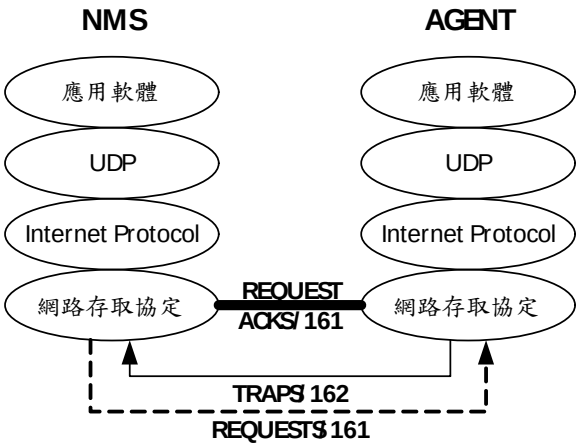
SNMP 通訊藍本間功能與特色的差異

隨著網路應用日趨普遍，有愈來愈多的企業透過能快速回應與 24 小時服務的電子化平台支援內部相關流程或是客戶的資訊服務。但是，隨著資訊服務愈來愈多元，企業建構網路的複雜度與需要購入的伺服器也相對愈多，系統與網路管理人員的擔子也就愈來愈重。一旦發生問題，相關人員就必須花費相當多的時間去找出發生問題的設備，然後再進一步排除發生的障礙 (賴明豐，2007)。而 SNMP(簡易網路管理通訊協定，Simple Network Management Protocol)，如圖一所示，是目前 IP 應用中最常被用來 “線上” 監測系統與網路運作狀況的通訊協定－透過 UDP 以 Unconnectionless 方式傳送與接收訊息，降低網路流量負擔。不過，爲了因應資訊技術與系統及網路管理人員的使用需求，SNMP 所使用的通訊藍本不斷改版，從 SNMPv1、SNMPSec、SNMPv2/SNMPv2u/SNMPv2c，一直到 SNMPv3，不同藍本對 SNMP 協定都有不同的強化。本篇文章的目的即在淺析 SNMP 不同通訊藍本的特色與其間的差異，供系統或網路管理人員參酌。

圖一　控制台→系統管理工具→服務

壹、 SNMPv1 的基本觀

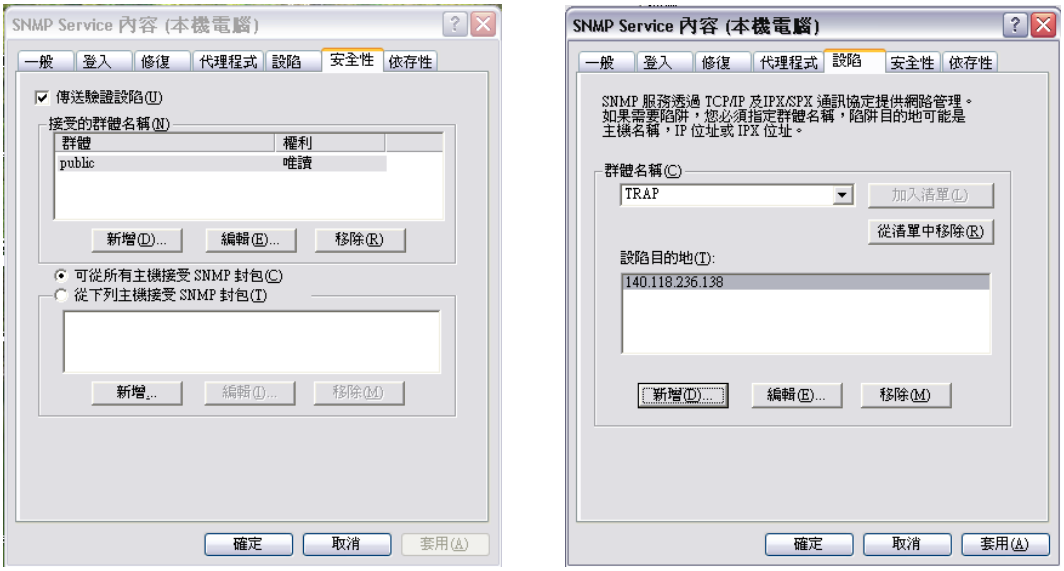
在 SNMPv1 裡，NMS 與 AGENT 間的通訊方式主要是建基於 TCP/IP 通訊協定，如圖二所示，事實上，目前幾乎所有想連上網際網路的通訊設備 (不論是 WINDOWS、UNIX，或是 ROUTER 與 SWITCH) 都必須透過這樣的 protocol stack，在機器之間提供資訊、傳遞訊息，SNMP 自然也不例外：



