

### 本章內容：

- \* 網路管理是什麼？
- \* 系統管理與網路管理
- \* 網路管理的功能層面
- \* 在談網管
- \* SNMP 網路管理

# 第三章

# 網路管理 與 SNMP

在本章中，我們要來看看促成 SNMP 創建的想法動力：網路管理。之前已經對網路管理概念稍有著墨，但到底什麼是我們所謂的網路管理呢？

## 網路管理是什麼？

如果你試著問十個人“什麼是網路管理？”，你很可能會得到十種不同的答案。當然，如果你問的只是十個剛好路過 7-11 的行人（而且每個“我不知道”的答案都分開計算的話），這其實也不足為奇；但是，如果這十個人恰巧都是你公司網路工程組或資訊系統管理部門的成員，那麼你一定會想：是不是哪裡搞錯了！現在再考慮不同的另外十個來自業務和行銷部門的可能答案，你才恍然大悟：即使網路管理有如此多種截然不同的定義，居然很少人完全明瞭其中真正的內涵。

說真的，這怪不了誰，而是網路本來就可以分成幾種不同的層級來看待。其中，網路維護（network maintenance）是最低階的一層，工程師們以鉗子、剝線鉗、電焊棒、數位多用電表、和網路分析儀來管理網路的“實體設施”。他們會爭論 10BaseT 和 10Base2 的優劣，並且會注意到，自從他們以 50 歐姆來取代那些 75 歐姆的終端接頭之後、網路運作效能又提生了多少之類的事情。

接下來另一層級，我們姑且稱為組態管理（configuration management），此一層級決定的是實體上和邏輯上的網路建置規劃。組態的內容包括連接到網路的各裝置、它們的連接方式、以及用來連接它們的其它設施；至於組態管理人員所要決定的事項包括了：如何劃分路由器的管轄範圍、主機該使用哪一種系統管理軟體、要提供固定式的 IP 位址還是使用 DHCP 伺服器、以及如何說服財務人員說我們的 Internet 連線需要 T1 頻寬等等。要是你不小心激怒了其中任何一個管理者，他們搞不好會更改路由器設定，使得所有來自你工作站的封包統統被吞掉，然後一連癱瘓好幾天，並且宣稱他們“一直在想辦法解決問題”。

層級再高一點的一群，被稱為是網路管理者（network administrator）。一旦網路組態穩定，這群被賦予管理權力的管理者就成為網路的主控者，他們的任務是執行網路的邏輯配置和服務運作，如監控集線器和路由器上可用的埠個數、將第 300 個使用者加入一只註冊了 256 人的伺服器、發現某網路介面控制卡違反了 CSMA/CD 傳輸原則、注意到某公司上下班時間的 Internet 連接頻寬、以及回應或是故意忽略所有求助的 email 訊息。身為網路管理者不是正在追逐別人，就是成為被人追逐的對象，其處境和“銀翼殺手”或“絕命追殺令”中的哈里遜福特有得比。

### 管理（Management） 或是治理（Administration）？

這兩個字眼看似同義，其實在概念上還是有點差別的。治理是與政策形成、帳號管理和成本分析的施行、工具設備、儀器、和個人檔案的維護等事宜相關，而管理則是與網管政策落實和工作指派有關，並且務必確保一切順利運作。你可以說：治理絕大部份是戰略性的，而管理傾向較為戰術性的，兩者都需要相當程度的技巧。

最高層級的是網路使用者（network user）本身也是網路中最無助的一群“管理者”。對使用者來說，網路管理不外乎是處理伺服器的登入和登出、刪除過時檔案、偶爾更換密碼或預設印表機佇列等事宜。以使用者的觀點，網路存取本來就應該快速，並且網路本身就應該提供使用者所需要的大部份服務。真正網路管理者只想防止使用者不小心地（或蓄意地）侵入破壞網路。

針對剛才的問題，我們不難推敲出一個合理的答案：網路管理是一連串處理手段和政策原則，使電腦網路不受網路大小或是工作量影響，而維持正常運作和工作效率。

## 系統管理和網路管理

我們已經談論過網路管理了，還有另一個你或許聽過的名詞是系統管理（system management）。雖然這兩個字眼往往似乎指向同一個概念，但其實卻是不可互相替換的。它們在定義上的確有一些重疊，而這往往導致混淆。這兩種管理工作內容都包括了自裝置如路由器、伺服器、和工作站等處搜集資料，但它們使用資料的方式卻是截然不同。

系統管理是監控和維護個別裝置的過程，裝置可能被配置成獨立運作的各個單位，或是連接到其它裝置形成網路。系統管理工作包括了安裝和升級軟體、製作資料備份、監控可用磁碟空間和電力等級、設定使用者帳號、以及安裝和移除系統服務。

