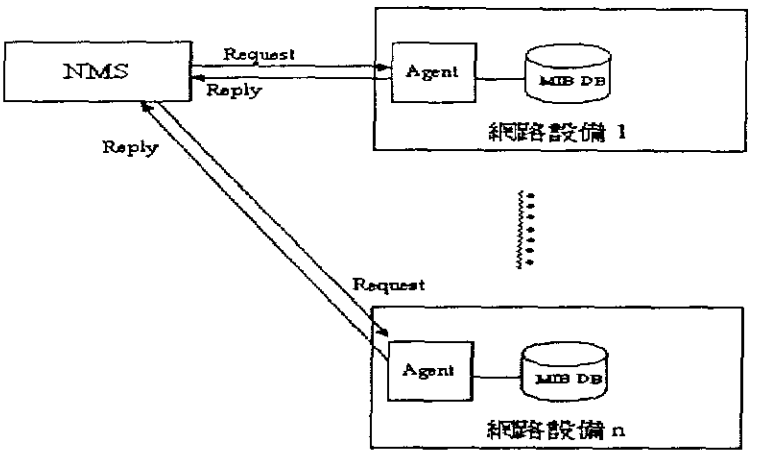


圖 2-21：SNMP 簡單網路管理協定架構圖

網路管理者與代管器間的互動關係中有三種模式可以選擇，第一種模式是主動偵測(Polling-Directed)模式，這種方式完全是由管理者主控，定時去偵測網路中每一個裝置的連通狀態以及讀者相關資訊。這種方式的優點是管理者掌握全部的資訊，可以提供管理者最詳盡的網路資訊，當初 SNMP 即是選用這種方法；而其缺點爲管理者必須逐一對所有的裝置定時進行偵測，如果時間間隔太短，會造成 SNMP 封包在網路上所佔的比例太高，影響網路正常的運作，若時間間隔太長，所得到的結果不足以表現出網路中的即時狀況。

第二種模式是自動回報(Trap-Directed)模式，這種方式與主動偵測模式正好相反，它是由代管器自行在裝置發生異常時，發出回報(Trap)通知管理者。這種方式的優點是造成的網路流量小，可以即時回報網路裝置的狀態；但是有一個很大的缺點，就是當網路裝置異常時，所發出的回報並不能保證管理者一定會收到，此外，SNMP 標準的回報(Cold Start、Warm Start、Link Up、Link Down、Authentication Failure 與 EGB Neighbor Loss)並不足以表示所有的狀況，大部份裝置需要使用到自訂的回報(Enterprise Specific)，而這些回報需要各廠商專屬的網管系統，才能得到最適當的問題解釋。第三種模式是自動回報偵測(Trap-Directed Polling)模式，它所採取的方式是在一開始時先對所有裝置進行偵測，然後間隔一段較長的時間才會重新偵測所有裝置，而這段時間內由回報來反應裝置的異常狀態，算是一種折衷的方式。這種模式的優點是可以節省相當大的網路流量，也可以減少代管器所需要的回應負擔。此法爲 SNMP 第二版所選用的方法，正符合網路

管理原則－盡量不使代管器負擔太多的工作。

SNMP 爲了能達到對管理資訊結構的彈性與延展性，於是定義了管理資訊結構(Structure of Management Information; SMI)，將管理物件的資訊定義爲固定的模式，透過對 ASN.1 的語法定義，各個系統之間的管理資訊得有一個共通的標準結構，而其資料架構方式則是以「樹」的方式展開，以達到階層化、彈性結構的需求，如圖 2-22 所示。

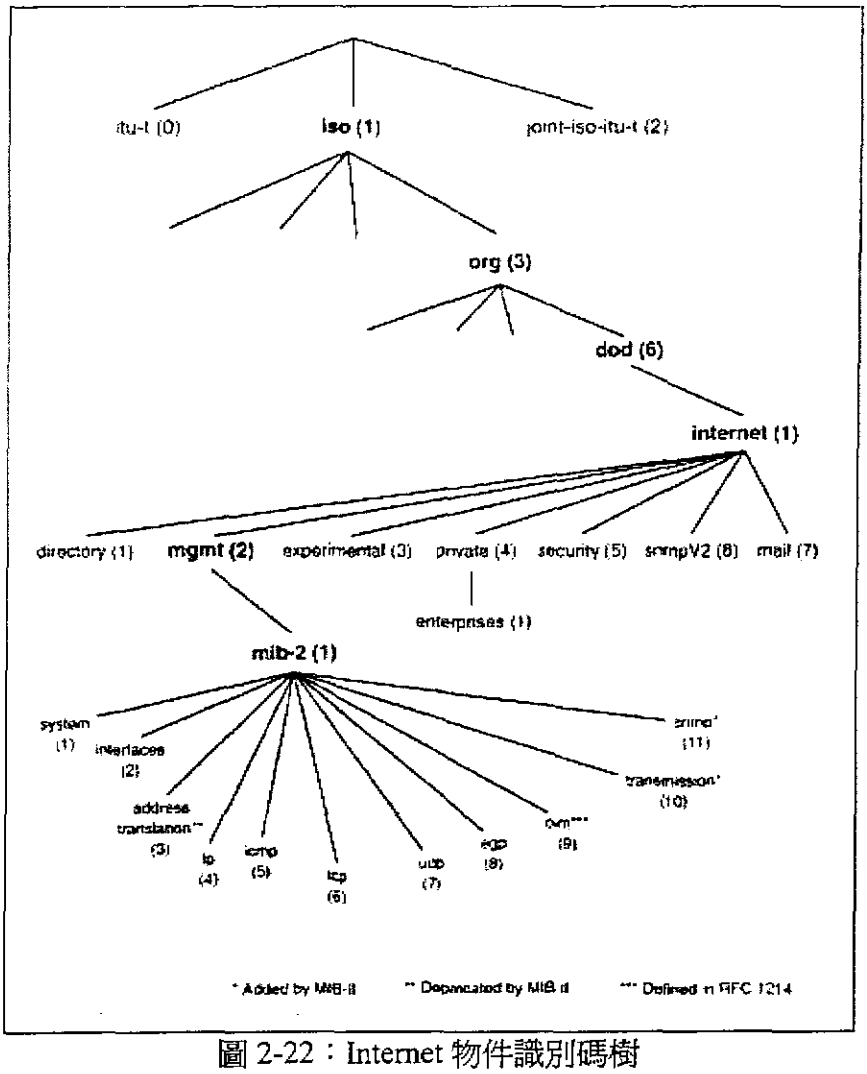


圖 2-22：Internet 物件識別碼樹

SNMP 定義的是通訊協定之標準，透過 SMI 對管理資訊的語法定義，各種網管系統可以將相關的管理物件資訊定義在一個管理資訊庫(Management Information Base ;MIB)內。MIB 可分爲標準的以及自訂的，標準的 MIB 會定義在 RFC 中，例如 MIB-II、Host MIB；

而 MIB-II 定義網路裝置的介面相關資訊等，Host MIB 則定義一台主機所應具備的資訊。對於不同的網路裝置，各家廠商可能會根據其裝置的特有性能來定義自訂 MIB(Private MIB)，因此，MIB 是 SNMP 中管理網路的重要依據，且爲管理者與代管器資訊溝通的依據。

SNMP 是以 UDP 架構爲主所發展出來的網管系統，「力求簡單」是 SNMP 的設計原則，因此被現今大多數的網路裝置所支援。事實上，SNMP 原本只有定義出五個基本指令(Protocol Data Unit;PDU)，以提供管理者與代管器進行溝通，這五個指令分別是：Get、GetNext、Set、GetResponse 以及 Trap。Get 是管理者向代管器要求傳回一筆資料；GetNext 是管理者向代管器要求傳回目前這筆資料的下一筆資料，這指令非常適合用在當管理者所希望得到的資料是不固定筆數時，一般爲裝置的即時資料，如路由轉換表；Set 是管理者向代管器要求設定該裝置的狀態或相關資訊；GetResponse 是指當管理者下達 Get、GetNext 或 Set 指令時，代管器使用這項指令作爲回應；Trap 是指代管器發現裝置有異常狀況時，主動回報管理者的指令。 由於 SNMP 原本提供的五項指令並不能符合現有之需求，因此，SNMP 第二版除了原有的五種基本指令外，還新增了可傳輸大量資料的 GetBulkRequest，以及與管理者間通訊的 InformRequest。

2.3.2.4 RMON

RMON (Remote Monitoring)可說是 SNMP 的加強版，由於 SNMP 在進行網路管理時需針對每個網路節點設備一一輪詢(Polling)，因此在進行網路區段（LAN 或是 Subnet）的管理便相當困難，容易造成網路的壅塞或是管理端過重的工作負荷，因此 RMON 的目的便是要達成分散式遠方監控網路管理的功能。RMON 的基本概念上則是讓被管理端的 MIB 資料能在「當地」便進行收集與分析，之後只要將彙總的結果傳送給管理端即可；而 RMON 的實際做法是在每一個網路裝置 RMON 代理器(RMON Agent)，並利用 SNMP 封包將 RMON Agent 所處理與收集的資料傳至網管系統，因此網管系統便可以直接取得遠端網路裝置的狀態，而由於 RMON Agent 先行將原始資料處理之後才傳送至網管系統，因此不僅避免未處理的大量資料在網路上傳輸，也減少了網管系統處理相關資料之負荷，不過因爲 RMON Agent 處理相關資訊仍需要使用 CPU 與記憶體，因此 RMON Agent 大部份仍是以獨立的機器來運作。

RMON MIB 是由九個物件群組所構成(如圖 2-23 所示)，每個物件群組都有各自的物件屬性：

a. 過濾群組：提供了一緩衝區，以便接收進來的封包或符合使用者自行定義過濾規則的封包。
b. 統計群組：可提供簡單的使用狀況、錯誤等統計數據，像送出封包數、廣播次數或載波碰撞等數據。
c. 歷史群組：根據統計群組中的資料與使用者需求，可進行不同的趨勢分析
d. 主機表群組：儲存每個主機的基本資料，包括廣播次數、多點傳播次數、錯誤封包數、送出與接收封包數目。
e. 排名群組：包含排序後的主機統計數據，像是提供前三名最忙碌的節點。
f. 警告群組：可以設定取樣的間隔時間和發生告警之上下限。
g. 封包擷取群組：可設定啓始與停止封包擷取的條件，調整緩衝區的大小等。
h. 事件紀錄群組：紀錄事件，如當超過發生警告上下限時將該事件紀錄下來。
i. 流量數據矩陣化群組：可將使用與錯誤資訊處理後整理成矩陣格式，用來比較任意兩節點的狀況。

RMON2 則加強對實體層(PHYSICAL LAYER)的流量資料收集。

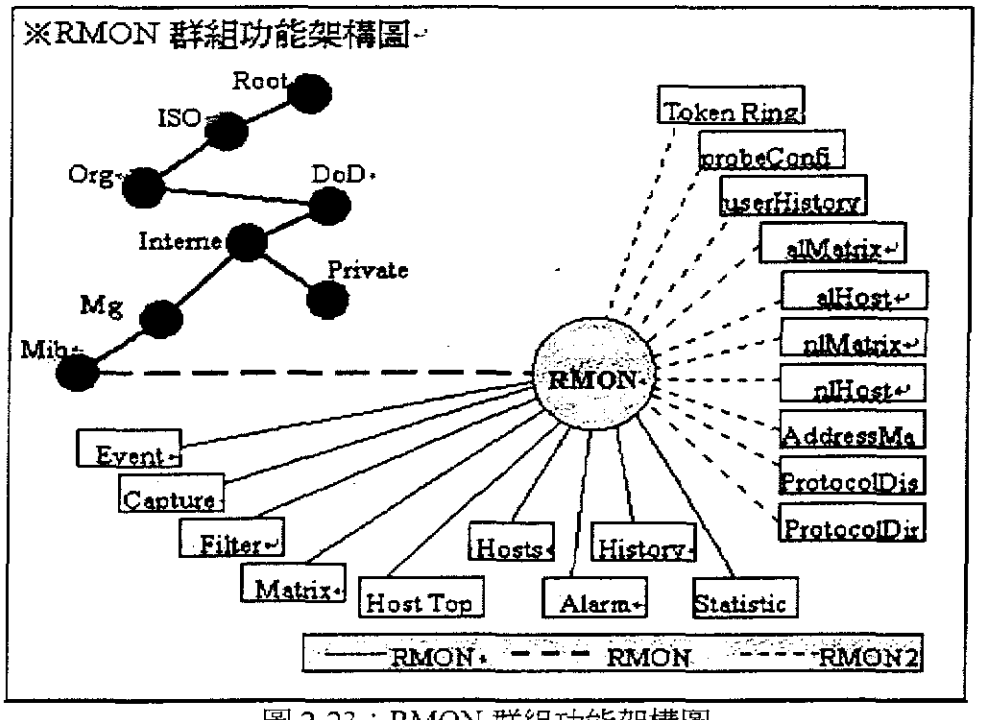


圖 2-23：RMON 群組功能架構圖

2.4 網路壅塞分析

自從一九九一年美國 NSF(National Science Foundation) 解除 Internet 商業用途的禁令之後，Internet 每年的使用人數及產業規模都以倍數成長的方式快速增加。但是真正開創 Internet 發展契機的敲門磚卻是九三年 NCSA 所推出的 Mosaic(第一套 Internet 瀏覽器)，之後至一九九五年底，網景的 Navigator 更把 Internet 熱潮推向另一階段的高峰。

由各種統計調查的資料顯示，全球 Internet 使用者人數以及連網主機都在快速成長當中，依據偉士林國際公司在九六年七月份的估計，全球大約有四千二百萬個使用者；而連網主機的部份，依據網路鬼才公司(Network Wizard)在同一時間的估計也將近一千四百萬台，未來兩者都將持續以高成長的比例成長。

由於 Internet 成長過於快速，目前網路遭遇到一些阻力，包括：

2.4.1 骨幹網路(Backbone Network)的頻寬不足造成嚴重的塞車

由於用戶數快速的增加，而 ISP 增加頻寬及線路的速度趕不上用戶增加的速度，網路壅塞已成爲全球普遍的現象。以全球 Internet 的最大市場－美國爲例，由於業者彼此激烈競爭，爭相擴建更快速的網路，目前骨幹網路已大多由 T3(45Mbps)更新爲 OC-12(622Mbps)。這種骨幹網路的舖設，技術上沒有太大的困難，假以時這個問題應可逐步改善。

2.4.2 接續網路 (Access Network)的頻寬也不足

這也是目前網路應用與服務所遭遇到的最大問題之一。解決網路壅塞，除了擴充網路頻寬的方法外，在現行架構中也有許多關於壅塞控制的機制與方法，主要有以下幾種：

2.4.2.1 Window-based congestion control

傳送端必須維持一個控制網路壅塞的視窗(congestion window)，而還沒有確認(ACK)回來的封包的序號(sequence number)必須在此壅塞視窗內，唯有符合壅塞視窗內條件內的封包才可以由傳送端這邊傳送出去。控制網路壅塞的視窗會因網路壅塞情形而調整。通常如果 ACK 正常收到會調大壅塞控制視窗，若是發生 ACK 無法在限定時間回來，則會調小壅塞控制視窗並調大限定時間值(timeout)，以避免太多太快的因爲超過限定確認時間因而重送的封包。

2.4.2.2 Network indicated congestion control

若網路發生壅塞(例如某一 router 的 buffer 大於某一 threshold 值)，則網路層協定可以採取以下兩種方法：

2.4.2.2.1 Forward Explicit Congestion Notification (FECN)

將通過壅塞節點(如 router)封包內的標頭(header)設定一個壅塞旗標(congestion indication flag)，當此封包到達接收端時，接收端便知道網路發生壅塞，再由傳輸層協定決定如何通知傳送端。ISO CLNP 與 ATM 均採用此方法。

2.4.2.2.2 Backward Explicit Congestion Notification (BECN)

發生壅塞時，必須要讓傳送端知道並降低其傳輸速度，所以在封包通過一壅塞的節點時最好是由此節點送給送端一個「通知壅塞」的控制訊息（choke packet）。ICMP 的 source quench（type=4，code = 0）就是用來通知送端壅塞的控制訊息。其運作流程大致如圖 2-24 所示。

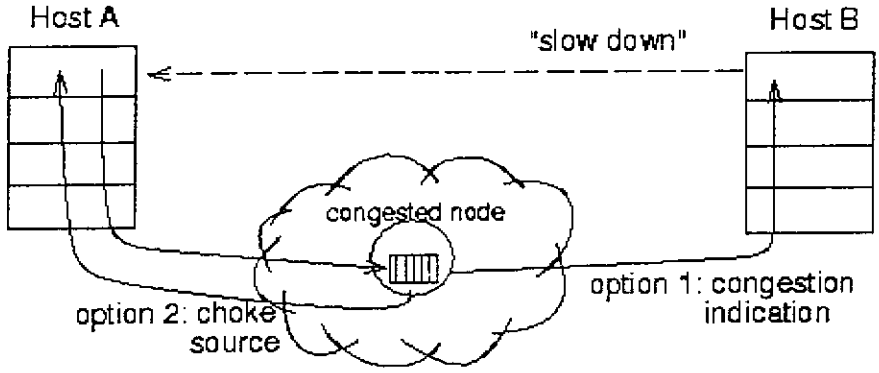


圖 2-24：Network indicated congestion control

FECN 因需收端再通知送端，所以通常反應速度較慢。而 FECN 與 BECN 均需網路層協定的幫忙也破壞了原來每一個 layer 是獨立自主的模組的的原則。

2.4.2.2.3 Rate-based source regulated congestion control

在高速網路中(如 ATM)如果利用網路的回應(feedback)訊息來通知傳送端網路壅塞在反應時間上稍嫌太慢。例如在 1 bits 的網路上傳送一個 225 bytes 的 packet 只要 1 μsec。如果 feedback 訊息要一秒才傳回送端，則此時送端可能以多送出一千萬個 packet 了。所以傳送端與接收端必須在建立連線時便商量好傳送速率，則我們可以利用 Leaky bucket 的方式在一定限制以下控制傳送端傳送封包的速率。其運作機制如圖 2-25 所示。Leaky bucket 主要的運作機制如下：

a. 每一個封包均需拿到一 token 才可以送出。
b. token 產生速率是 r，這也是傳送端傳送封包的平均速率。
c. token 沒有用的可以先存在 token bucket 中但此 bucket 最多只能存 b 個 tokens。
d. 在時間[t, t+a]中最多只能送 b+ra 個封包。

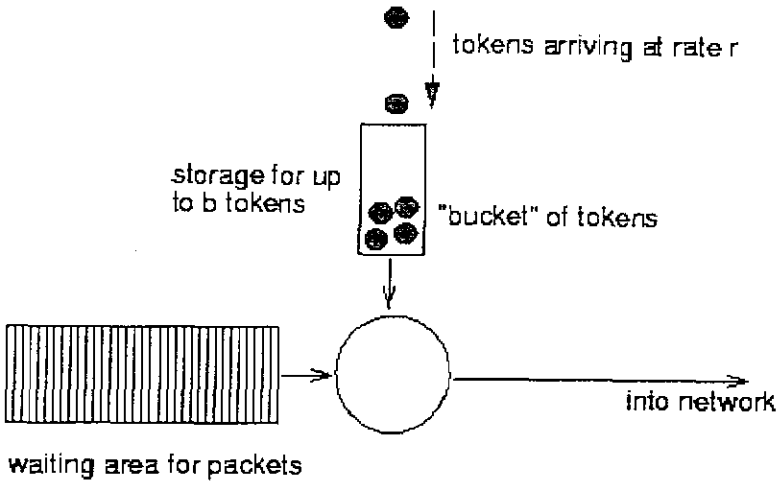


圖 2-25：Leaky bucket 的運作機制

2.4.2.2.4 Congestion Control by Buffer Preallocation

網路壅塞的發生的原因也有可能是因爲 buffer 太滿了，所以要避免網路壅塞可以從 buffer 著手。這個方法是在傳送端與接收端建立連線的時候，就在其路徑上的每一個節點的 buffer 均預留固定的空間給這連線使用。如此，只需送端依事先約定的速率傳送，每個節點上的 buffer 不會因其他連線的影響而不夠用。此方法最大的優點是連線間不會互相干擾，大量送資料的連線只會造成自己壅塞，不會影響別的連線。此方法的缺點是缺乏 multiplexing gain，造成網路效能較低。

2.5 網路繞送路徑分析（最佳控制點選擇）

繞送路徑的策略與選擇，是網路管理問題中相當重要的一環，尤其是繞送路徑的正確率會對網路流量與效能造成極大的影響。通常我們在分析繞送路徑的好壞會對網路頻寬的浪費、建立連線的時間、路徑的正確率、和路徑重建這幾個議題進行分析。

一般而言，繞送路徑的選擇可分爲靜態或動態繞送法。所謂靜態繞送法屬於非調整性的演算法，它依據網路節點流量與分佈的統計結果進行繞送路徑的選擇；而動態繞送法屬於可調整性的演算法，它同樣可依據網路分佈流量分析來決定繞送路徑，但是它會視目前的網路資訊改變路徑。關於路徑的繞送方法，目前主要有以下幾種方法：

2.5.1 氾濫式繞送法

氾濫式繞送法不需要有繞送目錄，當一有資料要傳送時，就以氾濫式的方法，將資料傳送給網路上所有的節點。這種策略雖然有助於傳輸容錯率但傳送資料時會造成大量且不

必要的資料流量。

2.5.2 最短路徑繞送法

所謂最短路徑繞送法，固名思義就是找出網路連線的最短距離路徑。距離的計算方法可以依據封包跳躍的次數、實際距離的長短等各種方法來評估「距離」的參數與向量。這是最簡易的路徑繞送方法，但是選擇的路徑卻未必是最佳，可能會有傳輸瓶頸與不可靠路徑的產生。

2.5.3 最少流量路徑繞送法

最少流量路徑的策略是依照目前測量的網路流量狀況，建立流量最少的路徑。測量網路流量的方式因不同的通訊協定而異，而即時的流量測量還可搭配歷史的統計資料，如此可以平衡網路的負載，提高網路頻寬的使用率與確保傳輸所需的品質。

2.5.4 最小耽擱時間路徑法

最小耽擱時間路徑法是以最早到達的路徑爲優先選擇。可以說是最短路徑與最少流量路徑法的組合，因爲最早到達的路徑可能是最短路徑或著是最少流量路徑，也就是所謂的平均較佳路徑。

2.5.5 距離向量繞送法(Distance Vector Algorithm)

每個路由器需維護一個繞送表，該表格記錄路由器本身至其他路由器的已知最佳距離，以及到達目的地需要使用那些線路。距離的計算方式可能有跳躍次數、封包延遲時間、佇列的數目、或其他計算的方式。路由器並定期與其他路由器交換表格資訊。假設以封包延遲時間當作距離的計算方式，且路由器已知鄰近路由器的延遲時間，則每隔固定時間，每個路由器會送給鄰近路由器一個含有對每個目的地預估時間的串列，而根據這些串列進行運算，路由器就可以找到最佳預估值，然後將這最佳預估值和其相對使用的線路置入繞送表中進行更新。距離向量繞送法的優點，就是步驟很單純，可以很輕易地實作出來。但其缺點是，若網路的拓樸有了改變，就需要花費較長時的時間交換資訊才能導出最佳路徑，而在這個過程中，很有可能形成所謂的繞送迴圈(routing loop)，造成網路資源的浪費。目前採用距離向量繞送法的繞送協定中，最爲人知的爲繞送資訊協定(Routing Information Protocol)。

2.5.6 鏈結狀態繞送法

鏈結狀態繞送法(Link State Routing)是目前較常使用於網路上的繞送演算法，其包含以下五個基本步驟：

a. 探查鄰近路由器的位址：路由器在每條點對點的線路發出一特殊的封包，線路另一

端的路由器則回應告訴它是誰。因爲每個路由器有唯一的網路位址，因此以這種方式判定並不會有名稱不一的問題。

b. 計算線路的延遲時間或成本：要計算線路的延遲時間，最基本直接的方法是由路由器利用線路發出一特殊的封包，線路的另一端收到封包後立刻送回，依據來回時間除以二，即可得到一個延遲時間的估計值，當然爲了求出較佳的結果，可多做幾次測試後取平均值。

c. 建立鏈結狀態封包：當蒐集好需要交換的資訊後，每個路由器建立一個含有所有資訊的封包，該封包包含傳送端的序號、時間、與一組相鄰串列，相鄰串列紀錄該路由器到達其鄰近路由路所需的時間或成本。建立鏈結狀態封包的時機可以每隔一段時間建立一次，或是當特殊事件發生如線路或路由器損毀與修復等。

d. 散佈鏈結狀態封包：散佈鏈結狀態封包的方法是利用洪氾法，而封包中的「序號」與「時間」這兩個欄位則用來控制這些分佈出去的封包，避免其因路由器或網路的損壞而讓封包無止盡地在網路上傳播。

e. 計算新路徑：一但路由器收集了完整的鏈結狀態封包，即可利用演算法，建構所有可能的最佳路徑，並將其演算結果放入繞送表中。

鏈結狀態繞送法雖然比距離向量繞送法要複雜，但是它避免了繞送迴圈的問題，因此可以有比較快的繞送速度。目前採用鏈結狀態繞送法的協定較有名的爲在 TCP/IP 上的開放式最短路徑優先協定(Open Shortest Path First)。