圖二　PROTOCAL STACK 與 SNMP

（資料來源：Mauro & Schmidt (2007)；本文整理）

基本上，NMS 與 AGENT 間的連結關係屬於 COMMUNITY 概念，有 READ-ONLY（指唯讀）、READ-WRITE（指可讀/可寫）與 TRAP（指認證失敗的訊息）三種。而這三種 COMMUNITY 名同時也代表 NMS 對 AGENT 進行管理時的深淺程度。各種支援 SNMP 管理協定的設備剛出廠時，都會先以 *PUBLIC* 字串代表 READ-ONLY，如圖三所示；*PRIVATE* 代表 READ-WRITE；*TRAP* 則是由 AGENT 端自行設定，看 TRAPS 是要傳送到哪一個 NMS 或機器上，如圖三所示：

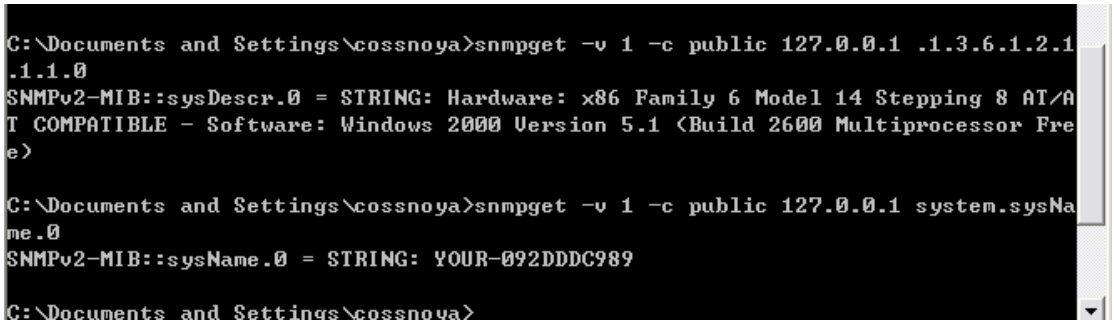


圖三　在圖一中 SNMP SERVICE 上點滑鼠兩次就會出現「SNMP SERVICE 內容」標籤，點在「安全性」與「設陷」的頁標上。

由上可知，SNMPv1 定義了一種主從式的管理架構，有 Client (AGENT) 與 Server (NMS)