我們之前概略介紹過的網路管理則包括了在裝置層次上、用來監看和維護網路健全運作的各項綜合機能。網路運作是否良好，是取決於目前裝置上操作工作的層級和多寡，至於不影響網路效能的裝置功能如與本機周邊設備的溝通，則不在網路管理的範疇之內。

系統管理和網路管理重心都同樣在於裝置的監看和控制，但系統管理將裝置視為是獨立的個體，或是一群相關服務的成員之一，而網路管理將裝置視為是組成網路骨幹的一小部份。你也可以這樣來看待兩者的差別：一者是只關心特定裝置的順利運轉，另一者是關心整體網路的健全運作。

你應該能了解，系統管理功能會對網路運作造成影響，例如備份伺服器上的大量資料、或是升級路由器的韌體，皆會對網路機能造成影響；而網路管理功能，如限制路由器的網路交通量，也必定會影響到網路上各個系統的運轉。

為了讓你對如何實施網路管理、為何實施網路管理、何處實施網路管理、以及何時實施網路管理等課題有些基本概念，接下來我們需要看看管理電腦網路的模型。

## 節點的種類

根據網路管理的基本模型，將網路上所有節點分成以下幾類：

- 受管節點 目前正在搜集並提供管理資訊的任何網路裝置。
- 管理節點 能夠自受管節點擷取管理資訊的任何網路裝置。
- 無法管理的節點 這類節點要不是無法支援網路管理，就是支援的是不相容的網管通訊協定。

每一個受管節點（managed node）上都有一支代理者執行程序，為管理節點所發出的管理資訊要求來服務。當一要求被收到時，會先通過檢查，看看發出要求的節點是否經過認可核准；如果是，該代理者便自節點搜集要求資訊，並以回應的形式將該資訊送回給發出要求的管理節點。

管理節點通常是工作站，上面有網路管理系統以應用軟體的形式執行中，並且配有交互式選單驅動或圖形化的使用者介面。管理節點也可能是稱為遠端監督（remote monitoring, RMON）偵測（probe）的自動化軟體程序，專門用於自受管理節點搜集管理資訊。一節點可以同時具備受管節點和管理節點的雙重身份，像同時有代理者執行程序和網路管理系統在執行的工作站就是一例，這類節點通常被稱為是雙面節點（bilevel entity）。

你可以試著想像，網路上大部份的裝置都能夠搜集它們效能和運作狀態的相關資訊，以標準化方式呈現該管理資訊，一幅分散式的管理藍圖會具體地浮現出來。使用網路管理軟體可以搜集和處理管理資訊，加以組織成一幅實際的圖像，它反映的正是整體網路的狀態與運作情況。

## 本地端 v.s. 遠端式管理

廠商一般會將網路裝置設計成不需要任何形式的網路管理也可以操作。然而實際的情況是，某些形式的本機式管理，如前端儀表板（front panel）或終端介面（dumb terminal interface），通常是不可或缺的，藉以設定該網路裝置的配置。裝置的網路管理功能設置可以在隨後該裝置的韌體升級時附加上去，或是以附加其它硬體的方式裝設於該裝置上。

## SNMP 特有的詞彙

談到這裡，你可能已經察覺到，SNMP 管理模式其實相當於主從式架構的資訊系統模式。SNMP 不傾向重複或濫用的如“用戶”、“伺服器”和“資料庫”之類的術語，而是定義它自己的詞彙，或是使用現成 OSI 網路管理慣用語。使用特定的詞彙，有助於避免大家誤解 SNMP 的概念，尤其是對於“用戶”或“資料庫”之類詞彙持有分歧觀點和意見的人們來說，SNMP 的定義更加精確。

並非所有網路元件都會記載它們關於網路的種種有用資訊。事實上，許多網路裝置的主要功能運作根本不需要網路，甚至根本沒有察覺它們是否接在網路上。想像一個將資料訊號從某種格式轉成另一種格式的裝置，假設這台裝置輸入介面連接的是光纖、輸出介面連接的是銅纜線好了，這個裝置只會注意到幾件事情：它自光纖接收進來的訊號、用於轉換訊號格式的處理程序、以及轉換好輸出至銅纜線的訊號。像這樣一個裝置或許會配有前端儀表，上頭有些指示燈號顯示目前狀態、一些輸入資料的按鈕、和一個數位螢幕以顯示資訊，也許還有一個粗陋的選單。它或許還支援串列介面（serial interface），用於附接非同步串列終端介面，以字元模式的選單形式提供存取本機裝置的管理資訊。藉由此種實體介面來操控裝置的方式，稱為本地端管理。

