

行政院所屬各機關因公出國人員出國報告書

(出國類別:實習)

『不同 TMN 網路維運管理系統及整合系統』
出國報告書

服務機關：中華電信股份有限公司

出國人職稱：股長

出國人姓名：巫文成

出國地點：美國、加拿大

出國期間：89年8月6日至89年8月19日

報告日期：89年12月30日

H6/c08904481

提供客戶高品質的通信服務，是每一電信公司所期望的。目前電信網路技術日新月異，各種新功能、新服務不斷推出，為的是要配合科技的進步帶給客戶通信上的便利，也是為了強化公司的競爭力，在電信自由化的環境下，唯有積極提供新穎服務、提昇服務品質、降低產品價格等，才不致被客戶所唾棄。

然而，就一個過去擁有龐大電信網路的公司而言，要隨著電信自由化的策略而轉型，談來又何容易。除了人力、組織需作適度調整外，那些龐大的電信網路，又如何一方面汰舊換新以提供新功能，另一方面整合不同系統之維運管理以節省維運人力，這些都是網路維運管理方面最重要的課題。

過去由於系統設備種類繁多，其所提供的維運管理功能又通常依不同廠商或不同類型的設備獨立運作，其輸出入介面、網管資訊格式及內容各自不同，因此電信網路之管理，往往須靠多個系統各自運作方能竟其功。如此，使管理工作需要較多人工作業，整個網路管理系統維運效率也無法提昇。提供客戶高品質、高效率的新服務，網路維運管理技術的提昇實不容忽視。

職奉派赴美國朗訊 (Lucent) 公司及加拿大北電網路 (Nortel) 公司實習不同系統網路維運管理及整合技術，本報告即綜合研習課程，彙整成五章，其內容摘述如下：

第一章 電信管理網路

第二章 北電網路管理系統

第三章 SDH 網路管理系統

第四章 Netminder 網路管理系統

第五章 感想與建議

在不同網路設備獨立維運管理運作之下，增加整體網路維運困難度，效率也無法提昇。各國際組織研究單位從 1989 年開始陸續研擬一系列電信網路管理標準，期使各家設備製造商能有所依循，使電信業者在使用不同廠牌不同設備時，系統之管理介面、資料格式等能互連運作良好，以減少人工作業，提昇維運效率。

北電網路公司的寬頻網路 (ATM) 及朗訊公司的同步數位階層 (SDH) 傳輸設備均為本公司目前積極建設的設備，於完工啟用後，對本公司整體網路具舉足輕重地位，其所提供之網路維運管理系統亦以電信管理網路之架構為準則。而 NetMinder 是朗訊公司所研發之另一個整合網管維運系統，它可監視整個網路元件、鏈路等之整體運作效能及訊務、障礙、控制等。對於語音、信號、網路所提供近乎即時之管理控制，維運人員可利用其控制功能，使網路運作最佳化。

第 1 章、 電信管理網路(TMN)	1
1.1. 概述	1
1.2. TMN 架構	1
1.3. TMN 與 OSI 之關係	5
1.4. SNMP-Based 網管架構	8
1.5. CMIP 網管架構	9
1.6. SNMP 與 CMIP 的比較	10
1.7. ATM 網路管理架構	11
1.8. CORBA based 網管架構	14
1.9. Web-based 網管架構	15
第 2 章、 北電網路管理系統	16
2.1. 簡介	16
2.2. NMS 架構	17
2.2.1. 工作站組態	17
2.2.2. NMS 階層架構	18
2.2.3. NMS 工具組(toolsets)	18
2.3. 北電寬頻網路之管理	22
2.3.1. Passport 網路管理	22
2.3.2. 網路管理通信介面	25
第 3 章、 SDH 網路管理系統	28
3.1. ITM 架構	28
3.2. ITM-SC 功能	29
3.3. ITM-NM 功能	32
第 4 章、 NETMINDER 網路管理系統	34
4.1. NetMinder NTP	34
4.2. NetMinder NTM	37
4.2.1. 資料收集	38
4.2.2. 告警功能	38
4.2.3. 控制功能	38
第 5 章、 感想與建議	39

第 1 章、電信管理網路(TMN)

1. 1. 概述

電信網路管理，基本上是以電信交換、傳輸或終端設備本身所提供的維運管理功能所達成的，由於電信科技的突飛猛進，電信網路種類繁多，各種設備所提供的維運管理功能通常是依不同廠商或不同類型的設備個別獨立運作，其輸出入介面、網管資訊格式及內容各自不同，系統間無法資源共享，功能上的整合亦有困難，這種以個別的維運管理系統各自運作，往往使電信網路管理工作需要較多的人工作業，整體的網管運作效率也無法提升，為克服此一難題，各網路服務提供者及政府部門、研究機構等，均積極加入研究，期能提供整合電信網路管理服務。

ITU-T 從 1989 年開始陸續研擬一系列的電信網路管理標準，希望能以開放式、標準化方式，一方面讓網路設備廠商有所依循，期使個各電信網路設備能提供統一標準的網管通信介面，另一方面對電信網路提供者可以建立獨立於電信網路之外的支援性網路，即所謂 TMN 管理網路。除了 ITU-T 外，ISO、IETF、ETSI、ANSI、ATM FORUM、RACE、EUROTELDEV、EURESCOM 等區域組織也都參與 TMN 之研究，期能訂出電信網路管理標準。

1. 2. TMN 架構

TMN 可視為由獨立之數據通信網路組成之管理網路，實際上網路之連結，則允許利用電信網路本身所提供之維運專用的數據通信通道來達成，圖 1.1 為 TMN 架構圖，它顯示 TMN 與電信網路是重疊的關係。

TMN 標準在 ITU-T 為 M 系列建議書，主要文件如 M. 3000 為 TMN 之簡介，M. 3010 說明 TMN 之原理，M. 3020 定義選擇標準通信協定之方法，M. 3200 定義 TMN 之管理服務，M. 3400 定義 TMN 之管理功能，M. 3100 定義一般性網路資訊模式，M. 3180 詳列 TMN 管理資訊目錄。

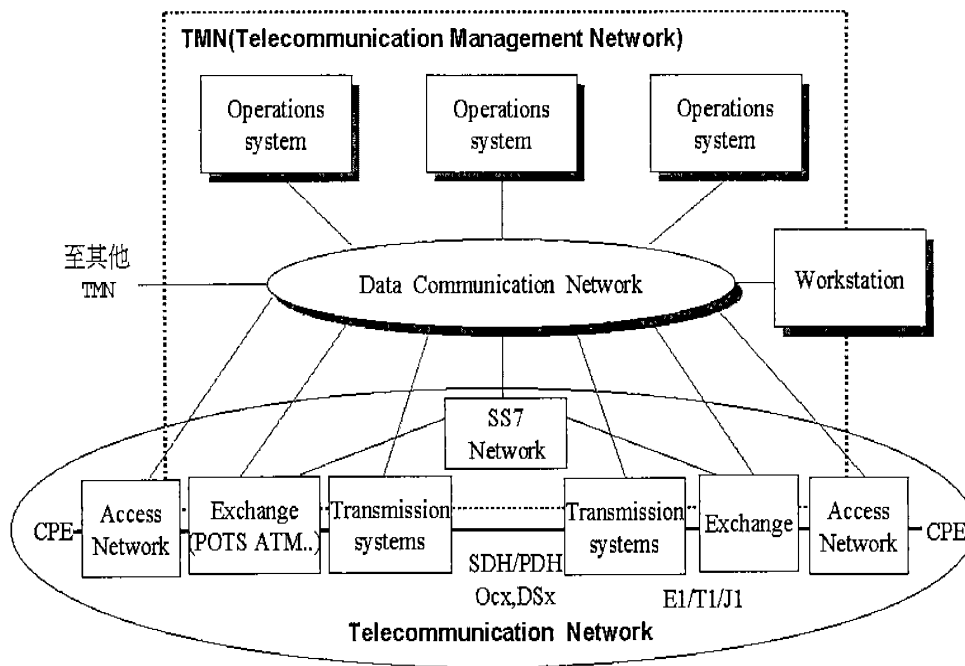


圖 1.1. TMN 架構圖

TMN 網路維運的架構可分為五個階層，包含網路元件層 (NEL, Network Element Level)，網路元件管理層 (NEML, Network Element Management Level)，網路管理層 (NML, Network Management Level)，服務管理層 (SML, Service Management Level)，以及企業管理層 (BML, Business Management Level)，TMN 階層化架構如圖 1.2 所示，各層間以 Q3 作通信協定，各層之功能說明如下：

(1) 網路元件層：

所有被管理的網路元件如終端設備、接取設備、交換設備、傳輸設備等，都屬於此層，網路元件層主要在執行管理指令、偵測問題、自我診斷、測試及切換等工作。

(2) 網路元件管理層：

同一種類型的網路元件，其中一個或多個網路元件可以由一個網路元件管理設備管理，並提供以下功能：

- 提供一個符合標準的界面連接網路管理層系統。
- 自網路元件收集關於該網路元件之狀態、告警、障礙信息、話務及帳務等資訊，並提供給網路管理層系統。
- 接受網路管理層系統之指令，作組態設定、障礙測試排除及安全管制等動作。

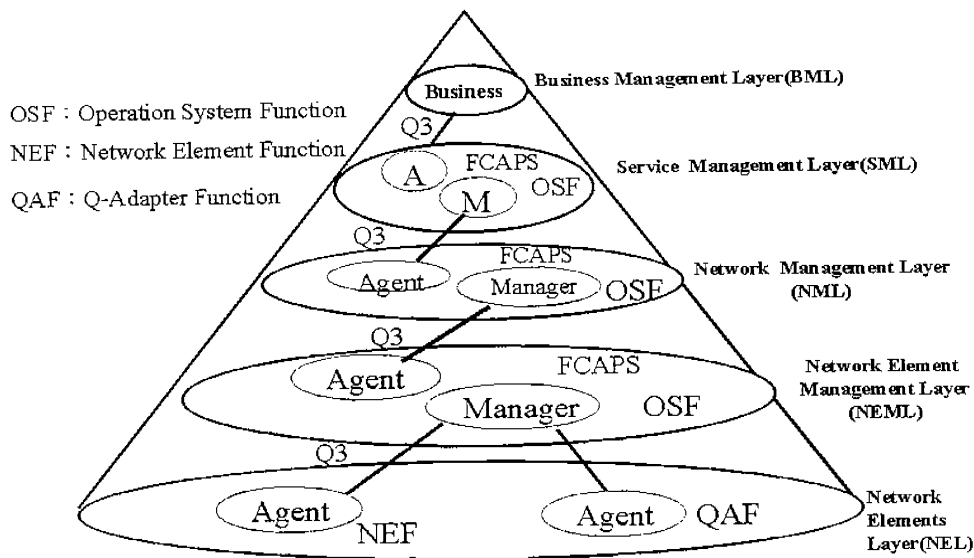


圖 1.2 TMN 階層化架構

(3) 網路管理層：

負責管理由網路元件管理層所展示之網路元件，提供管理網路的功能，並且組合整理所有跨越此網路的相關活動，以提供服務管理層對網路之需求。一種類型之網路元件可由一個網路管理系統管理，故有數個 LPOSS 配合各種接取網路元件，數個 SOSS 配合不同技術之交換設備，數個 TOSS 針對不同技術之傳送網路設備，而每一種網路有一個 NOSS 作整體網路之管理。

(4) 服務管理層：

服務管理層利用網路管理層所提供之資料及服務，提供給客戶或網路提供者相關服務，並負責與客戶有關之服務及新服務引進之管理。由於各種網路都可能提供多種的網路服務，那些網路的服務需要整合，必須周延考量，例如組織、作業流程、服務提供方式及資訊系統平台的整合等因素。

