SYSLOG 與 SNMP Traps 結合的應用

符光恩
國家高速網路與計算中心
kwengenfu@nchc.org.tw

李進興
福雷電子
vulcan_lee@aseglobal.com

摘要

本文中將 SYSLOG 與錯誤管理(Fault Management) 中佔極重要角色的 SNMP Traps 結合起來,使只支援 SYSLOG 協定的設備可以得到兩種協定的長處,配合 SYSLOG Analyzer 的分析和過濾的強項以及 SNMP 網管主機 Correlation 的精妙,將原本只是記錄用的 LOG 變成各類不同等級且可以即時處理的 SNMP Traps 達到具主動式管理的特性。

關鍵詞： SNMP Traps、SYSLOG、SYSLOG Analyzer。

1. 前言

SYSLOG[1] 和 SNMP Traps[5] 兩者均是設備和網管軟體溝通的重要協定。從 SYSLOG 的設計原理來看，主要偏重記錄，要達到主動式管理需要一些額外的努力，市面上有許多的 SYSLOG Analyzer[2]就可以達到這項需求。一般的作法是 SYSLOG Analyzer 將收到的 SYSLOG 經過分析後，以執行使用者預設的指令的方法，達到主動管理的功能。

本文中結合 SYSLOG 和 SNMP Traps 的想法其實相當簡單，主要是將 SYSLOG Analyzer 當成異質協定的轉換工具。在 SYSLOG Analyzer 篩選出重要的 SYSLOG 後，依重要性轉換成不同的 SNMP Traps，保留原來的 SYSLOG 內容，由收到的網管主機決定要執行的程序。

1.1 研究的背景和動機

為降低 SNMP Traps 數量[8]，發現 CISCO 設備產生 LOG 的同時，除送一份到 SYSLOG 主機，同時也會將這個 LOG，以 CISCO-SYSLOG-MIB[6] SNMP Traps 送到 SNMP 網管主機。分析送到 SYSLOG 主機以及 SNMP 網管主機的資訊內容其實是重複的，只是收到的協定不同而已。我開始有二種想法，第一種是關閉 CISCO-SYSLOG-MIB SNMP Traps 以減少不必要的資料重複；另一種想法則是以 SNMP Traps 來當作異質網管主機的共同語言，使各類網管主機未來可以用 SNMP Traps 來交換訊息。

1.2 研究的目的與方法

主要的目的如下：

- 減少 SNMP Traps 數。
- SYSLOG Analyzer 篩選出的 SYSLOG 以 SNMP Traps 的型式送到 SNMP 網管主機 。
- 必需很容易，即使非專業網管人員也可以操作。

經過網管資源的調查，決定利用 SYSLOG 伺服器上所附的 SYSLOG Analyzer，先行分析 SYSLOG 事件訊息，再利用指令，將過濾所得的 SYSLOG 訊息內容以 SNMP Traps 的方式送到網管主機。

為了達到目的我將整個計劃分三個階段實作：

- Device-Level 關閉所有 Cisco Device 的 SYSLOG Traps，確認設備的 SYSLOG 有送到 SYSLOG 伺服器。
- SYSLOG 伺服器-Level 將所有 SYSLOG 分類為 7 個等級，每個等級以不同的 SNMP Traps OID 送出。
- SNMP 網管-Level 將 7 個等級的 SNMP Traps 以 Critial、Major、Minor、Warning、Normal 五種等不同的等級呈現 。

2. 相關技術和探討

2.1 SYSLOG

主要是來傳送事件訊息(Event Message)之用，通常依類別(Facility)、重要性(Severity)、以訊息名稱(Message Name)來分類，而訊息內容(Message Text) 則用於說明整個事件。例如:

```
%SYS-5-CONFIG_I:  Configured  from
console ...
```

類別為 SYS，重要性為 5，訊息名稱為 CONFIG_I，訊息內容為 Configured from console…

重要性為 0-7 的整數，本文中利用它來進行分

類，其值愈小重要性愈高，利用此一特性轉換成重要性等級不同的 SNMP Traps 給 SNMP 網管主機。

2.2 SYSLOG Analyzer

為能分析、篩選 SYSLOG 資料，我們利用 SYSLOG 伺服器上的 SYSLOG Analyzer，這類工具主要是協助比對 SYSLOG 的文字，並執行使用者自訂的程序。

通常 SYSLOG Analyzer 需要另外安裝，本文中係利用 Ciscoworks2000 所附的 SYSLOG Analyzer，來啓動使用者自訂程序，以便將 SYSLOG 的原來內容，換成 SNMP Traps 的格式轉送給網管主機。