現在想像一下，你擁有數千台這樣的裝置，分佈於整個城市、國家、甚至大陸。就如同我們曾在第一章中所討論的，近端管理方式必須走訪每一台裝置來進行配置修改和效能監控，不論從時間還是金錢的角度來看，都是絕對行不通的。你需要的是某種形式的遠端式管理，讓你從單一定點就能存取到所有的裝置。

這種遠端式管理是如何運作的呢？假使要對你目前的裝置進行管理工作，你可以輕易地接上數據機到該裝置的串列埠，然後允許管理員自遠端撥入來監看你的機器。這個做法唯一的問題是：每一台裝置都必須有一台數據機才行，而且每次連接你都得手動將電話線連上指定裝置。毫無疑問的，這種做法的成本高昂，當你有上百台的裝置需要同時管理監看，這簡直是要命！

讓我們試著來改進原先的做法。你可以考慮利用某種管理代理伺服器，它是在電腦上執行的一種特別設計的軟體用以遠端管理你的裝置。這類伺服器將會直接建立串列連接到每項裝置，並且支援幾台數據機撥接連線。身為管理者所需要做的就只有撥接連線到該代理伺服器，然後向特定裝置要求管理資訊；接著，這台代理伺服器不是搜集你所要求的特定裝置資訊（並且為你製作格式便於瀏覽），就是直接傳遞給你該裝置軟體既有的管理選單資訊。

這的確是較佳的解決方案，你不再需要為每台裝置配備一台數據機，但你需要一個能夠處理許多串列連接的伺服器，而且你還需要投入額外的時間和精力來撰寫和維護該伺服器上的特殊管理軟體，這些工作都是非常累人的。

分散式管理模式是另一種選擇方案，每項裝置都是網路上的成員之一，並且允許擁有網路權限的管理系統來存取（是否聽起來有點熟悉？）。以該裝置目前正在處理的資料就可以進行網路的管理，而特殊的網路管理指令可以是包在實際被處理的資料中傳送（稱為 in-band 管理），或是該裝置還支援其它種專門只用來傳送管理訊息的網路（稱為 out-of-band 管理）。

## 網路管理的功能層面

網路管理是一個架構，也是用於規劃、實作和維護電腦網路的一套處理程序（你也可以叫它網路管理規範（paradigm））。不同的網路管理標準群組有很多，都具備各自的網路管理概念，甚至連“網路管理”一詞都有本身特殊的定義。

所有網路管理模型都朝向相同的中心主題，如安全防護機能與組態管理、效能管理、和故障監控管理。更複雜的網路管理模型還提供網路治理機能，如網路規劃（planning）、管理支援（support）、資產記錄（asset records）、以及帳號管理（accounting）和成本管理（cost management）。

許多人堅信，網路通訊協定本身就是網路管理架構，他們認為假使一裝置支援管理通訊協定，它理所當然的就支援管理架構，然而事實並非如此。雖然許多系統管理和網路管理通訊協定的確提供了特定裝置的相關資訊，包括有裝置的配置（configuration）和功能參數（provisioning）、效能監控、以及警訊回報等，但通訊協定本身只是提供解讀管理資訊結構的工具，而算不上是網路管理架構。

與其討論一套特定的網路管理規範（許多介紹網路管理主題的書已經談過了），不如簡要地介紹大部份網路管理理論強調的一些功能層面。這些功能層面適用於所有的平台，從最大最複雜的網路平台，到最簡單未連接的工作站平台都一體適用。

## 組態管理（Configuration Management）

網路組態是取決於網路上的裝置種類，以及這些裝置目前的功能參數。組態管理主要與路由器、橋接器、接線器、和主機的實體和邏輯連接有關，也與各種類的裝置如何配置運轉有關。實際的組態管理包含三方面：

- 元件清單（Inventory）包括網路上的整組裝置、或安裝於網路裝置上的整組硬體和軟體元件，以及它們的靜態相關資訊。
- 配置（Configuration）圖指出清單中各元件是如何相互連接的。
- 功能參數（Provisioning）指多變的操作參數，用以指定各元件該如何運作。

你可以在一般 PC 的 CMOS 設定程式中見到以上的組態管理。硬體元件清單內容包括有磁碟裝置、影像和儲存介面卡、週邊設備埠、以及網路介面控制卡。包括所有唯讀的裝置相關資訊如製造商名稱、型號與序列編號、以及韌體校正版本，都算是元件清單資訊的一部份。

配置圖描述所有清單元件的連接方式。對網路組態來說，此圖顯示了每個網路節點實體上和邏輯上與其它網路節點連接的方式；對網路中的裝置配置來說，此圖則指出哪一個裝置被哪一個介面卡控制、以及哪一張卡被插在哪一種匯流排上，同時也會指出某些特殊功能如 APM（Advanced Power Management）和 DMI（Desktop Management Interface）目前是否啟用中。