(5) 企業管理層：

負責企業的全盤規劃，並提供維運之間的一致性，通常此層只做到目標的設定，而非目標的達成，在某些情況下，它可提供充分之資訊而成為企業在執行某些行動時的焦點所在，由於它是企業整體管理的一部份，所以還須與其它管理系統有互動關係。

由於電信網路設備功能較為複雜，網管資訊較為繁多，以及部分網管運作需具即時性，再加上設備建置需廣佈於電信服務所及之處，導致各電信網路提供者對於如何建立 TMN 各有其作法，為進一步規範 TMN 之內涵，以提供較切實的開放式電信管理網路環境，ITU-T TMN 標準首先從功能性架構、資訊架構、及實體性架構三個觀點來描述構成 TMN 的元件，以下主要是從實體架構之觀點來加以介紹。

在 ITU-T M.3010 標準中有關 TMN 之實體架構，明確定義 TMN 之可能組成元件以及各元件間之網管互運介面，以作為建設 TMN 之依循準則，構成 TMN 之實體元件可包括：

- 運作系統(Operations System，簡稱 OS)
- 中介裝置(Mediation Device，簡稱 MD)
- Q 適配器(Q-Adapter，簡稱 QA)
- 數據通信網路(Data Communication Network，簡稱 DCN)
- 網路元件(Network Element，簡稱 NE)
- 工作站(Workstation，簡稱 WS)

上述這些元件在 TMN 中各有所司，各元件之選擇及所需數目可依網路規模、管理功能需求或實際電信管理組織階層考量而有所不同。處理有關監視、協調及控制 TMN 網管資訊，主要由一個或多個 OS 負責，各 OS 間可為平行互補之合作關係，或為階層式之上下屬關係，而當 TMN 規模較大或由多個不同通信媒介組成時，OS 與 NE 之間則可先藉由 MD 來負責網管資訊之儲存、轉換、過濾及彙整，MD 通常將所納管 NE 之網管資訊先行辨認、分析或統計，然後再以較整合性之網管資訊送至 OS，例如部分告警關聯性分析(Alarm Correlation)工作便很適合在 MD 執行，因此 MD 之存在可避免過多之網管細節資訊同時流入同一 OS，導致 OS 負載過重。

在 TMN 中，真正提供網管資訊及實際執行管理功能之元件為 NE，即實際之電信設備，而依 TMN 之原理，NE 可小至一片實際硬體卡，大至整個交換機系統，依據實際網管需要，通常 NE 需包含網管代理者(Agent)負責以標準的網管通信介面收送網管資訊，並驅動實際的網管動作。

TMN 雖然規範各 TMN 組成元件必需提供標準之網管通信介面以利相互連結，由於目前原有之電信設備所提供之網管通信

介面多為專屬而非標準網管通信介面，且無法重製或修改，這些 NE 勢必無法由開放式的 TMN 直接納管，因此，TMN 標準特別定義 Q 適配器，即 QA，其目的便是將非標準通信介面轉換為符合 TMN 標準之網管通信介面，因此目前現有之電信網路設備，可經由 QA 所做之轉換，與 TMN 介接。由於原來這些電信設備之網管通信介面各自不同，因此每一種電信設備都必須有專為其設計之 QA，方能為 TMN 所納管。

經由 MD、NE、QA 蒐集至 OS 之網管資訊或提供之網管功能，基本上都是以各元件間易於資訊交換的觀點訂定的，這些為 OS 所處理之網管相關資訊，則由 WS 將之轉換為以使用者觀點之介面，以提供良好之運作環境，因此實際的網管操作者，事實上可以不必瞭解真正所傳遞的網管資訊細節。

上述各實體元件，經由 DCN 將之連結起來，形成整個 TMN，彼此間之網管資訊傳遞，必須經由網管通信互運介面 (Interoperable Interface) 來達成，以解決因多家廠商及多種相容網路所引發的問題，在 TMN 範疇，所謂互運介面，非僅是通信堆疊之標準介面，更重要的是其運用此實體通信介面所傳遞的網管資訊 (Management Information)，例如，OS 與 MD 間所交換之網管資訊基本上是不同於 MD 與 NE 間的，同樣地，不管介於那些元件間，執行障礙管理功能時所需之網管資訊，基本上也與執行效能管理功能時有所差別，簡而言之，互運介面應包含通信堆疊、網管資訊、及管理功能，由於各實體元件在一 TMN 中所扮演角色不盡相同，彼此間之互運介面內涵便會有所不同，因此，TMN 標準便針對不同實體元件間之互運介面予於規定，並分別以 Q3 介面、Qx 介面、F 介面、及 X 介面命名辨別之。

所謂 Q3 介面為實體元件 OS、MD、NE、QA 分別與 OS 連結之互運介面，即 OS-OS，OS-MD，OS-NE 及 OS-QA 介面，Qx 介面為實體元件 MD、NE、QA 分別與 MD 連結之互運介面，即 MD-MD，MD-NE 及 MD-QA 介面，F 介面為 WS 與 OS 間之互運介面，X 介面為位於不同 TMN 之 OS 間之互運介面。一般而言，Q3 介面被視為 TMN 中最重要及最複雜之互運介面。

1.3. TMN 與 OSI 之關係

如同專為 Internet 網路管理所訂定之 SNMP 網路管理通信協定一樣，電信網路管理也需要一套能滿足各實體元件互運介

面需求之網管通信協定，TMN 所採用之網路管理標準是以 OSI 管理標準為基礎，亦即以 CMIP 為其網管通信協定，通信堆疊仍以依循 OSI 七層架構為主，因此，欲瞭解 TMN 互運介面標準，需先從 OSI 管理標準著手。基本上，OSI 管理標準包含 CMIS/P、MIM、SMFs 三個主要部分，CMIS/P(Common Management Information Service/Protocol)為用來傳遞網管資訊之通信服務與協定，主要提供 M-Get，M-Cancel-Get，M-Set，M-Create M-Delete，M-Action 及 M-Event-Report 七種網管通信服務，MIM(Management Information Model)為管理資訊模型，用來規範網管資訊結構與格式，而 SMFs(Systems Management Functions)則定義各種共通性的基本管理功能標準以供遵循。OSI 管理標準最大特色在其物件導向觀念，以其管理資訊模型為例，所有網管相關資訊均以物件方式表示，我們稱之為被管理物件(Managed Object，簡稱 MO)。MO 之特性主要由其所含之屬性值(Attribute)及通告(Notification)來表現，MO 之定義以所謂 GDMO(Guidelines for the Definition of Managed Objects)格式定之。管理者端可利用 CMIS/P 所提供之網管通信服務，對 MO 本身或部分屬性值執行存取動作來達成網管目的，而 MO 本身並能主動送出通告，經由代理者(Agent)以事件報告方式發送相關之網管資訊，此外，OSI 管理更規範了各種共通性的基本管理功能，即 SMFs，包含物件管理功能、狀態管理功能、關係管理功能、告警報告管理功能、存錄控制功能、事件報告管理功能、安全告警管理功能等約 22 種 SMF，其內容涵蓋組態管理、障礙管理、效能管理、安全管理、帳務管理等五種管理功能領域所需之基本管理功能。而每一管理功能，分別定義為其所需之支援性 MO 及屬性值，並進一步規範 CMIS/P 之參數以提供所需之通信服務。

OSI 管理標準所提供之管理功能，基本上是為了各種網管應用而設計的，針對 TMN 這種著重於電信方面應用而言，仍稍嫌不足，因此於 TMN 標準中，類似 SMFs 觀念，TMN 針對各種電信應用也規範了所謂的電信管理功能(Telecommunications Management Functions)，如圖 1.3 所示，這些管理功能可架於 OSI SMFs 之上，或與 OSI SMFs 扮演同樣角色。上層的各种電信應用服務便可由這些電信管理功能之提供來達成，此點是 TMN 標準與 OSI 管理標準不同之處。

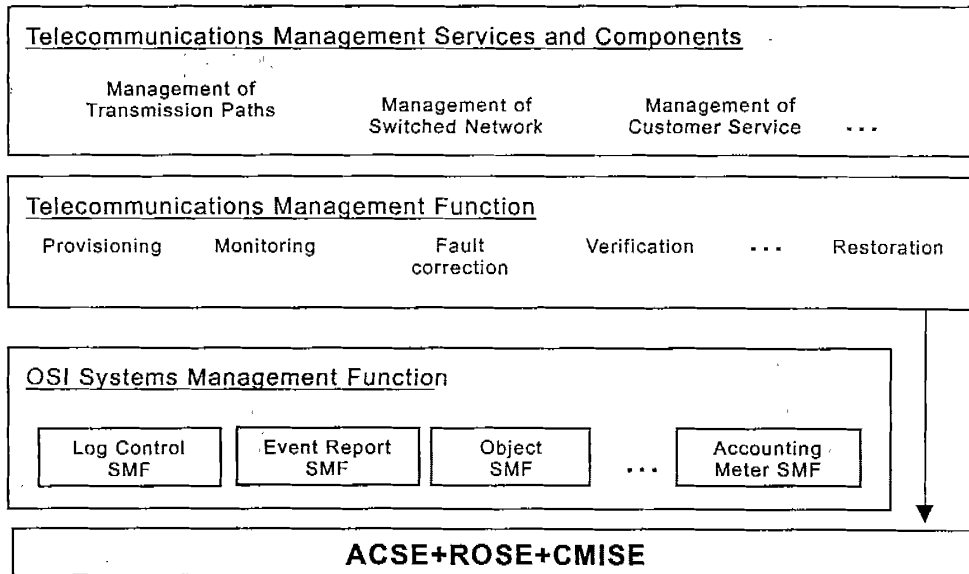


圖 1.3 TMN 電信服務與管理功能

OSI 管理標準雖然在 TMN 中扮演非常重要角色，但是 TMN 互運介面所引用之通信協定並非僅限於 CMIP，實際上，根據 ITU-T Q.812 有關 Q3 介面上層通信協定之描述，FTAM 也是 TMN Q3 介面在檔案傳送方面所引用之標準，因此，TMN 互運介面之內涵，可因各種電信應用之不同需求及介面所在之實體元件所扮演角色而有所差異。

至於 TMN 之應用領域，TMN 基本上涵蓋所有電信網路及設備之管理，由於 TMN 標準為近年來才逐漸發展成熟，因此提供 TMN 標準介面之電信網路設備，多以新進設備為主，主要包括：

- SDH 同步數位光纖網路
- ATM 非同步傳輸模式交換系統
- GSM 行動電話
- IN 智慧型網路
- PACS 個人接取通信系統

其中以 SDH 網路管理最為成熟。此外，各電信維運管理系統之互連及國際間電信網路網管資訊交換等整合性互運系統建置，亦為 TMN 標準之一重要應用領域。而若以管理層次面來看，從元件層、元件管理層、網路管理層、服務管理層至企業管理層，各層次之電信管理均為 TMN 標準應用之範疇，因此，從 TMN 之應用領域可看出其重要性。近年來由資訊及電信業界組成之

國際網路管理論壇(NM Forum)也極力投入 TMN 各項技術及標準規範之研究，而各主要資訊廠商如 HP、IBM、SUN、DEC、BULL 也紛紛推出 TMN 發展平台及工具。因此，以 TMN 標準為主的電信網路管理趨勢，愈來愈漸明顯。

1.4. SNMP-Based 網管架構 (如圖 1.4)

SNMP 通信協定用於 managers 和 agents 之間資料的交換，是一個定義資料結構的方法，這種樹狀 (Tree) 結構的資料叫 Managed Information Base (MIB)。

標準組織是 IETF (Internet Engineering Task Force)

產生的文件是 Request For Comments (RFC)

相關的 RFC 文件：1155, 1157, 1212, 1213, 1901-1908, etc.

