網路管理通訊系統簡介

◎黃志文

隨著網路通訊需求之蓬勃發展，全球多媒體訊息交流的急遽增加，頻寬通訊之需求與日俱增。為配合大量個人多媒體通訊流量與企業無縫隙連接需求，各種通訊網路相對應之網路管理系統應運而生，以滿足高品質與高彈性系統運作之需求，並期能滿足終端用戶高速、多元之網路服務。

對企業而言，網路管理是企業管理之服務管理中的一環，一個完整的服務管理包括網路管理及系統管理；其中網路管理負責管理網路元件，而系統管理則負責管理系統資源。網路與系統管理可以確保網路的品質，並協助管理者監控整個網路的狀況。因此，不管通訊環境與媒介為何，都需要有一套完善的網路管理架構與運作環境，以維護作業環境的品質與效率。有鑑於此，本文將說明網路管理的基本內容、網路管理兩大通訊系統架構，並介紹業界常用的網管系統。

1. 何謂網路管理(Network Management, NM)

網路管理的目的為確保網路資源使用之正確性、有效性及安全性。隨著OSI網路通訊協定標準陸續制定，網路管理的通訊協定與系統管理功能亦跟著標準化中。簡單來說，所謂的網路管理即網管人員透過某一網管系統來監控、管理與維護網路狀態，以確保服務品質及執行效能。

在 ISO OSI 所定義的網路管理模式(Network Management Model)共分成組織模型(Organizatio n Model)、資訊模型(Information Model)、通訊模型 (Communication Model)及功能模型 (Functional Model)。

(1) 組織模型定義在ISO 10040上，描述網路管理系統的組成、功能及架構，例如對Object、Agent及Manager做定義。

(2) 資訊模型主要在處理管理資訊的架構，例如 ISO 10165 描述 SMI (Structure of Management Information) 及MIB (Management Information Base)。

(3) 通訊模型在描述如何完成資訊交換，它是由三個部份所組成，包括：在應用層所運行的管理應用程序；在上層與下層之間及同層之間的管理操作。

(4)功能模型則定義了著名的網管五大基本功能，包括組態管理(Configuration Management)、障礙管理(Fault Management)、效能管理(Performance Management)、安全管理(Security Management)及帳務管理(Accounting Man-

agement)。

若以OSI網路管理定義之系統管理者與被管理者角色，依其支援功能則可分為管理通訊(Management Communications)、系統管理功能(System Management Functions)、被管理物件(Managed Objects) 等三部份。

1.1 管理通訊

管理者與被管理者經由通訊協定交換管理資訊。OSI網路管理係採用共同管理資訊服務元件(Common Management Information Service Element, CMISE)負責管理通訊能力之邏輯部分。CMISE可分為：

(1)共同管理資訊服務(Common Management Information Service, CMIS) ，規定OSI系統管理提供原始操作服務之使用者介面。

(2)共同管理資訊通訊協定(Common Management Information Protocol, CMIP) ，規定通訊協定資料單元 (Protocol Data Unit, PDU) 格式與其結合的程序。

CMISE使用者為了完成管理操作，首先必須透過結合控制服務元件 (Association Control Service Element, ACSE) 建立結合關係，再經由遠程操作服務元件(Remote Operation Service Element, ROSE) 要求遠端去執行相對應的管理操作。

1.2 系統管理功能

網路管理是對網路上的通訊設備進行有效監視和控制所採用的技術與方法。依據國際標準組織(ISO)制定的開放系統互連(OSI)規範，建議系統管理功能範疇(System Management Functional Area, SMFA) 應涵蓋五部分：

(1) 組態管理(Configuration Management)

允許網路管理者控制網路元件的組態以減輕壅塞、隔離故障節點等。

(2) 障礙管理 (Fault Management)

允許網路管理者偵測及診斷網路異常如錯誤碼過多、纜線斷裂、廣播風暴等，並儘速隔離及排除故障原因以維護網路正常運作。

(3) 效能管理 (Performance Management)

允許網路管理者監視並評估系統效能，並藉由系統參數的調整以期達成較佳運作。

(4) 安全管理 (Security Management)

提供網路管理者對資源存取保護能力，以防範未經合法授權使用者入侵網路使用資源與破壞系統運作。

(5) 帳務管理 (Accounting Management)

允許網路管理者分配資源使用並收取合理使用費。

OSI訂定一般性系統管理功能 (System Management Function, SMF) 來支援SMFA功能性需求，譬如狀態管理功能可用於故障管理與組態管理。因此，SMFA可視為結合SMF子集的一個應用。目前SMFs包含：

(1) 物件管理 (Object Management)

支援被管理物件建立與刪除、讀取與修改物件屬性值，並適時發出事件通知。

(2) 狀態管理 (State Management)