功能參數變數則指出某節點在機能上如何運作，以工作站來說，它的功能參數資料項包括了日期時間、軟碟和硬碟容量、快取記憶體設定值、硬碟定址、和所有硬體週邊設備埠的設定值。另外，APM 和 DMI 功能的控制參數也算是功能參數資訊之一。

系統或網路管理架構提供了單一介面，可用於讀取、比較和更改網路裝置的配置、元件清單、以及功能參數。此一架構包括有以使用說明的形式存在、記載有所有可能設定值的資料庫、線上說明檔案、或是技術支援電話號碼。不幸的是，沒有任何一個管理應用軟體可以獨立管理所有裝置的配置，這也使得一般的網路管理系統其實是包含了許多不同的應用軟體，以因應多種裝置的管理需求。

## 故障管理 ( Fault Management )

當網路上發生了未預期的事件時，可能會出現某種訊號，或是你可能會察覺到裝置的運作情況有異，這些事件可能指出網路遭遇了某些問題。如果問題對網路某服務造成了不良的干擾影響，那麼它就被視為是“故障”。問題和故障的偵測、辨認、隔離、回報和更正，都是故障管理著重的課題。

故障管理是最重要一種形式的系統或網路管理。能夠快速地偵測到影響服務的問題、向管理裝置回報，並且採取可能的改正措施的機制，其重要性當然遠超過其它形式的管理。

網路故障偵測可能是反應式 ( reactive ) 或是先發制人式 ( proactive ) 的。反應式故障偵測發生於當故障已經存在網路之中。舉例來說，路由器偵測到一個網路裝置已經沒有回應、或是兩台裝置使用同一個網路位址，於是該路由器便會送出反應信號 ( 稱為警告 ( alarm ) 或是警報 ( alert ) )，告知已偵測到故障。許多反應式故障偵測都是由使用者打電話給網路管理者報告發生問題。

先發制人式故障偵測必須採取主動出擊，根據問題的來源和症狀，在它真正對網路服務造成影響之前就先及早發現及早解決。像伺服器的硬碟使用容量超過 90 % 可能就是一項潛在故障因子 ( 如果磁碟使用容量達 100 % ，故障就真的發生了 )。一台網路裝置回報說接收到的封包有超過 5 % 的是損壞的，目前看來也許不算故障，但它是一項指標，指出目前問題的確存在，而且故障可能即將發生。

問題是，什麼樣的事件可視為是故障呢？一般來說，任何非有意導致且會影響服務運作的事件，都可視為是必須立即處理的故障，其中最常見、最緊急、且影響最大的，就是那些失去電力和網路連線損壞的裝置。至於韌體錯誤、以及功能參數設定錯誤的裝置等等，也經常是問題的淵藪。

要預測故障可能發生何時何地，是需要付出相當代價的，包括付出金錢來設置監測儀器，並且需要熟知網路運作的詳盡資訊，以及額外的網路頻寬以實施先發制人式故障偵測。由於這是耗費時間和成本的大工程，通常只有大型網路的管理系統上才會建置這類故障偵測機制。

## 效能管理 ( Performance Management )

如果一網路目前的可用頻寬達到尚可接受的最小程度、而且各節點所應付的網路交通量都在工作負荷量之內時，我們會說它運作情形良好。換句話說，還有很多空間可供動態使用，而且沒有工作過度或超出負荷的情況。

效能管理牽涉到監視網路效能和適當調整網路。該使用何種資料來提供效能評估標準，則取決於網路的種類，最常用的效能評估資料通常屬於封包層級，包括以下各項：

- 接收到的壞封包個數 ( CRC 或 checksum 錯誤 )。
- 回應逾時或封包重送次數。
- 遞送失敗的封包個數。

當網路上存在大量壞封包或封包傳輸時通常表示網路發生了某種問題。突然地自服務移除裝置或通訊連結，或是路由器的記憶體不足、無法應付所有工作，也可能是降低網路效能的罪魁禍首。

有些網路裝置能夠搜集訊號層級的網路相關統計資料，這類電子訊號的衰減 ( 訊號強度減弱或邊際損失 ) 現象表示可能網路某區段需要配置一個強波器，或是也許纜線某部份發生損毀。

效能監控不只牽涉到裝置目前的統計資料而已，也與它過去的效能歷史記錄有關。觀察裝置的效能歷史記錄可以發現過去數小時或數天中，該裝置發生了哪些事，且有助於判定系統是否曾經或即將遭遇不測。舉例來說：

- 如果伺服器的警報器響了，指出它的某硬碟已經用掉 90 % 的容量，你可以查查該硬碟的使用日誌，看看此一情形是否為不尋常事件；如果該硬碟經常用掉這麼多的容量，表示也許你應該升級到更大容量的硬碟。
- 如果你留意到通訊線路的訊號衰減和邊際損失現象過去三十天持續發生，或許表示電線正逐漸損壞，可能是由於環境污染或是遭到人為破壞。
- 歷史記錄顯示某頻道已經有數小時無法服務，提醒你應該查看一下警告和故障管理日誌，看看到底發生了什麼問題以及該如何更正。