2.6 斷線備援路徑選擇

隨著網路傳輸速度及使用頻寬的提昇，連帶使得網路故障對使用者及網路服務提供者所造成的損害亦與之劇增。因而，網路故障回復在網路世界中變成是一項不可或缺的功能。一般而言，斷線備援的策略可分爲以動態需求與事先定義兩種備援方式，其基本比較如表 2-2 所示。

表 2-2：動態需求與事先定義的比較

備援方式	動態需求	事先定義
資源	低	高
彈性	高	低
管理成本	低	高
訊息複雜度	高	低
復原速度	慢	快
最佳化	低	高

動態需求備援方式提供高彈性的路由路徑選擇當網路發生斷線的情形，相對地事先定義的備援方式則提供快速與簡單的

2.6.1 Automatic Protection Switching

在寬頻網路中因爲每秒能傳遞的資料量很大，一但網路出現問題，相對地也會出現很大量的損失，因此斷線備援的恢復時間非常重要。要讓備援恢復的時間減到最少，可以採用自動保護轉換(Automatic Protection Switching, APS)的機制，這個機制使用預先計畫，選擇點對點的備用路由。自動保護轉換機制有兩種基本的架構，1：N自動保護轉換機制架構是在N個網路通道中，建立單一的保護通道，一但任何一個網路通道出現問題，這一個單一的保護通道就可以藉由通道轉換控制器迅速備援有問題的網路通道，如圖2-26所示。

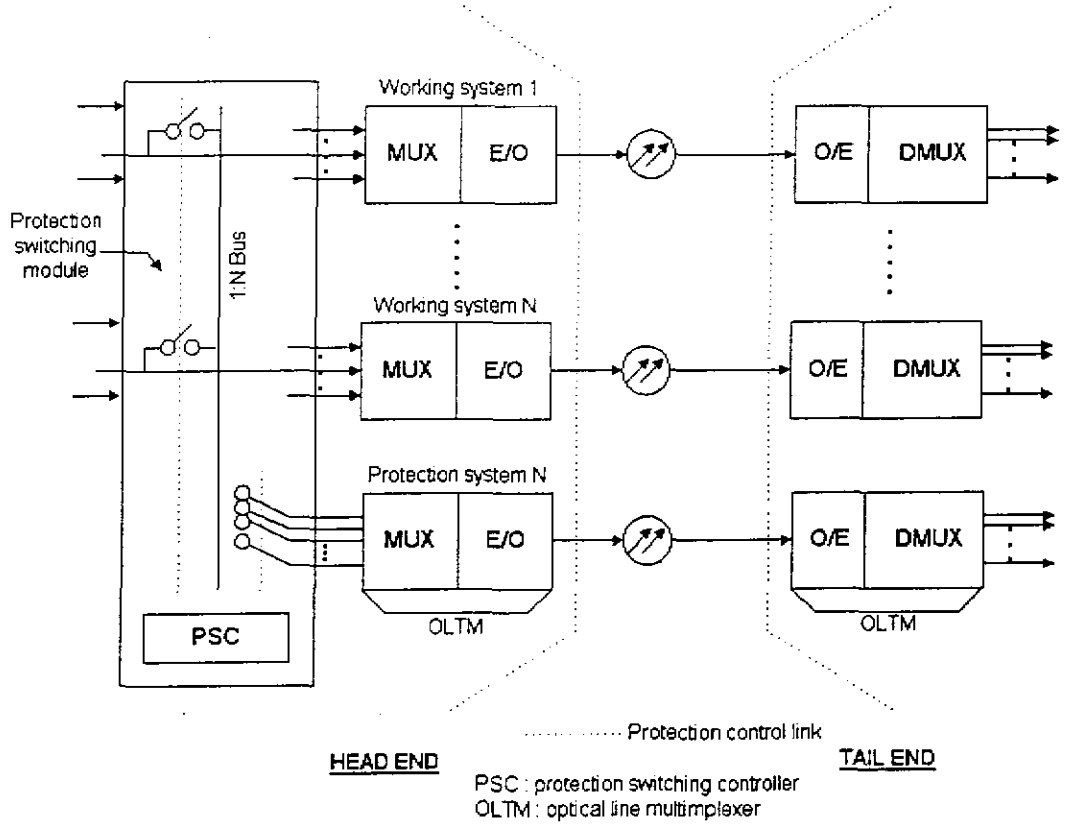
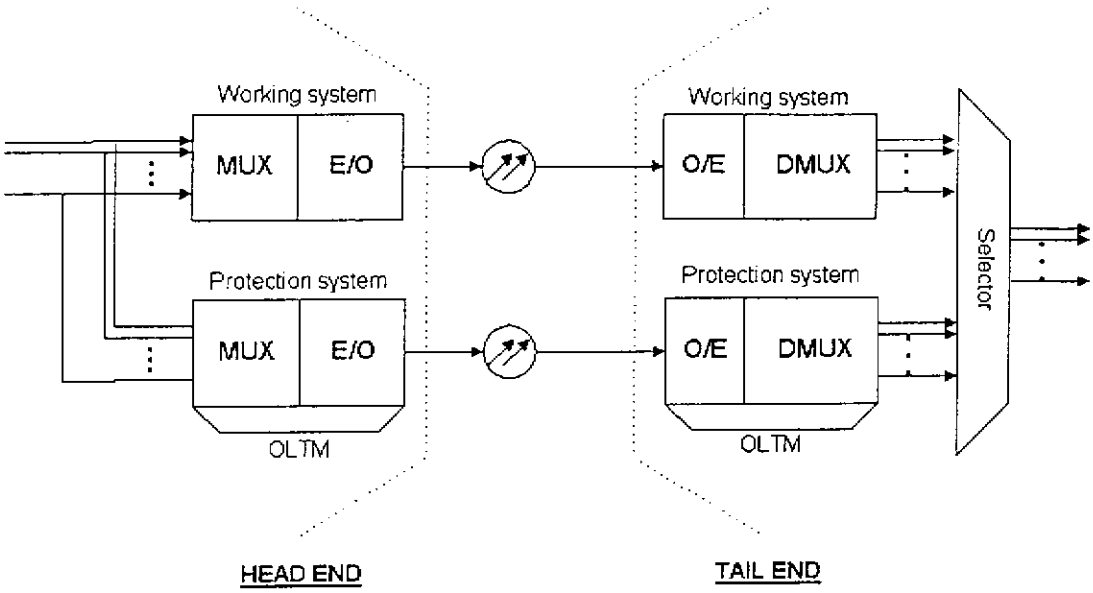


圖 2-26：*1:N APS architecture*

另外一種自動保護轉換機制架構是 1+1 的保護轉換架構，每有一個網路通道，就有一個

保護通道的建立，如圖 2-27 所示。自動保護轉換機制必需對整個網路的路由與能容納的流量有一個完整的規劃與了解，如此才能發揮其應有的功能。



PSC : protection switching controller
OLTM : optical line terminating multimplexer

圖 2-27：*1:1 APS architecture*

2.6.2 Self-healing Rings

一個能自我恢復的環狀網路，它包含了上到下(add-drop)的多工轉換器，讓網路發生問題的時候，可以進行反向的路由轉換，以達到線路備援的目的。利用這種方式可以增加網路的存活率並降低成本。其架構如圖 2-28 所示。

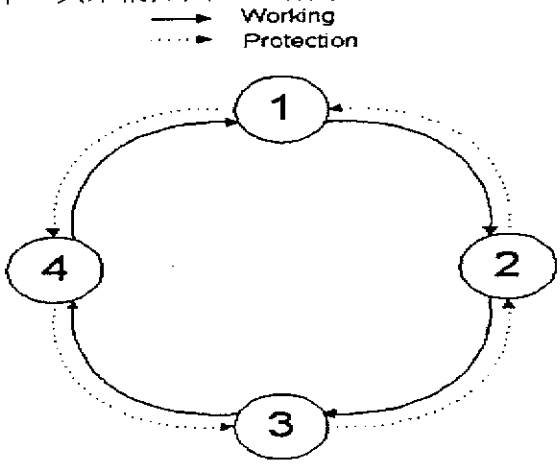


圖 2-28：*Self-healing Rings*

2.6.3 Network restoration

有許多斷線備援的機制都適用在一般的網路環境中，這些方法可以依照控制的機制而區分爲集中備援控制與分散備援控制，可以依照重新路由的方式區分爲 link based 與 path based，除此之外，也可以依照電腦計算的方式區分爲預先計算與及時運算。圖 2-29 顯示了以上所述三種形式的重新路由繞送方式。

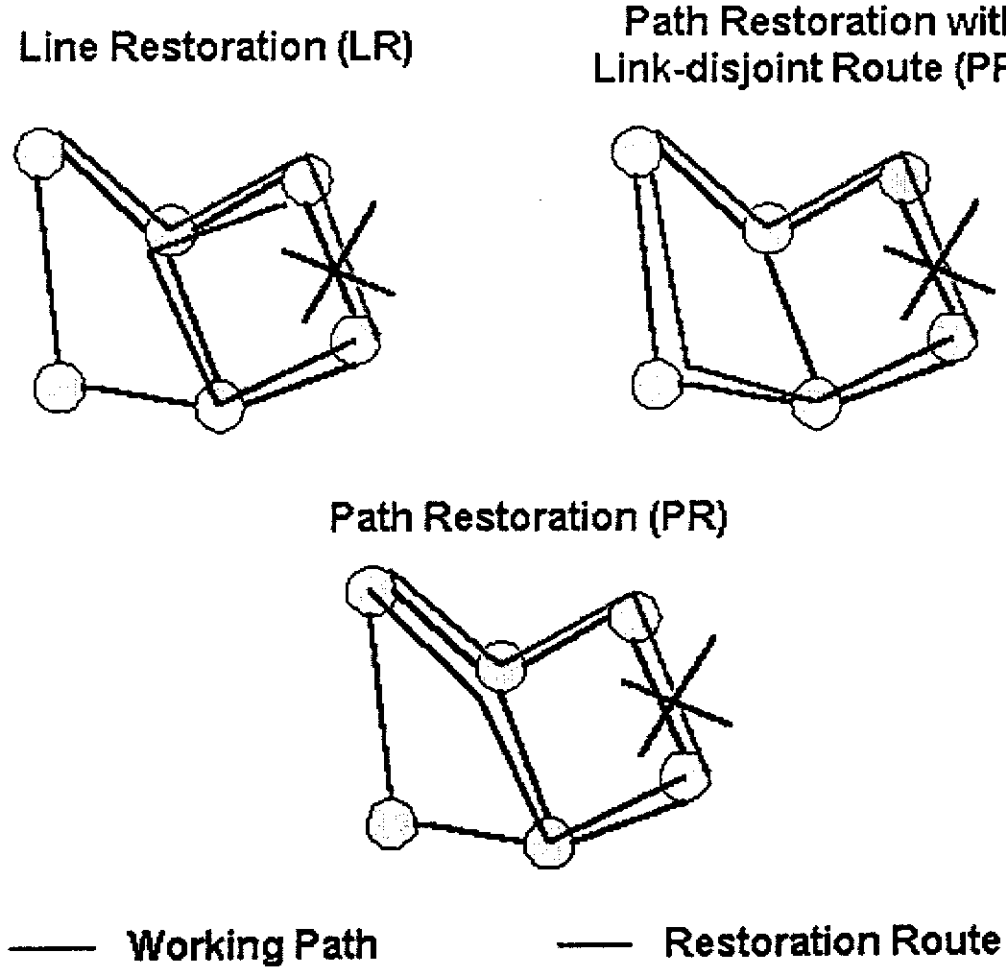


圖 2-29：*Three classes of network restoration by the type of rerouting*

3. 研究設計

3.1 網管工具分析準則

3.1.1 前言

網際網路大量的使用人口使得各式各樣網路系統與設備分散在各處，網路管理範圍變得更加廣泛，由於各廠商設備所支援的標準與規格不盡相同，使得網路上各種資源更加難以統一管理，尤其是各廠牌網路管理系統與其平台相依性很高，對於一個網路管理者而言，要管理這樣一個複雜的網路環境是很困難，網路管理工作不但要能快速了解網路環境最新狀況，也要能對各種網路設備作監控與管制，一旦網路發生問題時，才找出問題所在並且快速解決。網路環境由於機器並不是全部集中於同一地點，一旦發生問題，網路管理者常需花費甚多時間去找出真正發生問題的機器，然後才能開始去排除障礙。面對上述問題，若可有效運用相關的網路管理系統，將可協助網路管理者利用這一套管理方法針對網路上之各種機器設備加以規劃、監控和管理，進而能追蹤記錄網路上異常狀況，使得網路管理者能夠即時處理問題。此外亦可以進行長時期的資料蒐集，供分析網路使用成效，以提升網路服務品質。因此如何選擇一套合適的網路管理系統工具爲 2001 年企業公司網路的核心所在。認識及選擇網管系統工具之前，必須先了解「網路管理」到底是什麼？所謂的「網路管理」包括了哪些管理項目究竟使用了哪些標準協定？其實從字面上來看，可以知道網路管理就是要來管理網路，也就是經由網路管理系統，透過標準的通訊協定，與連接在網路上的各種不同設備做資訊交換，以取得這些設備的訊息、組態，藉以達到管理的目的。舉個例子來說，透過網路管理系統，我們可以知道接於網路上的設備其目前的硬體配備、網路流量、目前使用的狀態、CPU 及系統資源使用率並且可以畫出網路地圖、橫條圖、網路流量曲線圖及其他充滿資訊的圖形等。若軟體配合的恰當有些路由器或是智慧型的大型交換器或集線器，甚至可以針對某個有異常流量的埠做適當的處理；如關掉該埠或重新對該埠做起始動作，以維護整個網路的順暢及正常使用。除了負責管理整個網路秩序外，也負責網路的問題預防、網路設備的組態管理、網路效能管理和安全管理等。而這些網路種類則包括了一般的區域網路、廣域網路、現今流行的網際網路等，甚至一些專屬式的網路也都涵括在其管理的範圍。爲了達到上述的功能，一個網管系統基本上可以分爲四大部份：(1)通訊協定（Protocol）：負責網管系統與網路設備之間的通訊。(2)管理功能（Management Function）：提供網管系統的管理功能。(3)資料庫（Database）：有系統地儲存網路管理的各項資料。(4)圖形化人機介

面（Graphical User Interface；GUI）：提供圖形化人機介面，如圖 3-1 所示，簡化網路管理者的操作方式。

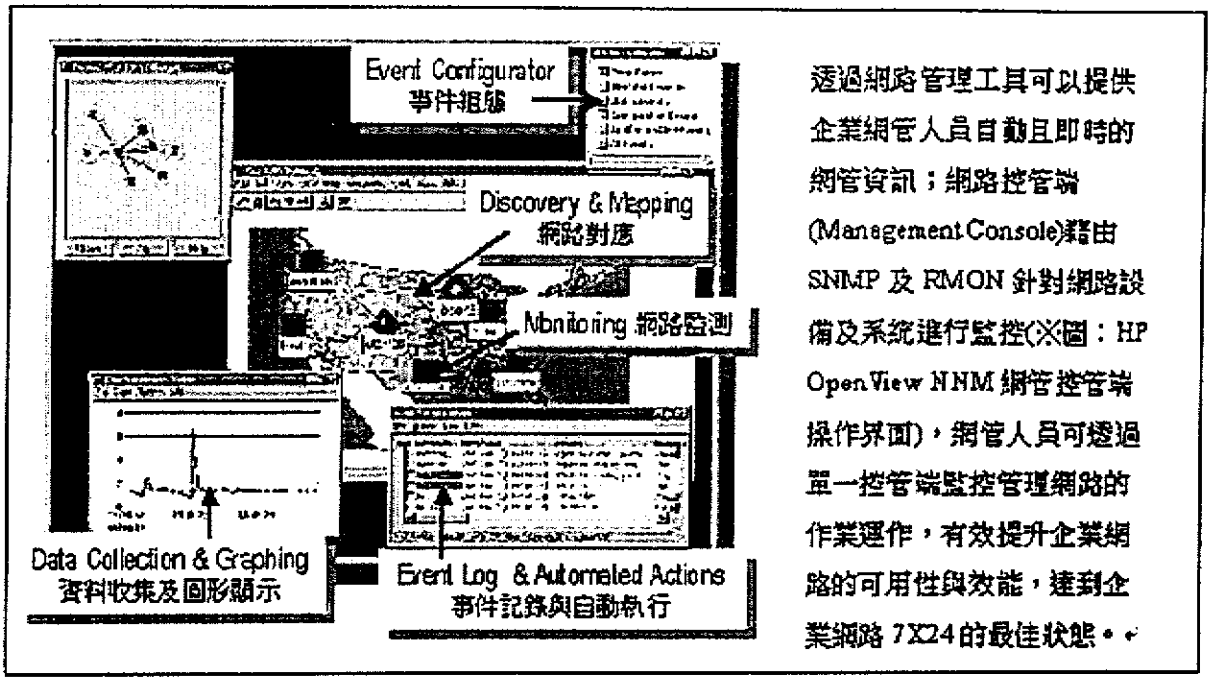


圖 3-1：HP OpenView NNM

3.1.2 如何選擇網管工具

企業公司在選擇網路管理工具時，當然得針對實際的需求才具有實質的效果與意義；此外，對於網路管理工具的考量上，也必須考量到企業網路未來的發展，否則因應每一次的成長而更新網路設備及管理工具是相當不划算的；所以，企業在選擇網路的建置及網管規劃時，最好能尋求具有專業網管技術團隊的顧問。不過企業對於網路管理工具的選擇建置上，可針對網管工具的使用性、功能性、價格性、整合性、延展擴充性、管理含括範圍、網管作業平台等方面來評估，市場上各廠牌的網管工具各有其著重的部份，網管工具較不同於一般系統軟體，因此企業在網管工具的選擇上必須謹慎。本章我們將以網管工具的標準面、功能面、價格面、市場面來分析比較目前一些較常用的網管工具，例如：Tivoli Platforms、HP Openview、CA Unicenter TNG、SunSoft SunNet Manager、Intel LANDesk、HP OpenView ManageX、HP OpenView、Microsoft SMS 及 Novell ManageWise 等等。

3.1.3 網路管理系統的標準分析

談到網路系統的管理，我們就談談網路管理上重要的組成要素(表 3-1)以及再來說明 SNMP、RMON 及 MIB 等名詞。

表 3-1：網路管理重要的組成要素

管理端	管理端是網路管理人員與網路之間的橋樑；管理端必須建置網路管理工具或能夠執行管理的應用軟體，以便針對網路上各被管理端進行監視、控制、資訊蒐集的功能。
被管理端	一般網路環境中具備被管理條件的節點設備，例如主機伺服器、工作站、路由器、橋接器、交換器、集線器等等，即可視爲被管理端。所謂被管理條件便是具有支援 SNMP 功能，現代的網路設備多已支援 SNMP。
MIB 值	網路管理必須仰賴各網路被管理端元件的資料數值，這些資料數值即爲 MIB 值(Management Information Base)，管理端便是藉由收集或改變被管理端的 MIB 值來達到網路監控管理的目的。
通訊協定	亦即管理端與被管理端之間的溝通語言，SNMP 本身就是一種通訊協定。

3.1.3.1 SNMP

網路是一種分散且異質的環境，面對網路上種種的設備，如果沒有方式跟這些設備「溝通」的話，相信要管理網路肯定是件不可能的任務，SNMP（Simple Network Management Protocol，簡易網路管理通訊協定）便是擔負起管理端與被管理端之間「溝通」的重要角色。SNMP 第一版是在1990 年五月由 RFC1157 所定義完成。SNMP 本身是通訊協定而非一種語言，它是實體間傳達資料的一組規則(James, D.M., 1999)。在SNMP 網管模型中定義了兩種管理物件(managemententities)，管理工作站和代理工作站，網路管理工作站(network management station ，NMS)通常是一台電腦，用來執行一個或更多個網路管理系統，而代理工作站則是負責監看管理節點、搜集它們的運作相關管理資訊，並且當管理系統需要管理資訊時提供該資料。Jianxin Li etal, 1995 指出能利用SNMP 通訊協定來提供管理資料的網路節點被稱爲是"可用SNMP 管理的"，管理資料本身是由一群整數資料、字串和MIB 變數所組成的，其中記錄了管理某節點所有的必要資訊，包含該節點的治理與安全管理政策，以及讓節點軟硬體的清單、配置和功能參數資訊，還有描述該節點目前的過去運作狀態的各項資料。MIB 變數包含了實際管理資料，用來決定待管節點的狀態和配置情，SNMP 定義了管理資料庫結構，遵循TCP/IP通訊協定並提

供指令給管理系統來處理MIB 變數中的資料項。RFC 1157 指出了SNMP 定義四種指令，透過"輪詢(Polling)"的方式來存取SNMP 代理者所維護的受管理物件，分別是Get 、GetNext 、Set 和Trap ，這四個指令便可以執行所有網路管理功能。SNMP 使用了結構化管理資訊(structure of management information ，SMI)、Abstract Syntax Notation One (ASN.1)與BasicEncoding Rules (BER)三種語言來表達管資訊。換言之，SNMP就如同分散式的應用程式，由網路管理端擔任一對多的要角，分散的各被管理端則負責控制自己的MIB值資料。因此，企業在著手網路的管理規劃及建置時必須清楚，您所擁有的網路設備是否「具備網路管理的標準」。目前SNMP的新版本爲SNMP V2 (又稱SMP)，提供網路管理上更多新的功能與安全性。

3.1.3.2 RMON

RMON (Remote Monitoring)可說是 SNMP 的加強版，隨著網路的發展，網路管理也需要更多功能的協助，爲了彌補 SNMP 網管不足之處所以有了 RMON 的產生。SNMP 在進行網路管理時針對每個網路節點設備一一輪詢(Polling)，因此在進行網路區段（LAN 或是 Subnet）的管理上便相當困難，容易造成網路的壅塞或是管理端過重的工作負荷，而 RMON 的基本概念上則是讓被管理端的 MIB 資料能在「當地」便進行收集與分析，之後只要將彙總的結果傳送給管理端即可；RMON 具備比 SNMP 更完整的網路監控分析、趨勢分析、OSI 的七層通訊協定、遠端監控、事件預警門檻等優點。

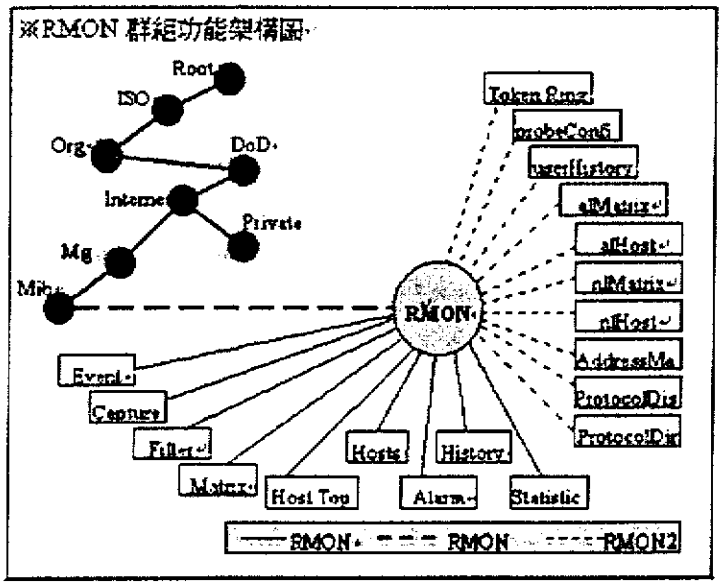


圖 3-2：RMON 群組功能架構圖

3.1.3.3 MIB

MIB(Management Information Base)，管理資訊庫描述所有受管理資訊的屬性資料，它是一樹狀結構，它的每個節點皆有特定的型別，其間的節點代表物件的分類，其末端的所有葉片即是SNMP 定義的物件。MIB 的頂層節點由國際標準機構之國際電子技術委員會(International ElectrotechnicalCommission ，IEC)負責定義，各子層以下的節點則由相關單位自行定義，Internet 的MIB樹主要定義於MIB-II (RFC-1158) 之下，MIB-II 之下主要定義了system 、interfaces 、at 、ip 、icmp 、tcp 、udp 、egp 、transmission 、snmp 等群組。MIB 所使用的索引稱爲OID(object identifier)，它將MIB 架構成一個樹狀的資料庫，樹上的每個節點都有一個特定整數的號碼，要取得其中某一點的值必須從樹根很下尋找，由樹根開始。