支援接收被管理物件狀態改變之通知與存取和修改狀態屬性值之程序。

(3) 關係管理 (Relationship Management)

支援被管理物件之間關係表示與管理。

(4) 示警報告 (Alarm Reporting)

支援偵測被管理物件異常狀態與示警通知之報告能力。

(5)事件報告管理 (Event-report Management)

支援事件選取標準以控制事件傳送，並提供啟始 (Initiating)、終止 (Terminating)、暫停 (Suspending)、及復始 (resuming) 事件報告送出之程序與選取標準修改之能力。

(6) 存錄控制 (Log Control)

支援事件追蹤與管理，提供啟始、終止、暫停及復始事件載錄之程序與更改存錄選取標準、從存錄中擷取資訊之能力。

(7) 安全示警報告 (Security-alarm Reporting)

支援偵測安全異常並發出示警通知之能力。

(8)安全稽核追蹤(Security-audit Trail)

支援事件載錄及稽核之能力，以評估開放系統安全性。

(9) 存取控制 (Access Control)

支援管理資訊存取控制與操作。

(10) 帳務測量 (Accounting Meter)

支援系統資源使用之查測與使用量之限量。

(11)負載量監視 (Workload Monitoring)

支援將資源使用統計量儲存於被管理物件屬性中以監控系統效能。

(12) 測試管理 (Testing Management)

支援符合性與診斷測試程序之管理。

(13) 摘要 (Summarization)

支援動態監控系統資源、彙總統計及分析系統效能。

1.3 被管理物件

網路管理系統的基礎在於網路資源的管理資訊應用。這些被管理資源以被管理物件 (Managed Object) 形式定義於資料庫中，以支援管理運作。而管理資訊模型的建立，根據開放管理結構(Open Management Architecture, OMA) 應包含：

(1) 管理資訊結構（Structure of Management Information,簡稱SMI）

(2) 管理資訊庫（Management Information Base, 簡稱MIB）

SMI 運用物件導向觀念去定義 MIB 架構，其中包括使用的資料型態及這些被抽象化資源如何表示與命名。一般而言，被管理物件組成元素包含：

(1) 屬性 (Attributes)：表示這些被管理資源特徵。

(2) 行為 (Behaviors)：表示這些被管理資源的行為模式。

(3) 通知 (Notifications)：當被管理物件偵測到內在或外來事件影響被管理物件時之告知。

對於系統每一節點 (node) 都維護相對應之MIB來反應在此節點上被管理資源狀態；因此，網路管理實體 (entity) 可透過讀取被管理物件屬性值來監視資源使用，並經由修改此屬性值來控制節點運作。

2. 網路管理通訊協定

業界常用的網路管理通訊協定包含OSI-based 的 CMIP over TCP/IP (CMOT)、SNMP 兩種。1988 年 the Internal Architecture Board (IAB) 將 SNMP 定為短期網管建議方案，CMOT則為長期方案。將SNMP 定為短期方案的原因是 IAB 深信TCP/IP 在短期內將會修改

為OSI-based 通訊協定。SNMP的任務是應付立即的網管需求，提供基本的網管工具並能支援實務上的網管功能的發展。

為了日後的整合，IAB規定SNMP 及CMIP使用相同的管理物件資料庫，因此，只定義了一種管理資訊架構 (SMI) 及管理資訊庫 (MIB) 讓兩種網管協定共用。不同的是為避免造成網路的負擔，SNMP 利用 Connectionless 的 UDP 為通訊協定；CMOT 則是利用可靠的 Connection-Oriented TCP 通訊協定做為底層通訊協定。

2.1 SNMP 網路管理協定

在網際網路(Internet)開始應用之初，並沒有像SNMP這類的網路管理通訊協定。當時比較有效率的工具只有Internet Control Message Protocol (ICMP)，其中最著名的就是 Packet Internet Groper(PING)；這個指令藉由 ICMP 的通訊協定向 Internet 的其他主機送出要求，收到此封包的主機送出回應(echo)給發送端，發送端可以藉此取得兩台主機之間的連線狀況，例如用來檢測對方主機是否還在線上、連線狀況是否正常等等。

隨著Internet開始受到更多的關注，同時使用者也以指數的級數巨幅成長，網路複雜度因而提升到前所未有的境界，因此，我們需要一個更加嚴謹而且功能更為強大的管理工具。而這個工具的起始點就是在1987年發表的Simple Gateway Management Protocol (SGMP)，我們所要探討的SNMP就是從SGMP衍生出來的網路管理通訊協定。