2.3 CISCO SYSLOG-MIB

這個 MIB 是 CISCO 的專屬 MIB，主要提供了一種以 SNMP Traps 的方式來表現 SYSLOG 的方法。當 Cisco 設備產生 SYSLOG 後會以 SNMP Traps 的方式將 SYSLOG 資訊，包括類別、重要性、訊息名稱、訊息內容等資訊送到 SNMP 網管主機。

本文中以這個訊息和 SYSLOG 伺服器所收到的訊息重複為由，將設備端的 CISCO SYSLOG-MIB SNMP Traps 關閉。

2.4 SNMP Traps

SNMP Traps 利用 UDP 162，是一種主動回報的機制，當一個設備支援這種協定時，可以在設備發生問題時主動通知網管主機，最常見的就是 Interface Up、Interface Down、 Device reboot 等狀況，當一個設備送出過多的 SNMP Traps 時通常反應出這個設備可能有異常的現象待解決。

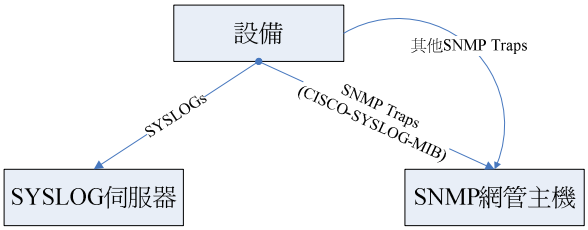
很多廠商會針對自己的硬體設計特有的 SNMP Traps。例如有些大型的 Router 會設計多個溫度計來偵測環境，當這些溫度計發現溫度異常時則會以 SNMP Traps 方式主動告知網管軟體。這有助於將管理功能的延伸管理不同設備的問題。

在本文中我們自訂 SNMP Traps 來當異質網管主機間共通的語言，例如當 SYSLOG 伺服器篩選出重要的 SYSLOG 後，將這個訊息轉換成 SNMP Traps 通知另一台 SNMP 網管主機。

3. 設計架構

3.1 規劃

原有架構如圖一所示，設備在送 SYSLOG 給 SYSLOG 伺服器的同時，將 SYSLOG 以 SNMP Traps 的方式送給 SNMP 網管，實際上二者是重複的資料。



圖一：改善前的架構

如圖二 所示，改善後的架構關閉了 CISCO-SYSLOG-MIB SNMP Traps，為了避免重要的 SYSLOG 資料遺失，由 SYSLOG 伺服器建立多條新的 SNMP Traps 通路，並依重要性分類以便將重要的訊息送到 SNMP 網管主機中，整個系統主架構不變，但資料流已經大量減少，並且依重要性粗分為七個等級。

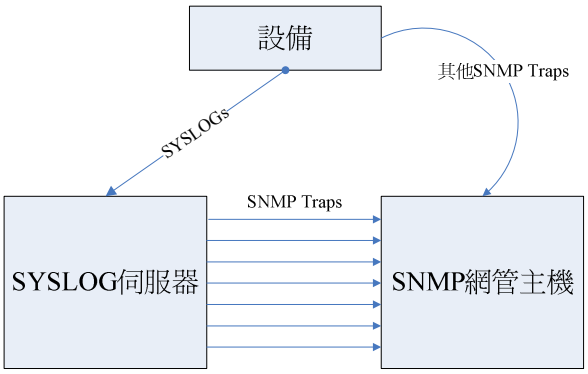


圖 二: 改善後的架構

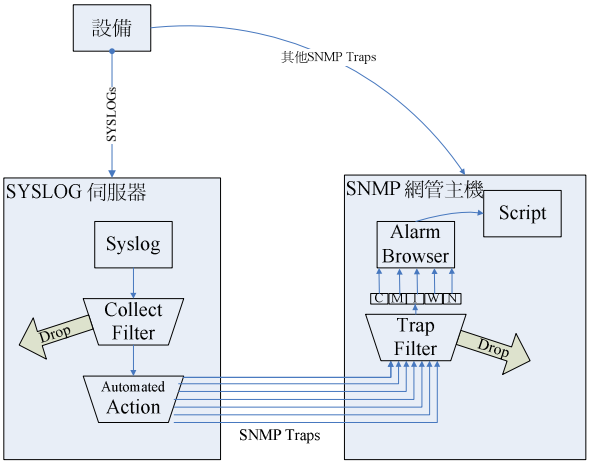
圖二的架構主要有二個改善：首先避免不必要的資料重複，另外在兩個異質的平台間，建立了以以 SNMP Traps 為基礎的溝通的管道。

在圖二的架構中也提供了非 Cisco 設備，或只支援 SYSLOG 而不支援 SNMP 的設備，可以經由 SYSLOG 伺服器當作跳板，將原本非即時處理的 SYSLOG 訊息，經由 SYSLOG Analyzer 變成可即時處理的 SNMP Traps 格式，交由 SNMP 網管主機執行必要後續處理。