3.1.4 網管系統之功能分析

國際標準組織 (International Organizationfor Standardization ，ISO) 訂定之網路管理標準的網路管理模式 (Open SystemInterconnection ，OSI)，爲目前研究網路管理依循的標準。ISO 將網路管理系統分爲五個管理功能：

a. 帳號管理(accounting management)：
   帳號管理其目的在結算網路使用者使用網路資源所需之費用與估算網路運作成本。
b. 組態管理(configuration management)：
   組態管理其目的在於辨認及管理網路的物件，主要功能包括網路物件組態的更改、物件的命名、收集物件的狀態資訊、起始、或在異常情形發生或工作負載改變時將某些物件關閉。
c. 錯誤管理(fault management)：
   錯誤管理其目的在迅速地找出並修正網路系統所可能發生的異常情況，主要功能包括錯誤偵測、錯誤診斷、錯誤追蹤與錯誤修護等。
d. 效能管理(performance management)：
   效能管理其目的在分析與改良系統的效能，主要工作包括監督與評估網路資源的使用效能，資料傳輸的效率等。並可依據所得的評估報告，適當地修改與調整系統的特性參數，以提高系統效能。
e. 安全管理(security management)：
   安全管理其目的在使網路能安全運作，並有效地保護網路系統中的各項資源，主要的工作包括認證、存取控制、資料加密及授權。

3.1.5 網管系統之價格分析

在價格分析上，目前在市場上一套商用的網路管理系統價格並不是很便宜。因此企業要選擇購買網管系統時，必須要根據自己企業內部網路的需求、系統平台等。不然沒有評估好就亂買一通，以為貴的就是好的，那可能到時買了之後發現所選擇並不適用於企業需求而後悔不已。

3.1.6 網管系統之市場分析

在對市場分析上，目前在市場上網管系統的數目非常的多，如何能選擇一個適合企業本身的網路管理系統以真正有效發揮其效用，的確是個頭痛的問題。不過我們可以分析目前相關產品在市場上的佔有率及評價來作為選擇購買時的參考依據。ManageX、HP OpenView、Microsoft SMS 及 Novell ManageWise。

3.2 個案訪談計畫

本訪談旨在整理出網路管理者針對流量分析、壅塞分析與路由繞送選擇在實務上的作法，因此將採取深度訪談的方式瞭解現況，並進而將個案實務作法與相關理論加以分析比較，最後推導出結論與建議。訪談依據研究性質、目的、或對象不同而有許多不同方法，包括：

a. 非正式訪談(informal conversational interview)：這是開放性、無結構性的訪談，如同日常生活閒聊，在雙方互動的過程中，讓問題自然的呈現。
b. 一般性訪談導引法(general interview guide approach)：這種訪談法亦稱為半結構式訪談，由訪談者提供一組提綱挈領的論題，以引發訪談情緒，在有限時間內探索、調查與詢問。
c. 標準話開放式訪談：這種訪談法即為結構式訪談，在訪談前，所有需要詢問的問題均被撰寫出並小心考量每一問題的字組，在於訪談中適當提出問題。

本研究計劃所採取的訪談方法將採用半結構性的訪談指引，以筆記的方式將訪談內容記錄下來，並在 24 小時之內進行整理。

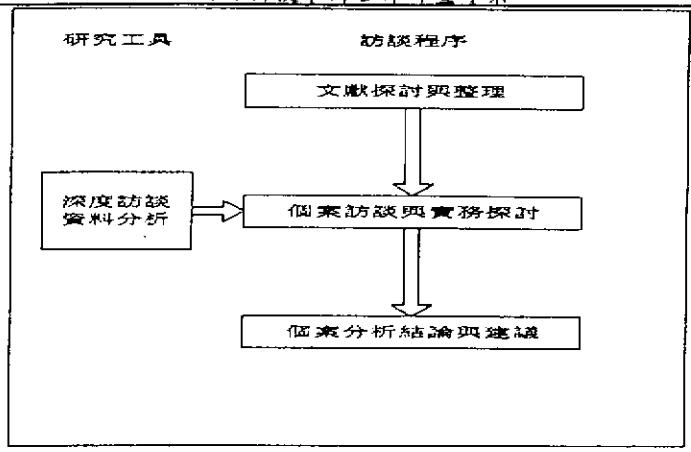


圖 3-3：訪談程序與工具

3.2.1 訪談對象

雖然校園網路與國軍網路在架構上不盡然相同，但是面對網路流量、壅塞、路由繞送選擇等問題在實務上的處理方式仍有國軍參考之價值。又由於本計畫在交通大學進行，因此將研究的對象鎖定在交通大學的校園網路。由於交通大學校園網路的相關事宜主要是由計算機中心的技術發展組負責，因此本研究將對校園網路的關鍵人物，計算機中心技術發展組的主管進行訪談。

3.2.2 訪談問題大綱，如表 3-2 所示：

表 3-2：訪談問題大綱

主題	子題
網路架構模型	貴單位所採用的網路架構標準爲何？
	連外，連內，骨幹，系所與宿舍，其選用的標準與策略爲何？
網路流量分析	貴單位網路所採用的網路流量分析工具爲何？
	選擇此工具的準則是什麼？
	流量分析的運作模式爲何？(架設位置與運作方法)
	哪些流量統計的資料對網管人員是重要的？
	如何藉由以上的資料發現異常狀況？
網路壅塞分析	如何處理貴單位網路壅塞的情形？
網路繞送路徑分析	貴單位網路的繞送路徑策略是什麼？ (靜態或者動態，爲什麼選擇這種方法)
斷線備援路徑選擇	貴單位網路的斷線備援策略是什麼？
	當發現攻擊情況時的應對措施爲何？
	當發生網路異常狀況的應對措施爲何？

3.3 網路模擬計畫

在網路規劃中，就如同在設計一個城市裡的道路系統，你得知道哪些人在使用哪些路徑、流量有多大、而且能容納的流量有多大、行程從哪裡開始、在哪邊結束，並且還要加以了解上述的因素的變化與時間的關係是爲何？如何道路系統車道不足，那麼會堵塞，而如果花掉大多經費去開太多條路雖可以不再有塞車現象，但是卻花費太多成本。因此在規劃一個網路時如何適當的測量及評估網路的容量是重要的。如果一開始評估錯誤，那麼之後才發現流量太多便會常常造成網路壅塞。根據這些的評估我們可以用來修正我們的網路規劃。在這裡我們將會探討如何去模擬規劃一個網路並且要如何去作分析及測量。

3.3.1 網路模式

在要介紹「網路模式」前，要介紹一下網路在 ISO/OSI （國際標準組織制定的開放系統連結）參考模型網路層（Network layer） 和傳送層（Transport layer）的「資料封包」、「通信協定」、「網路作業系統」以及主從式網路架構。

3.3.1.1 資料封包

在網路纜線裡，被傳送的資料並不是直接的被轉換成電氣信號（這個轉換是由 ISO/OSI 參考模型 的實體層所負責，把 0-1-0-1- 的資料以曼徹斯特編碼（Manchester Code） 的型式轉換成電氣信號， 這種編碼方式的優點是轉換出來的電氣信號比較容易被接收端辨識。）送進纜線，而是要經過包裝，就像是到郵局寄包裹一樣，要用統一規格的郵政紙箱，把要寄的東西裝進去，裝好封箱之後還要填寫包裹條，把寄件人、收件人的地址和寄送物品種類書寫清楚。在網路實體層中，資料的傳送是以電氣訊號的型式存在，也就沒有什麼包裝不包裝的問題，但在鏈路層上，資料就要經過包裝的處理（這個把東西裝進包裹，填好包裹條的動作叫做「打包」，相對 的收件人在收到包裹後，拆開包裹，取出物品，核對包裹條的動作叫「解包」，而寄送資料的包裹就叫做「封包」），以 IEEE802.3 乙太網路來講，它的鏈路層封包的格式是：

前置信號	收件位址	寄件位址	型態	資料	資料框檢查碼

其中前置信號（preamble）的作用是爲了要讓封包資料在交由實體層編碼爲電氣信號傳送時，在真正封包內容到達前，先引起網路上各節點裝置的注意（取得同步）。以專業的術語，這個長度爲八個位元組的前置信號叫同步字元。

接下來的收件位址、寄件位址、型態、和最後 的資料框檢查碼是屬於「包裹條」的記載內容，收件位址和寄件位址就相當於收件人地址和寄件人地址，由於這個位址是由鏈路層的媒體存取控制子層 （MAC sublayer）所使用，所以稱爲媒體存取控制位址（MAC Address ），媒體存取控制位址一般是 由網路硬體的製造廠商直接「燒」錄在裝置上，以乙太網路而言，每個節點的位址由六個位元組組成，其中前三個位元組是製造廠商註冊的編號，像 HP 的註冊編號是 080009（十六進制），Intel 的則是 00AA00；後三個位元組則是產品的流水號，由廠商 自行運用。就理論上來說，全世界每一片乙太網路卡、每一部乙太網路集線路、橋接器... 所擁有的 位址都是獨一無二的，所以在架設乙太網路時，我們不用像架 ARCnet 一樣得要擔心位址重覆的問題；但近年來無跳接點（jumperless）的乙太網路卡部分提供有用軟體設定媒體存取位址的功能，這項功能固然在網路管理上可以提供小小的便利（你可以把公司裡網路卡的位址依部門、電腦自訂規則編號 ，而不用像往常要另外做一份電腦的網路媒體存取控制位址對照表），但是不當的使用自定編號也可 能造成意外的麻煩，如果真的需要更改時，比較穩當的做法是不修改媒體存取位址前三個製造商註冊 的位元組，只更動後三個位元組的流水號就比較不容易出問題。

乙太網路封包中的型態欄有點像是寄送件品的種類（當然不像我們在寄包裹時，可以填上五花八門的內容，這裡的種類是事先定義過的資料型態代碼），型態欄事實上是由網路層的通信協定（包裹 的寄件人）來填寫，型態欄也隱含了資料欄的長度，因此收件人對資料欄內容的解讀完全要依賴它。資料框檢查碼是用收件位址、寄件位址、封包型態和資料欄內容以循環冗餘碼檢測（cyclic redundancy check－簡稱爲 CRC ）方式計算出來的一個三十二位元數值，這種演算法可以由一串字元計算出一個數值，而很難找到另一串長度相同，內容不同的字元可以計算出相同的數值，因此被使用在電腦 通信，資料儲存等領域作爲資料錯誤偵測。收件節點在收到封包之後，只要重新計算一遍 CRC 值加以 比較，就可以知道封包是不是原封不動的被傳送過來。 乙太網路封包中資料欄的長度範圍由 46 到 1500 個位元組，這裡面的內容事實上是由寄件方網路層的通信協定來決定，也就是說鏈路層封包傳送的服 務對象是網路層，同樣的網路層封包傳送的服務對象是運送層，如此由下而上，每一層都爲上層提供服務，就構建出一個完整的網路通信組織。

3.3.1.2 網路作業系統

網路作業系統（Network Operating System－ 簡寫成 NOS ）提供給使用者 ISO/OSI 網路參考模型 交談層、表識層和部分應用層的服務。用比較口語 的說法，「網路作業系統是經由網路連線提供資源共享服務的系統軟體」，而這些爲大家共享的網路資源要讓使用者感覺起來跟自己專屬的一樣（這是 網路參考模型第六層表識層的重點），同時要能管制每個用戶使用網路資源的項目和權限（這部分屬 於網路參考模型第五層交談層的範疇），要達成上述任務，網路作業系統的程式基本上分成兩部分， 一部分是負責提供資源共享服務，這部分的程式稱爲伺服器程式（Server）。另一部分則是提供終端 用戶存取網路上各個伺服器所提供的資源，這個部分的程式通稱爲用戶端程式（Client）。另外幾個 常見的名稱，像是重導程式（Redirector）或是服務請求程式（Requester） 也都是指用戶端程式。

3.3.1.3 主從式區域網路

以網路作業系統資源共享的型式來看，可以區分爲對等式（Pear-to-Pear，也有人直譯爲點對點式）和主從式（Client-Server）兩種區域網路。 主從式架構的區域網路是由一個（或數個）提供資 源給網路用戶共同享用的伺服器（Server），以及各個用戶的網路工作站（Client）所組成，伺服器依照所提供的資源來命名，像檔案伺服路提供了軟體共用、檔案共享的資源，列印伺服器提供了共用 的印表服務，通信伺服器讓網路上的用戶可以輪流使用數據機撥接服務，傳真伺服器讓每個人不用離開座位就可以發送傳真文件，唯讀式光碟機伺服器可以使網路上的用戶不用加裝唯讀光碟機就可以讀取光碟片裡的資料... 還有近年來逐漸受到企業重 視的資料庫伺服器，可以提供在網路上更有效率的 資料庫服務，同時擁有較好的安全性。主從式區域網路的優點是每個提供服務的伺服 器獨立性比較高，加上各司其職的體系，使服務的品質（速度和穩定度）都相當不錯，而在管理上， 由於資源的享用均透過伺服器，系統管理者只要在伺服器上做好用戶的建立，權限的設定就可以做好 用戶管理的工作。

3.3.1.4 對等式區域網路

對等式區域網路中，網路上的每一部電腦上的硬碟檔案、唯讀光碟機、印表機甚至於數據機都可以被網路上的其他用戶所享用（當然是在該電腦用戶授權開放的範圍內才行），也就說每部電腦都可 以同時扮演伺服器和用戶的角色，就資源共享的方向來看，對等式區域網路很徹底的達成這個目標。對等式網路作業系統一般而言，安裝、維護的程序都不複雜，系統軟體的價格也比較低，但是由於每 部電腦在使用別部電腦上的資源時，需要藉由對方電腦的中央處理單元進行實體的存取動作，使得在 效率上會比較

差。另外如果資源正被他部電腦使用時，因故當機或關機時，也會對其他用戶的作業造成不便。

3.3.2 網路模式的建立

一個網路模式建立與效率評估大概的分析大致步驟如下：(1)根據完成網路管理系統雛形,記錄網路傳輸狀況,了解網路系統實際運作。(2)將網路模擬系統的模擬結果和實際測量結果進行比較,完成改進網路模式和網路模擬系統。(3)藉已完成改進的網路模式和網路模擬系統,使網路管理系統雛形趨於完善。(4)根據完成之網路模式及網路管理系統所得資訊,完成網路效率評估。(5)根據評估結果,提出改善網路效能之可行方案,並作爲未來進一步研究之基礎。事實上，可以針對下列網路狀況進行分析：

a.. 資料流量分析

例如目前有多少人使用此網路、資料型態爲何(文字或資料庫查詢)、多久會更新資料、資料更新時網路的 Overhead 等，這項分析需整合系統整合業者及網路人員的資源一起去發掘。

b. 網路終端到終端的回應時間

此乃指網路使用者直覺感受到的使用狀況，基本上當你確定了應用程式和資料的型態後，可以透過一些網路分析儀器來測試，進而得到一個平均值；當然，若你是使用 TCP/IP 的話，也可自己寫一個程式用 ICMP 來測試此一回應時間。

c. 多重網路協定的考量

目前企業網路上經常有一、兩個網路協定(如 IP、IPX)，這些協定間的相互影響及如何去安排處理之優先順序等，都是網路分析師所應該考量的。

d. 多重網路拓樸的考量

在網路上時常會有不同的網路拓樸(如 BUS、星狀或環狀等)，這些多少會影響網路備援的設計，因此也是網路分析師須考量的。

e. 線路的設計

任何企業網路均離不開廣域網路的使用，因此在廣域網路中線路(Circuit)的安排和設計也會影響網路使用效率，因爲不同的線路安排均有不同的效能結果，例如使用專線和訊框傳送(Frame Relay)其線路安排也不同，反應在終端到終端的回應時間狀況自然也不同。

f. 成本效益考量

在網路分析的過程中，分析建置網路的成本及效益也十分重要，網路分析師須對網

路設備成本、營運相關成本(如教育訓練、維護成本、操作人員成本等)及通訊成本等做詳細的財務分析。

g. 資料封包進出處理模式

最後，網路分析師要對網路資料封包作一分析並建立一個進出處理模式，以了解各個應用程式所產生的資料量、屬性及相互之間的關係。

3.3.3 分析工具

在網路設計的過程中，網路效能分析工具是十分重要的，目前有一些軟體可以直接將網路分析儀或 RMON 所擷取的資料下載到這些效能分析工具中，進行實際模擬、分析等工作。而在網路監督與管理方面，當網路建置完成後便需要一套網路管理計劃，根據其所訂定的各項基準來考核網路現狀，以提供網路分析並進行改善工作，此時便須藉由網路監督系統來協助有效管理網路，而一般市面上網路監督分析軟體及工具甚多，其功能不外乎以下幾點：

a. 網路錯誤管理

網路最基本的管理便是錯誤管理，以往當網路發生問題時，管理人員是依經驗法則來解決問題，有時由於找不到問題發生時的網路狀況資料，因此只能重新啓動系統來解決問題。如今，網路監督工具提供了即時與歷史性的網路資料，網路管理人員可根據這些資料來解決網路問題，而解決問題的方法則由查看網路中重要節點的回應速度、發生錯誤最多的節點、發生錯誤量的時間圖，以及當時是哪個節點在傳資料給另一節點，由此來推算網路發生問題的地方(這網路除錯最花時間的地方)，最後再利用網路封包的解析來分析問題發生之原因。

b. 網路效能管理

進一步的管理便是網路效能管理，現行網路可能運作正常，但是在網路的效率方面可能已經發生潛在問題，而網路監督工具提供網路管理人員整體網路區段的效能、網路中某一區段網路協定使用量隨時間變化圖、節點間流量負載分析圖，甚至還包括網路中重要節點回應速度的效能。

c. 將網路服務文件化

由於網路與所有使用者息息相關，而且網路管理是長期的工作，網路管理人員經常需要提出以往的記錄資料與現有網路資料印表或存檔，因此網管系統最好能將網路的健康情況，也就是使用網路最多的節點，以及網路中流量最大的網路協定等網路服務文件化，且須定期且自動地產生，以減少網路管理人員的負擔。

d. 網路容量規劃

當網路管理人員將網路妥善管理之後，下一個階段便是網路的規劃，內容包含網路容量規劃和未來網路技術的了解。網路監督工具提供的網路服務文件化和數據化，將有助於網路管理人員的網路容量規劃，而其他的各種功能，如網路的區段分割資料、網路協定使用圖、網路節點流量圖及網路使用率時間圖等，皆可協助網路管理人員更有效率地解決問題，進而使網路管理人員有時間去作未來網路技術的研究。

3.3.4 分析方法

一般這些分析工具來大多是以下面方式來作爲分析依據的方法及方向：

a. 網路通訊型態

網路是一個封包交換、線路交換或細胞，在分析工具中以不同的網路通訊型態做原型模擬，讓使用者可判斷究竟是用哪一種線路(訊框傳送或專線)較適合自己。

b. 網路設備

有些分析工具建有不同廠商的路由器、ATM 交換機、多工器等資料庫，客戶可以藉此去做原型模型，同時也可以知道那家廠商之產品較合適自己的網路。

c. 網路協定

由於網路不會僅有一種網路協定，因此必須藉由模擬工具來協助設計網路，適當地安排網路協定的處理順序。

d. 不同資料流量的屬性

在網路上有許多不同的使用者應用程式在網路上執行，然而每一種應用程式均有其一定的網路特質，如回應時間、最少頻寬、資料傳輸模式、封包大小等，因此透過分析工具可以協助用戶找出此應用程式的特質，進而協助設計網路。

e. 流量分析

透過分析工具可以分析不同時段及流量型態，以幫助使用者了解網路所需的網路頻寬是多少？而在此頻寬中，網路終端到終端的回應時間又爲何？ 簡而言之，當你期望設計一個最適合自身企業的網路時，適當地利用這些分析工具是必需的，也許你會考慮到購製這些工具的成本過於昂貴，以及需要十分熟悉網路的專業人士去操作等現實問題。事實上，企業也可委託一些專業的網路顧問公司來協助這些網路分析工作。

4.1 網管工具剖析

4.1.1 前言

在前面第三章研究設計 3.1 節，我們研究了網管工具分析的一些準則，而依據這些準則我們可以將目前市面上一些較常用的網管工具大致分作構面來作分析及分類。

4.1.2 依據 ISO 定義網管的功能

以下本研究將目前常用的網管系統工具以功能分類(如表 4-1)：

表 4-1：網管工具的功能比較，資料來源：甲尚 IT 事業處

工具分類	功能概述	工具範例例
網路管理平台	網路架構管理、設備資產管理、網路效能管理與報表事件管理	OpenView NNM
設備管理工具	管理特定設備（通常爲單一廠牌）之設定、建構、效能、故障等功能通常可監控廠商之自創功能(Proprietary functions)	CiscoWorks 、OptivityTranscend 、D-View 、AccView
分析工具	分析特定區段之流量，通常爲 RMON2 標準之資料蒐集與分析	OpenView 、NetMetrix 、Armon
報表工具	將所蒐集的管理資料以各種方式呈現，主要提供長期趨勢分析與規劃之用	Openview Netmetrix Reporter, Service
錯誤診斷工具	通常是針對單一標的物（如針對乙太網路或廣域網路的封包分析工具，佈線檢測工具，負載測試工具，伺服器即時監督工具等等）的細部剖析。	Agilent Internet Advisor, LAN Analyser
網路安全工具	偵測或避免網路或系統遭受第三者侵入之工具。通常會根據網路封包之特徵作爲判別的依據，進而主動切斷可疑的連線（Sessions）	Openview Node Sentry 、Cisco PIX FireWall-1
效能檢視工具	檢視網路運作的反應效能與服務效能。通常都是以實際網路端點(end-to-end)爲基礎量測實際的反應時間。	Open view Net metrix、Response Time Workbench 、Pegasus
規劃模擬工具	根據實際運轉所收集的資訊，搭配對未來所要新增的服務或架構變更，先行規劃並模擬各種可能因素對網路的衝擊，以決定最佳的規劃方案。	Openview Service Simulator
品質策略管理工具	集中式品質策略管理工具，將所有的網路設備依照時段、應用程式類型、資料/語音/多媒體等分類決定應該有個服務等級，並自動設定相關之網路設備以達成服務策略之目標。	Openview PolicyXpert Packteer WebQos

4.1.3 網路管理系統的價格

以下我們從目前較常見的 14 種商用的網路系統，依其平台、特色及價格等來分類，提供作爲選擇網管工具時的參考。如表 4-2。

表 4-2：14 products cover the range of network sizeshttp://www.gcn.com/ **(June 5, 2000)**