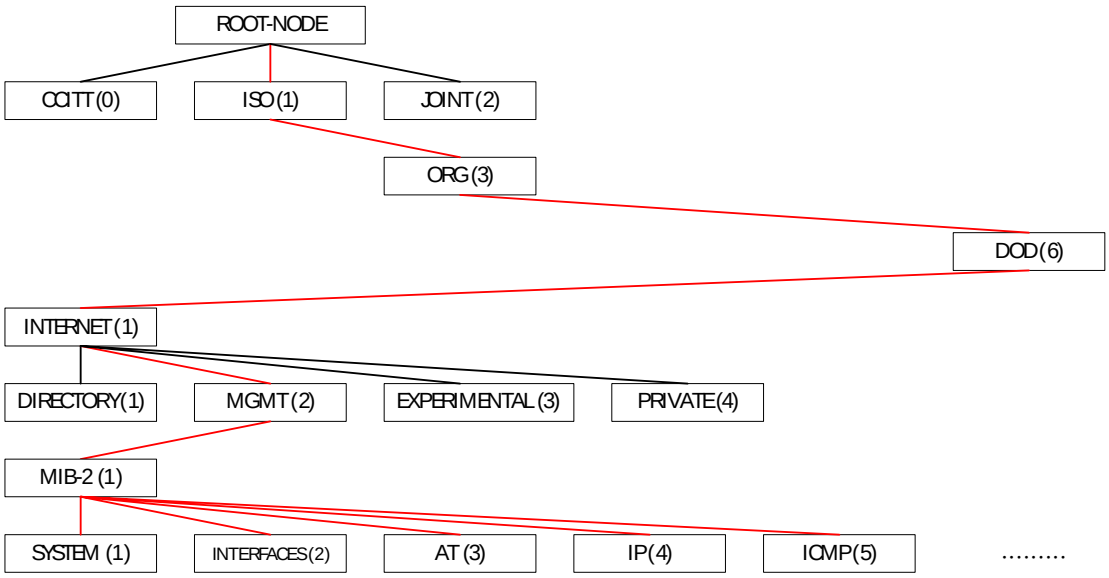
兩種角色，而且，可以是多對一 (指 CLIENTS 對 SERVER) 的從屬關係。而 AGENT 可以是一台用來提供企業資訊服務的伺服器、個人電腦、或是路由器與其他能夠支援 SNMP 管理協定的設備。平常，AGENT 就會定時地將相關資訊儲存在 MIB 的相應物件中以備 NMS 的詢查；NMS，則最好是一個專職用來做 SNMP 管理的伺服器，它會透過 SMI 所定義的結構讀取不同作業系統下內存的 MIB 參考物件瞭解不同設備的運作狀況。

在 SNMPv1 中，系統或網管人員可以透過 get、getnext、set、getresponse 與 trap 等 PDU (PROTOCOL DATA UNIT) 跟 AGENT(S) 交流訊息，並搭配 MIB (Management Information Base) 物件清單讓 AGENT 能瞭解 SNMP 目前 REQUEST 所指的資訊爲何，AGENT 就會依 NMS 所指的 VARBIND (Variable Binding) 取出相應的資訊，例如 NMS 想知道某 AGENT 在網路上的完整名稱，NMS 就可以將 VARBIND 設爲子樹的名稱 .iso.org.dod.internet.mgmt.mib-2.system.sysName.0，或是直接寫成 OID 的形式如 .1.3.6.1.2.1.1.1.0 也可以。



圖四　用 SNMPv1 去查詢本機 MIB-2 sysName 與 sysDescr 物件內存的資訊

由上可知，SNMPv1 中除了 NMS、AGENT 與 PDU 之外，還必須透過 MIB 來儲存 SNMP 在管理系統或網路時所需要參考到的參考物件，並透過 SMIv1 (Structure of Management Information version 1) 定義這些參考物件間的階層與從屬關係，如圖五所示，這樣清楚明確的架構大大降低了 NMS 進行管理的複雜度。基本上，SMIv1 賦予每一個參考物件一個用來識別物件的「代號」(Object IDentifier, OID)、用來定義資料表達與傳輸方式的「型別與語法」(Abstract Syntax Notation ONE, ASN.1)，以及用來定義物件編/解碼方式 (Basic Encoding Rules, BER) 的「編碼」 (a string of octets)，如 MIB-2 下就有 10 種群組，如圖四所示，SYSTEM (1.3.6.1.2.1.1)、INTERFACES (1.3.6.1.2.1.2)、AT (1.3.6.1.2.1.3)、IP (1.3.6.1.2.1.4)、ICMP (1.3.6.1.2.1.5)、TCP (1.3.6.1.2.1.6)、UDP (1.3.6.1.2.1.7)、GP (1.3.6.1.2.1.8)、TRANSMISSION (1.3.6.1.2.1.10) 與 SNMP (1.3.6.1.2.1.11)。