非連結式的 SNMP(Simple Network Management Protocol) 應用於 TCP/IP(ATM 網路的 M1、M2、M3 及 M4 界面)，主要由 SMI(Structure of Management Information)、MIB-II(Management Information Base)及 Protocol 三種元件組成，SMI 主要在描述各管理物件(MO)的命名規則，MIB-II 則是這些 MO 的結構化集合，SNMP Manager 經 UDP/IP/LINK，利用 Protocol 和 SNMP Agent 通信，去接取被管理資源內的 MIB，以交換網路管理資訊，共有 Get Request、Get-Next Request、Set Request、Get-Response 及 Trap 等五種 PDU，SNMP 較為簡單，擷取大量資料時較為緩慢，再加上 Traps 由 Agent 送出後，Manager 並未作回應，無法保證訊息的送達。

綜合而言，SNMP 的限制如下：

- SNMP 無法有效擷取大量資料。
- SNMP 的告警 (traps) 沒有確認機制 (Ack)，無法保證完整接收。
- 安全機制不完整。
- 沒有完整的命令式指令 (e.g. loopback test)。
- 管理指令不成熟，過於簡單。

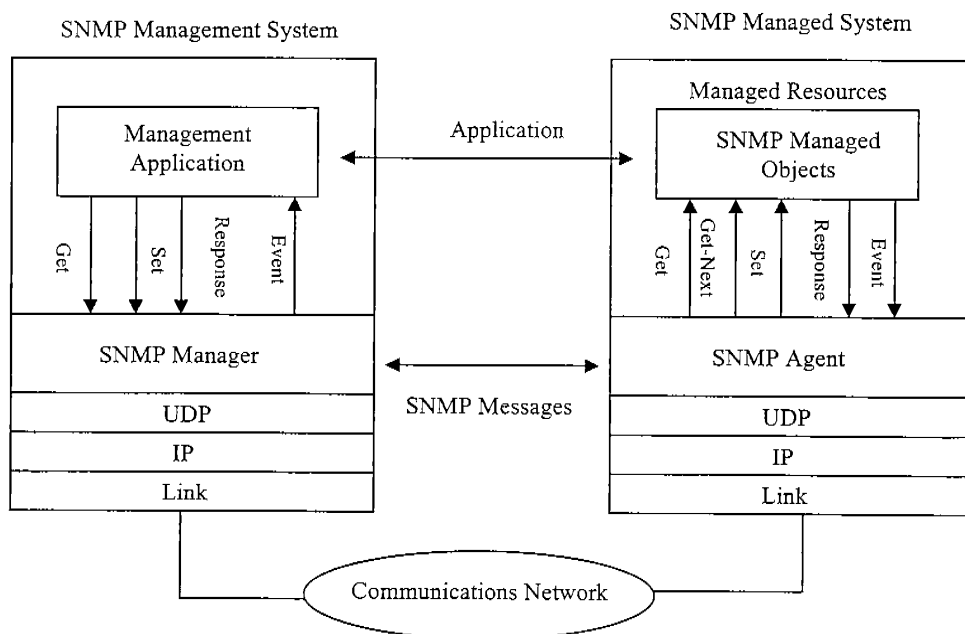


圖 1.4 SNMP-based 網路管理架構

1.5. CMIP 網管架構 (如圖 1.5)

SNMP 屬簡單型且非連結式網管架構，而 CMIP(Common Management Information Protocol) 須建立連結且較為複雜，其中 CMISE(Common Management Information Service Element) 是 OSI 應用層中的一種應用服務單元(ASE)，由 CMIP 及 CMIS 兩部份組成，CMIP 係由 Manager 發出 Request，再由 Agent 作出回應，CMIS 則由 M-GET、M-SET、M-CANCEL-GET、M-CREATE、M-DELETE、M-ACTION、M-EVENT-REPORT 等七種包裝成 CMIP 的 PDU 組成利用下層的 ROSE(Remote Operation Service Element)，傳送到他端相對應的 CMISE，以達成五大網管功能。ACSE(Associated Control Service Element)則負責提供系統管理應用程式，在交換網管資訊之前及最後，和對方網管應用程式建立及拆除應用結合(Application Association)的服務，也就是在利用下層的規約堆疊去完成連結後，ACSE 便退居幕後，由 CMISE 來完成管理功能，CMIP 可在系統間作多層的連結，如系統 A 的 Manager 經系統 B 的 Agent、Manager 連至系統 C 的 Agent，一個 Manager 也可能和許多 Agent 作管理資訊的交換，CMIP 在 ATM 網路內，主要應用於 M4 界面。

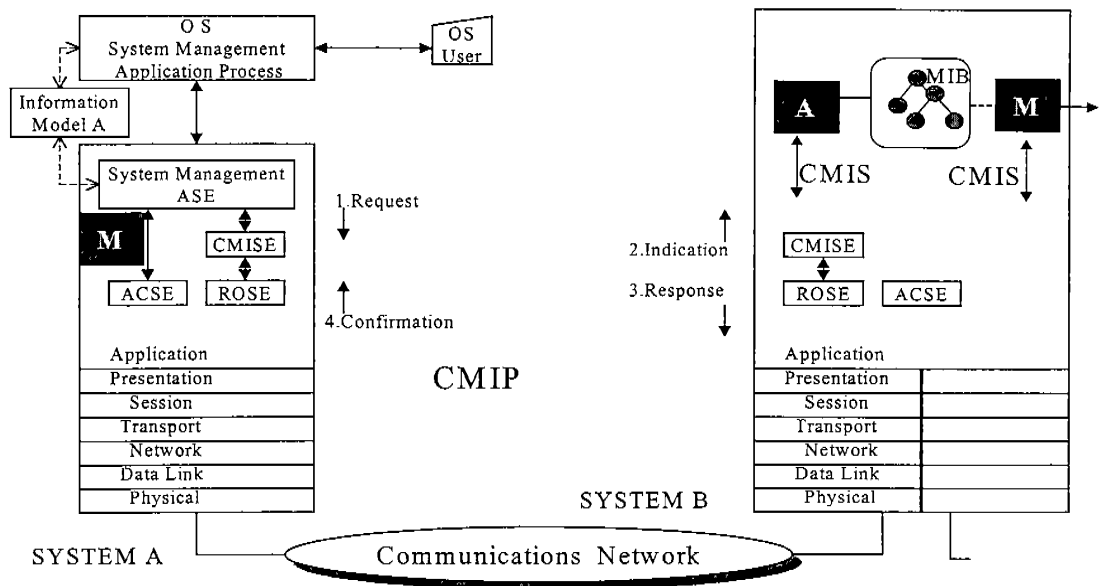


圖 1.5 CMIP-based 網路管理架

1.6. SNMP 與 CMIP 的比較 (如圖 1.6)

	SNMP	CMIP
Protocol Services	Attribute Oriented	Object Oriented
Communication	Connectionless	Association Oriented
Management Model	Polling-based	Event-based
Object Selection	Specific Name	Scope+ Filtering
Synchronization	Atomic	Atomic, Best effort
Linked Reply	No	Yes
MIB Browsing	Get-next	Flexible
Action	Side effect	Yes
Event Confirmation	Unconfirmed	Event Confirmation
Object Definition	Attribute	Attribute, behavior Notification, operation
Object Naming	Predefined static MIT	MIT, dynamic
Object Representation	Subset of ASN.1 and BER	ISO ASN.1 and BER

圖 1.6 SNMP 與 CMIP 的差異

1.7. ATM 網路管理架構

由 ATM FORUM 所提出的“M 規格”的端對端管理模式，將網管介面分為 M1~M5 五個管理介面，其介面參考架構（如圖 1.7），M1~M5 介面定義敘述如下：

M1：為 Private Network Manager 和 End User 間的介面
它是利用 SNMP 來傳送相關的資料流，以獲得用戶終端設備的故障及組態資訊。

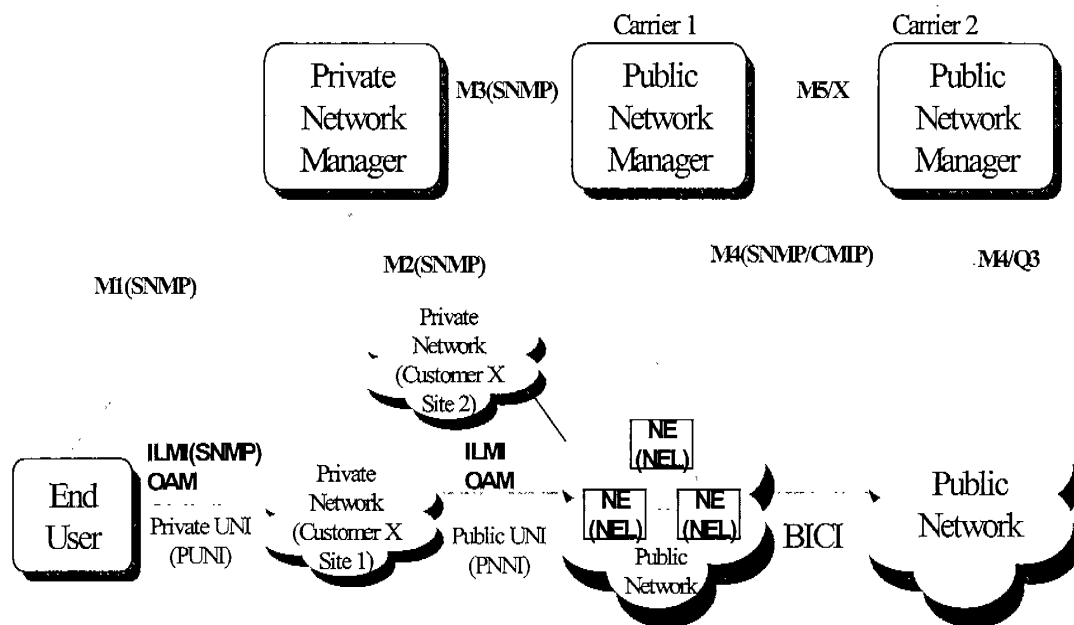
M2：Private Network Manager 和 Private Network 的介面
它也是利用 SNMP 來對私人企業網路內的交換機，進行故障及組態管理並接取性能及帳務資料。目前所有主要交換機的製造商皆支援 M1 及 M2 的界面規格。

M3：又稱為 CNM (Customer Network Management) 介面
它使得私人企業網路的 SNMP-Based 網管系統能和 Carrier 之管理系統互相整合，可從 Public Network Manager 處獲取所需要的管理資訊。ATM FORUM 將此 CNM 的能力分為兩個等級，其中等級一為狀態及組態的監視，它只允許用戶利用 SNMP 讀取其 UNI Link 的效能管理資料，或當 UNI Link 發生問題時，告知其警報訊息；而等級二可做虛擬組態控制，當客戶要增加 Site 2 的新鏈路，將兩個 UNI 都連到公眾網路時，即能由 M3 對此虛擬連結做增加／修改／刪除等控制能力。

M4：是公用網管中心和公用網路之管理介面
以定義業者如何管理其本身之大型公眾網路，來執行類似 M2 的功能。

M5：則定義兩公眾網路間的管理資訊流介面
包括業者間故障資料、組態管理、帳務資訊及服務需求程序的交換機制，以 TMN 模式來說，M4 即為 Q3 介面，M5 則為 X 界面。

M4 主要是以 CMIP 來獲得管理資訊，但由於市場需求的因素它也支援 SNMP，因此對這兩種 Protocol 皆有其各別的管理資訊庫 (MIB)。



BICI(broadband Inter-Carrier Interface)
 ILMI (Integrated Local Management Interface)

圖 1.7 ATM Forum 之管理介面參考架

M4(Q3)介面的網管系統可分為 Service Level View、Network Level View 及 NE Level View，敘述如下：

Service level view 關心的是如何由 Network level (如端對端的路徑) 觀點來提供網路服務 (如可用度、成本……等) 的需求，以及如何經由網路及全部相關的用戶資訊以符合這些服務需求。