廠商	產品	平台	特色	價格(美元)
Avesta Technologies Inc. New York 212-285-1500 www.avesta.com	Trinity 2.0.3	Windows, Unix	Discovery, mapping, SNMP trap and alert display, fault determination	$80,000 up
CoManage Corp. Wexford, Pa. 412-318-6000 www.comanagecorp.com	Integrated Service Manager 1.0	Windows	Device discovery, provisioning, service profiling, fault monitoring, performance management	$100,000 up
Computer Associates International Inc. Islandia, N.Y. 800-225-5224 www.cai.com	Unicenter TNG	Windows Unix, MVS, OS/400	Network discovery and performance, events and status, network security, software distribution, network storage, network workload, help desk, change management	$2,500 up
Compuware Corp. Farmington Hills, Mich. 248-737-7300 www.compuware.com	EcoScope 4.1 and EcoTools 7.1	Win9x, NT	Fault determination, application traffic monitoring network	$19,500 up for EcoScope; $695 premanaged server for Eco Tools
Hewlett-Packard Co. Palo Alto, Calif. 800-533-1333 www.hp.com	OpenView Network Node Manager 6.1	Windows, Unix	Network device discovery, network mapping, network failure cause analysis. trend	$4,995 to 16,995

			analysis	
Intel Corp. Santa Clara, Calif. 800-538-3373 www.intel.com	LANDesk Management Suite 6.3	Windows, Unix	Inventory, software distribution	$50 per node
Loran Technologies Inc. Ottawa 800-563-1178 www.loran.com	Kinnetics Network Manager 3.0	Hardware appliance	Discovery, mapping, fault finding, utilization trend analysis	$31,050 for 500 devices; includes training
Lucent Technologies Inc. Murray Hill, N.J. 888-767-2988 www.lucent.com	VitalSuite 7.1	Windows	Network connectivity montoring, network utilization trend analysis, application performance analysis	$44,000 for unlimited servers, 100 desktops and 50 network devices
MediaHouse Software Inc. Hull, Quebec 819-776-0707 www.mediahouse.com	ipMonitor 6.0	Windows	System monitoring and alerts, failure recovery	$350 up per license
Microsoft Corp. Redmond, Wash. 800-426-9400 www.microsoft.com	Systems Management Server 2.0	Windows	Inventory, software distribution, user ID maintenance	$48 per node
Netscout Systems Inc. Chelmsford, Mass. 508-244-4000 www.netscout.com	Netscout Manager Plus 5.7.2	NT, Unix	Network mapping, fault determination, utilization reports	$8,995 up
Nortel Networks Inc. Brampton, Ontario 408-988-2400 www.nortelnetworks.com	Optivity NMS 9.0	Windows, Unix	Fault management, provisioning, accounting, performance analysis, modeling, planning, reporting, access-level security	$9,995 up

Novell Inc. Provo, Utah 888-321-4272 www.novell.com	ManageWise 2.6	Windows, NetWare	Inventory, software distribution, user ID maintenance	$79 per node
Tivoli Systems Inc. Austin, Texas 800-284-8654 www.tivoli.com	NetView 6.0	Windows, Unix, MVS, OS/400, OS/2	Discovery of TCP/IP networks, display of network topologies, correlation and management of events and SNMP traps, monitoring of network health, gathering of performance data	$5,000 to $15,000

4.1.4 網路管理系統的市場

根據 Boston strategic marketing STAT 組織，特別針對 1999 年 Network World Network Management 裏的 1500 個讀者做調查，以確認主要的 Network Management 產品，以及調查企業對 Enterprise or LAN management platform 的使用狀況及客戶滿意度，典型的一些調查單位其 installed on-site 至少超過 5,000 個客戶，整個組織單位幾乎達到 18,000 個客戶，四分之一的調查單位爲 non-profit 的單位，而 profit 的單位比 1998 年營業額增加了 US$11billion，應用的產業涵蓋各行各業。在調查問卷中高達 90%以上均是選擇 Main trend 上的領導工具，較小的一部分爲其他工具，Freeware 的工具雖然有嚐試性，但是卻缺乏一些正式性的評估，且版本的變化缺乏 Reliability，故在 network management platform 上所觀察到的是那些領導性的廠商與產品，在 Enterprise Management 上主要有 Cabletron Spectrum 、BMC Software Patrol、Tivoli Platforms、HP Openview 及 CA Unicenter TNG，在 LAN Management 上主要有 SunSoft SunNet Manager、Intel LANDesk、HP OpenView ManageX、HP OpenView、Microsoft SMS 及 Novell ManageWise。

4.1.4.1 就客戶滿意度方面

在 Enterprise Management 方面以 Cabletron Spectrum Enterprise Manager 與 HP Openview ManageX 獲得使用者較高的滿意度(參閱表 4-3)。在 LAN Management 方面，以 HP OpenView ManageX 及 HP OpenView 獲得使用者最佳的滿意度(表 4-4)。

表 4-3：Enterprise Management

	Platforms Stack Up
Platform	Grade
Cabletron Spectrum Enterprise Manager	89
HP OpenView	87
Tivoli Platform	86
BMC Software Patrol	86
CA Unicenter TNG	82
Average of all rated platforms*	86

資料來源：STAT Resources，資策會 MIC 整理，1999 年 9 月

表 4-4：LAN Management

	Platforms Stack Up
Platform	Grade
HP OpenView ManageX	90
HP OpenView	87
Network Associates ZAC Suite	85
Novell ManageWise	84
Microsoft SMS	84
IntelLANDesk	83
SunSoft SunNet Manager	83
Seagate Desktop Management Suite	80
Average of all rated platforms*	86

資料來源：STAT Resources，資策會 MIC 整理，1999 年 9 月

4.1.4.2 就 Network Management Platform 特性

網管系統有四個主要特性可作爲評估，包括：Scalability、Integration、Management Capabilities 及 Overall value 。 在 Rating 的 Scale 上 90 以上等級爲 A、80 至 89 等級爲 B、70 至 79 等級爲 C、60 至 69 等級爲 D，產品若是在 85 以上就算是居於一個不錯的評價。雖然在 Enterprise Management 及 LAN Management 上有些領域是重複的，在差異上主要是在於規模的大小，LAN Management 的選擇公司大多採用一些 Small Network，而具有較多 Network 客戶的公司則通常具有 Enterprise Management Tool，或是兼具兩種類型。在特性評價上 Cabletron Spectrum Enterprise Manager 在 Scalability 方面高達 90%

(參閱表 4-5)。HP OpenView 在 Integration 方面與 Cabletron Spectrum 相同評價，BMC Software Patrol 與 Tivoli Platforms 在 Management Capabilities 有相同的評價，但在 Scalability 方面 Patrol 要比 Tivoli 較佳一些。CA Unaccented TNG 則是除了 Scalability 外幾乎均落後於競爭者。

表 4-5：Enterprise Management Tools Key Attributes

				Enterprise Management
Platform	Scalability	Integration	Management Capabilities	Overall Value
Cabletron Spectrom Enterprise Manager	90	87	89	88
HP OpenView	88	87	88	87
BMC Software Patrol	88	86	88	87
Tivoli Platforms	87	85	88	85
CA Unicenter TNG	88	84	86	81
Average of all rated platforms*	88	86	88	86
				* Includes products for which we didn't have enough responses to rate individually

資料來源：STAT Resources，資策會 MIC 整理，1999 年 9 月

在 LAN Management 上有些領域是重複的，HP 的 OpenView ManageX 與 OpenView 均居最高的客戶滿意度，其最主要原因是因爲具有極佳的 Scalability 與 Integration 的特性，故許多的公司均運用該平台以管理整個企業。在 Scalability 特性上 IntelLANDesk 與 Network Associates'ZAC 上均需要再加強(參閱表 4-6)。Network Associates'ZAC 在 Management 的表現上則僅次於 HP，Microsoft Systems Management Suite (SMS)與 Novell ManageWise 在整體滿意度上勢均力敵，SMS 在 Scalability 上表現較佳，ManageWise 在 Integration 與 Overall Value 上比之評價高。如果公司要專注加強這些特性，最主要影響的是 Overall value 預測性佔 72%，Platform scalability 及 Management capability 方面的影響性佔 60%，Integration capability 則對整體滿意度上影響程度較小。

表 4-6：LAN Management Tools Key Attributes

				Tools Management
Platform	Scalability	Integration	Management Capabilities	Overall Value
HP OpenView ManageX	88	89	88	88
HP OpenView	87	87	88	86
Network Associates ZAC Suite	83	81	87	84
Novell ManageWise	84	83	85	85
Microsoft SMS	85	80	85	84
Intel LANDesk	83	83	85	84
SunSoft SunNet Manager	86	83	85	83
Seagate Desktop Management Suite	84	80	86	81
Average of all rated platforms*	86	84	87	86
				* Includes products for which we didn't have enough responses to rate individually

4.1.4.3 網管系統具有多重特性爲評量關鍵

針對各個 Platform 以提供相關產品 Attribute 的評估考量(參閱表 4-7 及表 4-8)。其中 Spectrum 在 Performance Manager 上有很高的評價，同時被評量爲 Grade A 等級的產品特色爲：Configuration Management、Problem Management、Network Optimization Capabilities、System Optimization、Automated diagnosis，而 Tivoli Platform 在 Overall Satisfaction 方面與 Spectrum 相當，被評量較佳的特色爲：Overall Value、Asset/Inventory Management、Backup Management、Database Management 。CA Unicenter TNG 所不足需加強之處爲 Asset/Inventory Management、Directory Integration。在 LAN Management 方面，OpenView 在多項特色中均甚過 Microsoft SMS 如：Scalability、Integration with other management tools、Problem Management 及 Alert Correlation Management。SMS 的優勢則在於 asset/inventory management 及 software distribution，劣勢則在於 automated diagnosis。

表 4-7：Enterprise Management Tools Key Attributes

					Enterprise Management
Product Attributes	Cabletron Spectrum Enterprise Manager	Tivoli Platform	HP Open-View	CA Unicenter TNG	Average of all rated platforms*
Overall Value	89	90	87	83	86
Asset/Inventory Management	85	88	83	80	82
Backup Management	84	87	83	81	83
Configuration Management	90	86	85	84	85
Database Management	86	87	82	81	82
Performance Management	92	85	86	84	86
Problem Management	91	88	87	84	87
Security Management	89	87	84	83	85
Network Optimization Capabilities	91	85	85	83	86
Systems Optimization	91	84	84	83	84
Automated diagnosis	91	84	84	83	85
Automated corrective actions	88	82	82	81	83
Alert Correlation Capabilities	90	87	85	85	86
Directory Integration	89	82	82	80	83
Overall Satisfaction	89	89	87	83	87
					* Includes products for which we didn't have enough responses to rate individually

資料來源：STAT Resources，資策會 MIC 整理，1999 年 9 月

表 4-8：LAN Management Tools Key Attributes

				LAN Management
Product Attributes	HP Open-View	Microsoft SMS	Novell Manage-Wise	Average of all rated platforms*
Scalability	88	86	86	87
Integration with other management tools	88	82	85	85
Asset/Inventory management	81	83	81	84
Problem management	86	84	83	84
Software distribution	83	85	84	83
Server management	85	84	88	84
Network optimization capabilities	85	83	85	86
Automated diagnosis	85	80	82	85
Alert correlation capabilities	85	83	82	84
Directory integration	82	83	88	80
				* Includes products for which we didn't have enough responses to rate individually

資料來源：STAT Resources，資策會 MIC 整理，1999 年 9 月

4.1.5 網管工具簡介

本節我們將會介紹四個網管工具，Tivoli 的 NetView、HP 的 Open View、Microsoft 的 SMS 以及 MRTG。依其特色、功能面分析。

4.1.5.1 Tivoli 網路管理系統： NetView（圖 4-1）

同時提供 UNIX 及 Windows NT 等兩種作業系統之網路管理系統。系統架構以集中管理、分散式資料處理爲原則、實施企業網路資源管理與監控。提供(1)主從式（ Client / Server ）網管架構設計。(2)網路管理協定：以 SNMP 爲主，亦能接收 CMIP 網管協定。

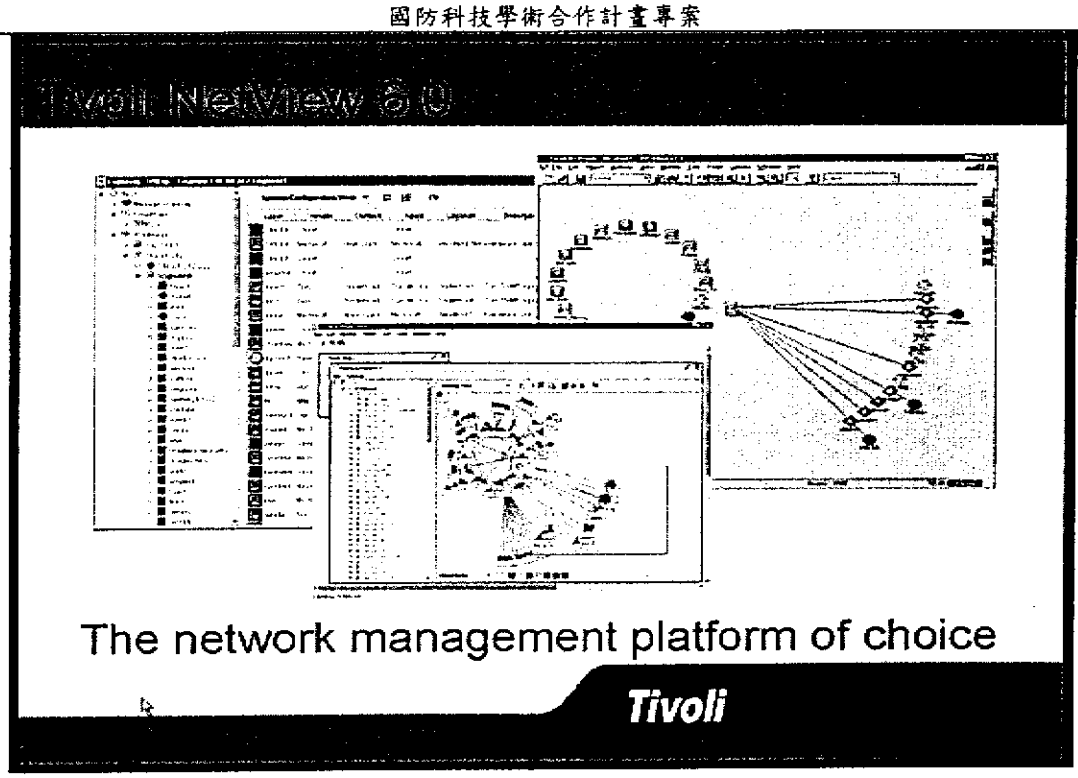


圖 4-1：Tivoli 網路管理系統

安全管理：授權管理者執行特定區域網管工作或特定網管功能。提供網管系統相互自動備援能力(Manager-to-Manager backup)。至於其他特色有：

a. 使用者圖形介面：符合 OSF / Motif 及 X-Windows 介面規定。

b. 圖形操控，使用滑鼠及鍵盤，以拖放方式（ Drag & Drop ）操作下列項目：
   - 顯示網路節點與裝置（ Devices ）
   - 顯示網路之地理、實體與資訊流向圖。
   - 編輯、裁適、增加或修改網路圖形及圖示（ Icons)。
   - 連續監測重要網路資源。
   - 觀察因網路架構變更而產生之事件。
   - 增加 Menu 項目：可自行撰寫應用程式並加入功能選項（ Menu bar)中。
   - 可整合其他網管運用，並可經選單或對話視窗方式取用網管功能。

c. 組態管理（ Configuration Management)：
   - 具備自動搜尋及監視網路上任何 IP 節點功能（ Auto-Discovery ），並自動繪製網路拓樸圖(Topology map)。系統即時偵測被管理物件之最新狀況，網路狀態變更時亦能自動更正，以呈現給管理者最新之網路圖。

- 網路拓樸圖可依照實際網路狀況做環狀、樹狀、匯流形及星狀網路排列。
- 可載入 MIB (Management Information Base) I、MIB II (RFC 1213)，及系統或網路廠商專屬之 MIBs (Private MIBs)。並可經由圖形介面，以指定與扣觸 (Click)的方式察看、取用與設定 MIB 值，來管理遠端網路設備。
- 查詢節點明細：使用滑鼠動作取得節點之明細資料，如聯絡人員姓名、位置、型號及網路架構等，並可編輯變更之。操作人員能依主機名稱、線路地址、IP 位址、物件形式等，尋找需要的目標。

d. 故障管理 (Fault Management)：
- 自動持續監視網路物件之狀況及連結性，並彩色顯示其情況於網路圖上。
- 以規範爲基礎的事件整合 (Rule-based event correlation) 工具。
- 圖形操控，以拖放方式。
- 提供事件與事件間之關聯性分析，以過濾不重要之事件。
- 定義事件形式與動作：提供事件發生時，系統所啓動之程式或步驟。
- 設定臨界值：操作人員可對各網路節點設定臨界值，交由網管系統定時查詢 (Polling) ，若發現超值時即提出報告或執行事先所定義之程式。

e. 診斷偵測功能：使用滑鼠指定障礙節點並執行下列測試：
- IP 測試：用 Ping 協定驗證網路連接。
- TCP 測試：TCP 連接測試。
- SNMP 測試：測試該節點是否有 SNMP Agent。
- 偵測及顯示封包經過路徑。

f. 效能管理 (Performance Management)：
- 提供圖形介面及時顯示網路之尖峰值與平均值。以圖形方式監看各項網路統計資料之尖峰值與平均值，並提供製作報表之樣本程式。
- 可對網路運作之重要數據設定臨界值。當系統設限超過時，警示網管人員， 經由持續監看 MIB 中的各數值資料，網管人員可預先調整網路，以防障礙發生。
- 操作人員可用滑鼠從 MIB 中選取物件 (Objects)，將其數值圖形化，及時顯示或設定目標值。
- 蒐集網路歷史性資料：蒐集各 SNMP 裝置之 MIB 中的數值資料，使用者可直接取用歷史資料，將其列印或存入其他試算表程式中。
- 支援下列關連式資料庫，方便資料管理、報表製作與產生 Sybase、Oracle、DB2、

MS SQL Server。

g. 提供分散式網管工具（Mid-Level Manager）（節省網管設備購置成本）：
- 執行遠端 SNMP 網管功能，減低因網管系統所造成的交通流量，節省網路頻寬。
- 提供與中心主網管系統雙向溝通的功能。

h. 支援 WWW 介面：遠端電腦可藉由 Web Browser 視窗執行下列網管功能：
- 被管理物件及時狀況呈現。
- 診斷偵測：針對被管理物件執行測試程式。
- 事件回應及通知。

i. 提供應用程式介面：緊密連結其他管理應用，包含終端用戶 API、SNMP API、事件過濾 API、 XMP API(SNMP 及 CMIP over TCP/IP，基於 OSF 之 DME 技術)。

4.1.5.2 HP 網路管理系統

4.1.5.2.1 HP OpenView Network Node Manager v6.1

OpenView 是一套功能強大的網路管理作業平台，也是目前最普遍使用的網路管理系統之一。HP OpenView 產品家族可在各種硬體與作業系統下使用，客戶可依自身的需求選擇最合適的開發環境。透過 HP 協力廠商或原廠支援，HP OpenView 亦可在 AT&T NCR 、Data General 、Group Bull、Hitachi、NEC 與 Stratus 等廠牌的硬體上執行。此外，HP 也一直將 OpenView 授權給其它硬體大廠，確保 OpenView 是在業界最廣泛硬體品牌上執行的管理解決方案。HP OpenView 可自動掃描網路上可接受網管之網路裝置，並自動顯示網路架構圖。並具有網路狀況訊息顯示功能，可控制各端點之開放及封閉。具有偵測各端點之傳送量，以分配 HUB 上的負載，支援 HP Network Devices ,HUB, EtherSwitch , Bridge, Jetdirect, Dail-A-Lan, Router ..等。HP OpenView 爲用戶提供整合性的網路、系統、應用程式、和資料庫 管理解決方案，可在多廠牌的運算環境中使用，HP 表示它目前在全球 已植入超過十萬個網路系統。其中 OpenView Network Node Manager 是其主要的網路管理解決方案，它把網路及連接設備以簡潔的圖形化顯示界面表現出來，幫助 IT 管理人員評估網路效能、預知網路中斷、以及預估網路成長或重組的可能影響。Open View 使用了四種資料庫形態來運作，包括了 OVW object database ，map database ，topology database 與 trend data database ，其中 topology database 與 trend data database 資料爲存放於關聯式資料庫，而 OVW object database ，map database 則存儲存於磁碟檔案中

4.1.5.2.2 HP Open View ManageX

HP Open View ManageX 是管理 Windows NT 作業系統、資料庫、應用程式與 Intranets 的整合性解決方案，使用者可輕鬆的從 ManageX Management Console(管理控制台)有效地監控數以千計的 NT 工作站與伺服器，無論是在當地或是世界各地。ManageX 是第一個根據 Micrsoft Management Console (MMC 微軟管理控制台)所發展出來的解決方案，依循微軟最先進的技術包含分散式原件物件模式 DCOM、ActiveX 所設計，提供功能強大、容易操作的管理解決方案，可用來確保 Windows NT 系統及應用程式的穩定性與運作效能；ManageX 可大幅降低成本並提供管理工作自動化，發揮最大的投資效益。對於倚賴 Windows NT 環境的組織，ManageX 不錯的管理解決方案。

4.1.5.2.3 ManageX 五大管理方案

應用程式管理 ManageX 有超過 150 種預設的管理政策(Policy)，可管理並確保 Microsoft Exchange , SQL, IIS Server 等以 NT 爲基礎的應用程式、Intranets、Lutos Notes/Domino、Oracle 資料庫及防毒軟體 Norton Anti-Virus 和 McAfee Virus Scan、儲存備份軟體 HP OV OmniBack II 和 Seagate Backup 等，提供應用程式的回應時間與穩定性的最佳化。(1)效能管理：維持 NT 系統最佳的運作時間，具有即時效能診斷及應用程式運作量測之功能。(2)事件管理：採用預防式管理，管理者可從中央控制台建立各事件日誌的關係並加以統合，再而啓動修正的動作。(3)遠端管理：可同時管理多台系統，如更新服務項目、變更密碼、關閉或重新啓動遠端機器。(4)容量規劃管理：利用記錄檔系統及應用程式效能資料，進而提供基準報表及趨勢分析。

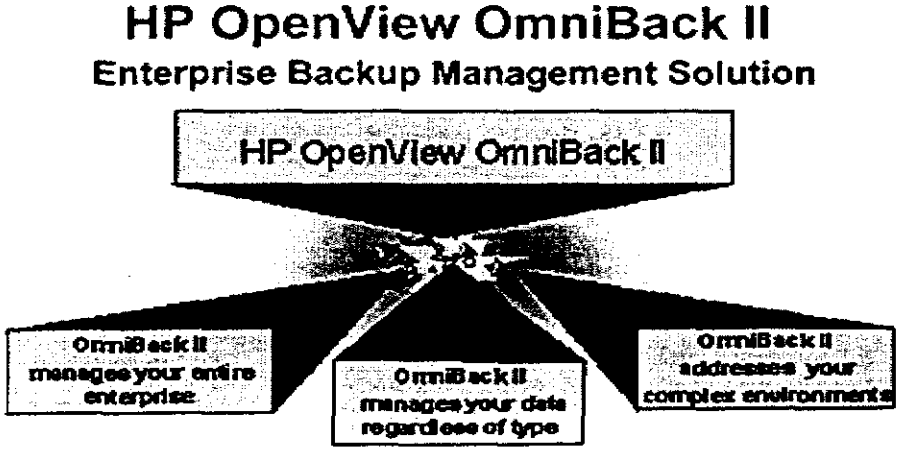


圖 4-2：HP OpenView OmniBack II v3.5

4.1.5.2.4 HP OpenView OmniBack II v3.5（圖 4-2）

HP Open View OmniBack II 是提供全面性的資料備份與復原功能，降低對重要應用程式的影響，爲異質環境創造一個全面整合的備份解決方案。OmniBack II 提供各式各樣的備份方式，包含全部、增加、線上、離線備份，並能對網路和設備的失效做重試的動作直到成功爲止，也能有選擇性的自動備援到其他設備；其內建監視器可輕易的控制備份與回復的處理，經事件登錄可藉由瀏覽器、電子郵件、廣播訊息以及 ITO 整合或 SNMP 記錄式來通知 IT 人員處理。

a. 提供高取用性的解決方案
- 提供全球化分散式企業環境資訊資源高度取用
- 不必關機就能進行及時資料備份
- 第一個具叢集功能的資料管理解決方案
- 提供線上備份與復原
- 透過災難復原功能迅速回應
- 可適用於混合 UNIX、Windows NT 與 NetWare 的企業系統環境
- 適用於 Oracle、Informix、Sybase、Microsoft Exchange、Miscrosoft SQL Server 等資料庫，以及 SAP、Baan 等應用程式。

b. 降低整體擁有成本(TCO)
- 完善的權限授與功能可發揮最佳的資訊人事工作效率。
- 可整合現有儲存設備與磁帶資源，並支援主要的資料庫、應用程式和平台，保障現有硬體的投資。
- 易用的 GUI 界面與智慧型操作精靈，消弭環境的複雜性及減少昂貴的學習訓練時間。
- 具成本效益的多磁帶機連接能力，讓多個系統可共享磁帶館。

c. 排除效應瓶頸
- 多層(multi-tier)架構，讓使用者可由單一系統集中控管本地與遠端的資料備份/復原作業。
- 提供使用者最快速的備份/復原作業，減少網路的工作負載。
- 平行處理每個磁碟機的資料流，以最快的速度同時驅動多個磁帶機進行備份作業。

d. 提供可靠、高度自動化的資料保護功能

- 提供預防式管理與監控服務品質的能力（如存取電子郵件系統或 SAP 應用程式）透過應用程式反應測量 ARM，並運用資源來源整合 DSI，可與其他 HP OpenView 服務管理解決方案完全整合。
- 高階管理者功能可集中管理整個企業，節省系統管理人員作業時間。