## 其它功能層面

還有許多其它形式的管理可能會用在特殊網路管理架構中，包括有以下幾種：

**安全管理 (Security management)** 包括所有避免未經授權的個人存取、使用和變更網路的相關措施。其中包括了實體的安全管理、如隔離主要的網路元件，以及邏輯的安全管理、如系統密碼和網路資料加密處理。

**帳號管理 (Accounting management)** 用於決定網路運作和管理的成本 (成本管理)，並且監看使用率以為收費依據 (收費管理, chargeback management)。

**資產管理 (Asset management)** 包括儀器、設施、和人員的統計資料紀錄。

**規劃管理 (Planning management)** 包括分析未來網路需求走向擴充規模 (節點個數)、網路容量升級 (採用更高頻寬的網路技術)、或是裁減規模。

## 再談網管

談到這裡，你可能會問：“為何網路管理功能不是每件裝置必備呢？”對大部份路由器和設備來說，網路管理是常見的附加功能。而且普及的作業系統如 UNIX、Novell NetWare 和 Microsoft Windows，以及通訊協定如 IPX/SPX 和 TCP/IP 所賜，你可以很容易地為大部份作為檔案伺服器和工作站的主機增加網路管理功能。

除此之外，還有很多的裝置無法直接支援網路管理機制，甚至連代理伺服器的標準管理規格都拿它們沒輒。在網管功能與成本取捨之間，裝置的製造商可真是左右為難！以下這些公正的原則標準是他們不可不看的：

### 管理介面必須合乎標準

管理介面（management interface）呈現管理資料，以供網路上其它裝置存取使用。很明顯地，共用同一種管理機制的裝置都應該擁有同樣管理介面，而且當這個介面被其它數個標準組織公認為是國際標準、並且廣為業界採用支援時，這個管理介面的可信度就會大大提高。

### 管理介面必須具備擴充性

很少有網路只含有完全同質且相容的裝置。事實上從超級電腦到廚房設備，任何東西都有可能直接連上網路，或是利用代理伺服器間接上網，因此管理介面一定要有足夠的擴充性，以支援任何種類的必要資訊來監控任何網路裝置。

### 管理介面必須具備可攜性

如果你製造許多種網路裝置，或是支援許多種網路技術規格，成本考量就成為關鍵。你必須試著儘量重覆利用你所開發的軟硬體元件，要記得使用許多不同裝置都同時支援的、且可被實作成可攜式單一軟體套件的網路管理通訊協定。

### 管理機制必須是花費不高的

又完美又萬能、並且隨插即用的網路管理方案是不存在的，也不可能存在，但是基本的管理機制是可以設計成滿足通用的需求，並且無須修改即可套用於各種不同的裝置上。果真如此，那麼裝置的製造商需要開發整合和支援的，就只有用來管理該裝置的程式碼而已。

### 管理機制必須只以軟體實作

如果管理系統要求每個受管系統都必須與特定管理硬體裝置整合才能進行管理工作，那麼基於成本和收益比例太低的理由，製造商是不太可能採用這樣的管理機制。而且有這麼多種的網路裝置受管，光是標準化就得花上數年時間並投入巨額成本，遑論要為它們打造出通用的管理硬體裝置了！

### 其它廠商必須支援管理機制

在標準的管理系統，若沒有人用也是枉然。另一方面，如果製造商發現同行競爭者的產品全都支援某一種普及的網路管理機制，他們一定會立刻加入支援行列。

### 顧客必定想要並迫切需求管理機制

最重要的原則是，提供顧客想要的，也提供他們需要的。在購買網路系統或裝置時，網路管理通常被顧客視為必要的功能，但很少有客人真的是要建立一套網路管理架構，甚至連網路管理系統的規劃部署都很少人實現。你所提供的網路管理方案，必須是合乎標準的，並且符合實際需求；更重要的是，它的操作必須很簡單。

## SNMP 網路管理

SNMP 網管模型完全符合方才提出的必要條件。SNMP 是針對分散式網路架構所設計的，每個網路節點搜集描述過去和目前狀態的管理資訊，並且提供給同樣位於網路上的管理系統來存取使用。

## SNMP 網管模型

SNMP 定義兩種管理物件 (management entity)：管理者和代理者，你也可以分別視它們為“管理別人的”和“被人管的”。在現實生活經驗中，你或許早已見識過這種管理模式（要注意，光是 SNMP 還不夠，它需與其它管理條件相配合，如狀態報告、和星期一早上 9:00 的人員會議等）。