Network level view 關心的是代表網路的實體及邏輯資訊、網路元件間如何相關連，以提供端對端 (End-to-End) 的連結，此層在組態管理 (CM) 方面包括傳送網路 (Transport Network) 內之次網路 (Subnetwork)、鏈路的提供、連結的設定、保留、修改及釋放等，在故障管理 (FM) 方面，包括 ATM 次網路發生障礙時的告警通知、隔離、改正及連結測試，並能沿著次網路的連結或區段，來執行 OAM 細包的折回測試。在效能管理 (PM) 方面，包括次網路對細包的處理能力、UPC/NPC 擁塞控制及 AAL

(有些 PVC 是在公眾網路內處理，如 IWU) 性能監視、OAM 資料的性能管理 (如細包的遺失、誤插入) 等。

NE level view 主要關心的是管理網路元件的資訊，以個別基礎來管理每一個 NE，ATM FORUM 對 CMIP、SNMP、AAL、CES 以及 ITU-T 的 I.751 皆有詳細說明，唯目前多支援 PVC (SVC 為 optional support)。

NE level view 的介面需求

(一) CM 方面包括：

- (1) ATM NE 組態識別及改變報告。
- (2) V-UNI (Virtual User Network Interface)、BICI (Broadband Inter-Carrier Interface)、BISSI (Broadband Inter-Switching System Interface) 等組態。
- (3) VP、VC 鏈路的交叉連結及 VPC、VCC 的組態。
- (4) VPC、VCC 區段端點的組態。
- (5) 信號通道及 SVC 服務路由的組態。
- (6) 自動產生 ATM NE 報告的管理系統控制 (如 Suppression)。

(二) 在 FM 方面包括：

- (1) ATM 網路元件、實體設施及 ATM 鏈路／連結等發生失敗時的自發性報告。
- (2) ATM OAM 細包折回測試的啟動。
- (3) 以 OAM 細包作連續性檢查。

(三) 在 PM 方面包括：

- (1) 實體層 (SONET 及 DS3 路徑) 的效能監視。
- (2) 傳輸聚合層效能監視。
- (3) ATM 層 protocol 監視。
- (4) UPC/NPC 流量控制監視。
- (5) 信號通道 Protocol 監視。
- (6) 使用 OAM 細包作效能監視。

(四) 在 SM 方面包括：

- (1) 系統安全管理。
- (2) 每一安全服務使用機制法則的管理。
- (3) 接取控制服務的管理。

1.8. CORBA based 網管架構 (如圖 1.8)

電信維運支援系統之開發技術已進入物件導向 (Object-Oriented) 的時代，但因維運系統林立及異質性平台等問題使得各種物件導向語言難以相互溝通，以致於系統與系統間很難進行資料的交換或存取，因此亟須一套可跨平台、跨語言之新技術，以便讓每個系統的軟體元件開發者進行專業化的分工，OMG (Object Management Group) 提出了 CORBA (Common Object Request Broker Architecture) 規格，用以加強軟體的可攜性 (portability)、再利用性 (reusability) 及互通性 (interoperability)。CORBA 採三層式架構，在傳統的 Client/Server 間，加入了中介層 (middleware) 的 ORB (Object Request Broker)，Client 端用單一的程式界面及 IIOP (Internet Inter-ORB Protocol) 和中介層溝通、ORB 主要提供 Language、Platform 及 Location Independent 介面，扮演物件中介的角色，讓物件透過地在分散式環境之下發出需求與接收回應作為互運 (interoperability) 的基礎，物件間的通訊只需知道彼此名字 (Object Reference)，Server 端則可以是一群伺服器來提供服務，分散負擔。CORBA_Based 提供了物件導向之軟體再利用，應用程式極易移植於符合 CORBA 架構之不同平台，此種分散式架構使得系統容易彈性擴充，並適於作異質環境之整

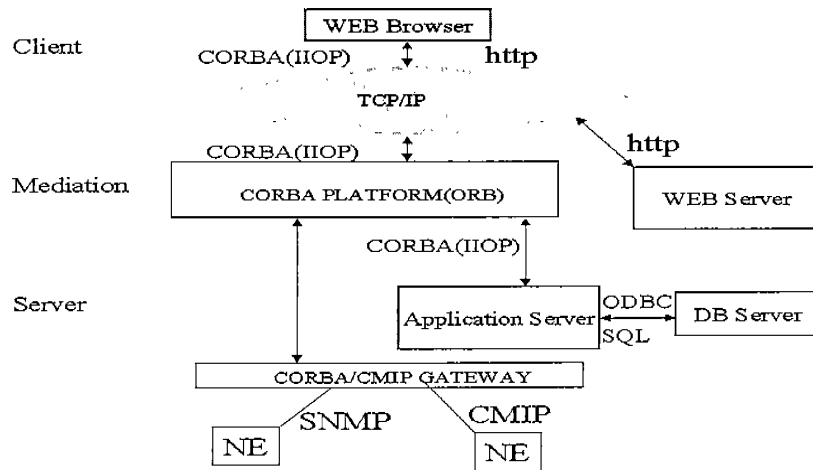


圖 1.8 CORBA based 網管架

合。

1.9. Web-based 網管架構(如圖 1.9)

Web-based 網路管理除仍維持原有之 Manager、Agent、protocol、MO 四種管理要素外，將整個維運管理網路分為 3 層 (Tier)，如圖中之 User (Tier 3) 端以 Web Brower (如 IE、Netscape) 啟動管理應用，再以 HTTP 透過 Internet/Intranet，連結至 Tier 2 的 Web Server(如 Microsoft IIS)後，Web-Server 以 CGI (Common Gateway Interface) 連結外部應用式，來執行 FM、CM、AM、PM、SM 等五大網管功能，再由 PROXY Coordinator 轉換成 SNMP/CMIP，去和 Tier 1 的被管理設備，做管理資訊的交換，採 Web-based 的網管系統會即時反應網路的最新資訊給所有線上的維運人員，而不同處所之維運人員所看到的網路資訊皆完全一致，各地的維運人員可透過 Web Browser 同時獨立進行維運，再者因其具簡單且一致的架構，利用 hyper link 極易進行軟體的統一更新，並共享表現方式豐富的網管資訊內容，故為今後網管發展的主要趨勢。

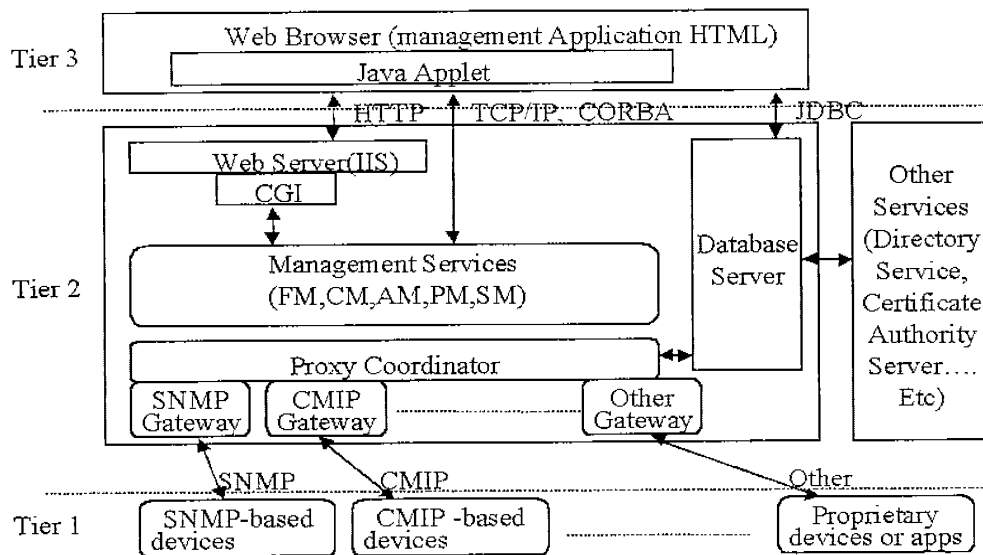


圖 1.9 Web_Based 網管架構

第 2 章、北電網路管理系統

2.1. 簡介

北電網路之網管維運系統具備 TMN 網路管理之 FCPAS 五大功能，其應用軟體建置於 UNIX-Based 工作站，用以管理 DPN 及 Passport 網路。此網路系統之硬體需求如下：

- monitor:
A 20-inch(or larger) color monitor is recommended
- CPU :
Any Sun hardware platform or SPARC-compliant platform that supports the Solaris 2.6 or 2.7 operating system software can be used.
- CD-ROM drive :
required for installing most software packages, including the Solaris and NMS software.
- Memory :
a minimum of 96 MB are required.
- Disk drives :
a minimum of a 2-GB drive is required for the storage of the Solaris and NMS software. This figure does not include the space required for collection of any data from the network.
- Tape drive :
highly recommended for maintaining system backups
- High speed interface package :
recommended for X.25 network connectivity in excess of 19.2 kbps, and required for Frame Relay connectivity

軟體需求如下：

- Sun Solaris operating system :
The Sun Solaris 2.6 or 2.7 package is required at NMS Release 12.2
- NMS :
This software consists of several packages that comprise the network management software. A valid run-time license must be purchased from Nortel Networks to access these packages.
Note : Depending on the devices in your network, NMS software may be required from a separate CD, the NMS Companion CD.

- Sun Solstice X.25 9.1 :
This optional software package is required for X.25 connectivity to a DPN module. An X.25 connection is used for managing networks containing both DPN modules and Passport nodes.
- Sun Solstice Frame Relay 2.0.1 :
This optional software package is required for Frame Relay connectivity to a Passport node. A Frame Relay connection is used for managing Passport-only networks.
- Sun HSIS/S 2.0 :
This optional software package provides a high speed interface between the network and the NMS. It is recommended for X.25 network connectivity in excess of 19.2 kbps, and required for Frame Relay connectivity.
- Additional third-party packages :
Additional third party software packages supported under the Sun Solaris 2.6 or 2.7 operating systems may be installed. If installing additional software packages, ensure that the system is properly engineered (disk space, processor power, memory) to support these packages and that they are Year 2000 compliant.

2.2.NMS 架構

2.2.1. 工作站組態

網管工作站可為 stand-alone 組態或 server 組態，如圖 2.1 所示，stand-alone 組態適合 200 個 node 以下小型網路，可以包括一個或多個 stand-alone 工作站，直接與網路相連，stand-alone 系統包含一個簡單的計算平台，內含網路管理之所有軟硬體設備。Server 組態應用於大的網路與操作團隊的環境，它可共用電腦資源，減少硬體配備及管理之費用。

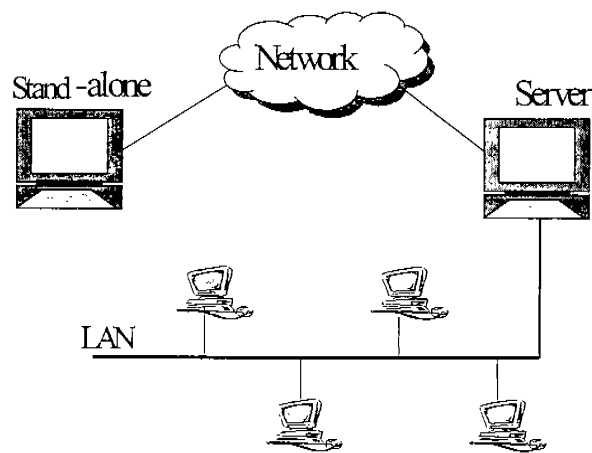


圖2.1 網管工作站組態

2.2.2.NMS階層架構

北電公司之 Passport 或 DPN 網路管理分為三層：

- 應用層(Application layer)
- 介面層(Mediation layer)
- 網路層(Network layer)

如圖 2.2 所示，應用層提供管理者與網管系統間之介面，主要包含網管工作站及其所提供的一些應用軟體，如障礙管理(Fault Management)、監視管理(Surveillance Management)、及供裝管理(Provisioning Management)等。