圖五　SMI 樹

（資料來源：Mauro & Schmidt (2007)；本文整理）

貳、 SNMPv1 與 SNMPv2 間的差異

到了 1992 年，爲了解決 SNMP 安全上的顧慮，SNMPSec 通訊藍本出爐，可是，卻因爲設計得過於複雜而叫好不叫座。隔年，以 SNMPv1 藍本爲基礎的 SNMPv2p (PARTY-BASED SNMPv2) 概念出現，主要是爲了強化 SNMPv1 在管理 AGENTS 上的效能，包括強化 NMS 間資訊交流與互動的機制，以及增加 NMS 對 AGENT 間進行整批指令處理的能力，這對使用者來說相當有幫助，不過，卻對 SNMP 應用開發人員卻造成不小的困難。

因爲，SNMPv2p (RFC 1441-1452)將 NMS 與 AGENT 間資訊傳輸的過程區分爲兩個階段: transmission/receipt 與 access control，SNMP 開發人員必須針對不同階段提供不同的安全保障模式。另外，在 PDU 的部份，也細分成 READ、WRITE、RESPONSE、NOTIFICATION 與 INTERNAL 五個類別，這五個類別依其是否需要產生 ACKS 的需求又可以進一步劃分成 CONFIRMED 與 UNCONFIRMED 兩群，使得 SMI 也需要連帶地進行更動，大大加重 SNMP 管理系統開發人員的負擔。因此，1996 年 SNMPv2p 的簡化版 SNMPv2c (這也是目前一般人所稱的 SNMPv2，主要是簡化了 SNMPv2p 中定義的安全管理機制) 開始被提出來，其後又因爲安全處理機制設計上的差異 (Kozierok, 2005)，再分支出 SNMPv2u 與 SNMPv2* 二個藍本 (RFC 3410)。

基本上，SNMPv2 通訊藍本與前一版不同的地方有三個：加入批次執行資訊存取的指令、統一 SNMP 中 GET 與 SET 的 PDU 格式方便資訊交流與互動的機制，以及新增用來確認 NMS 已收到由 AGENT 送出的資訊的 NOTIFICATION，相關的指令有 getbulk、notification、inform 與 report。

不過，SNMPv2 的通訊藍本中雖然有定義 report 這個指令的構想，但是，目前仍然未被實作出來；inform 則是允許 NMS 間互通資訊，相關的行爲模式跟方法都與 GET/SET 類似

故不再多加介紹。因此，本文針對 getbulk 與 notification-type PDU 進行解析，如下所述：

(1) getbulk 主要強化 NMS 一次擷取多個 MIB 物件的能力，骨子裡其實就是 SNMPv1 getnext 指令執行多次的結果，不過，它在指令格式中多了 nonrepeaters (即-Cn1) 與 max-repetitions (即-Cr3) 兩個欄位，以便用來計算純量物件與非純量物件的個數。以圖六的指令來看，sysDescr 是唯一的純量物量，因此，它會回傳七個 VARBINDS，即 N+(M*R) = 1+(3*2) = 7。

```
C:\Documents and Settings\cossnoya>snmpbulkget -v2c -c public -Cn1 -Cr3 10.10.3.
32 sysDescr ifInOctets ifOutOctets
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 15 Model 6 Stepping 2 AT/A
T COMPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600 Multiprocessor Fre
e)
IF-MIB::ifInOctets.1 = Counter32: 627
IF-MIB::ifOutOctets.1 = Counter32: 627
IF-MIB::ifInOctets.2 = Counter32: 20545836
IF-MIB::ifOutOctets.2 = Counter32: 1778686
IF-MIB::ifInUcastPkts.1 = Counter32: 7
IF-MIB::ifOutUcastPkts.1 = Counter32: 7
```