網路管理站台 (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 (network management system) (令人混淆的是，它也叫 NMS) 應用程式。通常中型至大型的管理系統會架設在另一個稱作網路管理組套 (network management suite) (你可以猜到它也叫 NMS) 的軟體平台上，如 HP OpenView 和 IBM NetView。管理人員使用管理站台來發出要求，以自受管節點處取得管理訊息，而管理站台在接收到要求的資訊後，會將該資料呈現給管理者。

管理代理者所扮演的角色，是監看管理節點、搜集它們的運作相關資訊（管理資訊）、並且當管理系統需要管理資訊時提供該資料。在 SNMP 管理模型中，管理站台上的管理應用程式處理了大部份的管理工作。為什麼呢？因為管理者的電腦和資源通常是專用於處理管理事務，而受管節點常常還有其它更重要的工作要應付。

節點主機一般不是管理系統就是管理代理者。果真如此，那 SNMP 管理模型就真的是夠簡單了，然而 SNMP 物件還是有運作上的種類區分：

- 同時執行管理工作並且接受管理的節點（雙面節點, bilevel entity）。
- 能夠理解多種版本 SNMP 通訊協定的節點（雙語節點, bilingual entity）。
- 作為其它裝置的代理伺服器的節點（閘道器或中間層級的管理者）。
- 被 SNMP 以外的其它管理機制所管的節點。
- 完全無法管理的節點。

網路管理系統和管理代理者可能同時存在同一節點上，Windows NT 就是現成的例子，它可以同時允許 SNMP 服務和 SNMP 網路管理應用程式在同一個平台上執行。事實上，很有可能所有 SNMP 管理節點上都有另一個 SNMP 管理代理者程式在執行，使得其它管理系統得以辨認出該 SNMP 管理節點。

先前提過，至少有二個以上不同版本的 SNMP 管理標準可以在網路上使用。同時支援 SNMPv1 和 SNMPv2 管理標準的節點被稱為是“雙語的”(bi-lingual)，而管理節點很有可能是網路上的雙語節點。

所謂 SNMP 代理伺服器代理者，指的是代表無法支援 SNMP 代理者管理的其它裝置來執行管理服務的一種管理節點。這類代理者可以代表可能不存在網路上的週邊設備和測試儀器，也可以代表作業系統中的執行情序。

除了 SNMP 以外，其實還有許多其它的系統和網路管理通訊協定。如果一節點支援的是非 SNMP 的其它管理通訊協定，然而另外有一懂得多種通訊協定的代理者可以代表該節點，替該節點將管理要求訊息轉換成它可以解讀的形式；即使該節點不直接支援 SNMP，它仍然可以成為 SNMP 管理模型中的一份子。

至於無法提供任何形式管理資料的節點，就不在 SNMP 管理模型的管理範疇之內了。

## 社群名稱 (Community Name)

SNMPv1 定義以社群 (Community) 為基礎的治理架構來管理 SNMP 元件。每個 SNMP 社群群體至少包含一個代理者和一個管理系統，並且擁有一個邏輯代號稱為“社群名稱”。群體的每個成員所送出的訊息含有經過編碼的社群名稱，又稱之為“社群字串 (community string)”。訊息接收者藉由訊息的社群字串，來辨認該訊息是屬於那個社群。

藉由受管節點接受或拒絕含有特定社群字串的要求訊息，可以知道該受管節點是否屬於該社群。舉例來說，如果一 SNMP 代理者接受了所有含有“public”社群字串的要求訊息，表示該 SNMP 代理者明白宣告它是屬於“public”這個 SNMP 社群；如果同一個 SNMP 代理者拒絕了所有含有“private”社群字串的 SNMP 要求訊息，表示該 SNMP 代理者不認為它是“private”這個 SNMP 社群的成員。所有管理節點之所以要歸屬於某 SNMP 社群，是為了要與受管節點互動交流。如果一管理節點所送出的 SNMP 訊息含有某社群的名稱，該管理節點就屬於該 SNMP 社群。

指定社群名稱給受管節點的命名工作由網路管理人員來執行，命名有許多可能的依據，如功能 (“PRINTER” 社群)、位置所在 (“Engineering Lab” 社群)、使用者 (“Software Group” 社群) 或是裝置製造商 (“PairGain Technologies” 社群)。社群名稱一經決定就很少會再變更，除非網路的管理配置有重大變動。

一般來說，如果 SNMP 代理者未被設定成屬於任何社群，那麼無論 SNMP 要求訊息包含任何社群字串，該 SNMP 代理者都將會接受和處理之。實際上，此類節點算是屬於網路上所有現存的 SNMP 社群。