4.1.5.3 Microsoft SMS(圖 4-3)

安裝容易、使用簡便有精靈引導的安裝程式會在安裝時自動地設定 Systems Management Server 與 Microsoft SQL Server?，更可達到節省成本的目的。與其他 Microsoft BackOfficeO 家族元件和介面之間更佳的整合，更可降低管理者的訓練成本，同時也使得工作執行更加容易，並確保能夠完成正確的步驟。Non-intrusive 用戶端軟體會在背景中執行，降低訓練的需求，並加強對遠端使用者的支援。Windows NTR 整合的 granular security 讓管理者可彈性地處理工作而無須擔憂安全性風險。詳細的硬體與軟體清單：使用 CIM 訂立自動收集正確資訊的規範，而無須親臨桌面。最新的清單使得軟體分配更加可靠，遠端疑難排除也更有效率。回報每台 PC 上安裝的應用程式，協助辨別機器上無法回報千禧年問題、過時或非法使用的軟體。遠端診斷與控制：監視網路交通與建立網路伺服器和裝置的地圖，以快速辨別網路問題。遠端控制全球的機器，減少修復伺服器與桌面所花費的時間。軟體計量：使用追蹤軟體幫助規劃使用權的購買與升級。監視與限制應用軟體的使用，避免違反授權合約。診斷工具：網路追蹤 - 建立網路伺服器與裝置的地圖，以幫助管理者了解與檢修網路。網路監視：藉由監視網路交通來辨別網路問題，如不需要的協定、重複的 IP 位址與經由 Internet 闖入網路的外人。遠端診斷：藉由在遠端執行應用程式、與使用者“談天”、重新開機或甚至是控制鍵盤與滑鼠，以減少花費於修復網路上任何伺服器與桌面問題的時間。伺服器健康監視：提供 Windows NT Server 與 MicrosoftBackOfficeR 程序上的即時效能資訊，來維持重要的伺服器與應用程式之執行。網路拓樸探索在影響目前可用網路頻寬最小的情況下，探索及對映出網路拓樸、用戶端與作業系統。地圖可用來辨別和排解可能會與標準 Systems Management Server 作業衝突的網路、裝置和伺服器所引起的問題。Year 2000 適應性檢驗：辨別安裝於所有電腦上的 BIOS，並使用該項資訊判別它們對千禧年的順應狀態。使用軟體清單中尋找 Microsoft 軟體，並判別千禧年適應狀態。使用報告可追蹤企業中千禧年的狀態，並自動分配與安裝千禧年更新軟體。支援不同環境：安裝簡易可

供小型網路使用，也可放大至成千上百之用戶端的網路。有條不紊地管理清單、軟體計量和將軟體分配給遠端的使用者。可在 Novell Netware NDS 與 bindery 環境下工作。

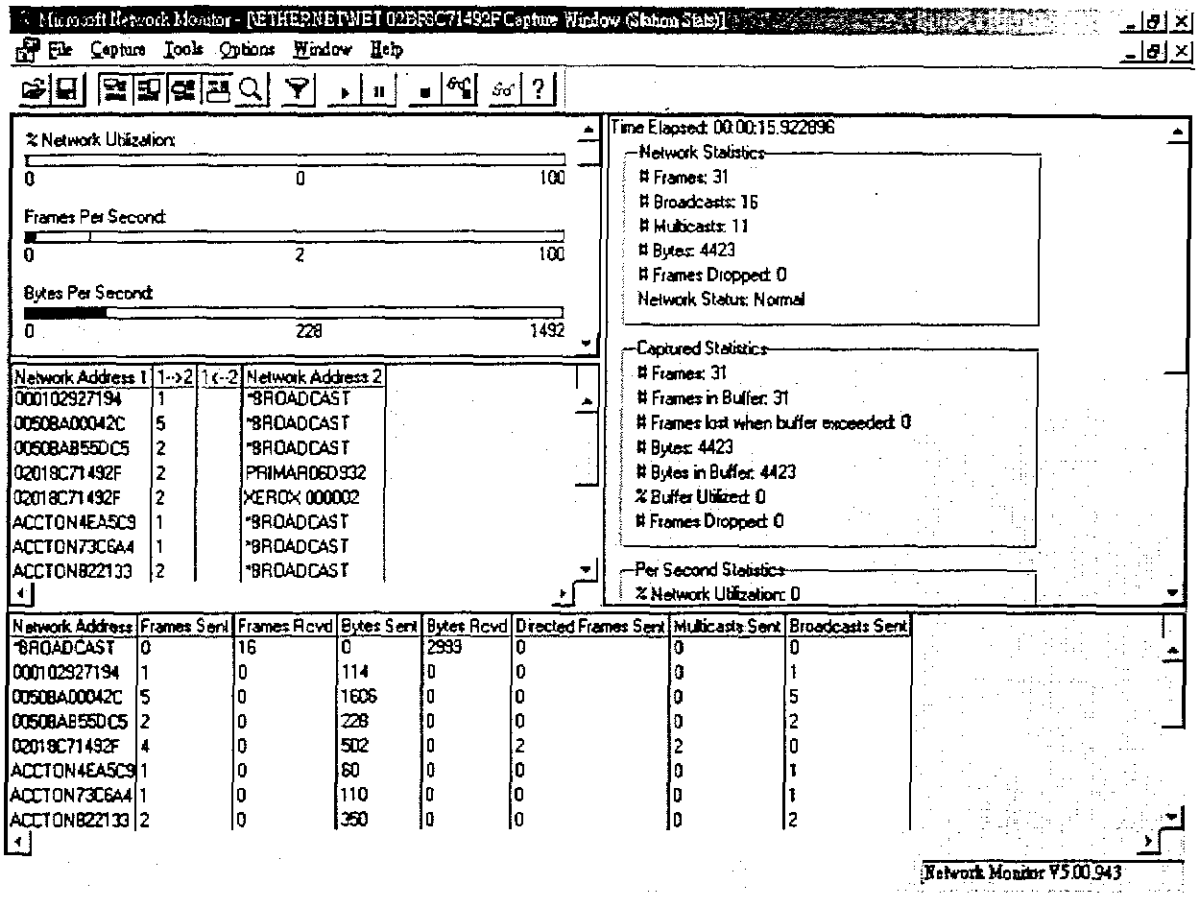


圖 4-3：Microsoft SMS

4.1.5.4 MRTG

MRTG(Multi Router Traffic Gather:：圖 4-4)是一個支援 SNMP 的網路設備取得流量資訊，來進監測並繪製圖表的工具。它會顯示由 router 或其他網路設備所搜集而來的流量使用狀況及其他統計資料，並自動產生 WEB 畫面內容及 GIF 圖檔呈現在用戶端的瀏覽器。因爲 MRTG 強大的功能，使的運用的層面十分廣範，以下列舉幾個常見的用途：顯示網路設備中的系統 CPU 的負載。(2)顯示網路設備中系統記憶體的使用率。(3) 顯示遠端存取伺服器上的 modem 的使用狀況。MRTG 會將所有取得的網路效能資料搭配每個受測介面的其他資訊，以圖形的方式顯示出來，總共會提供四項統計圖表，分別將傳

輸率以每天、每週、每月及每年的方式呈現。還有最重要的一點 MRTG 是免費的，而且功能不輸給企業級的 open view 等軟體。由於可以自行去修改原始碼改成適合自己網路需求的緣故，是以目前許多學術網院上的網路中心都幾乎用 mrtg 來統計網路的流量，例如台灣大學、中央大學等。

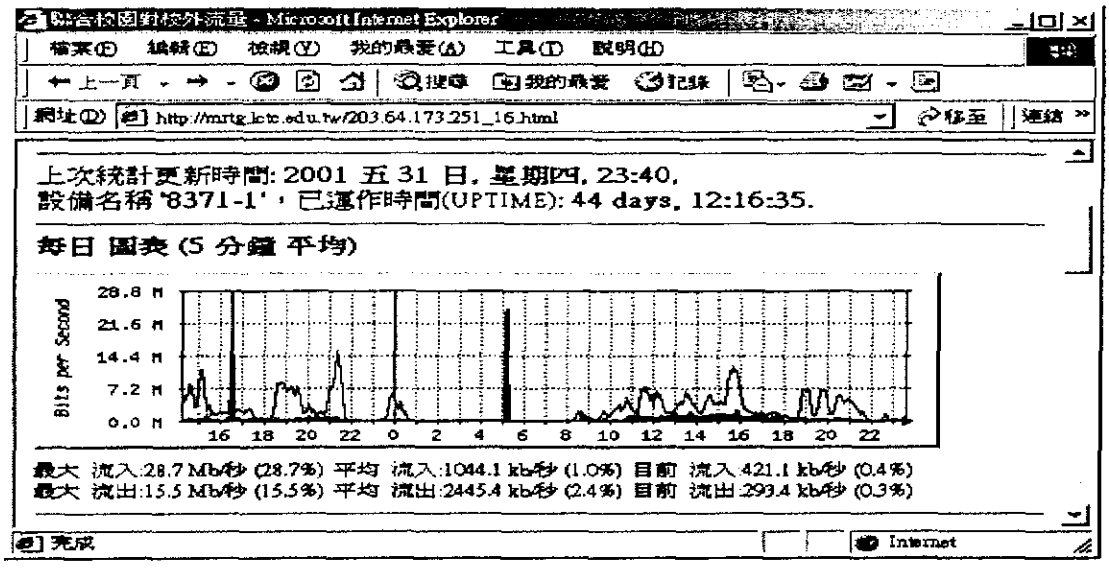


圖 4-4:MRTG

4.2 個案訪談結果

4.2.1 網路架構

「一般來說網路架構圖基於安全的考量都有一定的敏感性與機密性。也就是說各大區域網路中心網站所發佈的網路架構圖可能都不是真的。不過，善用一些共享軟體，事實上，可以協助網路管理人員。」

雖然在交大的網頁，有一些網路架構的大致說明，但是計中主管在訪談中提到，網路架構之於安全的重要性，也因此，除了網頁上可透露的資料，他表示無法繼續提供本計畫再進一步的內容。

事實上，網路架構圖是網路管理中很重要的參考資訊，它能使管理者清楚的知道整個網路架構環境並進行管理與監控。網路架構圖上可包含主機、路由器、橋接器、交換器、集中器等網路設備，以及各網路設備的連接情形，網路線路圖、網路設備的 IP 位址或設備名稱等。

4.2.2 網路流量分析

*「流量分析可以解決壅塞問題嗎？即使使用 **netflow** 與 **MRTG** 等的工具，其幫助仍是有限。這主要是因爲流量分析多爲點對點，對於點與點之間的封包交換情形其實並不容易取得。換句話說，點與點之間的壅塞問題才是最大的問題，這時候，根據網路架構做交叉比對則不失爲好方法。*

雖然如此，良好的流量分析資料仍然幫助管理者進行路由的策略，除此之外，這些資料也有助於爭取頻寬與路由路徑。」

「流量分析軟體所獲得資料，因爲具有累積性，例如每日每週每月等，所以也不容易取得某一當下的狀況，供事後的分析。」

流量分析，在網路管理中的角色應該屬於工具的角色，網路管理者除了思量流量分析的資料要如何搜集，更重要的事情是如何將這些搜集來的資料加以分析與應用。

*「由硬體來收集網路流量的資料大致分爲以下幾種方式：一種是利用網路穿過的設備來統計資料，例如 **Cisco** 的設備就有提供這種功能，將我穿過的封包依照 **IP** 或*

MAC 的分類來累積。但是要讓設備統合整個網路上的流量，就必須所有的設備都採用相同廠商或規格才行，就實務上實施並不容易。另一種收集網路流量的方式則採用 RMON 的方式監控整個網路。」

自從 1997 年起，台灣學術網路的骨幹部分，已改採行 ATM 協定，由於 Layer 2 協定的改變，傳統收集網路資料的方式已經無法繼續使用。也因此許多網路廠商如 Cisco，都在其高階產品上支援 proprietary 的網路流量監測系統。以 Cisco 爲例，在他們發展的 Netflow 系統中，除了增進系統效能的 caching 與 switching 等功能外，也包含了將網路流量資訊輸出到網管工作站，使特定的程式可以做後續的分析統計工作。

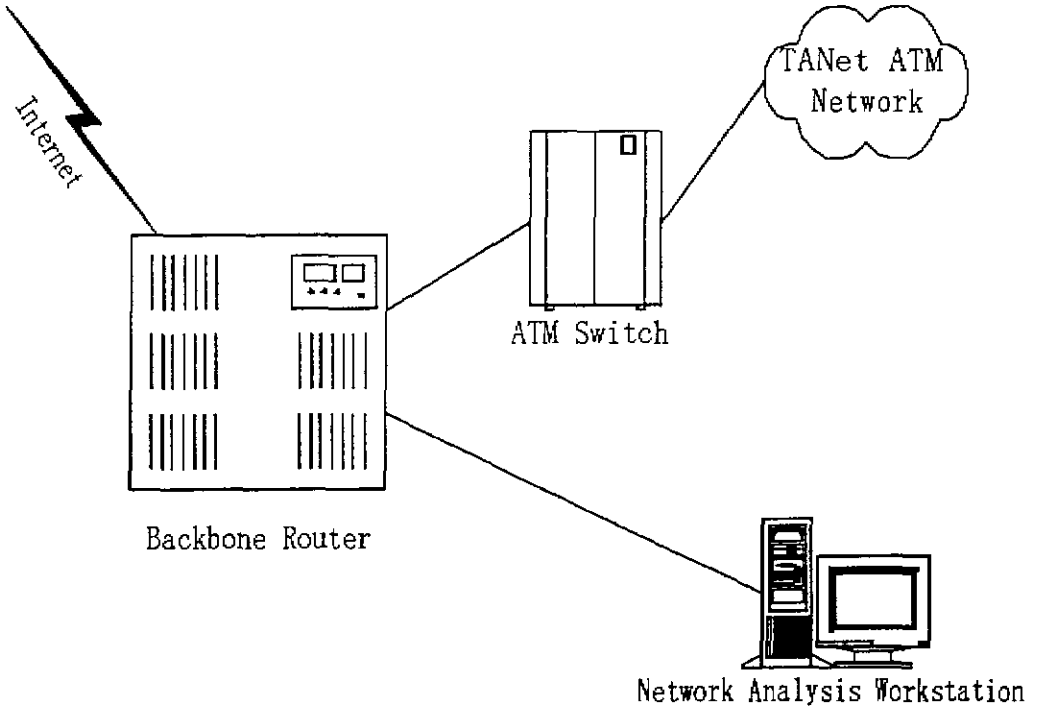


圖 4-5 目前所使用的流量統計方式

以上的流量統計方法，最大的缺點就是毫無標準可言，各家產品林立，互不相容，且後續網管所需的軟體通常也須向原廠購買，無法從第三者獲得支援。然而，單就 Cisco 的 Netflow 而言，由於其輸出的資料結構有公開，因此就可以利用自行發展的分析軟體，分析其上的內容。

4.2.3 網路壅塞分析

「產生網路壅塞的原因就一個區域網路來說，主要有以下幾點：
第一點就是網路卡設定不當，例如全雙工，半雙工的設定問題，由於有些設備不支援全雙工，若設定全雙工會導致設備產生錯誤。
*第二點就是設備故障，例如：電源不穩與故障，這會造成資料的破碎，讓所有在網路上傳送的資料 **CRC** 錯誤，導致網路資源的浪費而造成壅塞。*
*第三點就是大量使用 **Microsoft** 網路芳鄰服務造成網路壅塞。*
*第四點就是 **UDP** 的應用也容易造成網路壅塞，例如使用特殊埠(**port**)，如 **ICQ**；或者採用廣播的傳輸方式。最後一點則是網路攻擊，網路攻擊亦會造成網路壅塞，如阻斷服務(**DoS**)的攻擊。不過我認爲此不爲 **LAN** 壅塞的原因，這是來自 **INTERNET** 因素。」*

解決以上網路壅塞的方式，以實務上的應用來說，最方便、有效的方式是採用 Listen 的方式，用 Sniffer 的工具來監控並解決問題。如果我們 Sniffer 發現網路使用量呈現不合理的狀態，很有可能就是網路卡設定不當的問題；如果流量比例不對，很有可能就是網路芳鄰造成壅塞問題。如果發現很多在奇怪埠傳遞(port)的封包，那就可能是 UDP 應用所造成的壅塞問題。

*「網路上 **sniffer** 的方式與作法可以用：*
***sniffer** 的軟體工具。(在網上有許多 **shareware**)。*
*另外，有些設備本身就有提供流量統計的功能，並依照 **ip**、**MAC**、**port**，定時分類統計，運用這些資料來觀察網路上是否有異常狀況。*
*當然，在廣域網路的專線模式架構下，如果直接在在 **hub** 上 **listen**，例如在 **Layer2 switch** 上 **Listen**，其實是無法下手的。這個時候，可以利用 **switch** 上提供的 **duplicate** 功能，將所有的流量資料複製到管理者可以掌控的範圍，這時就可以利用 **sniffer** 工具監控。*
*如果遭受 **DoS** 攻擊時，也可以用 **sniffer** 的方式應對。*
*當資料在光纖上傳輸時，可以在實體部分的一些技巧，例如利用分線技巧偷取一部分傳遞的光，藉此來 **Listen** 傳輸的狀況。」*

「當發生壅塞的時候，可以考量其發生的問題可能是當地的區域網路，或者是目的地的區域網路發生問題，當然也可能是兩地之間的網路出現問題。如果是當地或者是目的地的區域網路出現問題，那麼發生的狀況又可以回歸到上述所說網路壅塞的五個原因之中，而且通常都以網路芳鄰服務最有可能壅塞的原因。但是如果是中間的網路出現問題，除了可能是網路流量太大的問題，也有可能是網路架構設計的問題。」

*「**Ping** 的功能很多，根據發送不同 **bytes** 數目的回應具有不同意義。」*

要如何檢驗網路壅塞的地方，計中主管建議 ping 是一種方便又實用的作法。ping 指令可讓管理者偵測自己的 PC 與其它電腦或網路設備間的連線狀況，但是並不是百分之百的作法，因爲某些地方會把 ICMP 的功能除去。儘管如此，利用 Ping 的交叉比對，仍能大致找尋出發生網路壅塞的問題區域。例如，當我們發現連上 PC home 很慢時，可以先 ping 到 hinet，看看連線狀況如何，如果還不錯，那問題可能就是發生在 hinet 至 PC home 這一段，不過這裡有一個最大的問題就是管理者必須熟悉這些地方的基本網路架構。針對 ping 的運用，計中主管建議：

*「運用 **Ping** 交叉比對的方式，可以先針對一些較具指標性的網路中心，例如 **AOL**，台大計中，中山計中等。」*

4.2.4 網路繞送路徑

「路由的選擇可依據以下幾個考量點：
首先，頻寬的負載重不重。
其次，路由中間的節點是否可以被控制。
再者，路徑的傳輸是否可靠。
當然，路由選擇也必須依照應用的狀況與需求。
此外，流量的起伏大小也是需要考量的。」

由於路由中間的節點，常常是無法由網路管理者完全控制的，所以學理上找尋最短路徑的方法，在實務上有其執行困難的地方，許多網路繞送路徑的選擇常是以上考量點與現實環境的妥協方案。此外將所有網路應用所需的頻寬切割，例如我們可以將 email 服務獨立出來，這對一些路由的選擇或者頻寬的分配都有一些幫助。換句話說，清楚了解應用程式的類型，依其對於頻寬的消耗量或特性進行適當的控管，是比較合理的作法。例如戰情傳遞，這種需要快速反應的資訊，它的優先順序就很高，甚至可以有專門且特殊的路由來傳遞這種資訊。

4.2.5 斷線備援

「斷線備援的方式是取決於斷線的原因，一般而言非硬體線路的問題，都可以用更改路由傳送路徑來解決路由路徑轉換的問題，而更改路由傳送的路徑是普遍的處理方式，同樣更改路由的考量與前面所講路由選擇的考量點是一樣的，這個組織與管理者重視什麼樣子的考量層面，路由路徑的選舉方式也會因此改變。但是萬一斷線的原因是因爲線路的問題，例如光纖被挖斷了，或者是停電造成設備的當機，路由路徑的轉換可能就幫不了多少忙，而實體的設備的修護則是此時的策略，當然在修護前，如何找到線路損壞的部分，亦是一門不小的學問，曾有某學術單位花了三、四天的時間才找出斷線的問題是因爲實體線路損壞的緣故。」

根據計中主管表示，校園區域網路內，網路不通的原因有百分之九十的機率是從路由產生的問題，只有百分之十的機率是因實體線路損壞(可能是施工被挖斷)而造成網路不通。針對非實體線路的問題，計中主管建議：

*「網路不通時，**MRTG** 這個工具可以幫忙找到問題的所在。而 **netflow** 只能測量一個時間內的平均流量統計，不能知道到底問題是在哪。」*

網路如果出現斷線的情形，對於所有的網路使用者都會造成不便，因此對於斷線備援的問題，計中主管提到實際的演習是非常重要的，誰也沒辦法保證，備援的問題可以如紙上談兵的順利。

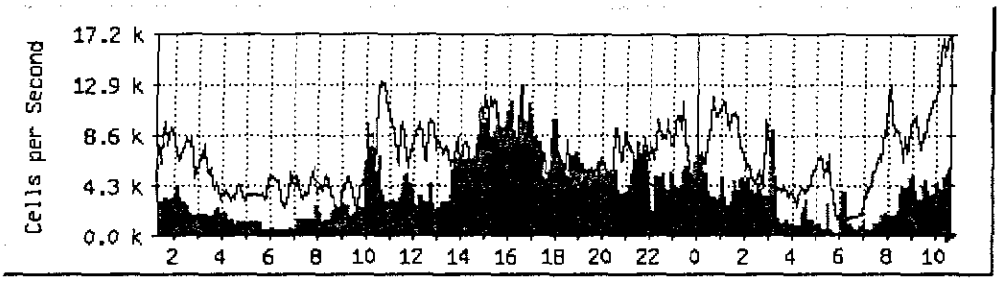
4.3 個案模擬分析

瞭解和掌握網路上的使用狀況一直是網路管理者非常關切的問題，因爲在目前網路頻寬不足的狀況下，如何對現有的網路做調整和對未來的設備擴充作預估，這些重要的評估都必須在對於現階段網路的使用狀況能有充分了解的基礎上，才能客觀的做出合理的決定。要了解網路狀況最重要的關鍵在於瞭解網路的流量及相關各類網路服務的使用情形。我們以 5 個 LAN，1 個 WAN 的網路連線模式作爲我們一個分析的模擬個案範圍。工具爲 MRTG、netflow 工具。主要將所取的資料圖表作流量的分析、壅塞的分析、網路繞送路徑分析以及斷線備援路徑選擇。我們對 LAN 的區網中心間實體層所作的流量分析，是利用 MIB2(RFC1213) 中定義的 Interface Group 中的 IntOut 和 IntIn 這兩個 MIB 變數，配合 MRTG 軟體達成了對各區網中心的實體層線路作流量監測。這些重要的統計資料反應了各區網間頻寬使用狀況，對各區網網管人員都有重要的參考價值。但因爲是實體層的流量資料，有許多過境和本地的流量全部包含在這些流量資量中，這些資料無法提供各區網中心互相間的流量資料。但這些流量資料對於未來的頻寬規劃和有極爲重要的價值。