圖六　getbulk 指令測試

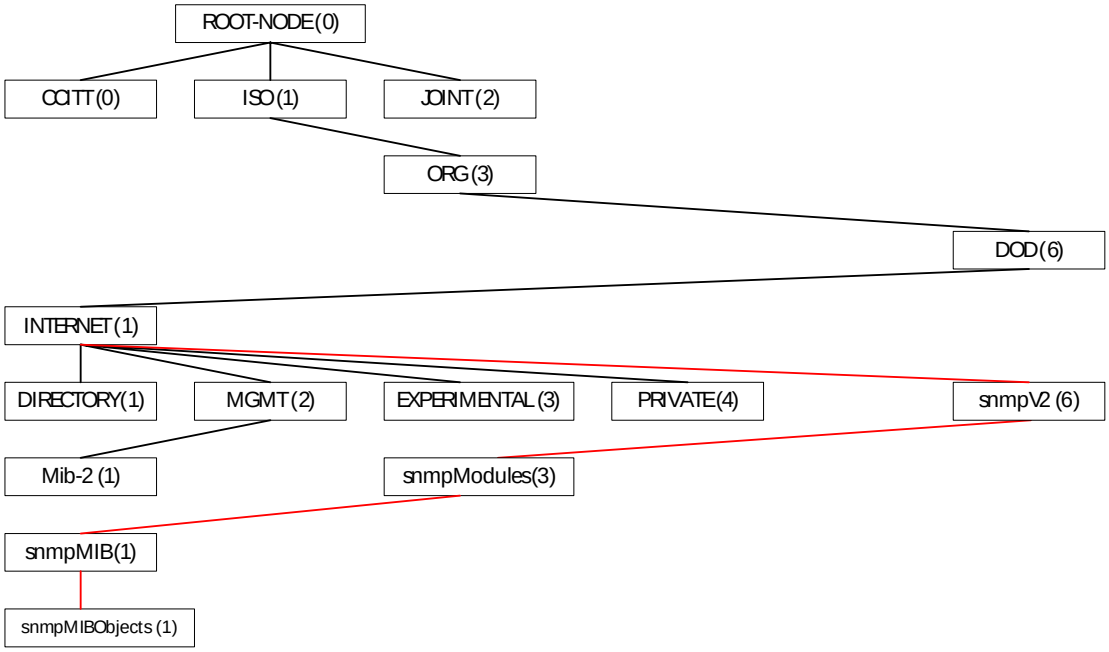
(2) notification 主要是用來標準化 SNMPv1 TRAP 的 PDU 格式，讓繫結清單從 VARIABLES 變成 OBJECTS (Mauro & Schmidt, 2007)。本文透過「snmptrap -v2c -c public 10.10.3.32 '' '' .1.3.6.1.6.3.1.1.5.3 ifIndex i 2 ifAdminStatus i 1 ifOperStatus i 1」或是改成 .iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTraps.linkDown 來檢視 NOTIFICATION-TYPE 的 PDU 訊息內容，如圖七所示：

```
Frame 25 (112 bytes on wire, 112 bytes captured)
    Arrival Time: Jun  1, 2007 11:15:44.259240000
    Time delta from previous packet: 0.000009000 seconds
    Time since reference or first frame: 7.855031000 seconds
    Frame Number: 25
    Packet Length: 112 bytes
    Capture Length: 112 bytes
    Protocols in frame: eth:ip:udp:snmp
Ethernet II, Src: 10.10.3.3 (00:03:7a:12:94:a1), Dst: 10.10.3.32 (00:17:31:99:09:fb)
    Destination: 10.10.3.32 (00:17:31:99:09:fb)
        Address: 10.10.3.32 (00:17:31:99:09:fb)
        .... ...0 .... .... .... .... = Multicast: This is a UNICAST frame
        .... ..0. .... .... .... .... = Locally Administrated Address: This is a FACTORY DEFAULT
address
    Source: 10.10.3.3 (00:03:7a:12:94:a1)
        Address: 10.10.3.3 (00:03:7a:12:94:a1)
        .... ...0 .... .... .... .... = Multicast: This is a UNICAST frame
        .... ..0. .... .... .... .... = Locally Administrated Address: This is a FACTORY DEFAULT
address
    Type: IP (0x0800)
Internet Protocol, Src: 10.10.3.3 (10.10.3.3), Dst: 10.10.3.32 (10.10.3.32)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 98
  Identification: 0x9a69 (39529)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (0x11)
    Header checksum: 0x85eb [correct]
        Good: True
        Bad : False
    Source: 10.10.3.3 (10.10.3.3)
    Destination: 10.10.3.32 (10.10.3.32)
User Datagram Protocol, Src Port: 2555 (2555), Dst Port: snmp (161)
    Source port: 2555 (2555)
    Destination port: snmp (161)
    Length: 78
    Checksum: 0x5411 [correct]
Simple Network Management Protocol
    Version: 2C (1)
    Community: public
    PDU type: GETBULK (5)
    Request Id: 0x00000de7
    Non-repeaters: 1
    Max repetitions: 3
    Object identifier 1: 1.3.6.1.2.1.1.1 (SNMPv2-MIB::sysDescr)
    Value: NULL
    Object identifier 2: 1.3.6.1.2.1.2.2.1.10 (IF-MIB::ifInOctets)
    Value: NULL
    Object identifier 3: 1.3.6.1.2.1.2.2.1.16 (IF-MIB::ifOutOctets)
    Value: NULL
```