圖 3-1 顯示一區域網路中數個 SNMP 社群之間的關係圖，其中大部份的節點都只屬於一個社群，但有些是同時屬於兩個或三個社群。舉例來說，路由器被指定成同時屬於“Engineering Lab”和“campus”兩個社群，而印表機伺服器同時屬於“campus”、“PRINTER”、和“public”三個社群。標有“All Communities”的社群則包括了所有目前未指定社群名稱的 SNMP 受管節點，因此實際上這些受管節點算屬於網路上所有現存的 SNMP 社群；而一般說來，網路應用程式可能傳送 SNMP 訊息給已知社群名稱的任何社群，因此大部份的管理節點也都會屬於“All Communities”社群。

## SNMP Proxy Agent

本章稍早曾經提過，一個 proxy agent（代理伺服器代理者，或簡稱 proxy）是能幫其它裝置執行管理服務的網路節點。一個 SNMP proxy 能夠讓原本不支援 SNMP 管理要求（甚至連 SNMP 網路通訊協定本身都不支援）的裝置也能被 SNMP 監控和管理。

一個 proxy agent 能允許用 SNMP 應付以下情況：

- 管理無法支援 SNMP 代理者的裝置。
- 管理其它非使用 SNMP 管理代理者的裝置。
- 允許其它非 SNMP 管理系統來存取 SNMP 代理者。
- 為其它 SNMP 代理者提供類似防火牆的安全防護機能。
- 轉換不同規格的 SNMP 訊息。
- 在單一網路位址下，合併多個受管節點。

要支援 SNMP 代理者，裝置必須要有足夠的記憶體容量和夠強的 CPU 運算能力來支援至少一小型作業系統和一套網路通訊協定堆疊。許多特定用途的裝置，例如：電話、傳真機、印表機、和數據機，都不是被設計來支援任何網路管理、或甚至網路介面的。要透過網路來管理這類裝置，非得靠 proxy 的幫忙才有可能。