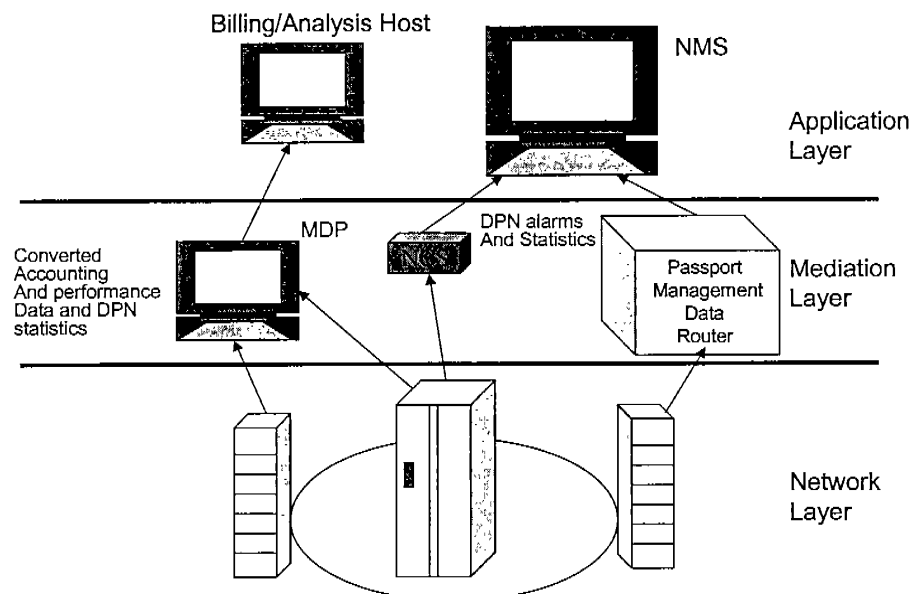


圖2.2 NMS架構

介面層負責處理終端使用者與被管理設備間之連繫，它將應用層與網路層間之網路資料、使用者指令、及網路元件之回應等作轉換傳送，在網管系統工作站與 DPN 及 Passport 網路間執行的例如 DPN 網路控制系統(NCS)，Passport 管理資料路由器(FMDR)以及管理資料供給器(MDP)等。網路層包含 DPN 及 Passport 網路元件。

2.2.3.NMS 工具組(toolsets)

NMS toolsets 由一些相關的網路管理工具(NMS tool)所組成，如提供障礙管理與監視管理的 adviser toolset 及

供裝維運管理之 Architect toolset 等，至於 NMS tool，如 command console tool、Component Provisioning tool 等，均為 toolset 之一部分，維運操作人員依其權責由管理者設定不同的 NMS toolset 及 tool 範圍，以下為一些基本的 toolsets：

- NMS Advisor:
provides the fault management tools used for monitoring and managing the Passport nodes
- NMS Admin:
provides administrative tools used for managing the NMS processes running on the workstation
- NMS Architect DPN:
provides tools used for provisioning DPN modules and manipulating the application versions loaded and running on the DPN modules
- NMS Architect Passport:
provides tools used for provisioning Passport nodes and manipulating the application versions loaded and running on the Passport nodes
- Device Inventory:
Provides tools used for reporting on the hardware and software configuration of selected devices in your network
- Utilities:
miscellaneous tools such as UNIX access, NTP Viewer, and NMS Help

2.2.3.1.NMS Advisor toolsets

NMS Advisor 提供文字與圖形之畫面，供維運操作人員瞭解整個網路之元件狀態、障礙、告警等訊息，俾作進一步分析並採取適當之處理。NMS Advisor tools 包含下列功能：

- Network Status Bar:
provides a high-level view of the current network status. This tool monitors a set of statistical indicators gathered from the GMDR database. Some of these indicators quantify troubled elements of the network, including the number of active alarms and the number of components out-of-service.
- Network Viewer:

displays network topology and shows real-time status for network nodes, links, and subcomponents, It also provides network model editing capabilities.

- **Component Status Display:**
provides a textual representation of the organization components at the region, site, node, component, and subcomponent levels in the network. It displays the same information as the network Viewer, but in a textual rather than graphical format.
- **Component Information Viewer:**
merges state-, alarm-, and problem-based surveillance into one tool. The Component Information Viewer enables you to diagnose network faults by targeting faulty components and their related components. You can then determine the impact of these faults, view the current state and problem state of these components, and view the alarms and status that have led these components to their current state.
- **Alarm Display:**
enables you to view alarms and logs received from Passport nodes. Extensive filtering capabilities are provided to facilitate the management of alarms.
- **Command Console:**
is the operator command interface for the Nortel Networks family of data networking products. The Command Console enables you to issue commands and receive responses from Passport components.
- **Performance Viewer:**
enables you to collect and display performance information about network components. It is used to help trace faults in the network, collect information about network load, and generate statistics for reporting and analytical purposes. This information is displayed in a graphical format.

2.2.3.2.NMS Architect toolsets

NMS Architect toolsets 主要提供網路的供裝功能，包含 DPN tools 及 Passport tools 部分，分述如下：

DPN tools

- **Component Provisioning:**
used for adding, changing, deleting and viewing service

data for DPN modules.

- Envelope Editor:
Used to view, modify and create service data envelopes for DPN modules.
- Service Data Backup:
provides a means for backing up master configuration files (MCF) on DPN modules and for storing the MCFs on a backup disk, an NMS server or a DPN 100 module.
- Service Data Restore:
used for retrieving service data backups from the backup source and restore the MCFs to a specific DPN module.
- Global Data Manager:
used for distributing global service data to DPN modules.
- Software Substitution: used to upgrade software images on the DPN modules.
- Software Distribution:
used for transferring DPN software images from the workstation or a DPN RDS (Remote Distribution Site) to other DPN modules.
- Service Data Conversion:
used to convert service data from an older NMS release version to a newer NMS release version.
- Service Integrity Simplification:
automates the process of populating the Network Reporting System database and executing the NRS-based Service Integrity Check tool in order to check the network wide integrity of DPN and Passport service data.
- Network Activation:
allows the user to automate all of the steps required to activate, confirm and commit a view after it has been provisioned and downloaded. The automated actions can be applied to multiple DPN modules concurrently, or in a specific order when the activation is considered critical.

Passport tools

- Component Provisioning:
used for adding, changing, deleting and viewing provisioning data files for Passport nodes.
- Service Data Backup:
used to backup all provisioning data files and application

version information from a Passport node to a Passport Data Storage site.

- Service Data Restore:
used to restore Passport service data from a specified Passport Data Storage site to a specified Passport node.
- Software Distribution and Configuration:
used for configuring and downloading Passport software from the Passport Software Distribution Site to the Passport nodes.
- Service Integrity Simplification:
automates the process of populating the Network Reporting System database and executing the NRS-based Service Integrity Check tool in order to check the network wide integrity of DPN and Passport service data.
- Network Activation:
allows the user to automate all of the steps required to activate, confirm and commit a view after it has been provisioned and downloaded. The automated actions can be applied to multiple Passport nodes concurrently, or in a specific order when the activation is considered critical.

2.3. 北電寬頻網路之管理

2.3.1. Passport 網路管理

北電寬頻網路 Passport 之網管系統利用 Frame Relay 虛擬電路連接到 Passport 的網管介面(NMIS) (如圖 2.3 所示), 在工作站與 Passport 之 IPIFR (IP Interface over Frame Relay) 間利用 Frame Relay PVC 建立 IP session, 此時 Passport 網路被視為 inter LAN 交換 (ILS) 網路, 網管單位可利用 IP over Frame Relay 或 IP over Ethernet 連接。Passport 的網管部分包含 Component Administration System (CAS)、Network Management Interface System (NMIS)、Data Collection System (DCS)

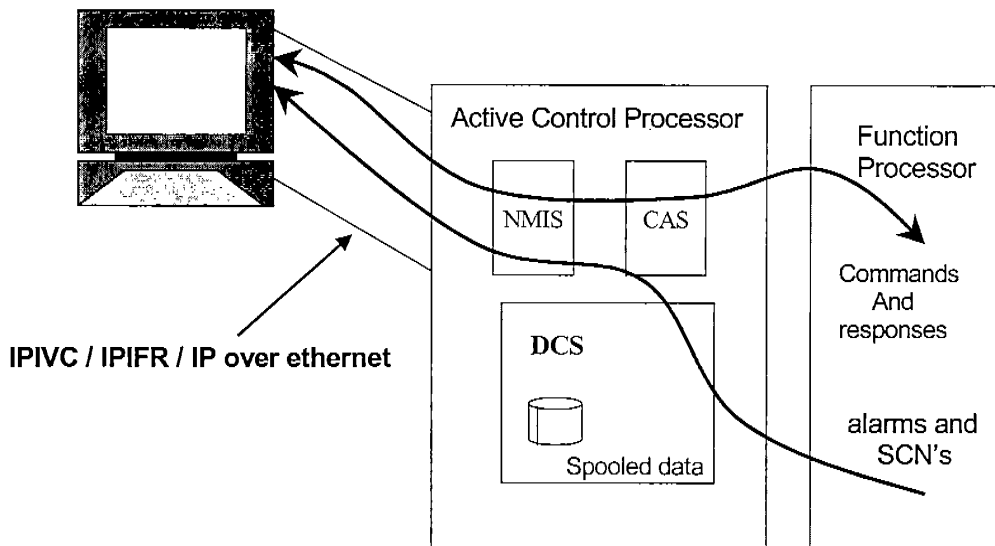


圖2.3 Passport 網管連接方式

2.3.1.1. 元件管理系統 (CAS)

元件管理系統是命令與控制系統，執行網管的要求，啟動適當元件作測試，並回覆要求者偵測結果，CAS 負責所有供裝與控制命令，以及各網路節點供裝資料之管理。

2.3.1.2. 網路管理介面系統 (NMIS)

網路管理介面系統提供一組外部的介面以連接 Passport 節點與網管設備，網管設備經由 Local operator、Telnet、FTP、FMIP、SNMP 等方式接取 Passport 網路，所有 Passport 網路的管理資料如控制指令、供裝指令、告警、狀態、計費、操作員資料、偵錯資料等，均經由 NMIS 傳送。

2.3.1.3. 資料蒐集系統 (DCS)

資料蒐集系統儲存 Passport 網路管理資料，它與所有 Passport 次系統介接，以便接收網管資料，必要時將資料排序或複製，再傳送到 NMIS。DCS 管理告警流程、狀態改變、操作員檔、計費資料、即時偵錯紀錄等資料，這些資料是由應用處理程式非同步產生並送到 DCS，DCS 將這些資料儲存，並整理成輸出格式，送至 NMIS 或其他 Passport 檔案儲存系統。DCS 蒐集下列資料：

- Alarms:
Generated asynchronously from a particular system on a control processor (CP) or a function processor (FP) when certain events occur, such as an engineering condition, a degradation of service, a failure of hardware, or a failure of software.
- State change notifications:
Generated asynchronously from a control processor or function processor when the OSI state of a component changes. These notifications can be used by the NMS surveillance system to determine the impact of a given failure.
- Accounting information:
Generated for services based on a virtual circuit at a time-of-day change over (when the rates for a service change based on the time of day) and when a call is set up or cleared. The accounting records for a time-of-day changeover must be generated at approximately the same time for the changeover to be accurate.
- Logs:
Logs are the operator commands and responses that an operator enters. These logs are used for tracking system operation and for security purposes.
- Debug data:
Is generated when a debug user turns on a debug data stream. These data streams must only be turned on in consultation with Nortel support staff.
- Statistic records:
Statistic records are generated (if the statistics collector is provisioned) at regular intervals by selected components. These records contain information for off-switch processing such as cells discarded and link utilization.
- SNMP traps:
SNMP traps are generated asynchronously from a particular system on a control or function processor. Traps occur as an alert to fault conditions and are sent to requesting SNMP management stations.

DCS 包含下列元件：

- Agents:
Agents, found on each control and function processor, are responsible for collecting the data types generated on

their card. Agents send this data to collectors on the control processor.