4.3.1 流量分析：

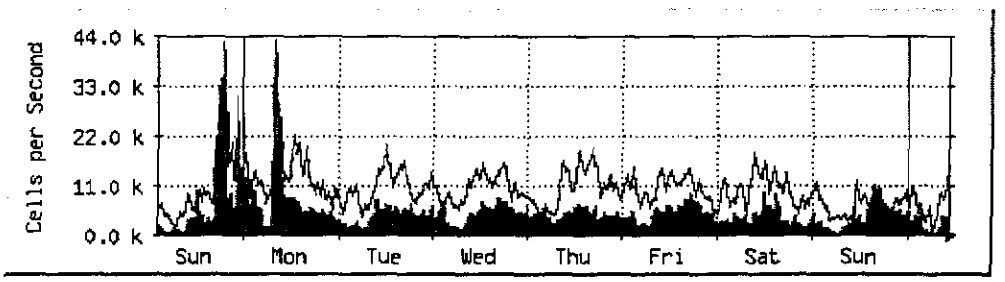
我們所使用的 MRTG 會將所有取得的網路效能資料搭配每個受測介面的其他資訊，以圖形的方式顯示出來，總共會提供四項統計圖表，分別將傳輸率以每天、每週、每月及每年的方式呈現。每日統計圖中以每 5 分鐘均一次的方式顯示近 36 小時的傳輸率計算結果。平均算法是由連續選取情況下，每個輸出或輸入位元組間的差異，並不是累積的總合或次數。也就是說顯示的數值是目前的結果與前一次結果間的差異再除以二次結果間隔的時間。其水平(X)軸以每二個小時爲一個單位，而垂直(Y)軸則由 0 到某個給定的最大值來顯示。在這個統計圖中顯示分別由 ifOutOctets 和 ifInOctets 二個物件所取得的介面輸出輸入的資料量。在統計圖之下則是關於統計結果的圖說內容。在這個例子中，輸入流量是綠色，而輸出的部份則是藍色。另外，在下面則有一些簡短的總結資料。包含最大傳輸率、平均傳輸率以及目前傳輸率。

每日' 圖表 (5 分鐘 平均)



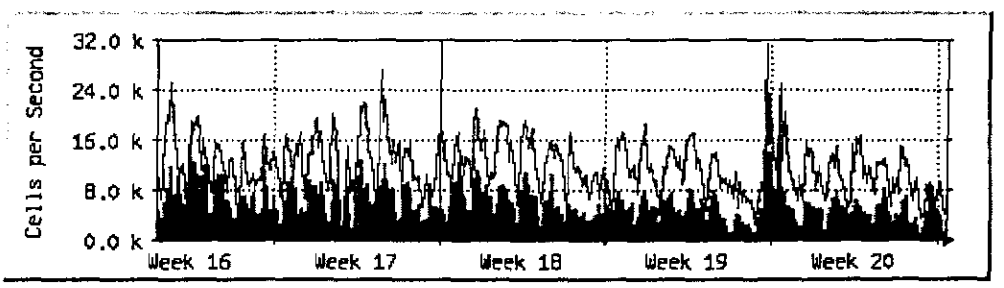
Max In:	12.9 kCells/s		Average In:	3881.0 Cells/s		Current In:	5900.0 Cells/s
Max Out:	17.1 kCells/s		Average Out:	6699.0 Cells/s		Current Out:	17.1 kCells/s

每週' 圖表 (30 分鐘 平均)



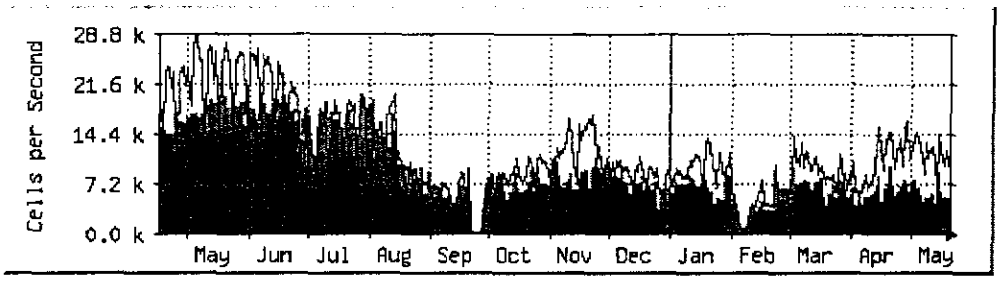
Max In:	38.7 kCells/s		Average In:	5276.0 Cells/s		Current In:	4631.0 Cells/s
Max Out:	43.0 kCells/s		Average Out:	10.5 kCells/s		Current Out:	15.8 kCells/s

每月' 圖表 (2 小時 平均)



Max In:	24.6 kCells/s		Average In:	5881.0 Cells/s		Current In:	3614.0 Cells/s
Max Out:	31.1 kCells/s		Average Out:	11.8 kCells/s		Current Out:	9330.0 Cells/s

每年' 圖表 (1 天 平均)



Max In:	20.4 kCells/s		Average In:	9356.0 Cells/s		Current In:	3556.0 Cells/s
Max Out:	28.7 kCells/s		Average Out:	11.7 kCells/s		Current Out:	9199.0 Cells/s

GREEN ###	Incoming Traffic in Bytes per Second
BLUE ###	Outgoing Traffic in Bytes per Second

圖 4-6：MRTG 圖表

在下面我們將會介紹幾個 MRTG 的流量圖來分析目前網路流量以及可能的網路狀況。

圖 4-7 流入量及流出量都滿檔，而且流入流出頻寬預設是一樣大。

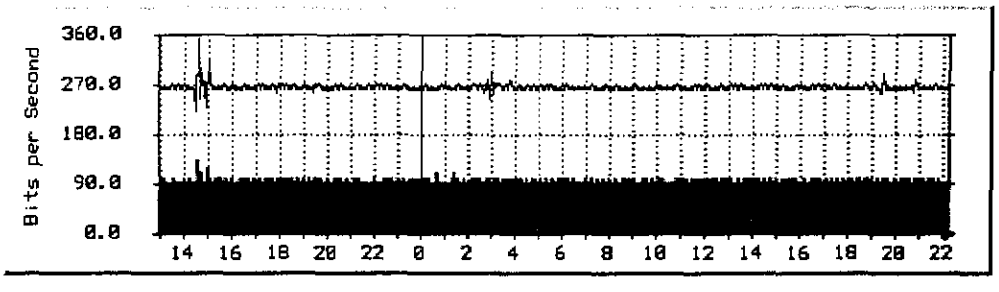


圖 4-7

圖 4-8 流入量及流出量都滿檔，但是流出的頻寬是較大而流入的頻寬限制較小。

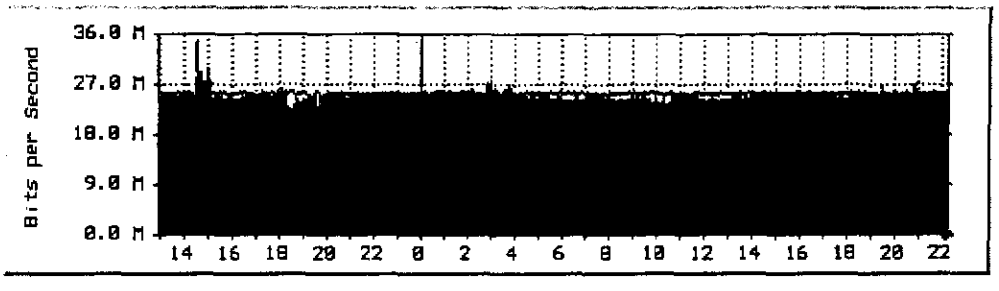


圖 4-8

圖 4-9 流入量滿檔，但是流出的量沒有滿檔。

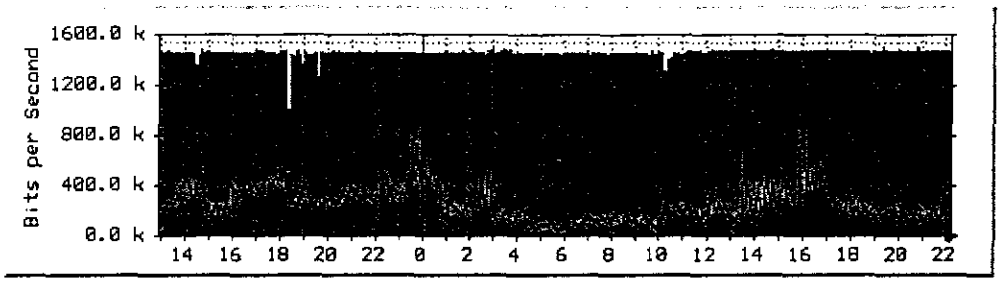


圖 4-9

圖 4-10 只流入不流出，可能流出的頻寬有限制。

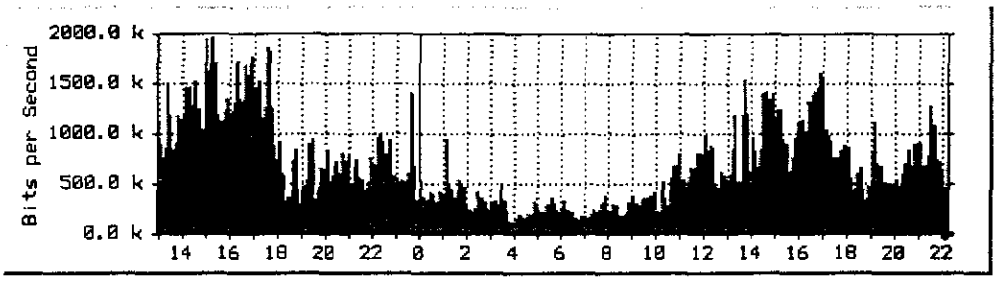


圖 4-10

雖然說 mrtg 是一個很不錯的網管工具，但是 mrtg 大多只監測出某一段時間的流量大小，但是至於是那個 service 或 ip 所佔的流量比率則不能從 mrtg 的統計圖中看出來。我們可以用另一個軟體叫 Netflow 的網管工具來測量。從 Netflow 中，我們可以得到各 ip 以及各種 service 的在網路流量中所佔的比例。這點對我們在分析及統計流量上非常有用。Netflow 也是 web 介面的網管軟體（如圖五），非常好操作。Netflow 有一個很好用的地方，可利用 TOP N 的功能，抓到前幾名流量異常大的 IP 位址 ，馬上可以查到使用此 IP 的使用者，我們可以先用 email 或電話去警告該使用者節制。目前在許多的網路大概都是 mrtg 配合著 netflow 來作爲網管的系統工具。MRTG 提供即時流量統計圖以及網路連線狀況，而 Netflow 提供量化的 netflow 資料，統計各種流量連線的資料分析。由於 netflow 所送出的資料量非常大，平均每個小時資料量大約是 250MB，因此整個系統需要很強的計算能力以及很大的硬碟空間。

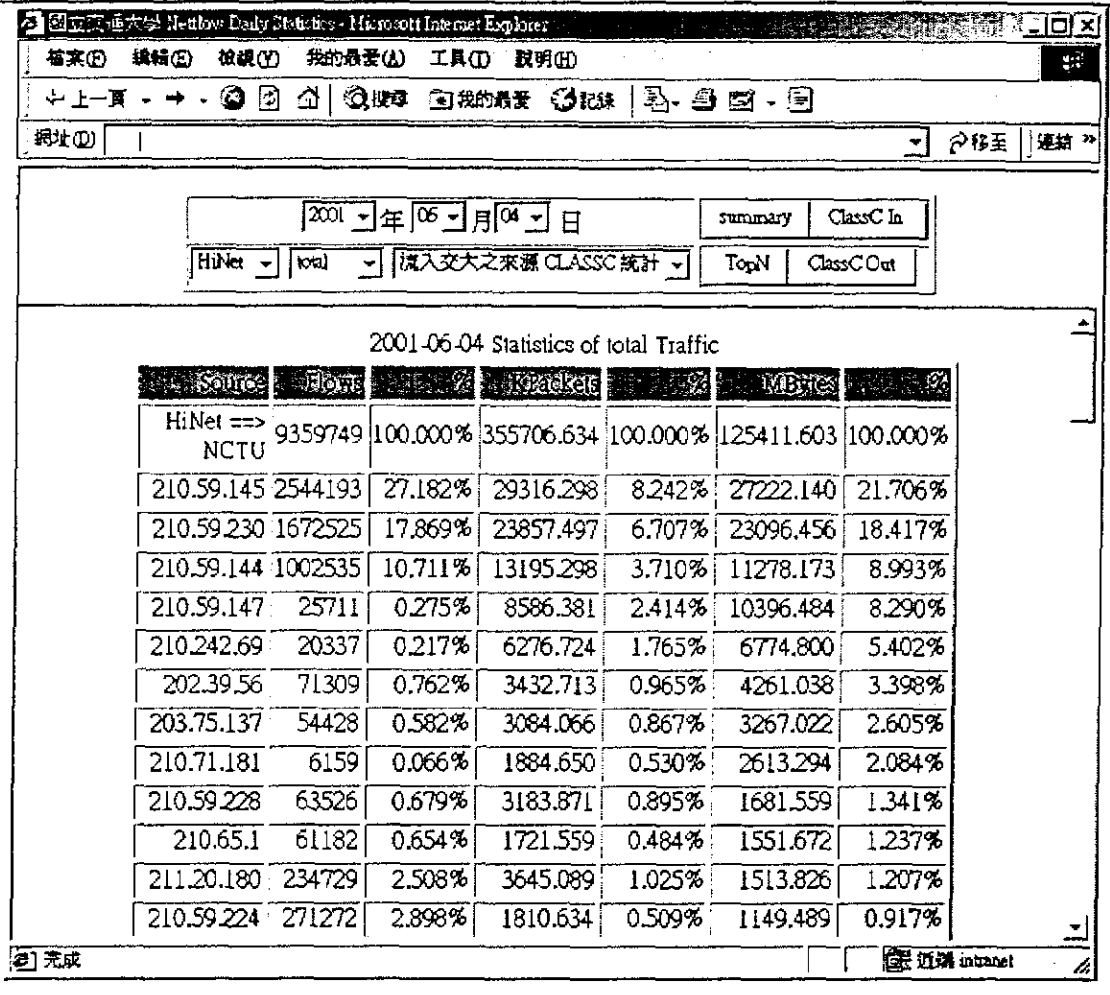


圖 4-11：Netflow WEB 操作介面

4.3.2 壅塞分析

我們可以從 mrtg 以及 netflow 來觀看出目前網路的狀況有否發生壅塞的情況。例如圖 4-12 所示：：

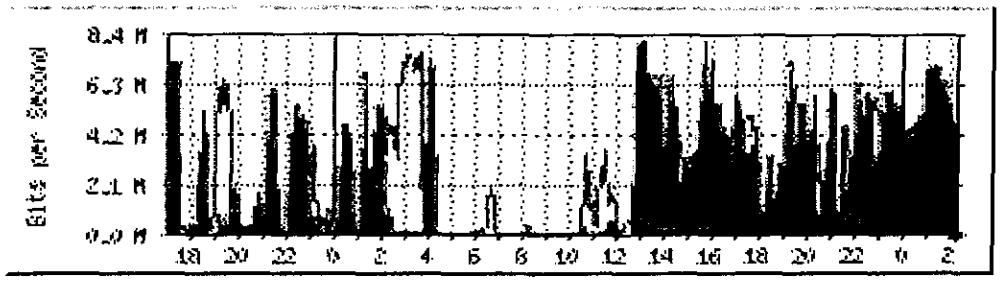


圖 4-12

我們可以看出來，在中午 12 點到晚上 2 點網路一直是很突然的急增，這可能會使我們的網路頻寬被佔滿，然而從 MRTG 我們只能知目前網路可能的狀況，這時我們可以再使用 netflow 來看看這段時間是那個 ip or service 在大量使用網路的頻寬。如圖 4-13 所示我們可以看出目前 www 的 service 是佔 81%左右的流量，可能此時有使用者在利用 www 下載大量的檔案資料。而圖 4-14 我們可以看出那一個 ip 所佔的量是最大。

Application	Flows	%	KPackets	%	MBytes	%
total	8612122	100.000%	199361.181	100.000%	135092.356	100.000%
www	6975760	80.999%	108614.566	54.481%	103858.232	76.879%
others	305312	3.545%	48479.809	24.318%	18267.957	13.523%
pop3	86665	1.006%	5236.352	2.627%	4482.559	3.318%
smtp	188456	2.188%	8278.814	4.153%	3607.428	2.670%
ftp-data	39142	0.454%	16459.855	8.256%	2401.607	1.778%
telnet	103708	1.204%	7666.028	3.845%	1699.640	1.258%

圖 4-13

Destination IP	Flows	%	KPackets	%	MBytes	%
LAN A ==> LAN B	11172920	100.000%	119994.272	100.000%	703793.420	100.000%
140.113.54.50	1397759	12.510%	9161.089	7.635%	45831.824	6.512%
163.19.163.252	227602	2.037%	3340.611	2.784%	25854.294	3.674%
140.126.136.250	203751	1.824%	2954.646	2.462%	21812.630	3.099%
140.126.1.2	209745	1.877%	2234.016	1.862%	15968.323	2.269%
140.126.21.134	21349	0.191%	1092.859	0.911%	11526.435	1.638%
163.19.1.11	190911	1.709%	1741.741	1.452%	9925.639	1.410%

圖 4-14

在面對網路壅塞時，大概原因可能很多，例如網路卡的設定問題或大量使用 Microsoft 網路芳鄰服務造成網路壅塞，網路攻擊亦會造成網路壅塞，如阻斷服務(DoS)的攻擊。我們通常可以採取幾項作法，如果我們發現是我們網域某一 ip 在傳送大量的資料封包，而已這些封包已經造成我們網路的壅塞的話，我們可以用幾個方式來要求對方節制。:

第一是用 Router 指令來限制。Netflow 有一個很好用的地方，可利用 TOP N 的功能，抓到前幾名流量異常大的 IP 位址 ，馬上可以查到使用此 IP 的使用者，我們可以先用 email 或電話去警告該使用者節制。不然我們可以利用 Cisco Router 裡的:Show arp | include xx.xx.xx.xx 指令找出他的 MAC address，對此 MAC address 在 switch 作鎖定動作。鎖定方法很簡單，只要將此 MAC 位址指向目前爲 down 的 interface 即可。第二是公布名單。最後則是鎖網路卡。

4.3.3 網路繞送路徑分析：

當我們由 mrtg 及 netflow 發現網路有壅塞情況時，也許是在我們網路繞送出了問題，中間某一點不通，我們這時可以考慮選擇其他的繞送路徑。在先前章節中我們有討論並訪談過交大的計中主管，他的建議是

a. *路由(route)的選擇可依據以下幾個考量點：(1)頻寬的負載重不重。*
b. *路由中間的節點是否可以被控制。*
c. *路徑的傳輸是否可靠。*
d. *依照應用的狀況與需求。*
e. *流量的起伏大小。"*

由於路由中間的節點，常常是無法由網路管理者完全控制的，所以學理上找尋最短路徑的方法，在實務上有其執行困難的地方，許多網路繞送路徑的選擇常是以上考量點與現實環境的妥協方案。

4.3.4 斷線備援分析：

當我們在使用 mrtg 以及 netflow 時有時會碰到網路斷線時，在這時 mrtg 的圖表可能如圖 4-15、圖 4-16 所示。圖 4-15 顯示了目前網路是不通的，沒有流量可以測量。而圖 4-16 是指出過去一整年裡，四月份有段時間，網路是不通的。一般而言，網路斷線可能是硬體出了問題或是軟體問題，實體的線路被挖斷了或是網路設備故障等等爲硬體問題，這較少發生。而軟體問題則常發生在路由此時可能就必需更改路由傳送路徑，而更改路由

傳送的路徑是普遍的處理方式，同樣更改路由的考量與前面所講路由選擇的考量點是一樣的。如果是硬體問題，例如實體線路損壞。此時實體的設備的修護則是此時的策略，不過在修護時，如何找到線路損壞的部分，是較困難的部份。

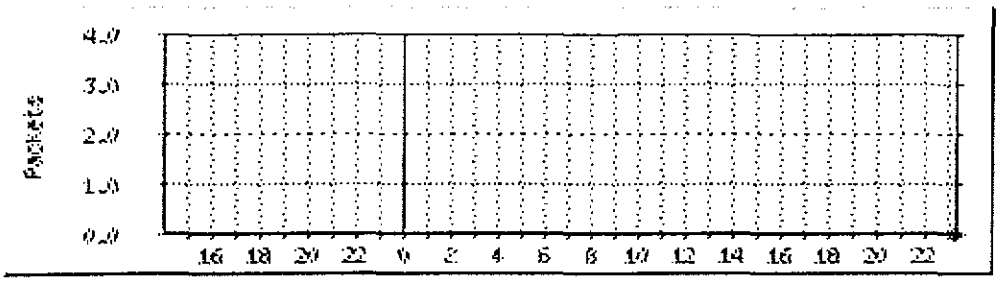


圖 4-15 :每日 圖表 (5 分鐘 平均)

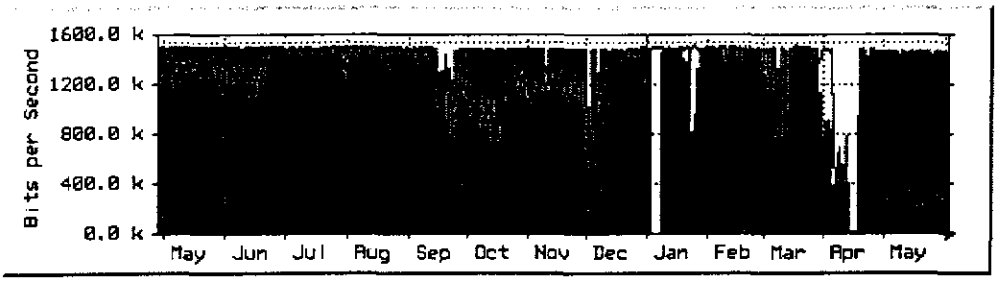


圖 4-16：每年 圖表 (月 平均)

5. 結論與建議

5.1 研究結論

由於資訊科技日益精進，世界各國紛紛將資訊技術應用於軍事、經濟、通信、媒體、財經、交通及教育等系統，以期提昇國家整體之競爭力。網路整合提供資訊共享，提高整體效益及備援性。但資訊網路整合面臨下列幾項問題：(1)不同網路標準、協定無法相連通?(2)網路各節點流量控制與分析瓶頸之所在？(3)網路控制點斷線後如何調整型態以達成系統備援的效果？DII 則是一個結合通訊網路、電腦、軟體、資料環境、應用軟體、武器系統介面、資料、安全防制，以及能滿足使用者對資訊的處理與傳遞的需求的資訊網。換言之，對國防部的使用者，特別是作戰人員，國防資訊基礎建設(DII)須能提供無缺失的、安全的資訊以協助決策與達成任務。

本計畫參考美軍國防資訊系統網路提出一具參考之網路架構分析與方法，以作爲在國防資訊網路建置之參考與依據。總結所取得的具體成果在於

a. 利用本研究成果所完成手冊，據以發展此技術之相關模擬技術。
b. 利用本研究成果，提供目前工業界使用之相關網路通訊及管理標準(如 ATM、SMDS、SONET)及諮詢以利國防資訊相關建設計畫順利推動。
c. 利用本研究成果，用現有之網路模式或參考美軍 MILNET 以作爲分析之基礎，經模擬結果可以提供國軍發展國防資訊基礎建設之網路分析之參考。
d. 利用本研究成果，以模擬方式計算出網路中最佳網路控制點(Control Point)位置以提供 DII 網路設計之參考。
e. 利用本研究成果，以模擬方式執行各種網路架構模式之點與點流量(Flow Control)及網路性能及壅塞(Congestion Control)分析。
f. 利用本研究成果，以模擬方式執行網路控制點斷線時，重新建立連線及路境(Routing)之各種因應方案分析。

5.2 研究限制

本研究部分訪談內容可能觸及區網中心的網路敏感性議題，儘管研究者強調所得資料僅於本計劃研究用，但因受訪者可能會有所顧忌而對回答有所保留，因此將會影響本次訪談之結果。

5.3 未來研究建議

爲因應資訊科技之衝擊，面對未來資訊作戰環境，現代化國防必須對資訊網路整合技術進行研發，以達成各系統間之整合需求，滿足網路之透通、各系統間裝備「互換性」、資料之「互通性」及「資訊安全」，進而提高系統整體之「存活性」、「維持性」、「擴充性」及降低「維護成本」。針對國防資訊基礎建設之四大部份：(1)資訊基層(Foundation)-程序及技術性事項(Program and Technical Activities)、(2)通訊與電腦基礎建設(Communications and Computer Infrastructure)、(3)共用應用程式(Common Applications)、(4)功能應用程式(Functional Area Applications)：功能應用層軟體是由指揮與管制、情報、任務支援等功能組織(functional community)所發展。其中通訊與電腦基礎建設所包括的項目：(1)國防資訊系統網路(Defense Information System Network)、(2)整體資訊處理(Enterprise Information Processing)、(3)控制中心(DII Control Centers)、(4)基地及部署地的通訊與電腦基礎建設(Base and Deployed/Afloat Communications and Computer Infrastructure)、(5)情報部門的通訊與電腦基礎建設(Intelligence Communications and Computer Infrastructure)整體資訊處理(Enterprise Information Processing)。