整個SNMP網路管理架構，是由以下四個基本元素所組成，其架構圖如圖1：

(1) 管理裝置 (Station) ：負責管理、監視群組上的其他網路節點。具有資料分析、監視等管理功能的應用程式以及儲存網路管理資訊的資料庫。

(2) 管理代理人(Agent)：在受管理、監視的網路節點上接收、回應管理裝置的要求。

(3)管理資訊庫(Management Information Base)：為了要管理網路上的資源 (Resource)，我們將資源定義為物件(object)並儲存在管理資訊庫中，每個管理代理人都與管理資訊庫溝通，省去管理裝置對每個網路節點進行輪詢(Polling)所浪費的網路資源。

(4)通訊協定(Protocol)：與節點之間溝通的通訊協定。其中包含下列三個主要通訊指令：

(i)Get：管理裝置藉由這個指令取得網路節點中的物件資料值。

(ii)Set：管理裝置藉由這個指令設定網路節點中的物件資料值。

(iii)Trap：管理代理人可以利用事件(Event)來提醒管理裝置該網路節點所發生的狀況。

除此之外，配合實際網路狀況SNMP還定義兩個重要的管理架構：

(1)Trap-directing polling：網路的架構隨著使用者增多而複雜化，如果管理裝置仍然對網路上的每一個節點進行輪詢的話，會浪費太多不必要的頻寬。這也是為什麼SNMP要採用MIB的概念，在某個物件的數值達到一定的標準之後才進行輪詢或是讓每個網路節點在某些條件下(例如網路壅塞、斷線)才主動向管理裝置進行回報；而管理裝置收到回報之後，視情況進行錯誤管理。

(2)Proxy：針對網路上某些不具備完整的UDP/IP通訊協的節點(像是數據機、

橋接器等等)，我們沒有辦法直接對這些節點進行管理，此時必須藉由委託代理人(Proxy Agent) 對這些節點進行監控與管理。

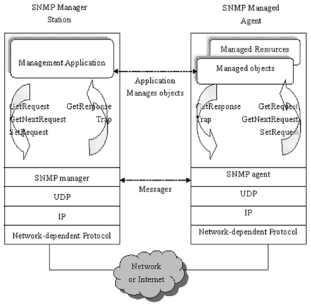

圖1：SNMP網路管理基本架構

目前於SNMP網管協定共分成三個不同的版本，以下就SNMP v1、SNMP v2與SNMP v3的內容作描述：

1. SNMP v1：相關定義可由 RFC 1155、RFC 1157、RFC 1212 與 RFC 1213 中找尋。在 SNMP v1 中，代理人(Agent) 以訊息 (Message) 的形式與管理裝置進行溝通。每個SNMP訊息包含了版本編號(version number)、通訊名稱(Community Name)、五種通訊協定資料單位(PDU)，如下表(a)~(f)。

(a) SNMP Message

Version	Community	SMTP PDU

(b) GetRequest, GetNextRequest, SetRequest, SMTPv2trap, InformationRequestPDU

PDU-Type	request-id	0	0	variable binding

(c) GetResponse PDU

PDU-Type	request-id	error status	error index	variable binding

(d) GetBulkRequest PDU

PDU-Type	request-id	non-repeaters	max-repetitions	variable binding

(e) SNMP v1 trap PDU

PDU-Type	enterprise	agent-addr	generic-trap	specific trap	time-stamp	variable binding

(f) variable-bindings

Name1	Value1	Name2	Value2	...	NameN	ValueN

2. SNMP v2：相關定義可由 RFC 1901、 RFC 1902、 RFC 1903、RFC1904與RFC1908中找尋。在開始探討SNMP v2與v3之前，我們必須要知道，這兩個版本並非用來取代原本的v1，而是對v1所缺少的部份進行補強。首先是資料傳輸的加強，在SNMP v1中，每次的溝通(transaction)限制了固定的資料傳輸量，造成了管理裝置與代理人必須進行多次的溝通，同時也消耗了可觀的頻寬。針對這個缺點，SNMP v2增加了一個新的指令GetBulk，如圖。

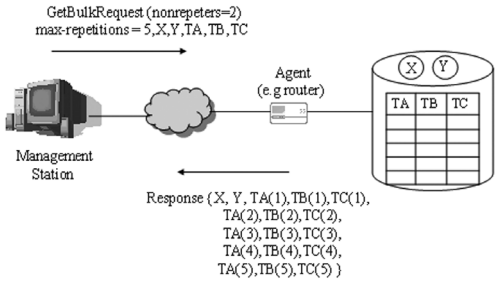

圖2：SNMPv2 GetBulk管理架構

SNMP v2還提供了另外一個nonatomic GET指令來增加資料傳輸的效率。SNMP v1中，如果使用GET指令要取得一或多個變數值，而代理人沒有辦法傳回多個使用者要求的變數值時，必須要重新使用GET進行要求；而SNMP v2的nonatomic GET指令可以忽略這項錯誤，儘可能的傳回使用者要求的變數值，藉此減少彼此溝通的次數。