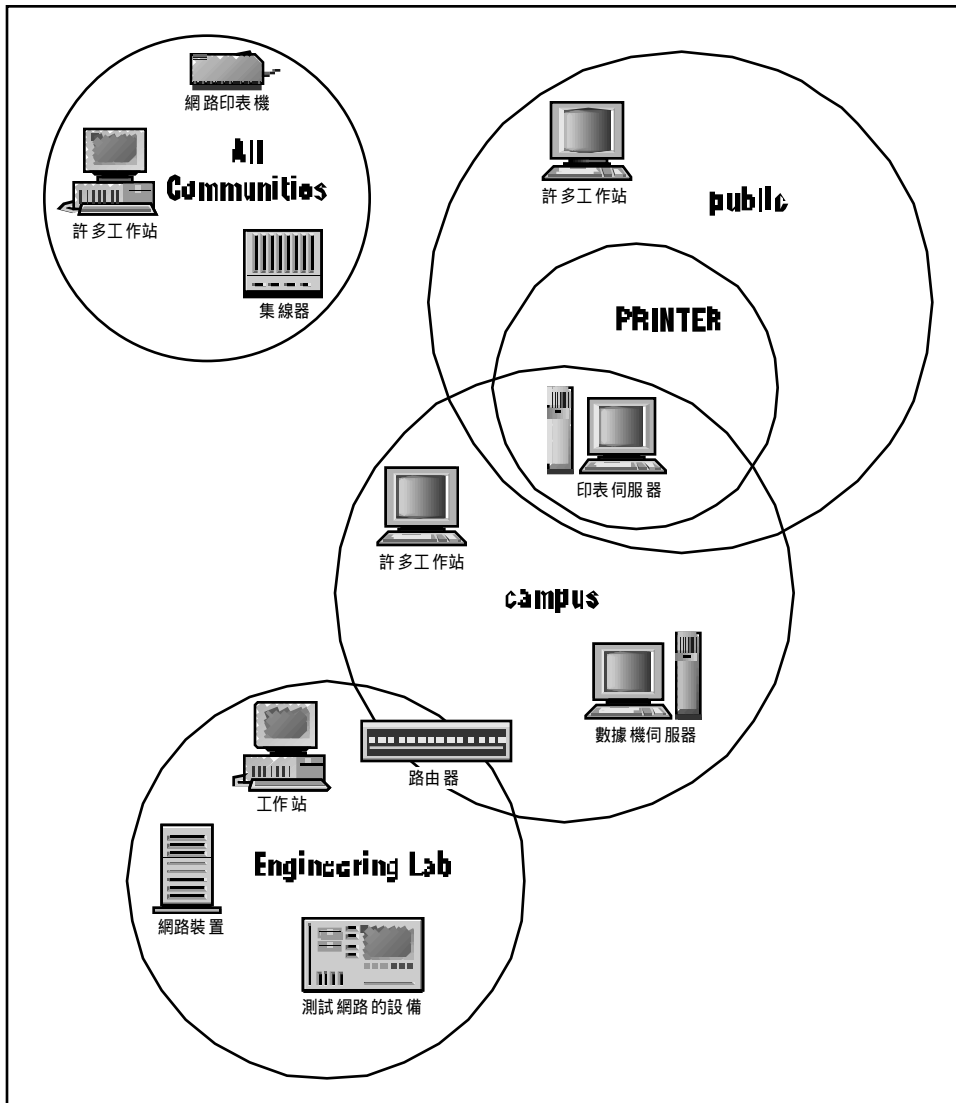


圖 3-1 : SNMP 社群。

proxy agent 本身在網路裝置上執行的一個 SNMP agent 程序，該裝置監看 non-SNMP 裝置以取得特定的管理資訊，並且儲存起來以供其它 SNMP 管理節點使用。至於該網路裝置本身則可能直接透過裝置上的 agent 來監看，例如，使用 AT

指令集 (AT command set) 透過數據機交談，或是間接使用感測器來搜集該裝置的溫度、電壓值和訊號強度... 等資料；也可能是一個 proxy agent 悄悄在該受管裝置上執行，而該裝置壓根兒就沒察覺此事。

Microsoft SNMP 服務本身就是一個 proxy agent，可以代理任何 Windows 工作站可存取的可管理裝置，例如，數據機、印表機和網路介面控制卡。proxy 也可用於管理 Windows 作業系統中的軟體執执行程序，並且該軟體不需要刻意支援 SNMP 管理。

## SNMP Gateway Agent

Proxy 的動作也很像閘道器 (Gateway)，將管理的要求由某管理通訊協定轉換到另一種。此類 proxy 實際上並沒有執行管理指令，而只是扮演使用不相容網路管理協定的管理系統和裝置之間的轉換媒介。

舉例來說，兩個不同的 SNMP 版本所使用的訊息格式是截然不同的：支援 SNMPv1 標準的裝置，理所當然無法解讀由 SNMPv2 管理系統所發出的服務要求訊息，反之亦然。因此，需要代理伺服器將 SNMPv2 要求訊息轉換成 SNMPv1 的格式，讓受管裝置能夠處理，而且來自受管裝置的 SNMPv1 回應訊息也必須轉換成對應的 SNMPv2 格式，讓管理系統能夠正確地解讀它。【註】

被代管 (proxied) 的裝置可能與 proxy agent 存於相同網路中，但也可能是以週邊裝置的形式附接在 proxy 上頭 (如數據機卡插在主機板的插槽中) 或是從遠端相接 (例如：用纜線或紅外線所連接的印表機)，只要管理資訊可以某種方式傳送於受管裝置和 proxy 之間即可。

Proxy 可被設計成是閘道器，以便能夠用一個網路位址就存取到數個可用 SNMP 管理的裝置。要求管理資訊的 SNMP 訊息先送到 proxy，然後再根據不同要求傳給合適的受管裝置來處理，而回應訊息也是先送到 proxy，然後再傳回給管理系統。Proxy gateway 也可作為多個代理者的單一 trap 訊息目的地，負責將 trap 訊息轉送給適當的最終目的地。

---

註 請注意，在此一情況下，若使用雙語管理系統 (bilingual management) 或代理者，就不需要 proxy 了。

Proxy agent gateway 也可當作防火牆來用，提供單一窗口以執行所有的 UDP 確認（封包層級的過濾）和 PDU 稽核（應用層級的過濾）工作。藉由檢查來源位址，可以確認 SNMP 訊息是不是來自經過授權可以發出 Get 或 Set 要求的位址，來路不明、未經授權的要求訊息會被閘道器攔截掉。

Proxy agent 看似解決了不少問題，然而在某些情況下，這只是短期的權宜之計。但是，撰寫一個 proxy 解譯程式，至少聽起來比為裝置建置全套管理支援要來得吸引人。表 3-1 總結了使用 proxy 的優劣。

表3-1：使用 proxy agent 在管理上的優缺點。

proxy 的優點	proxy 的缺點
為原本 SNMP 無法存取的裝置提供虛擬 SNMP 管理。	通常難以設計和實作。 可能無法發揮裝置所有的管理能力。
自外界一般網路隔離專屬或不相容的特殊通訊協定。	需要其它網路元件或執行程序的配合。
允許網路元件支援多種通訊協定，合併多個代理者於單一的集中存取位址。	使得除錯更為複雜。
與全套通訊協定堆疊和 SNMP 代理者相比，實作時間較短。	可能會讓排除網路故障的工作更加困難。
讓 non-SNMP 節點有機會能夠透過 SNMP 來存取。	危險的是，實作者可能會相信短期的權宜之計是好的長期解決方案。