圖七　notification-type PDU 訊息內容

除了上述新興指令之外，SNMP 爲了強化 SNMPv1 管理設備的效能，也將 SMI 由原來的第一版更新爲 SMIv2，擴增物件定義的描述項，包括 UnitsParts、MAX- ACCESS、STATUS 與 AUGMENTS，並重新界定 SNMPv2 新興物件在 SMI 中的階層與從屬關係，如圖八所示。另外， NMS 與被管設備互傳資訊時的格式 (textual conventions, ref. RFC 2579) 也開始進行規範；NMS 所下指令在 AGENT 端執行時如果發生問題，SNMPv2 也新增了一群新的回應訊息

供系統或網路管理人員參考。



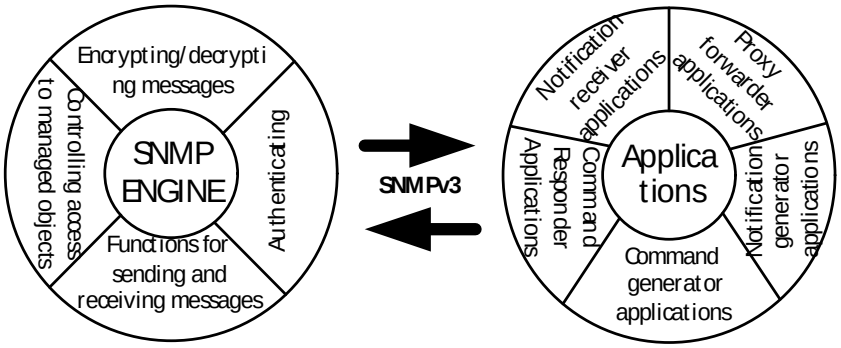
圖八　SMIv2 樹

（資料來源：Mauro & Schmidt (2007)；本文整理）

參、 SNMPv3 的特色

從 SNMP 演進的歷史來看，1988 年 SNMP 整合了 SGMP 與 HEMS 的優勢廣爲系統與網路管理人員所使用，更在很短時間裡，SNMPv1 正式成爲業界的標準 (RFC 1157)、在 1991 年整併進 MIB-II (RFC 1213) 的管理規範中。從功能來看，第一版的 SNMP 在管理與安全的操作上都存在問題；但是，SNMP 從第二版通訊藍本開始針對管理能力進行強化，但安全保障卻仍有很大的改進空間，常受系統與網路管理人員的垢病。直到 2000 年以後，SNMPv3 整併了 SNMPv2u 與 SNMPv2* 通訊藍本的設計概念，完整的安全管理雛型才慢慢具體起來！