3. SNMP v3：相關定義可由RFC2271、RFC2272、RFC2273、RFC2274及RFC2275中找尋。SNMP v3由三個模組組成：訊息處理與控制模組(Message Pro-

cessing and Control Module)、本地端處理模組(Local Process Module)以及加密模組(Security Module)。其中最重要的就是加密模組。不同於 SNMP v1 與SNMP v2的是，以往的版本都是以明文的方式來傳輸密碼，假使有心人士攔截到傳輸密碼的封包就可以得知真正的密碼。而SNMP v3提供了認證(Authentication)、保密(Secrecy)與管控存取(Access Control)三種資訊安全的機制。認證的機制使的代理人確認該命令是否來自經過授權的管理裝置，因此，每個管理裝置及代理人都必須共享一把金鑰(Secret key)，管理裝置使用這把金鑰計算出一段訊息認證碼(Message Authentication Code)並將其附加在訊息之後，代理人收到訊息之後，用相同的金鑰進行計算，並將結果與收到的訊息認證碼比對，相同即代表來源是經過授權的管理裝置而且沒有經過任何第三者的修改。

此外，對於現在規模漸趨廣大的網路架構，以往的集中式網路管理已經不足以應付目前的狀況。因此，分散式的網路管理應運而生，與集中式相比，分散式有比較好的錯誤容忍度、擴充性以及較低的管理與通訊成本。此外，若其中一台管理主機發生故障，那麼連帶屬於該主機管理範圍的資訊都會消失。

雖然SNMP也逐漸走向分散式管理的型態，相較之下，OSI的CMIS/CMIP更能提供智慧型管理。然而，因為架構太過複雜而且缺乏硬體的支援，OSI的標準並沒有獲得廣泛的使用。因為SNMP是一個廣泛接受的標準、有眾多的使用者，架構簡單。也因此出現了將Mobile Agent整合進SNMP的想法。所謂的Mobile Agent是一種反向思考的概念，我們常常把資料放到程式裡面，然而Mobile Agent的概念卻是將程式碼轉移到資料裡。

2.2 TMN網路管理協定

有鑒於電信網路的複雜，及其影響層面日趨廣大，為了能整合現有及管理系統，ITU-T乃著手制定電信網路管理標準TMN，希望發展一個管理如此龐雜網路的系統時能有所依據。由ITU-T在發展推廣的TMN平台，希望能夠提供SNMP的資訊傳播介面，TCP/IP搭配在遠端終端模擬器的功能，如此管理者就可在管理中心充分監控全部網路。

TMN之功能架構圖如下圖3所示。TMN的功能結構是以許多的功能區塊(Function Block)所組成。這些功能區塊提供了TMN的一般管理功能。並在各個功能區塊間，以資料交換功能(Data Communication Function, DCF)作資料的交換與傳遞。分述如下：

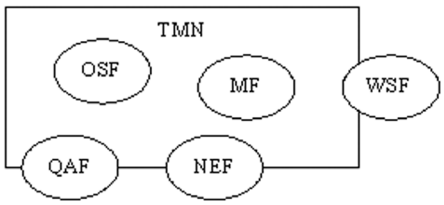

圖3：TMN功能架構圖

(1) Workstation Function (WSF) block：此功能是將TMN的資訊直譯為資訊管理人員可以理解的資訊。

(2) Operation System Function (OSF) block：此功能主要的工作是收集電信網路上所有的相關資料，並監控網路元件的狀況，並回應系統管理者的要求，提供管理

工作的服務；此外OSF間，還必須進行資訊交流。因此OSF可說是TMN最重要的部分。也是維運系統的功能區塊。

(3) Network Element Function (NEF)Block：主要的目的在於回應來自網路上的指令，並能監控網路元件的動作。

(4) Q Adaptor Function (QAF)block：相似於NEF的功能，主要提供在TMN與非TMN之間的參考點(Reference Point)聯繫。

(5) Mediation Function (MF)block：提供NEF(或QAF)與OSF之間的資訊轉換、儲存、過濾、以及提供部分WSF所需的功能區塊。

對於每一個功能區塊，TMN又再細分成幾個功能單元(Function Components)，其中包括提供管理功能的MAF(Management Application Function)，以及存放管理資訊的MIB(Management Information Base)，以及與資訊相關的PF(Presentation Function)與HMA(Human Machine Adaptor)；此外為了使所有的功能區塊互相獨立，降低設計與維護的成本，ITU-T定義出數種參考點(Reference Point)來作為不同功能區塊間以及與外界溝通的介面。如WSF與OSF、WSF與MF間的參考點f及x、g、q等等不同的溝通功能方塊的參考點，如下圖4。