在未來戰爭領域中，可能會經歷一場「真正的軍事革命」，只需利用鍵盤和滑鼠就能擾亂或破壞敵人的指揮管制資訊系統。換言之，藉由「網路武力」爲主的戰略資訊作戰，可經由電腦網路發起作戰行動。舉凡敵人的資訊系統，從零件供應直到射控引導等，都可能遭到干擾。如何藉由發展電腦網路，甚至實務的大規模演習，應該是我國電腦專家，例如來自大學、研究機構、和訓練中心，爲保障國家社會安全前提下所努力的目標。就未來研究建議而言，國軍電腦網路，除了參考美軍的先進作法外，更應該考慮自行發展獨特的系統，以防止網路駭客的侵擾，特別是在作業系統，摒除微軟的牽制，利用開放性原始碼的作業系統發展屬於國軍的網路作業平台，當然，在達成互通時，也兼顧到我國國軍在使用網路時的安全性與自主性。

參考文獻

一、中文部份：

1. 羅濟群編著，商用資料通訊，民 85 年
2. 于方(民 89 年)，動態繞送法設計自動輸送機系統的派工員，國立交通大學工業工程與管理學系碩士論文
3. 潘玉峰，依流量需求動態調適群眾式的隨意型無線網路，元智大學電機與資訊工程研究所碩士論文
4. 簡榮成(民 89 年)，廣域網路流量監測與分析工具之製作，國立中正大學電機工程研究所碩士論文
5. 蔡佳宏(民 89 年)，針對壅塞網路的 TCP 流量控制之設計與分析，國立中正大學電機工程研究所碩士論文
6. 陳麗媛(民 89 年)，在 AIS 平台上實現網際網路流量，國立中正大學電機工程研究所碩士論文
7. 李成泰(民 89 年)，儲存爲基的 TCP/IP 區域網路拓樸探索與管理系統之建立，輔仁大學資訊管理學系碩士論文
8. 謝瑞宏(民 89 年)，分散式多重智慧型代理軟體爲基之網路流量擷取系統之研究，輔仁大學資訊管理學系碩士論文
9. 林胤昌(民 89 年)，於寬頻網際網路提供無壅塞傳輸服務的頻寬與緩衝區管理，國立臺灣大學資訊管理研究所碩士論文
10. 陳兆芳(民 89 年)，一個以分類元系統建構之動態適應式網路路徑決定方法，國立交通大學資訊科學研究所碩士論文
11. 羅濟群、梁文嘉、陳紹俊、吳顯東、高正一，Internet 之網路管理標準與應用，全球網際網路雜誌第二期
12. 文魁資訊股份有限公司，TCP/IP 疑難排解
13. 朱國華(民 86 年)，TCP/IP 通訊協定及網路架構研析，財政部財稅資料中心
14. 楊素秋，TANet 寬頻骨幹實施 IP 通訊協定的分析探討，國立中央大學計算機中心
15. 陳郁堂、游順發、臺彥博，即時性乙太網路之子網路頻寬管理系統，國立臺灣科技大學電子工程系
16. 游張松(民 84 年)，從 FDDI 到 ATM 的網路規劃
17. Steve Maxwell 著，丁昶文譯(民 90 年)，UNIX 網路管理工具
18. 楊素秋、曾黎明(民 89 年)，TANet 區網國內 ISP 訊務品質之監測與分析，2000 年台灣區網際網路研討會，PP 966-972

二、英文部份：

1. Rajiv Dighe, Qiang Ren and Bhaskar Sengupta (1995), A Link Based Alternative Routing Scheme for Network Restoration under Failure
2. D.Rumpel (1996), Experience in Training Operators for Network Restoration

3. Hoyoung Hwang, Kanghee Kim, Yanghee Choi and Chong Sang Kim (1998), Virtual Backup Network for Broadband Network Restoration
4. Robert MacDonald, Li-Oing Chen, Chao-Xing Shi and Boris Faer, Requirements of Optical Layer Network Restoration
5. Prashant Chandra, Yang-hua Chu, Allan Fisher, Jun Goo, Corey Kosak, T.S. Eugene Ng, Peter Steenkiste, Eduardo Takahashi and Hui Zhang (2001), Darwin: Customizable Resource Management for Value-Added Network Services
6. Sally Floyd (2001), A Report on Recent Developments in TCP Congestion Control
7. Zueng-Shuo Yang, An Experiment on Optimal Routing
8. D. Medhi and R. Khurana (1995), Optimization and Performance of Network Restoration Schemes for Wide-Area Teletraffic Networks
9. Internetworking Technology Overview, June 1999
10. Wei-Ping Wang and David Tipper, Recovery Routing in Wide Area Packet Networks
11. Fang Lu, ATM Congestion Control

三、網站部份：

1. Network Survivability，http://optcom.korea.ac.kr/Homepage/surviv.htm
2. ATM 專家論壇，http://www.tl.gov.tw/forum/atm/content.htm
3. 富智光纖寬頻通信，http://www.wisinfo.com.tw
4. 台灣學術網路，http://www.edu.tw/tanet/index.html
5. 台灣大學計算機中心，http://info.ntu.edu.tw/ntucc
6. 北京大學網路服務中心，http://www.pku.edu.cn/network
7. 清華大學計算機與通訊中心，http://www.nthu.edu.tw/ccc/index.html
8. 中央大學電算中心，http://www.cc.ncu.edu.tw
9. 交通大學計算機與網路中心，http://www.cc.nctu.edu.tw

中國互聯網路資訊中心(CNNIC)
網站訪問統計術語和度量方法
1999 年 12 月

一，介紹

中國互聯網路資訊中心(CNNIC)是成立於 1997 年 6 月 3 日的非盈利管理與服務機構，行使國家互聯網路資訊中心的職責。其宗旨是爲我國互聯網路用戶服務，促進我國互聯網路健康、有序地發展。隨著互聯網路在國內的飛速發展，廣大互聯網站迫切地需要瞭解他們的網站的訪問量資訊，於是他們採用了一些國內或國外的對於網站的訪問量進行測算和度量的服務。然而，這些服務面臨著一個重要的難題，即缺乏對訪問統計指標的權威定義和度量標準，既缺乏官方的標準也缺乏事實上的標準。各個服務提供商提供了不同統計口徑的統計指標，出於商業考慮，服務提供商往往也不公開他們的統計度量方法。對於網站來講，由於使用了不同的網站訪問統計服務，因而他們獲得的報告無法和其他網站的訪問統計報告進行比較。這種報告缺乏對廣告客戶的吸引力，一方面制約了網站的盈利空間，另一方面也制約了互聯網路的發展。對於廣告客戶來講，他們同樣面臨著困惑，因爲他們判斷不出選擇哪一個網站播出他們的廣告會收到更好的效果，他們的廣告投資應該與網站訪問量成正比，而可比較的網站訪問統計報告是他們進行投資的依據。

中國互聯網路資訊中心（CNNIC）建議的網站訪問統計術語和度量方法正是希望能夠提出一種具有可比性的、可被廣泛接受的網站訪問統計的標準。我們的任務就是建立一套網站訪問統計的術語，並對其度量方法提出建議。我們希望以此文檔作爲網站訪問統計的指導方針，幫助網站的建設者、網站的訪問者、網站的廣告客戶更全面更準確地獲得他們想要瞭解的資訊，爲他們精確地計劃、執行、實現他們的網上商業專案提供依據。

此文檔提供了網站訪問統計術語的解釋和對度量方法的建議，這將有助於網站使用一種通用的語言向外界發佈訪問統計的資訊。

我們起草這個建議是爲了促進互聯網路事業在國內的發展。我們也希望此文檔能夠引起互聯網路界的注意，使大家關注網站訪問資訊的度量。因爲我們真誠地希望互聯網網站能成爲廣告客戶更爲友好的媒體平臺，使互聯網站能夠走上持續發展的道路。

二，統計實現方式

對網站的訪問資訊的統計，我們建議採用如下的實現方式：

這種方式是對 Web 伺服器生成的日誌文件進行分析，這種日誌文件有時是原始的文件，有時是由第三方統計機構在伺服器端加入的模組生成的。這種方式的優點是可以定制自己格式的日誌文件，採用加密演算法和壓縮日誌文件的技術，以保證日誌文件的真實性和可靠性，並且降低傳遞日誌文件所產生的網路流量，適用于第三方機構進行網站訪問量的認證度量工作。當然這種方式也有自己的不足之處，包括難以做到即時的統計分析，而且在伺服器端的附加模組有可能降低 Web 伺服器的性能。在文檔中，當提及此方式時，我們稱爲分析日誌文件的方式

三，如何標識訪問者

標識網站的訪問者是網站訪問統計的基礎。不恰當的對訪問者的標識是目前多種訪問統

計服務提供的報告難以比較的根本原因。目前還沒有十全十美的標識訪問者的方法，因此多種訪問統計服務使用了不同的標識訪問者的方法是可以理解的。我們希望能夠提出一種具有可比性的、可被廣泛接受的網站訪問統計度量的標準。

訪問者（**Visitor**）

定義：

一個與網站有交互操作的個人。

度量方法：

我們建議採用以下方法作爲度量、識別訪問者的方法。先採用 IP 位址來標識訪問者，不同的 IP 位址表明不同的訪問者。當來訪的 IP 位址相同的時候試圖通過跟蹤文件（Cookie）來標識訪問者，不同的跟蹤文件（Cookie）表明不同的訪問者。在伺服器端加入的模組生成的含有擴展內容的日誌文件可識別出訪問者的跟蹤文件（Cookie），這將彌補原始日誌文件未記錄跟蹤文件（Cookie）的不足。跟蹤文件（Cookie）是指由伺服器向瀏覽器發送帶有 Set-cookie 頭資訊的 HTTP 回應，支援跟蹤文件（Cookie）的瀏覽器將在本機硬碟上保留一小片用於標識自己身份的資訊。不同的跟蹤文件（Cookie）可以表明不同的訪問者。

評論：

標識網站的訪問者是網站訪問統計的基礎。

用戶（User）和訪問者是同一術語，它們的含義相同。

1，單純使用跟蹤文件（Cookie）的方法存的問題。

（1）並不是所有瀏覽器都支援跟蹤文件（Cookie）。

（2）支援跟蹤文件（Cookie）的瀏覽器中有些允許採用不接受任何跟蹤文件（Cookie）的策略。

（3）跟蹤文件（Cookie）可以被某些程式或被手工刪除掉。

（4）如果用戶同時使用多種瀏覽器，則每個瀏覽器會保存不同的跟蹤文件（Cookie）。

（5）當用戶重新安裝作業系統或重新安裝瀏覽器時，跟蹤文件（Cookie）都有可能丟失，除非用戶手工保存它們。

（6）瀏覽器只能保存總共 300 個跟蹤文件（Cookie），每個跟蹤文件（Cookie）有 4K 的容量限制，每個域或伺服器只可以在用戶端放置 20 個跟蹤文件（Cookie）。

（7）存在著關於跟蹤文件（Cookie）侵犯訪問者隱私權的爭論。

跟蹤文件（Cookie）存在著種種爭議，但它仍然是值得推薦的方法之一，支援使用跟蹤文件（Cookie）的意見包括：

（1）由 Web 伺服器回應的包含 Set-cookie 的頭資訊不會被代理伺服器（Proxy）緩存（Cache），代理伺服器（Proxy）將傳送 Set-cookie 頭資訊給客戶瀏覽器。同樣地，包含 Cookie 的客戶請求的頭資訊也將被代理伺服器（Proxy）轉發給 Web 伺服器。因此，跟蹤文件（Cookie）是目前簡單而有效的識別使用代理伺服器（Proxy）訪問網路的用戶的方法。

（2）目前國內使用最廣泛的瀏覽器 Internet Explorer 3.x、4.x、5.x、Netscape 3.x、4.x

及 Opera 3.x 均支援跟蹤文件（Cookie），只有 1%的訪問者使用除此之外的其他瀏覽器。
（3）在默認狀態下，上述瀏覽器都採用接受所有跟蹤文件（Cookie）的策略。
（4）對於大多數友善的網站，跟蹤文件（Cookie）提供了一種方便訪問者訪問的機制，而不是一種偷窺用戶訪問路徑的工具。
2，通過 IP 地址識別訪問者是一種很常用而且值得推薦的方法之一，使用 IP 地址識別訪問者的優點是：
（1）對於直接連接在互聯網路上具有唯一 IP 位址的電腦，IP 位址可以準確地標識電腦及其來源。
（2）相對跟蹤文件（Cookie）來講，IP 位址跟蹤到電腦，而跟蹤文件（Cookie）跟蹤到瀏覽器。同一 IP 位址的電腦有可能由於同時使用多種瀏覽器而保留有多個跟蹤文件（Cookie），因此 IP 位址更好地標識了單獨的電腦。

通過 IP 地址識別用戶也存在一些問題。從 Web 伺服器的訪問日誌中無法全部識別通過代理伺服器（Proxy）訪問網路的用戶。儘管有時可以從 HTTP_USER_AGENT 環境變數看出訪問者使用了某種代理伺服器（Proxy），但仍然無法得知他到底是哪個訪問者。因此我們選擇採用 IP 位址爲主，跟蹤文件（Cookie）爲輔的方式來標識訪問者。

四，網站訪問量指標及度量

唯一訪問者（**Unique Visitor**）

定義：

唯一訪問者是指在一特定時間內第一次進入網站，具有唯一訪問者標識（唯一位址）的訪問者。這一特定時間建議爲一整天。

度量方法：

在同一天內，只記錄第一次進入網站的具有唯一訪問者標識的訪問者，在同一天內再次訪問該網站則不計數。

評論：

也稱日唯一訪問者（Daily Unique Visitor）。獨立訪問者、獨立訪客、獨立用戶、唯一用戶和唯一訪問者是同一術語。唯一訪問者提供了一定時間內不同觀眾數量的統計指標，而沒有反應出網站的全面活動。

月唯一訪問者（**Monthly Unique Visitor**）

定義：

同上。特定時間建議爲一整月。

度量方法：

在同一月內，只記錄第一次進入網站的具有唯一訪問者標識的訪問者，在同一月內再次訪問該網站則不計數。

用戶會話（**User Session**）

定義：

用戶會話是指具有唯一訪問者標識（唯一位址）的訪問者進入或再次進入網站的過程。

度量方法：

訪問者在 20 分鐘內與網站有交互活動則被認爲是同一次進入網站，不記錄新的用戶

會話數：當訪問者持續 20 分鐘與網站沒有交互活動，當他再次訪問網站時訪問者被認爲再一次進入了網站，記錄新的用戶會話數。
評論：
用戶進出數、訪問數（Visit）和用戶會話是同一術語。用戶會話不應該被解釋爲網站的訪問人次或訪問人數，但是用戶會話是相對接近網站訪問人次或訪問人數的指標。網站的精確的訪問人次或訪問人數難於被統計。用戶會話比唯一訪問者更能說明網站的全部活動，它表明了網站的使用頻率。
頁面閱覽（**Page View**）
定義：
一次頁面閱覽就是一次頁面的下載，訪問者成功地閱覽到頁面應該在他的瀏覽器上完整地看到該頁面。
度量方法：
一次瀏覽器請求即可算作一次頁面閱覽。
評論：
以一次瀏覽器的請求算作一次頁面閱覽並不是完全準確的。
1，代理伺服器（Proxy）緩存（Cache）和瀏覽器緩存（Cache）使伺服器記錄的請求數少於實際顯示在訪問者瀏覽器上的頁面數。
2，在帶寬小、回應時間長的情況下，訪問者可能在頁面顯示之前就跳轉至其他頁面瀏覽，因此即使伺服器記錄了訪問者的請求，但實際上並沒有被訪問者閱覽到。
3，醒目頁面（Splash Page）和空隙頁面（Interstitial）不應該被記錄入頁面閱覽次數之中。
4，動態的由程式生成的頁面應該記入頁面閱覽次數中。
5，含有幀（Frame）的頁面應該只被記錄一次頁面閱覽，即使含有幀（Frame）的頁面會產生對多個文檔的請求。
使用分析日誌文件的方式進行統計，醒目頁面（Splash Page）和空隙頁面（Interstitial）會被日誌文件記錄，在分析時應該忽略計算特定的醒目頁面（SplashPage）和空隙頁面（Interstitial）。在日誌文件中會記錄對特定的程式（如 CGI 程式）的請求，因而由這些程式動態生成的頁面也可以被計算。日誌文件識別不出含有幀的頁面，使用分析日誌文件的方式進行統計，這個誤差可以被接受。
頁讀數、頁面查看、閱覽（View）、頁面印象（Page Impression）、頁面請求（PageRequest）和頁面閱覽是同一術語。
請求（**Request**）
定義：
爲了獲得伺服器上的一個資源（可以是文本、圖像或任何可以被包含在頁面內的元素），瀏覽器和它連接的伺服器之間進行的一次單一連接。
度量方法：
對於使用分析日誌文件的方式進行的統計，日誌文件中一條記錄就是一個請求，通過對這些記錄的統計來獲得度量的資料。

評論：
命中（Hit）和請求是同一術語。當頁面請求指對 HTML 文檔的請求時，頁面請求是請求的一個子集，當頁面請求指訪問者頁面閱覽數時，請求和頁面請求的含義不同，在某些情況下，請求不被記錄在頁面閱覽或頁面請求內。
五，訪問者特徵指標及度量
瀏覽器（**Browser**）
定義：
一個用於定位和閱覽 HTML 文檔的程式（例如：Netscape Communicator、Mosaic、Microsoft Internet Explorer）。
度量方法：
可以從日誌文件中獲得瀏覽器類型的資訊，以此獲得統計的資料。
評論：
通常可以獲得軟體廠商的名字、瀏覽器的版本等資訊。但是瀏覽器字串（BrowserString）沒有標準的格式，這是分析它的一個困難之處。
平臺（**Platform**）
定義：
訪問網站的訪問者使用的操作平臺。
度量方法：
同分析瀏覽器一樣可以分析瀏覽器字串(Browser String)來獲得關於操作平臺的資訊。
評論：
考慮到特殊的瀏覽器如 WebTV 和 SEGA，稱爲操作平臺比稱爲作業系統更恰當一些。它們可以通過伴隨 URL 請求而來資訊加以識別。
瀏覽器語言（**Browser Language**）
定義：
瀏覽器所用的語言。
度量方法：
可以通過瀏覽器字串（Browser String）來得到瀏覽器的語言，HTTP_ACCEPT_LANGUAGE 環境變數也可以反映瀏覽器所希望接收的 HTML 文檔的語言。
評論：
並不是所有瀏覽器都可以獲得它所用的語言。使用分析日誌文件的方式無法獲得瀏覽器語言的資料。
功能變數名稱（**Domain Name**）
定義：
互聯網路上對應於電腦的 IP 位址的文本地址，它是連接在互聯網路上的電腦的正式的名字。
度量方法：
度量功能變數名稱實際上是考察遠端電腦所在的一級或二級域（Domain），

如：.com、.edu、.cn、.com.cn、.net.cn 等等。REMOTE_HOST 環境變數和日誌文件都會記錄遠端電腦主機名和功能變數名稱，但並不是所有情況下都可以獲得遠端電腦的主機名和功能變數名稱。

評論：

並不是所有連入互聯網路的電腦都可記錄其主機名和功能變數名稱，大部分電腦被記錄的仍然是 IP 位址而不是它們的主機名和功能變數名稱，對於沒有主機名和功能變數名稱的電腦，統計其所在域時應標明"未知"。不同的伺服器及其配置，會影響到是否可以獲得遠端電腦的主機名和功能變數名稱。可被反向解析 IP 位址的遠端電腦往往會被記錄下其主機名和功能變數名稱，但是在記錄日誌文件時進行 IP 位址的反向解析將增大伺服器的負荷，尤其對訪問量很大的網站。可以在分析日誌文件時再進行 IP 位址的反向解析，當然這也將減慢分析的速度。

指引鏈結（**Referrer**、**Referral Link**）

定義：

訪問者點擊一個頁面中的鏈結而被引導至當前 HTML 頁面，則該鏈結是當前頁面的指引鏈結。

度量方法：

從 HTTP_REFERER 環境變數和對伺服器日誌文件的分析中可獲得指引鏈結的資訊。

評論：

有時候也會遇到指引頁面（Referring Page）一詞，它們的意義相近，在瀏覽器中總是由指引的 URL 到達目標的 URL。

六，訪問者行爲指標及度量

每頁面請求的平均時間（**Average Time Per Page Request**）

定義：

訪問者每次多個頁面請求的平均時間。

度量方法：

用戶會話的第一次請求至最後一次請求間的時間 ÷ （用戶會話期間的頁面請求數－1）。

評論：

每頁面請求的平均時間應該在一個比較大的範圍內求得，計算用戶會話時長之前應該已計算出這個值。

用戶會話時長（**User Session Length**）

定義：

一次用戶會話的時間長度。

度量方法：

用戶會話的第一次請求至最後一次請求間的時間 ＋ 每頁面請求的平均時間。

評論：

用戶訪問時長和用戶會話時長是同一術語。

平均用戶會話時長（**Average User Session Length**）

定義：
網站訪問者用戶會話的平均時間長度。
度量方法：
總計的用戶會話時長 ÷ 用戶會話數。
評論：
平均用戶訪問時長和平均用戶會話時長是同一術語。
返回訪問（**Return Visits**）
定義：
在一特定時間內，訪問者在不同用戶會話中再次訪問網站的次數。
度量方法：
度量在一特定時間內，訪問者在不同用戶會話中再次訪問網站的次數。
評論：
這一特定時間可以由進行統計的機構決定。建議的時間可以是一天或者不設置這一特定時間，後者可以表明訪問者總共訪問該網站的次數。返回訪問的次數表明了網站的受歡迎的程度。
七，其他可度量指標
帶寬（**Bandwidth**）
定義：
網站流量的度量標準（以資料傳遞的千位元組爲單位）。
度量方法：
使用分析日誌文件的方式進行統計可以根據日誌文件中每條記錄中返回文件的大小來統計網站的帶寬。
重載（**Reload**）
定義：
訪問者點擊瀏覽器中的重載（Reload）按鈕或者是刷新（Refresh）按鈕重新載入當前的頁面的動作。
度量方法：
用分析訪問日誌文件的方式進行統計，當訪問者執行重載操作時都會重新發起對該頁面的請求，可以將 30 秒內相同的請求判斷爲訪問者執行了重載的操作，記錄重載次數。
評論：
重載操作的數目無法完全準確的被判斷。我們建議並列頁面閱覽數和重載數，而不必從頁面閱覽數中減去重載數。迎程度和訪問者對網站的忠誠度。
點擊（Click）
定義：
一次點擊是指訪問者的滑鼠在一個超文本鏈結上的一次單擊，目的是爲了沿著它的鏈結獲得更多訪問者感興趣的資訊。
度量方法：
只有使用分析日誌文件的方式可以統計出對於某個超文本鏈結點擊次數。

評論：
點擊數量（Click-Through、Clickthrough）和點擊是同一術語。點擊通常被用於網路廣告的統計。
點擊率（**Click Rate**）
定義：
點擊鏈結的百分比。
度量方法：
點擊數除以鏈結所在頁面的請求數。
評論：
收益（Yield）和點擊率是同一術語。點擊率有多方面的價值，在網路廣告中，它是廣告有效性的表現，它表示訪問者已到達廣告客戶的網站，而且這些網站還可以提供其他資訊。
廣告請求（**Ad Request**）
定義：
指訪問者對頁面中廣告元素的請求。
度量方法：
廣告請求的度量方法參考頁面閱覽的度量方法。
八，討論（FAQ）
Q.
統計的實現有沒有其他方式？
A.
另一種方式就是在希望進行統計的頁面上嵌入一段統計的代碼，這段代碼引用了另一伺服器上的資源，這個資源通常是由一個 CGI 程式（或其他類似的程式）動態生成的，當訪問者訪問該頁面時，將向此 CGI 程式（或其他類似的程式）所在的那一台伺服器發出請求，這樣該頁面被訪問的資訊及訪問者的資訊就會同時被那個 CGI 程式所記錄。這種方式易於做到即時的統計分析，統計資訊較爲豐富，而且不會增加 Web 伺服器端的負荷。但是這種方式容易被欺騙，也容易由於帶寬等原因而造成統計資訊收集的失敗。這種方式由於易被欺騙而存在著不安全的因素，也許在安全問題得以解決之後，它將成爲更好的統計實現方式。從易用性，內容豐富的程度來看，對這種統計方式的探索是有價值的。
Q.
爲什麼用戶會話的時間期間定爲 20 分鐘？
A.
我們參考了國際互聯網路界關於用戶會話時間期間的使用，發現主要使用的時間期間爲 30 分鐘和 20 分鐘。這個時間期間將影響到用戶會話數的度量，如果該時間期間更加接近於用戶在網站上的平均停留時間，則用戶會話數將更加接近於網站的用戶訪問人次數。CNNIC 對國內部分網站的統計表明，用戶在信息量大的網站上停留的時間更長一些。我們認爲目前用戶會話時間期間定爲 20 分鐘是合適的。我們會調整這個時間期間

以適應國內互聯網路的發展。

Q.