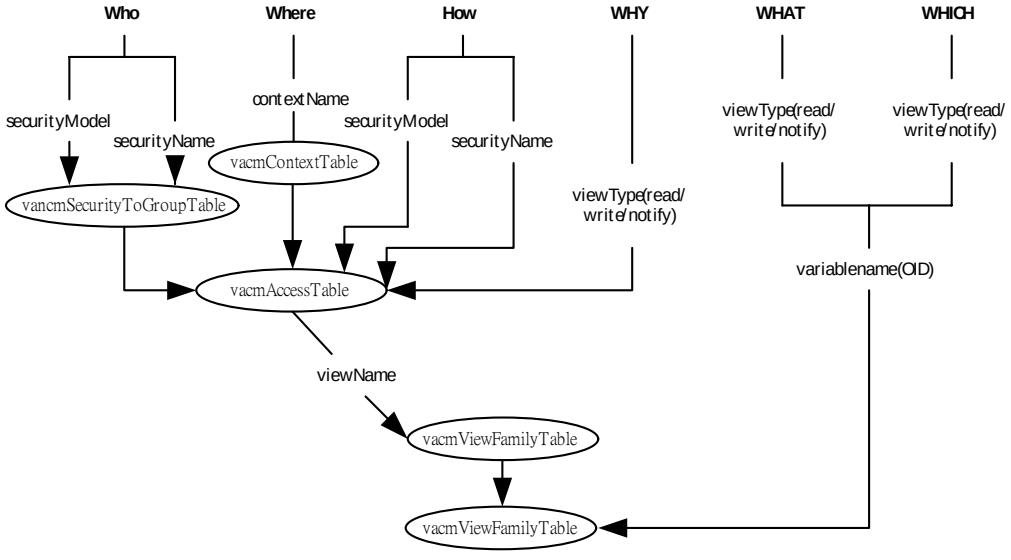
因此，SNMPv3 所使用的管理藍本仍是沿用前一版所定義的內容，它唯一的目的就是解決 SNMP 的安全問題。不過，爲了能增加 SNMP 通訊藍本改版與開發相關應用程序或系統的彈性，它捨棄了前版 AGENT/NMS 的概念；不論是 AGENT 或 NMS 都稱爲 SNMP ENTITY，每個 ENTITY 都是由一個 SNMP ENGINE 與多個 APPLICATIONS 所組成，如圖九所示：



圖九　SNMPv3 ENTITY 架構

資料來源：Stallings (1998); 本文整理

爲了能符合 SNMPv3 架構調整的需要 (Mauro & Schmidt, 2007)，ENTITY 內 ENGINE 與 APPLICATIONS 進行資訊交流與互動時所用的行文慣例也作了相應的改變，其目的主要是希望用較精確的方式解譯前藍本所定義的資訊型別，包含 snmpEngineID、snmpSecurityModel、snmpMessageProcessiongModel、snmpSecurityLevel、sanmpAdminString、snmpTagValue、snmpTagList 與 KeyChange。SNMPv3 整個認證的機制 (如圖十所示) 涵蓋了整個訊息，但加密的機制則定義在 contextEngineID、contextName 與 PDU 的範圍；認證使用的方法有 MD5 與 SHA1 兩種；加密則是以 CBC-DES 演算法來完成。不過，SNMPv3 爲了降低系統或網路管理者需要記憶太多密碼的負擔，也設了一個 LOCALIZED KEY 機制，讓管理者可以在不同 ENTITY 中使用相同的密鑰。



圖十　SNMPv3 存取控制/認證機制設計

資料來源：Mauro & Schmidt (2007)