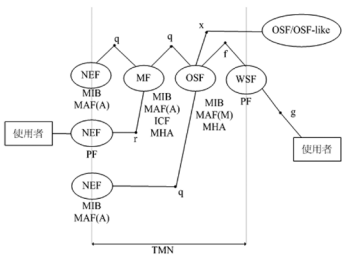

圖4：TMN之功能區塊描述

TMN的另一個重點是定義實體架構與介面，由實體架構之元件和元件間的介面所組成的TMN架構。此介面架構圖如下圖5所示：

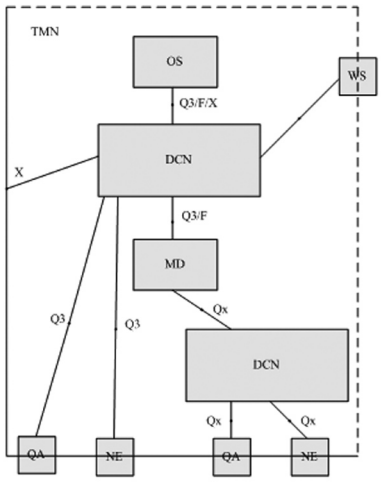

圖5：TMN實體架構與介面

相關實體內容描述如下：

(1) OS：Operation System，主要負責網路管理應用之部分，是整個網路管理核心。

(2) MD：Mediation Device，提供OS與NE間之介面。

(3) NE：Network Element，是網路中的各個通訊設備，負責管理資源。

(4) QA：Q Adaptor，提供無法遠端管理的網路元件之網路存取。

(5) WS：Workstation，負責OS的使用者介面，給遠端管理使用。

(6) DCN：Data Communication Network，用以連結上述元件的相互連結與之間的資料傳遞與溝通。

至於TMN最重要的維運系統功能區塊OSF的網路功能，以網路階層的概念分割

為四個階層。在最新M.3010的TMN架構中，包含了TMN網路功能分層的範例，定義了Business、Service、Network、Element 等管理階層，如下圖6所示：

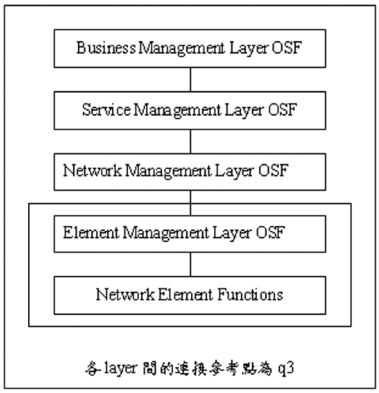

圖6：TMN之功能階層架構

TMN中所有的管理運作步驟，皆是遵循如同OSI之管理者與受理者(Manager-Agent)的運作模式。下圖7即是整個TMN中，一個管理控制的流程。在此過程中，我們可以了解，下達指令要求的即是管理者，而接受指令並予以回應的即是受理者，而依據網路的層級架構，最終網路元件的Agent即是必然的受理者。

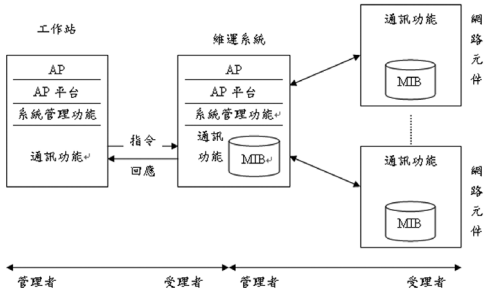

圖7：TMN管理運作流程

上圖7左所指的工作站，即是網路管理者所用的操作介面，由工作站下達的指令，直接送給負責的維運系統處理，此時維運系統可能自行回應，也可能需要再向後端的網路元件Agent或其他維運系統下達指令要求，待得到回應後，再回應給工作站。無論在工作站上或是維運系統上都有相似的結構，共可分為四大功能階層：

(1) 通訊功能部分：用以接收或傳送資訊，採用的是CMIP(Common Management Information Protocol)。

(2) 系統管理功能(SMF，System Management Function)：提供了最基本的網路系統管理函數，而且所有的功能皆由OSI制定認可。

(3) 應用程式(AP)發展平台：結合系統管理功能與通訊功能的應用程式。

(4) 應用程式(AP)：由各家系統業者依平台工具各自發展。

TMN管理架構之所以重要，是因為TMN如同OSI一樣有完整的架構，若採用這個標準來建構網路管理系統，業者的投資就可以獲得保障，因為轉換模組可以將一些舊的非標準訊號轉成標準介面；且各個階層皆獨立負責運作一完整的功能，故不管做更新或維護的動作，都會相對的容易許多。除此之外，當新的科技或服務出現時，業者只需採購依標準介面設計的設備就可以符合網路管理需求，不必將整個網路管理系統重新架構一次。