- Collectors: Collectors, found on the active control processor, are responsible for transferring the appropriate data records to the NMIS and for spooling the appropriate records to the Passport shadowed file system.
- Spoolers: Spoolers, found on the active control processor, are responsible for writing the appropriate data types to the Passport file system.

2.3.2. 網路管理通信介面

網路管理通信介面包含 IPIVC、IPIFR、IP over Ethernet 三種，茲分述如下：

2.3.2.1. 虛擬通道 IP 介面 (IPIVC)

虛擬通道 (VC) IP 介面利用 DPN-100 將網管工作站與 Passport 網路連接，使用 IP over X.25 通信介面，也就是利用 DPN 虛擬通道建立 TCP/IP 連接通信(如圖 2.4 所示)

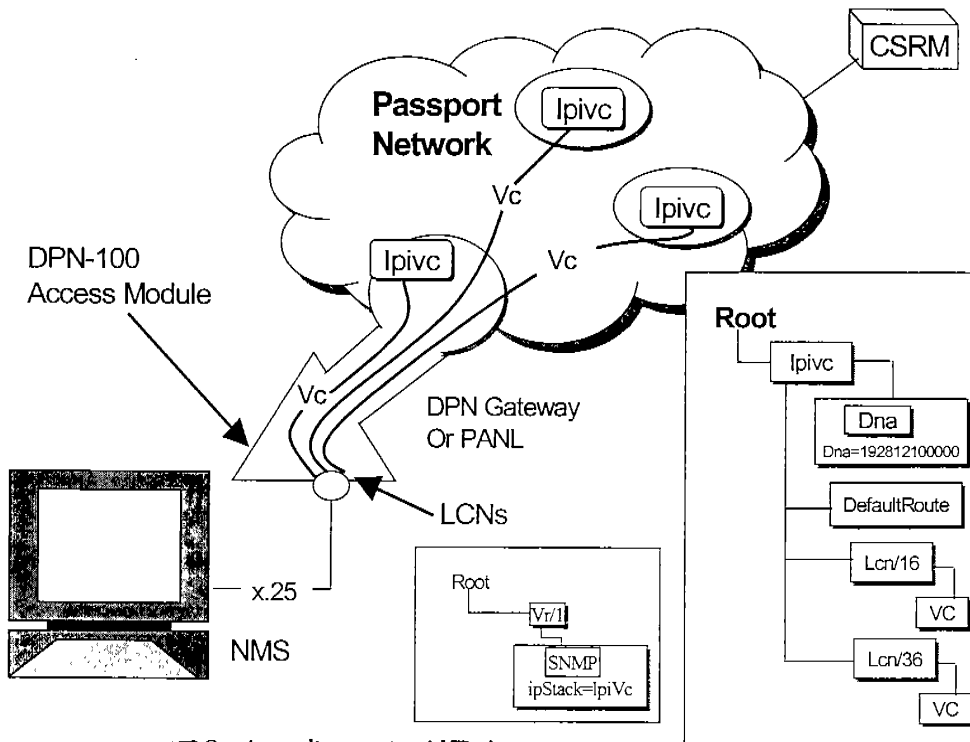


圖2.4 虛擬通道IP介面

2.3.2.2. Frame Relay IP 介面 (IPIFR)

Frame Relay IP 介面有兩種連接方式如(圖 2.5 所示)。第一種直接由 Passport 之 Frame Relay 埠提供網路管理介面，其 IPIFR 元件使用 Frame Relay 虛擬通道建立 TCP/IP 連接通信。另一種使用 Frame Relay 接取設備 (FRAD) 提供網管工作站與 Passport 網路節點之連接，FRAD 支援不同之通信規約，如 TCP/IP 及 X.25，FRAD 將 IP Frame 包裝成 Q.922 Annex A frame，為提供與 Passport 網路節點之連接，FRAD 必須符合網際網路 RFC1490 標準以連接路由器。FRAD 也必須提供一般介面如 RS-232、V.35、RS-422、X.21/V11、DCE、DTE 等。IPIFR 的虛擬通道稱為永久虛擬通道 (PVC)，PVC 可以伸入一些網路，每一個網路各自提供並維持其連接之部分，IPIFR 之虛擬通道將亂序之封包予以重整，並消去重送之多餘碼框。

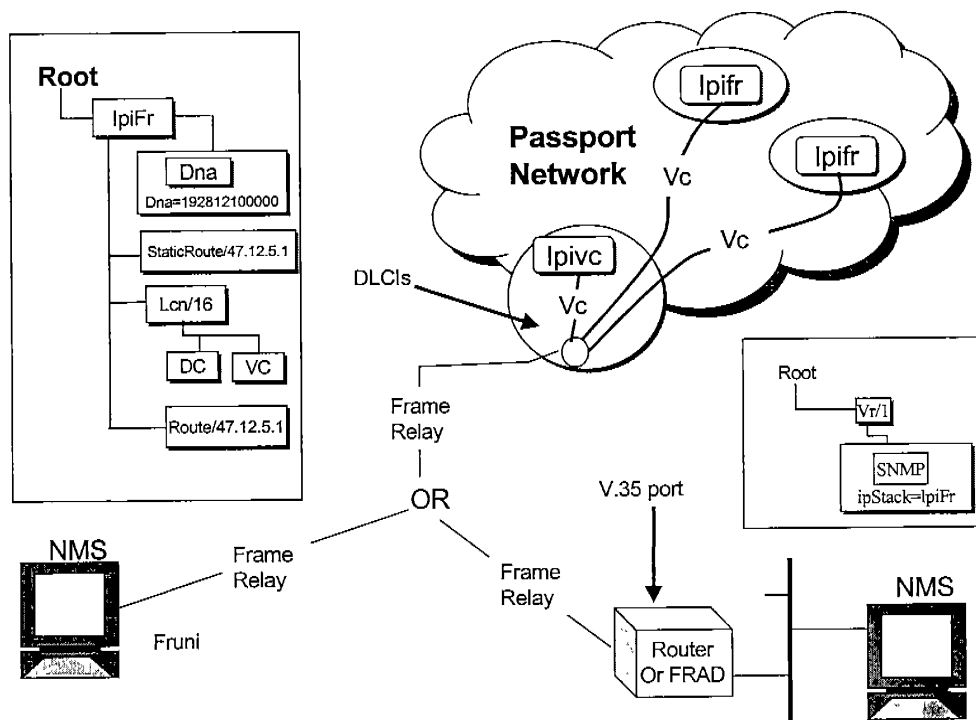


圖2.5 Frame Relay IP介面

2.3.2.3. 乙太網路 IP 介面 (IP over Ethernet)

網管工作站亦可以使用 VRIP (Virtual Router Internet Protocol) 與 Passport 網路節點連接 (如圖 2.6 所示), 它是直接連接在 Passport 網路節點之虛擬路由器上, 使用 LAN 介面如 10 Base T/100 Base T 乙太網路或 Fr DTE, 透過虛擬路由器與 LAN 架構, 網管工作站可與所有 Passport 網路節點連接, 它的優點是:

- Frame Relay 軟體, 不需 FRAD 或外部路由器
- 減少網路管理連接之複雜性
- 容易達到網管系統冗餘與工作分擔之組態

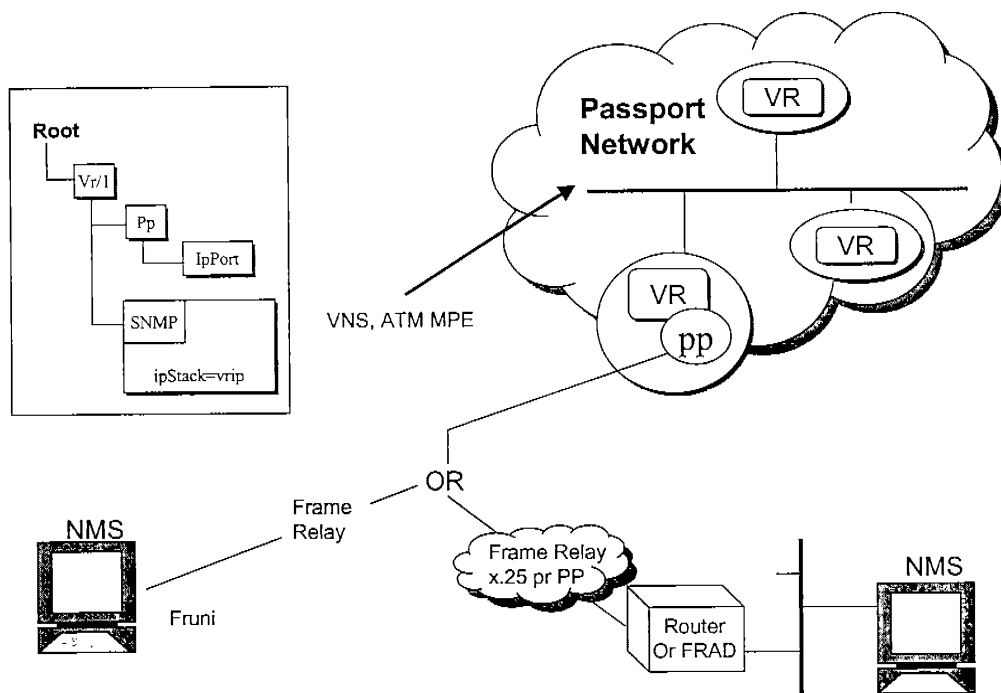


圖 2.6 IP Over Ethernet

IP over Ethernet 之連接方式支援 Inter LAN Switching (ILS) 架構, 可以使用 Telnet、FTP、FMIP 或 SNMP 來管理。

第 3 章、SDH 網路管理系統

本章介紹 Lucent 公司之 ITM (Intelligent Telecommunication Management) 設備

3.1. ITM 架構

Lucent 公司之 ITM 階層式架構如圖 3.1 所示，分為元件層 (Element Level)，元件管理層 (Element Management Level) 以及網路管理層 (Network Management Level)，它與 TMN 網管架構相呼應，如圖 3.2 所示，其相關通信介面如下：