廣告客戶想知道他們的廣告確切地被訪問者看到的數目，而不是僅僅知道訪問者曾發出過請求。用什麼指標可以回答廣告客戶的問題？

A.

我們非常理解廣告客戶想知道他們廣告實際被看到的數目的要求，但實際上是無法完全準確地度量出這樣的資料的。如其它媒體一樣，廣告客戶爲潛在的閱覽數量付費（如按印刷的數量）。我們所能獲得的準確的資料只有訪問者發出的請求。在此文檔中我們建議統計於"請求"的層次而不是"遞送"的層次，因爲網站是否成功地將內容遞送給用戶是由多方面因素決定的，其中包括網路的狀況和用戶的行爲偏好等，所以難以被精確統計。可以用廣告請求這一指標來近似表明訪問者看到的廣告的數目。

Q.

我們的網站想瞭解訪問者是從哪一個省、市、自治區來訪的，可是似乎沒有這方面的統計指標？

A.

儘管訪問者的地理位置是一個很有價值的資訊，但列出訪問者是由哪個地理區域來訪的是很困難的，僅僅由 IP 地址來判斷以地域劃分的訪問者來源是不可靠的，而且目前也沒有近似的指標來表明訪問者的地理位置。

Q.

頁面閱覽和頁面請求似乎是不同術語，爲什麼這份文檔認爲它們是同一術語呢？

A.

頁面閱覽一詞側重於測量訪問者真實看到的頁面，頁面請求則側重於由訪問者發起的請求數量，即使最後可能訪問者並未真正閱覽到頁面。認爲它們是同一術語有兩個原因，其一是曾經提到的我們建議統計於"請求"的層次而不是"遞送"的層次，因此這兩個詞的度量方法是一致的，其二是我們希望此文檔能夠簡化過於繁雜的術語，將術語的數量精減，並有統一的解釋。但當提到伺服器接收到的對 HTML 文檔的請求時，仍可以使用頁面請求一詞。

Q.

我看到報紙上有報道說"某某網站首頁訪問量在兩個月內達到 70 萬人次"，這是什麼意思？

A.

這是不準確的說法，因爲精確的訪問人次在目前的技術水平下是無法被測量到的，將用戶會話數解釋爲訪問人次是錯誤的。如果網站的用戶會話數爲 70 萬，則報道就應該說"某某網站用戶會話數在兩個月內達到 70 萬"而不是"某某網站首頁訪問量在兩個月內達到 70 萬人次"。

Q.

這些術語的定義和度量方法實現在我們現有的系統上是否很困難？

A.

對於大多數網站來講，這並不會是一個大問題。因爲在起草這份文檔時，我們參考了

一些國內外現有的統計和度量網站訪問量的服務和軟體工具，事實上它們基本已經在使用這些術語和度量方法。但是網站訪問量的統計和度量還是一個缺乏標準的領域，我們起草這份文檔的初衷之一正是希望此領域能夠變得有章可循。

九，其他術語

瀏覽器緩存（**Browser Caching**）

定義：

爲了加速瀏覽，瀏覽器在用戶磁片上對最近請求過的文檔進行存儲，當訪問者再次請求這個頁面時，瀏覽器就可以從本地磁片顯示文檔，這樣就可以加速頁面的閱覽。但是，Web 伺服器可能因此而未計算一個頁面或廣告已被閱覽的次數。

代理伺服器緩存（**Proxy Caching**）

定義：

由代理伺服器對已下載的頁面的存儲。代理伺服器是作爲對互聯網上頻繁請求的文件的一個容器，這樣一些訪問者可以下載相同物件而使用更少的帶寬。但是，Web 伺服器可能未計算一個頁面或廣告已被閱覽的次數。

評論：

瀏覽器緩存和代理伺服器緩存是網站訪問統計最難解決的問題，但緩存的方式節約了網路的資源，提高了網路的效率。

伺服器（**Server**）

定義：

向所有訪問者提供服務的電腦，有時也指伺服器程式。

客戶（**Client**）

定義：

指網路的用戶所使用的電腦，有時也指被用於聯繫和從伺服器程式獲得資料的程式即客戶程式，伺服器程式通常在另一台電腦上。

跟蹤文件（**Cookie**）

定義：

永久性的用戶端的 HTTP 跟蹤文件（Cookie）是一些包含訪問網站的訪問者資訊（例如用戶名）的文件。這些資訊由網站在訪問者在第一次訪問時提供。伺服器將資訊記錄於一個文字檔案中並且將文件存儲在訪問者的硬碟上。當訪問者再次訪問相同的網站時，伺服器會獲得這個跟蹤文件（Cookie）中的內容，並且根據這些內容向訪問者提供相應的內容，或識別訪問者的身份。

日誌文件（**Log File**）

定義：

Web 伺服器或代理伺服器創建的文件，包含伺服器上訪問活動的全部資訊。

頁面（**Pages**）

定義：

所有網站是電子頁面的集合。每個網頁是一個包含文本，圖像，或媒體物件的 HTML（超文本標記語言）文檔。一個頁面可以靜態或者動態地產生。

醒目頁面（**Splash**）

定義：

醒目頁面是指在網站主頁面之前的一個基本頁面，通常突出網站的特點或作廣告。醒目頁面在經過短時間後可能移到主頁面上來。

空隙頁面（**Interstitial**）

定義：

空隙頁面是一個在訪問者和網站間內容正常遞送之中插入的頁面。空隙頁面被遞送給訪問者，但實際上並沒有被訪問者明確請求過。

返回代碼（**Return Code**）

定義：

伺服器對瀏覽器請求返回的代碼，表明傳輸是否成功以及原因。

網站（**Web Site**、**Site**）

定義：

在互聯網路上包含訪問者可以通過瀏覽器查看的 HTML 文檔的場所，網站宿主於伺服器上。

統一資源定位器（**URL**）

定義：

統一資源定位器是確定互聯網路上一個精確位置的方法。如：http://www.cnnic.net.cn/cnnic/reg/domain/domainapp.html 就是一個 URL。正如前面例子所示，一個 URL 由四部分組成：協定類型（http://），機器名（www.cnnic.net.cn），目錄路徑（/cnnic/reg/domain/），以及檔案名（domainapp.html）。

萬維網（**World Wide Web**、**WWW**、**W3**、**The Web**）

定義：

萬維網是一個基於超文本的、分散式的電腦系統，萬維網被發展用於向互聯網路用戶提供一種便利直觀的訪問資訊的方法。

廣告（**Ad**）

定義：

網站上任何充當商業工具傳送消息或吸引用戶的內容。典型地採取圖片的形式或文本消息，但是也可以是任何 HTML 文檔元素，例如那些根據需要而運行的 Java Applet 或 Shockwave 程式。

橫幅廣告（**Banner**）

定義：

在網頁上通常鏈結到廣告客戶站點的廣告圖片。橫幅廣告是網上廣告的主要的形式。標準的橫幅廣告尺寸有：1，468 x 60 圖元 2，392 x 72 圖元 3，234 x 60 圖元 4，120 x 240 圖元 5，120 x 90 圖元 6，120 x 60 圖元 7，125 x 125 圖元 8，88x 31 圖元

每千次頁面閱覽成本（**CPM**）

定義：

顯示的廣告印象 1000 次的費用總計。

評論：

這一量度是從印刷廣告借用的。由於不是所有頁面閱覽最終都看到廣告（例如翻滾一個頁面）。每千次頁面閱覽成本常被解釋爲每千次廣告閱覽成本。M 表示羅馬數字的一千。這是一個正在形成的網站廣告的標準定價模型。

中國 Internet 發展大事記

1987 年 9 月 20 日，錢天白教授發出我國第一封電子郵件"越過長城，通向世界"，揭開了中國人使用 Internet 的序幕。錢天白教授負責的 CANET(Chinese Academic Network)國際聯網專案是在 1986 年由北京市電腦應用研究所實施的科研專案，其合作夥伴是原西德的卡爾斯魯厄 KARLSRUHE）大學。錢天白教授發出的這封電子郵件是通過義大利公用分組網 ITAPAC 設在北京側的 PAD 機，經由義大利 ITAPAC 和德國 DATEX—P 分組網，實現了和德國卡爾斯魯厄大學的連接，通訊速率最初爲 300bps。

1988 年 12 月，清華大學校園網採用胡道元教授從加拿大 UBC 大學（University of British Columbia）引進的採用 X400 協定的電子郵件套裝軟體，通過 X.25 網與加拿大 UBC 大學相連，開通了電子郵件應用。

1988 年，中國科學院高能物理研究所採用 X.25 協定使該單位的 DECnet 成爲西歐中心 DECnet 的延伸，實現了電腦國際遠端連網以及與歐洲和北美地區的電子郵件通信。

1989 年 5 月，中國研究網（CRN）通過當時郵電部的 X.25 試驗網（CNPAC）實現了與德國研究網（DFN）的互連。CRN 的成員包括：位於北京的電子部第 15 研究所和電子部電子科學研究院、位於成都的電子部第 30 研究所、位於石家莊的電子部第 54 研究所、位於上海的復旦大學和上海交通大學、位於南京的東南大學等單位。CRN 提供符合 X.400（MHS）標準的電子郵件、符合 FTAM 標準的文件傳送、符合 X.500 標準的目錄服務等功能，並能夠通過德國 DFN 的閘道與 Internet 溝通。

1989 年 9 月，國家計委組織對世界銀行貸款專案中關村地區教育與科研示範網路（NCFC）工程承擔單位的招標。NCFC 是由世界銀行貸款"重點學科發展專案"中的一個高技術資訊基礎設施專案，由國家計委、國家科委、中國科學院、國家自然科學基金會、國家教委配套投資和支援。專案由中國科學院主持，聯合北京大學、清華大學共同實施。當時立項的主要目標就是在北京大學、清華大學和中科院三個單位間建設高速互聯網路，以及建立一個超級計算中心。

1990 年 10 月，錢天白教授代表中國正式在國際互聯網路資訊中心的前身 DDN-NIC（當時尚未正式成立 INTERNIC，而是由美國國防部 ARPANET 網路中心 DDN-NIC 負責全球互聯網路功能變數名稱和 IP 地址的分配）註冊登記了我國的頂級功能變數名稱 CN，並且從此開通了使用中國頂級功能變數名稱 CN 的國際電子郵件服務。由於當時中國尚未正式連入 Internet，所以委託德國卡爾斯魯厄大學運行 CN 功能變數名稱伺服器。

1991 年，中國科學院高能物理研究所採用 DECNET 協定，以 X.25 方式連入美國斯坦福線性加速器中心（SLAC）的 LIVEMORE 實驗室，並開通電子郵件應用。

1992 年 6 月於日本神戶舉行的 INET'92 年會上，中科院錢華林研究員約見美國國家科學基金會國際聯網部負責人，討論中國正式連入 Internet 的問題，但被告知，由於網上有很多美國的政府機構，中國接入 Internet 有政治障礙。

1992 年，NCFC 工程的院校網，即中科院院網（CASNET，連接了中關村地區三十多個研究所及三裏河中科院院部）、清華大學校園網（TUNET）和北京大學校園網（PUNET）全部完成建設。

1993 年 3 月 2 日，中國科學院高能物理研究所租用 AT&T 公司的國際衛星通道接入

美國斯坦福線性加速器中心（SLAC）的 64K 專線正式開通。專線開通後，美國政府以 Internet 上有許多科技資訊和其他各種資源，不能讓社會主義國家接入爲由，只允許這條專線進入美國能源網而不能連接到其他地方。儘管如此，這條專線仍是我國部分連入 Internet 的第一根專線。專線開通後，國家基金委大力配合並投資 30 萬元，使各個學科的重大課題負責人能夠撥號連入高能所的這根專線，幾百名科學家得以在國內使用電子郵件。

1993 年 3 月 12 日，朱鎔基副總理主持會議，提出和部署建設國家公用經濟資訊通信網(簡稱金橋工程)。

1993 年 4 月，中國科學院電腦網路資訊中心召集在京部分網路專家調查了各國的功能變數名稱體系，提出並確定了我國的功能變數名稱體系。

1993 年 6 月，NCFC 專家們在 INET'93 會議上利用各種機會重申了中國連入 Internet 的要求，且就此問題與國際 Internet 界人士進行商議。INET'93 會議後，錢華林研究員參加了 CCIRN 會議，其中一項議程專門討論中國連入 Internet 的問題，獲得大部分到會人員的支援。這次會議對中國能夠最終真正連入 Internet 起到了很大的推動作用。

1993 年 8 月 27 日，李鵬總理批准使用 300 萬美元總理預備金支援啓動金橋前期工程建設。

1993 年 12 月，國家經濟資訊化聯席會議成立，國務院副總理鄒家華任主席。

1993 年 12 月，NCFC 主幹網工程完工，採用高速光纜和路由器將三個院校網互連。

1994 年 1 月，在中美科技合作聯委會前，美國國家科學基金會同意了 NCFC 正式接入 Internet 的要求。1994 年 3 月，開通並測試了 64Kbps 專線。

1994 年 4 月初，中美科技合作聯委會在美國華盛頓舉行。會上，中科院副院長胡啓恒代表中方向美國國家科學基金會（NSF）重申連入 Internet 的要求，得到認可。

1994 年 4 月 20 日，NCFC 工程通過美國 Sprint 公司連入 Internet 的 64K 國際專線開通，實現了與 Internet 的全功能連接。從此我國被國際上正式承認爲有 Internet 的國家。此事被我國新聞界評爲 1994 年中國十大科技新聞之一，被國家統計公報列爲中國 1994 年重大科技成就之一。

1994 年 5 月 15 日，中國科學院高能物理研究所設立了國內第一個 WEB 伺服器，推出中國第一套網頁，內容除介紹我國高科技發展外，還有一個欄目叫"Tour in China"。此後，該欄目開始提供包括新聞、經濟、文化、商貿等更爲廣泛的圖文並茂的資訊，並改名爲《中國之窗》。

1994 年 5 月 21 日，在錢天白教授和德國卡爾斯魯厄大學的協助下，中國科學院電腦網路資訊中心完成了中國國家頂級功能變數名稱(CN)伺服器的設置，改變了中國的 CN 頂級功能變數名稱伺服器一直放在國外的歷史。由錢天白、錢華林分別擔任我國 Internet 的行政聯絡員和技術聯絡員。

1994 年 6 月 8 日，國務院辦公廳向各部委、各省市明傳發電《國務院辦公廳關於'三金工程'有關問題的通知(國辦發明電[1994]18 號)》。自此，金橋前期工程建設全面展開。

1994 年 6 月 28 日，在日本東京理科大學的大力協助下，北京化工大學開通了與 Internet 相連接的試運行專線。

1994 年 9 月，中國電信與美國商務部布朗部長簽定中美雙方關於國際互聯網的協定，協定中規定中國電信將通過美國 Sprint 公司開通 2 條 64K 專線（一條在北京，另一條在上海）。中國公用電腦互聯網（CHINANET）的建設開始啓動。

1994 年 10 月，由國家計委投資，國家教委主持的中國教育和科研電腦網（CERNET）開始啓動。該專案的目標是建設一個全國性的教育科研的基礎設施，利用先進實用的電腦技術和網路通信技術，把全國大部分高等學校和中學連接起來，推動這些學校校園網的建設和資訊資源的交流共用，從而極大地改善我國大學教育和科研的基礎環境，推動我國教育和科研事業的發展。

1994 年，由 NCFC 管理委員會主辦，中國科學院、北京大學、清華大學協辦的 APNG（亞太地區網路工作組）年會在清華大學召開。這是國際 Internet 界在中國召開的第一次亞太地區年會。

1995 年 1 月，中國電信分別在北京、上海設立的通過美國 Sprint 公司接入美國的 64K 專線開通，並且通過電話網、DDN 專線以及 X.25 網等方式開始向社會提供 Internet 接入服務。

1995 年 1 月，由教育部（當時國家教委）主管主辦的《神州學人》雜誌，經中國教育和科研電腦網（CERNET）進入 Internet，向廣大在外留學人員及時傳遞新聞和資訊，成爲我國第一份中文電子雜誌。

1995 年 3 月，中國科學院完成上海、合肥、武漢、南京四個分院的遠端連接（使用 IP/X.25 技術），開始了將 Internet 向全國擴展的第一步。

1995 年 4 月，中國科學院啓動京外單位聯網工程（俗稱"百所聯網"工程）。其目標是在北京地區已經入網的 30 多個研究所的基礎上把網路擴展到全國 24 個城市，實現國內各學術機構的電腦互聯並和 Internet 相連。在此基礎上，網路不斷擴展，逐步連接了中國科學院以外的一批科研院所和科技單位，成爲一個面向科技用戶、科技管理部門及與科技有關的政府部門服務的全國性網路，取名"中國科技網"（CSTNet）。

1995 年 5 月，中國電信開始籌建中國公用電腦互聯網（CHINANET）全國骨幹網。

1995 年 7 月，中國教育和科研電腦網（CERNET）連入美國的 128K 國際專線開通。

1995 年 8 月 8 日，建在中國教育和科研電腦網（CERNET）上的水木清華 BBS 正式開通，成爲中國大陸第一個 Internet 上的 BBS。

1995 年 12 月，中科院百所聯網工程完成。

1995 年 12 月，中國教育和科研電腦網（CERNET）網路一期工程提前一年完成並通過了國家計委組織的驗收。

1996 年 1 月，成立國務院資訊化工作領導小組及其辦公室，國務院副總理鄒家華任領導小組組長。

1996 年 1 月，中國公用電腦互聯網（CHINANET）全國骨幹網建成並正式開通，全國範圍的公用電腦互聯網路開始提供服務。

1996 年 2 月 11 日，國務院第 195 號令發佈了《中華人民共和國電腦資訊網路國際聯網管理暫行規定》。

1996 年 3 月，清華大學提交的適應不同國家和地區中文編碼的漢字統一傳輸標準被

IETF 通過爲 RFC1922，成爲中國國內第一個被認可爲 RFC 文件的提交協定。

1996 年 7 月，國務院資訊辦組織有關部門的多名專家對國家四大互聯網路和近 30 家 ISP 的技術設施和管理現狀進行調查，對網路管理的規範化起到了推動作用。

1996 年 8 月，國家計委正式批准金橋一期工程立項，並將金橋一期工程列爲"九五"期間國家重大續建工程項目。

1996 年 9 月 6 日，中國金橋資訊網（CHINAGBN）連入美國的 256K 專線正式開通。中國金橋資訊網宣佈開始提供 Internet 服務，主要提供專線集團用戶的接入和個人用戶的單點上網服務。

1996 年 11 月，中國教育和科研電腦網（CERNET）開通 2M 國際通道。

1996 年 12 月，中國公衆多媒體通信網（169 網）開始全面啓動，廣東視聆通、天府熱線、上海熱線作爲首批站點正式開通。

1997 年 4 月 18 日至 21 日，國務院在深圳召開全國資訊化工作會議。會議確定了國家資訊化體系的定義、組成要素、指導方針、工作原則、奮鬥目標、主要任務，並通過了"國家資訊化 95 規劃和 2000 年遠景目標"，將中國互聯網列入國家資訊基礎設施建設，並提出建立國家互聯網資訊中心和互聯網交換中心。

1997 年 5 月 20 日，國務院頒佈了《國務院關於修改〈中華人民共和國電腦資訊網路國際聯網管理暫行規定〉的決定》，對《中華人民共和國電腦資訊網路國際聯網管理暫行規定》進行修正。

1997 年 5 月 30 日，國務院資訊化工作領導小組辦公室發佈《中國互聯網路功能變數名稱註冊暫行管理辦法》，授權中國科學院組建和管理中國互聯網路資訊中心（CNNIC），授權中國教育和科研電腦網網路中心與 CNNIC 簽約並管理二級功能變數名稱.edu.cn。

1997 年 5 月 31 日，北京化工大學切斷衛星專線，接入中國教育和科研電腦網（CERNET）。

1997 年 6 月 3 日，受國務院資訊化工作領導小組辦公室的委託，中國科學院在中國科學院電腦網路資訊中心組建了中國互聯網路資訊中心(CNNIC)，行使國家互聯網路資訊中心的職責。同日，國務院資訊化工作領導小組辦公室宣佈成立中國互聯網路資訊中心(CNNIC)工作委員會。

1997 年 11 月，中國互聯網路資訊中心（CNNIC）發佈了第一次《中國 Internet 發展狀況統計報告》。截止到 1997 年 10 月 31 日，我國共有上網電腦 29.9 萬台，上網用戶 62 萬人，CN 下註冊的功能變數名稱 4066 個，WWW 站點 1500 個，國際出口帶寬 18.64Mbps。

1997 年 12 月 8 日，國務院資訊化工作領導小組審定通過了《中華人民共和國電腦資訊網路國際聯網管理暫行規定實施辦法》。

1997 年 12 月 30 日，公安部發佈了由國務院批准的《電腦資訊網路國際聯網安全保護管理辦法》。

1997 年，中國公用電腦互聯網（CHINANET）實現了與中國其他三個互聯網路即中國科技網（CSTNET）、中國教育和科研電腦網（CERNET）、中國金橋資訊網

（CHINAGBN）的互連互通。

1998 年 3 月，第九屆全國人民代表大會第一次會議批准成立資訊產業部，主管全國電子資訊產品製造業、通信業和軟體業，推進國民經濟和社會服務資訊化。

1998 年 7 月，中國互聯網路安全產品測評認證中心通過國務院資訊化工作領導小組辦公室驗收，開始試運行。

1998 年 7 月，中國互聯網路資訊中心（CNNIC）發佈了第二次《中國 Internet 發展狀況統計報告》。截止到 1998 年 6 月 30 日，我國共有上網電腦 54.2 萬台，上網用戶 117.5 萬人，CN 下註冊的功能變數名稱 9415 個，WWW 站點 3700 個，國際出口帶寬 84.64Mbps。

1998 年 7 月，中國公用電腦互聯網（CHINANET）骨幹網二期工程開始啓動。二期工程將使八個大區間的主幹帶寬擴充至 155M，並且將八個大區的節點路由器全部換成十億位元路由器。

1999 年 1 月，中國互聯網路資訊中心（CNNIC）發佈了第三次《中國 Internet 發展狀況統計報告》。截止到 1998 年 12 月 31 日，我國共有上網電腦 74.7 萬台，上網用戶數 210 萬，CN 下註冊的功能變數名稱 18396 個，WWW 站點 5300 個，國際出口帶寬 143M256K。

1999 年 1 月，中國教育和科研電腦網（CERNET）的衛星主幹網全線開通，大大提高了網路的運行速度。同月，中國科技網（CSTNET）開通了兩套衛星系統，全面取代了 IP/X.25，並用高速衛星通道連到了全國 40 多個城市。

1999 年 2 月，中國國家資訊安全測評認證中心（CNISTEC）正式運行。

[後記]

爲了真實地記錄我國 Internet 的發展歷程，促進我國 Internet 的健康發展，受資訊產業部及 CNNIC 工作委員會的委託，CNNIC 承擔了《中國 nternet 發展大事記》的編輯工作。目前這個《中國 Internet 發展大事記》只是一個初稿，儘管 CNNIC 的工作人員在編輯過程中力求做到準確、公正，但其中肯定會有疏漏，希望各界朋友提出寶貴意見，以便進行進一步的修改補充，反饋意見請發給 walterwu@cnnic.net.cn。《中國 Internet 發展大事記》初稿及今後的修訂稿將放在 CNNIC 網站上。