3. 網路管理系統

以CMIP為主的TMN網管系統多為電信業者搭配電信系統獨立開發，缺乏共通性，但基本架構及功能則不離以上所述，

故不在此單獨介紹；但有些系統業者仍提供使用者相關開發工具，如AdventNet，以使設備能接受TMN網管系統管理。此外，AdventNet也提供SNMP相關Tool Kits及完整的發展元件，所以如果想自行發展網路管理工具，AdventNet會是很好的選擇。如果還想更深入，可以參考開放原始碼的Tobi Oetiker MRTG (the Multi Router Traffic Grapher)。

另外這裡一定要提的網路管理系統是偉大的為HP Openview系統。Openview提供現成的套裝管理工具，也提供發展環境，讓使用者發展適應性網路解決方案，網路上的還有相關使用者論壇提供強力的支援。從系統初始至今，Openview已經不只是單純的網路管理系統，現在已能提供網路系統的管理及龐大的適應性企業解決選擇方案。

3.1 HP Openview網路管理系統

由於 HP Openview 網管系統是SNMP-based網管系統，故通訊方式遵循前述之標準SNMP架構及協定規格。HP Openview網管系統雖只支援SNMP及SNMPv2C通訊協定，但在Scalability及Distribution上做了很大的改善；另外也提供各式Filters，目的是增加系統的效率，減少網路交通的負擔，特別是如果使用的網路是容易壅塞或昂貴的網路資源，如衛星網路等。

由於SNMP未制定網管介面的部份，HP OpenView網管系統便以SNMP為基礎，利用以下方式改進系統的擴充性、分散性及系統效能。

(1) 以Collection Station分擔Management Station及網路的負擔，使得網路管理的架構由中央集權式演化為Fully centralized、Centralized hierarchical、Hierarchical及Cooperative Independent等四種網管架構可以利用。

(2) 以Management Consoles負責分擔系統顯示工作，並可由多人分別管理不同網路狀況，而不影響系統效能。

(3) 提供瀏覽器介面(Web Browser Interface)，如下圖8。

(4) 可定義必要物件子拓樸圖 (On-Demand Submaps)，使可能原有的上千個佔用系統資源的物件，不需全部顯示，而只需顯示出使用者需要的物件，節省大量的系統資源。

(5) 以Filters減少系統管理的資料量或使用者監看的資料量，增進系統效能及減少使用者監看到重覆的網段。

(6) 以事件重傳 (Event Forwarding) 方式，將網路上任何節點所發生的事件重傳到任一Management Station上。

(7) 以分散監看臨界點 (Distributed Threshold Monitoring) 的方式，由當地的站台直接監看當地的網路狀況，而不需由Management Station透過較慢的廣域網路收集監看網路的趨勢資料；必要時才觸發處理程序，可減少很多廣域網路的流量。

(8) 提供容錯 (Fault Tolerance) 功能，提高系統的可靠度。

Hp Openview 以不同 View 概念提供使用者適應性的管理視窗，如圖8，網路管理員可藉由視覺化管理介面，以商業服務(Business View)角度管理企業對IT資源需求的績效與衝擊等問題。由網路管理系統延伸的商業管理解決方案，如圖9，更提供IT與企業團隊共同介面以改善網路與企業資源的管理與績效。