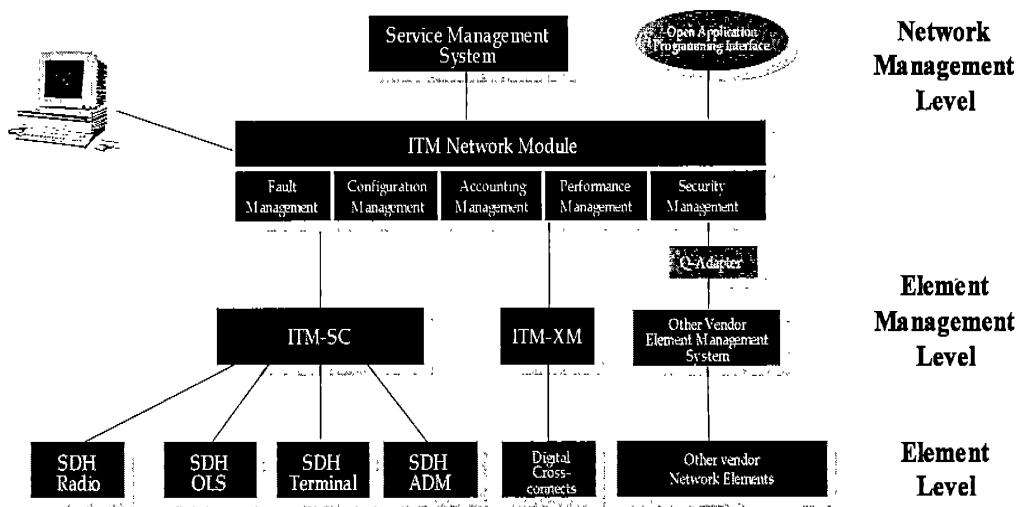


圖 3.1 ITM 階層式架構

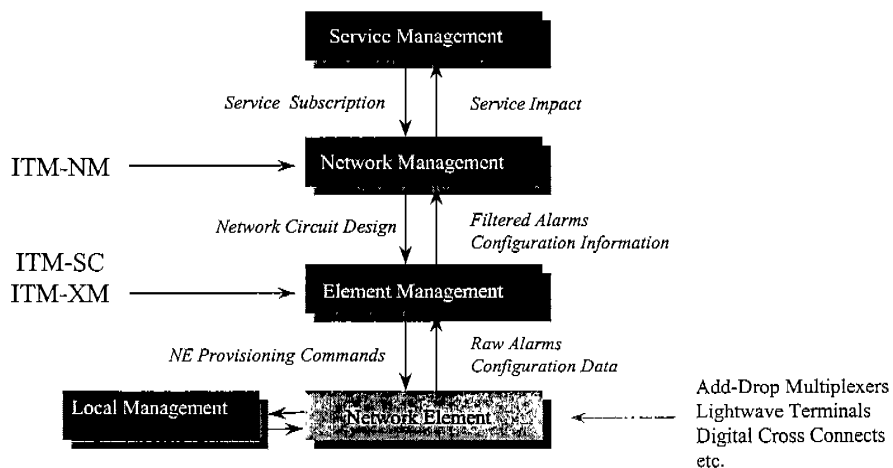


圖 3.2 ITM 與 TMN 架構

- EMS to NML:
 - proprietary interface to ITM-NM, TCP/IP protocol
- EMS to NE:
 - standard 7 layer OSI stack, CMISE/CMIP protocol
 - Q-LAN to Gateway NE
 - IS-IS routing within SDH DCC (from Yellow: L1+L2, to support larger networks)
- Information model
 - based on Q.3 and G.774 optimized to reduce NE memory and Processing Needs
 - improve upload times & response times
- Extra:
 - advanced resynch mechanism to quickly align NE and EMS MIB

使用者介面軟體：

- Graphical User Interface (GUI)
 - User Interface Process (UIP) + MAP
 - ITM-NM slave UIP
 - OSF/MOTIF compliant: point & click, pull down menus, pick lists
 - help on all screens, on-line documentation
 - color coding, print reports, not available options hidden
- Operating System
 - HP-Unix
 - HP-Vue environment

3.2. ITM-SC 功能

ITM-SC(Sub controller)之功能如下：

障礙管理(Fault Management)功能：

- 連續對網路元件監視
- 提供告警等級
- 顯示／確認告警訊息
- 現有及歷史檔
- 告警分類與過濾
- 告警總表以圖或列表顯示
- 由人機介面以可看或可聞訊息顯示
- 告警屬性（種類、日期、時間、位置、嚴重等級、網路元件）儲存在即時檔

- 經確認後之告警訊息存放歷史檔
- 每一告警之等級可由操作人員修改
- 每一網路元件每一障礙之告警起動與關閉
- 傳送告警訊息至 ITM-NM

組態管理(Configuration Management)功能：

- 網路元件管理上載／下載／同步
- 設定網路元件參數
- 設定 DCN 參數
- 設備保護控制
- 設定通信埠與交接點
- 設定 NE 資料 (名稱、位置、單元種類)
- 同步管理
- 使用者通道設定
- 動／關閉 DCC 連接

效能管理(Performance Management)功能：

- 資料蒐集
- 效能資料顯示 (圖示或表列)
- 輸出效能資料
- 連續監視終端設備
- 直接傳送到 ITM-SC
- 儲存每 15 分鐘監測資料達 31 天
- 資料為可由圖表顯示或印出之格式
- Per TP near end four parameters :
 - ES : Errored Seconds
 - SES : Severely Errored Seconds
 - UAS : Unavailable Seconds
 - BBE : Background Block Errors
- Network layers-VC12, VC3, VC4, MS, RS
- Enable/disable PM on TP level or clicking GUI sub rack
- After association loss regain of PM data
- Data Archiving
 - Allows a long term view of the managed transport network

- Overcomes the default storage intervals
- Data available for Quality of Service Analysis
- Can be stored on DAT
- Archive format is human readable

安全管理(Security Management)功能：

- 使用者登入控制
 - Access via login id's and passwords
 - User profile:
 - Operator (view)
 - Supervisor (view and change)
 - Administrator (startup/shutdown, archive/restore, set-up users)
- 網路元件 Compatibility Check

地域性冗餘備援功能：

ITM-SC 可依地域性(Geographic)配置 Redundancy 設備互相支援 (如圖 3.3 所示) 功能如下：

- 保護 ITM-SC 設備 failure
- 保護 ITM 與 NE 間之 loss (例如 cut in Q-LAN, fiber, DCC)

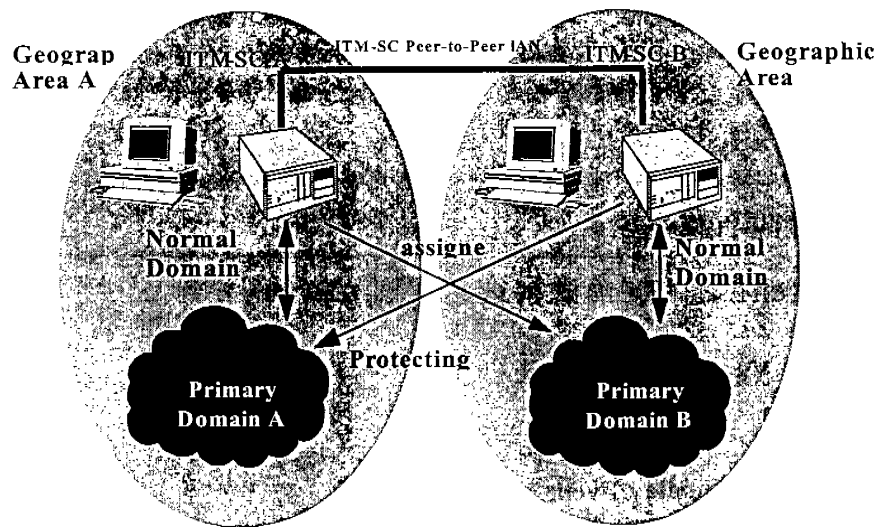


圖 3.3 區域冗餘備援方式

其運作方式如下：

- 網路元件被指配於兩組 TTM-SC 系統
- ITM-SC 系統以對等 LAN 架構互建
- 平常一個 ITM-SC 對應一個網路元件
- 自動保護開關，修復後由人工切回

圖 3.4 為 ITM-SC 負荷分擔運作方式

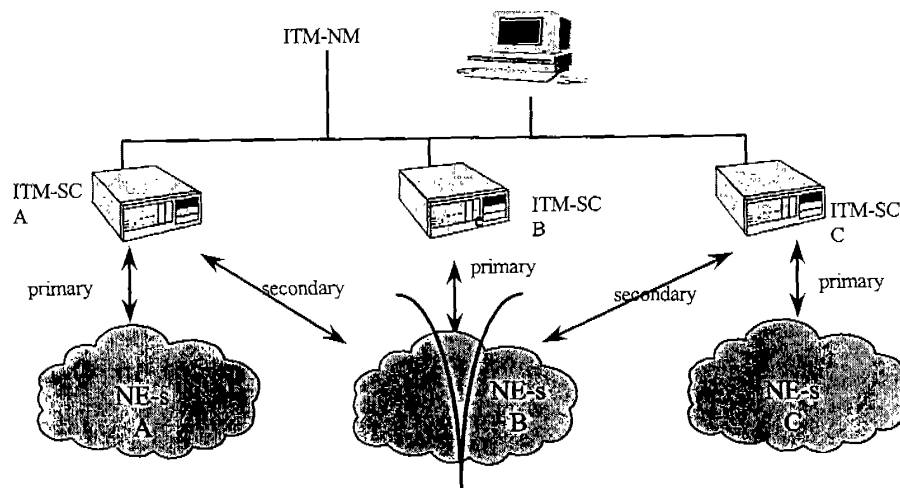


圖 3.4 ITM-SC 負荷分擔運作方式

3.3. ITM-NM 功能

Lucent 之 ITM 網路架構如圖 3.5 所示

ITM-NM 之功能如下：

- 障礙管理功能：
 - Display Event Notifications
 - Correlate Failures to Services
 - Verify Path Continuity
- 效能管理功能：
 - Display Performance Data
 - Compute Service-Quality Indicators
 - Assess Grade-Of-Service Violations
- 組態管理功能：

- Live Network Inventory
- Point-and-Click Path Provisioning
- Service-Design Flow-Through
- 安全管理功能：
 - Task Partitioning
 - Geographical Partitioning
 - Service Partitioning

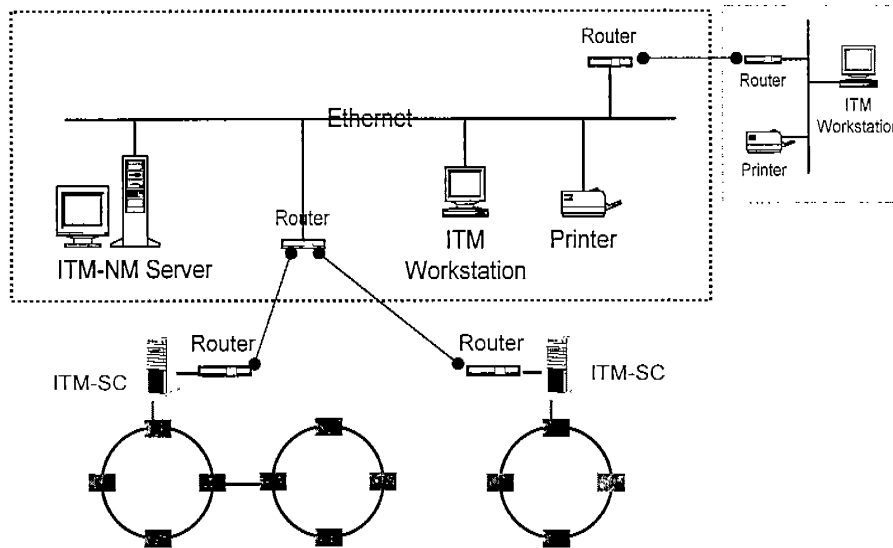


圖 3.5 ITM 網路架構

第 4 章、NetMinder 網路管理系統

NetMinder 是 Lucent 公司網路管理系統的名稱，包含有網路障礙管理 NTP(Network Trouble Patterning)、網路話務管理 NTM(Network Traffic Management)、網路容量設計 NCE(Network Capacity Engineering)等模組，它們提供即時網路管理維運功能。

NetMinder NTP 收集網路建立呼叫過程中之異常訊息，加以統計分析，提供告警，並找出障礙源，減少語音及信號網路的異常發生，NetMinder NTP 監督網路運作，顯示各網路元件之服務狀況。

NetMinder NTM 對語音、信號、智慧型網路提供近乎即時訊務管理功能，當訊務過載或設備故障而造成網路障礙時，維運人員可利用 NTM 中心來控制訊務流向，使其達最佳化運作，NetMinder NTM 支援國際、國內、區域、市內、智慧型以及無線等網路之訊務管理，提供監視、分析與控制網路訊務之功能。

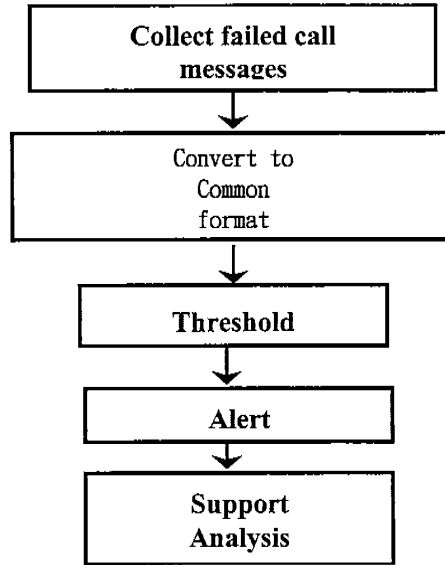
NetMinder NCE 提供訊務資料之收集與分析，以支援網路設備之設計，經由分析訊務資料，網路提供者可以更有效地使用網路設備，明顯地改善設備使用效率，所以 NetMinder NCE 之目標在使其顧客提高網路資源的利用度，因此可讓客戶獲得最佳服務。