肆、 結論

SNMP 是一個用來管理 IP 網路上系統與通訊設備的管理協定，因此，有愈多愈多的管理人員開始透過這樣簡便的機制，降低伺服器與網路運作效能監控的沈重負擔。但是，隨著應用範圍愈趨廣泛，原本單純的管理機制也必須因時制宜。由上面的討論可以知道，SNMP 各藍本設計的重點都有不同，不過，基本上，可以概分爲管理能力與安全保障兩部份，如表一所示：

	SNMPv1	SNMPsec	SNMPv2p	SNMPv2c	SNMPv2u	SNMPv2*	SNMPv3
發展時間	1990-1991	1992	1993	1996	1996	1999-2002	2002-2003
管理能力	◗	◗	◕	●	●	●	●
安全保障	D	◗	◗	D	◑	◑	●
相關 RFC	1155, 1157, 1157, 1213	1351, 1352, 1353	1441, 1442, 1443, 1444, 1445, 1446, 1447, 1448, 1449, 1450, 1451, 1452	1901, 1902, 1903, 1904, 1905, 1906, 1907, 1908	1909, 1910	2576, 2578, 2579, 2580, 3410, 3411, 3412, 3413, 3414, 3415, 3416, 3417, 3418	2570, 2576, 2786, 3410, 3411, 3412, 3413, 3414, 3415, 3416, 3417, 3418, 3584

註：●優；◕好；◗普通；◗需加強；D差

表一　SNMP 藍本間差異的比較

（資料來源： Kozierok (2005)；本文整理）

從 1990 到現在，SNMP 歷經了七個不同藍本的演進，以管理能力來看，直到 SNMPv2c 才見完整；以安全保障來看，則是到 SNMPv3 才經整合 SNMPv2u 與 SNMPv2*藍本的相關機制後安全保障才見完整。目前，市場上大部份的系統或網路設備都是支援 SNMPv1 或 SNMPv2 二個藍本；只有少部份的高階設備開始支援 SNMPv3 通訊藍本。

因此，系統與網路管理人員必須瞭解，並不是所有設備支援的 SNMP 通訊藍本都相同，即便是差別最小的 v1 與 v2，NMS 能下的指令也有不同。如果管理人員本來就很器重 SNMP 管理機制，但卻又擔心這些設備在管理過程中的安全風險，那麼，就必須問清楚廠商該設備如何進行 SNMP 通訊藍本的升級動作，不過，這通常需要再多花上一筆費用，而且，管理人員也必須詳細考量因 SNMPv3 的加入，致使網路產生不穩定現象的可能性 (Cole, 2005)。另外，功力較高的管理人員自己也可以透過適當的程式語言撰寫管理系統，如 PERL、

C/C++或 JAVA，提高整個管理策略上的彈性。

參考文獻

1.賴明豐 (2007). "淺析 SNMP 與網路管理間的關係." 科技政策智庫，取文時間：2007.10.28；取自：http://thinktank.stpi.org.tw/eip/index/techdoc_content.jsp?doc_id=1185199060901&ver_id=1

2.Mauro D.R. and Schmidt K.J. (2007). "Essential SNMP 2e." TAIPEI: O' REILLY.

3.Kozierok C.M. (2005). "TCP/IP Internet Standard Management Framework and SNMP Versions (SNMPv1, SNMPv2 Variants, SNMPv3)." The TCP/IP Guide, 取文時間：2007.06.02；取自：http://www.tcpipguide.com/free/t_TCPIPInternetStandardManagementFrameworkandSNMPVer.htm.

4.Stallings W. (1998). "SNMPv3: A Security Enhancement for SNMP." IEEE Communications Society, 取文時間：2007.06.03；取自：http://www.comsoc.org/livepubs/surveys/public/4q98issue/stallings.html.

5.Cole E. (2005). "SNMP 的革命進程." 資安人科技網，取文時間：2007.06.03；取自：http://www.isecutech.com.tw/feature/view.asp?fid=593.

（本文由國家實驗研究院科技政策研究與資訊中心 副技術師賴明豐、助理技術師李樹民 提供）