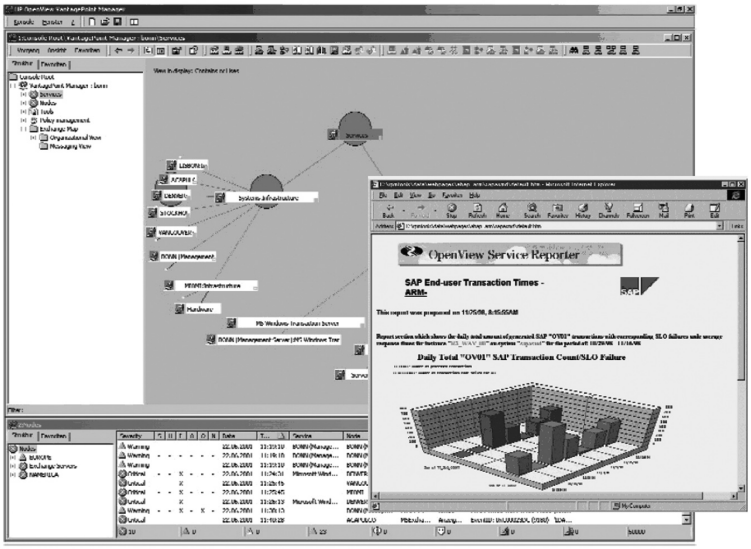

圖8：HP Openview基本管理介面

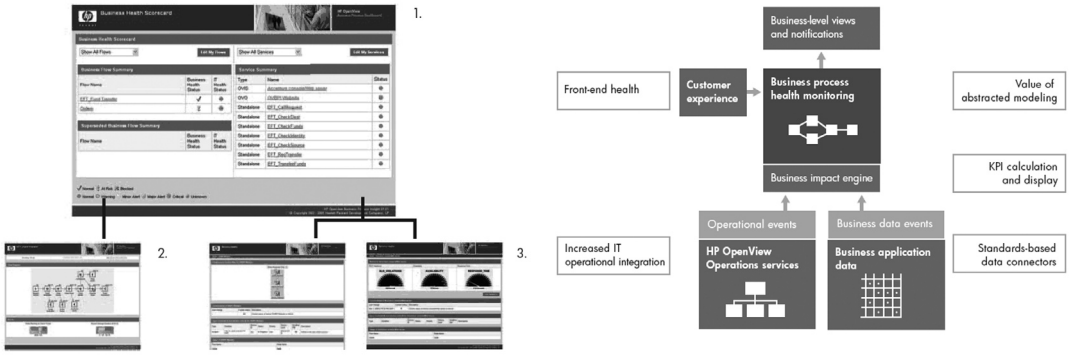

圖9：HP Business Management 解決方案

時至今日，Openview不再只是網路管理系統，而已經發展為適應性企業管理解決方案如下圖10；應用層面從網路基礎建設的調校與最佳化、IT資訊服務自動化到企業IT資源及服務管理等，端看企業如何使用與發展該管理平台。

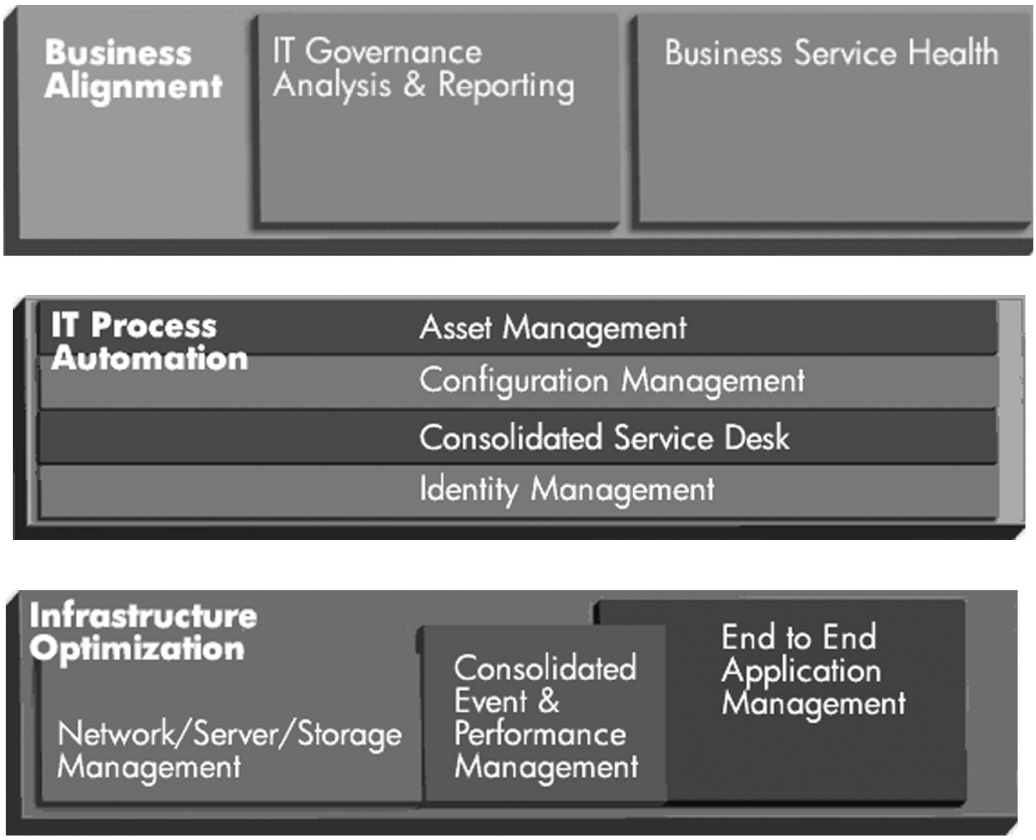

圖10：HP Openview完整的管理方案

3.2 AdventNet網路管理系統與發展工具

如果你只是想發展與使用網路管理工具，那麼建議使用AdventNet強大的發展工具。AdventNet的網路管理架構如圖11，並提供以下特性。

(1) 統一的圖形化管理介面。

(2) 網路可視性：藉由 Discovery 、Physical and logical topology、Maps、Centralized event management、Graphs Graphs 及Statistical information等功能，達到使網路活動可視性的目的。