4.1. NetMinder NTP

NTP 提供下列功能以發現並分析網路障礙：

- 從交換機收集呼叫失敗記錄
- 將這些記錄整理成共同格式(Common Format)
- 每一筆記錄加入其他網路元件曾經有呼叫建立失敗的資訊
- 在格式化記錄中尋找有問題的錯誤型式
- 顯示出有問題的記錄
- 提供複雜的工作，讓維運人員決定那一型式代表有問題，以及問題發生地點，並且將其修復。

以上敘述可用下列流程說明之。



呼叫異常資料(CIM)通常為 ASCII 格式，其內容因不同交換機種而異，CIM 加入已發生過之呼叫建立失敗的資訊而成為共同格式異常資料(CFIM)，由 CIM 變成 CFIM 之流程如圖 4.1 所示，

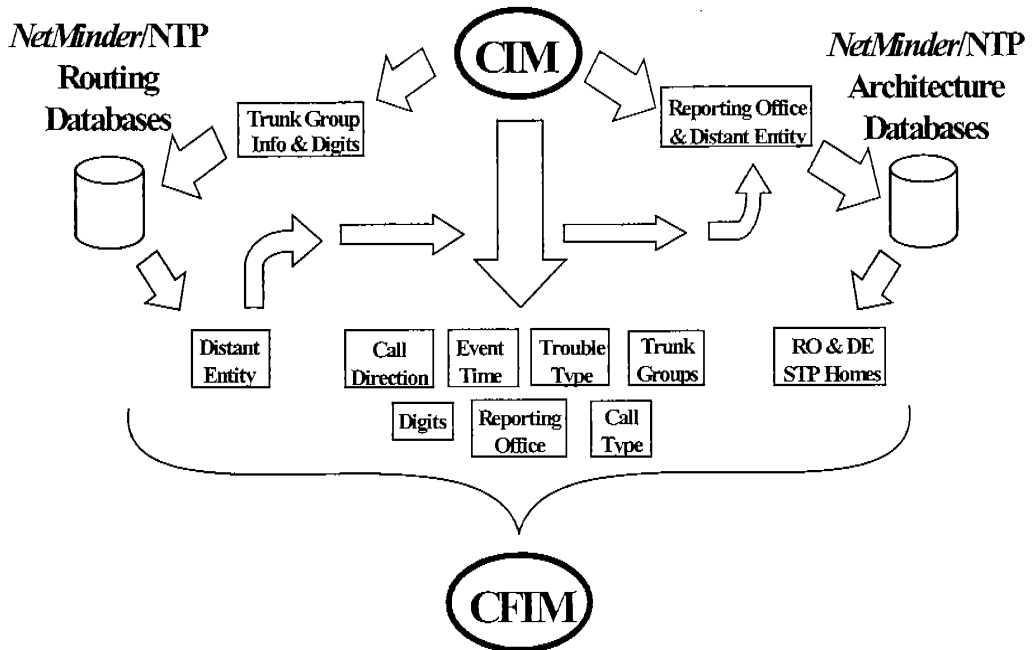


圖 4.1 CIM→CFIM 流程

以下為 CFIM 之格式

Date time	RO	RS	DS	DE	FDC	TC	Digits
03/15/00 07:35	pitbpadg43t	nywh	shok	dnvrcozja20	1613	dsf	8006777133
03/15/00 07:35	msdnwi231t	brma	shok	dnvrcozja20	1613	dsf	8006770086
03/15/00 07:35	rcmdvait03t	prri	shok	dnvrcozja20	1613	dsf	8006774477
03/15/00 07:35	wndrflt101t	fvjs	shok	dnvrcozja20	1613	dsf	8006772443

RO = reporting office
RS = reporting office STP pair home
DS = distant entity STP pair home
DE = distant entity
FTC = final disposition code
TC = trouble category
Digits= dialed digits

NTP 設定界限值(threshold)，在 5 分鐘內之 CFIM 資料判斷設備之障礙發生，向維運人員告知(alert)，告警的判斷值是根據歷史資料而定，而且會自動調整。

告警訊息的格式如下：

Alert #	Netwrk Elem	Type	FDC	TC	AL	Status	5-min Alerts	5-min Count	1st Datime	Last Datime
9518	dnvrcozja20	de	1613	dsf	cr	open	4	3801	03/15/00 07:20	03/15/00 07:35

Alert # = a number used for identification purposes
Netwrk Elem = the network element identified as likely to have a problem
Type = de means distant entity, re means reporting entity
AL = the degree of severity of the problem - cr means critical
Status = the state of being open or closed, as selected by the analyst
5-Min Alerts = the number of 5-minute periods this problem was detected
5-Min Count = the number of CIMs (failed calls) associated with this alert
1st Datime = the first 5-minute period this problem was detected
Last Datime = the most recent 5-minute period this problem was detected

Note: There will usually also be additional information, for example, the number of consecutive 5-minute periods this problem was detected.

NTP 在分析障礙點供維運人員修復，主要工具是資料顯示軟體，將 CFIM 資料中與告警有關的資料顯示出來，這些資料並可供各種不同的運算，除了呼叫建立失敗問題外，NTP 可偵測的障礙問題尚包括：

- Routing Errors
- Number Portability Errors
- SCP Provisioning Errors
- Authentication Failures
- Call Setup Failures
- SS7 Protocol Errors
- Traffic Congestion
- Link Failures
- Software Bugs in Network Element
- Generics
- SCP, HLR, and VLR Data Corruption Errors, etc.....
- Vacant Codes
- Network Element Failures
- Translation Errors
- Facility Failures
- Trunk Continuity Check Failures
- SCP Time-Outs
- Killer Trunks
- MF Signaling Failures
- Glare
- Handoff failures

4.2. NetMinder NTM

Lucent 之 NetMinder 系統之網路話務管理(NTM)符合 TMN 之網路效能管理 (Performance Management) 功能，它提供話務監視、計算，並改善服務品質。NetMinder NTM 硬體架構如圖 4.2 所示，網路效能資料如電路群、交換機資料之收集均基於 ITU-T Q.823 電路交換共同資料模式 (如圖 4.3)

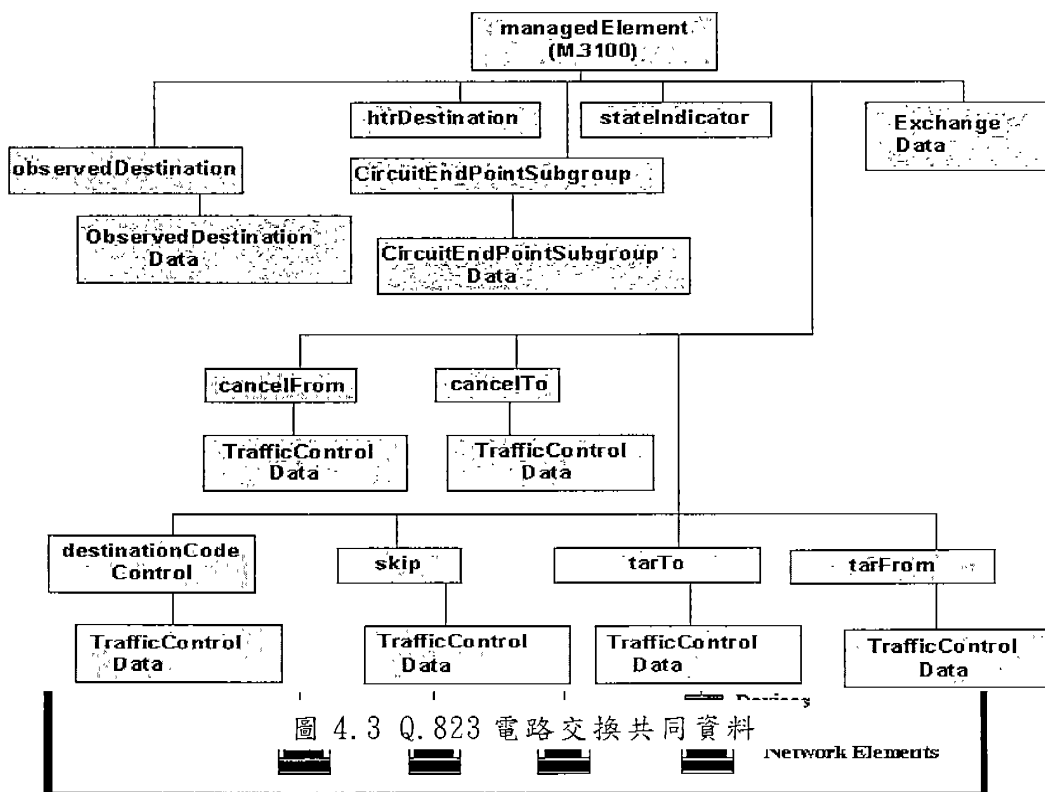


圖 4.2 NetMinder NTM 硬體架構

4.2.1. 資料收集

監視資料如電路群、交換機、終端等資料，NTM 每 5 分鐘

由交換機收集資料並予計算，這些資料被整理成共同資料模式並予儲存，再由網路話務管理者所設定之判斷值檢查決定是否需要告警。

4.2.2. 告警功能

NetMinder NTM 自動偵測網路資料，並與管理者所設的判斷值比較，當實際值超過設定之管理值時，即產生告警

4.2.3. 控制功能

當 NetMinder NTM 完成話務資料之收集、處理、顯示工作，網路話務管理者可使用控制功能，以反應網路之阻塞或故障，控制方式分為手動和自動，手動控制又分為保護性及擴充性控制兩種，保護性控制是用來抑制網路阻塞，使用 Skip、Cancel Form、Cancel To、Destination Code Control 等功能，擴充性控制係將正常迂迴路由作擴充性之迂迴，以紓解網路繁忙或故障，使用 Temporary Alternative Routing From(Tar From)、Temporary Alternative Routing To(Tar To)等控制功能。

第 5 章、感想與建議

1. 本公司擁有龐大的通信網路，不論交換、傳輸、數據……等設備，其廠牌種類繁多，品質各異。雖然設備可順利介接，以達成整體網路通信之目的，但由於各種設備往往各具有獨立的網管維運功能，每一廠商所提供的管理介面均為專有的格式，實際維運管理上很難達到整合的效果。各種設備由不同的人員管理維護，不但人力運用效率差，在維運品質上，也無法做到快速、有效的地步。目前本公司正面臨民營化的挑戰，不但組織、人力精簡，品質效率也要提高，各單位有必要積極檢討其設備維運的功能與架構，提高維運人力運用效率。
2. 網路通信維運管理標準之研究，均以客戶導向的服務管理為指標，期能滿足客戶之需求，今後提供客戶 SLA (Service Level Agreement) 的需求，亦大勢所趨，所以整合電信網路維運管理系統，其良好的設備運作功能固屬重要，亦應加強客戶服務需求之探討與設計，使新的系統整合發揮更實際的功效。
3. 隨著時代的進步，各種電信網路技術不斷的發展，設備亦隨之更新，網路所能提供的服務功能增加，通信品質亦提昇。而在這自由化競爭的環境，各電信業者又如何取得市場優勢，無庸置疑的，除了產品價格外，就是服務品質。所以在建構一個高品質、高效率的電信網路之時，其整合性維運管理系統亦不容忽視。若能在各種設備採購建置時，先深入考慮其全面性運作功能，並提供標準的網管維運通信介面，則對本公司未來的設備維運管理、人力的運用效率以及客戶服務品質，均有莫大助益。如此可降低產品價格，市場競爭力亦可望隨之提高。