(3) 元件管理：所有網路元件與設備的中央式組態管理。

(4) 遠端監控：提供大型與分散式網路管理功能，並利用Distributed Mediation Server就近蒐集統計網路資料，再回傳相關資訊給網管中心。

(5) 可擴充架構：依使用者網路的成長與需求提供可繁衍的網路管理架構。

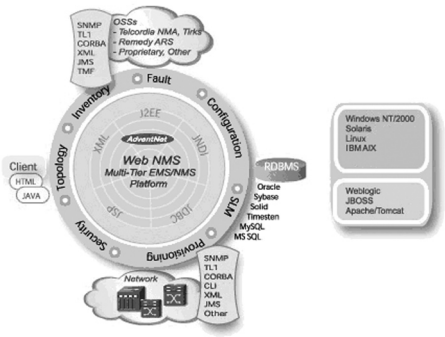

圖11：AdventNet網路管理架構

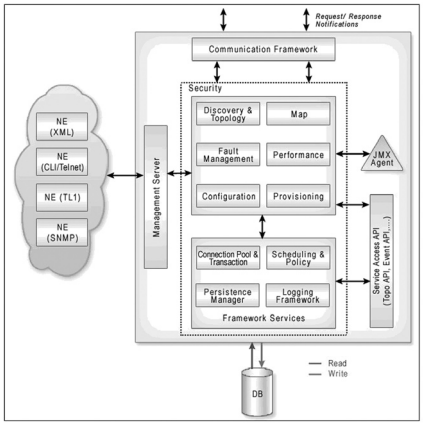

圖12：後端Server基本架構

AdventNet的網路管理系統提供Fault Management、Configuration Management、Discovery、Performance Management、Security、Inventory Management及Web-based graphical user interface等功能，形成後端Server的基本架構如圖12。

除了網路管理系統的完整套裝功能外，AdventNet還提供相關Java-based主從兩端的網管平台的發展工具，如圖13，讓開發者可以快速發展所需的客製化網管系統。

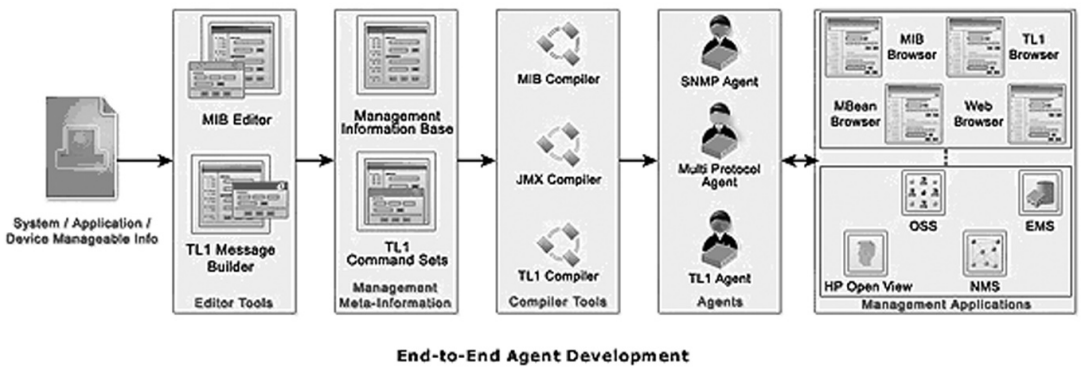

圖13：AdventNet SNMP Agent Java Toolkit

4. 結論

由於SNMP以UDP為基礎，導致網管訊息可能會遺失或重覆，相對的以TCP為傳送協定的CMOT則定義嚴謹，且提供完整功能，故講求穩定的電信管理網路TMN(Telecommunications Management Network)大多仍以CMIP為網路管理協定的第一選擇。

以資料傳輸為主的Internet，由於基礎網路建設早已由較高bit error rate的同軸電纜轉換為穩定的光纖網路，故以UDP傳送的SNMP網管系統反而因架構簡單及節省頻寬而廣泛流行；加上電信網路IP化與語音多媒體封包於網路傳輸的趨勢助長下，SNMP網管系統大有後來居上的態勢。

本文簡單介紹了網路管理的基本內容、網路管理兩大通訊系統架構，並說明業界常用的網管系統。除了希望能讓有興趣的讀者了解網路管理系統的基本概念外，藉由網管系統軟體簡介，更希望讀者能以此為起點，找到或發展適用的網路管理系統。