3.2 實作過程

實作過程中利用公司現有的 Ciscoworks2000 主機當作 SYSLOG 伺服器；現有的 Openveiw 當作 SNMP 網管主機。也可以選用其他的軟體來實作，並無特別的限制，而選擇 Ciscoworks2000 的主要原因是該軟體內建 SYSLOG Analyzer 所以無需另行安裝。

圖三將 SYSLOG 伺服器以及 SNMP 網管主機的內部功能以圖形的方式展示出來：



圖三 系統架構圖

3.2.1 Device-Level

以 Cisco 設定為例，關閉 CISCO-SYSLOG-MIB SNMP Traps, 的方式如下:

```
no snmp-server enable Traps SYSLOG
```

如此可以關閉和 CISCO-SYSLOG-MIB 有關的 SNMP Traps 而不會影響其他 SNMP Traps 的傳送。

3.2.2 SYSLOG 伺服器-Level

如圖三所示，SYSLOG 伺服器 可以粗分為三個部份，SYSLOG、Collect Filter、Automated Action。

3.2.2.1 SYSLOG

這一部分是 UNIX 均會提供的功能，因為 Ciscoworks2000 SYSLOG Analyzer 的需求，必需將 SYSLOG 的設定檔(/etc/SYSLOG.conf)加入以下設定，才能供將 SYSLOG 的資訊交給 Ciscoworks2000 的 Collect Filter 來處理：

```
local7.info /var/log/SYSLOG_info
```

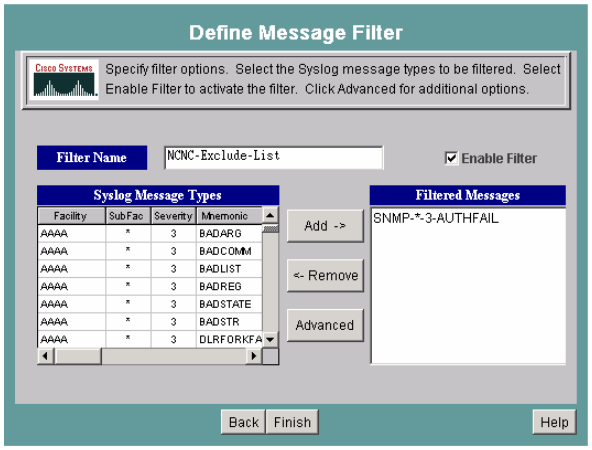
3.2.2.2 Collect Filter

本文中的 Ciscoworks2000 Collect Filter 提供了分析及過濾二項功能：

舉分析的功能而言， Collect Filter 可以根據類別、重要性、訊息名稱以及訊息內容來分析，如圖四所示，以訊息類別=SNMP、重要性=3 及訊息名稱=AUTHFAIL 來分析符合條件的 SYSLOG。

舉過濾的功能而言，由於設備發現 SNMP Authentication Fail 時，會以其他 SNMP Traps(見圖三) 的管道直接將 SNMP Traps 送給 SNMP 網管主機，同時也會產生一筆 SYSLOG 送到 SYSLOG 伺服器，這是另一種型態的資料重複，這類的資料重複可以在 Collect Filter 中進行過濾。

如圖四所示， Ciscoworks2000 Collect Filter 將符合 SNMP-*-3-AUTHFAIL 的 Authentication Fail 的訊息在 Collect Filter 階段即過濾掉。



圖四：過濾不要的 SYSLOG

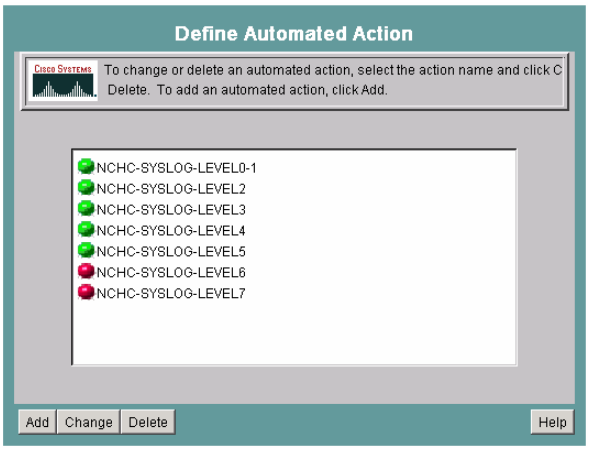
3.2.2.2 Automated Action

本文中將 SYSLOG 依重要性分類為 0-7 級 如表一所示， 其中第 6-7 級在 Collect Filter 中先行過濾不會送 SNMP 網管主機。

表一：根據 SYSLOG 的重要性對應到其它元件

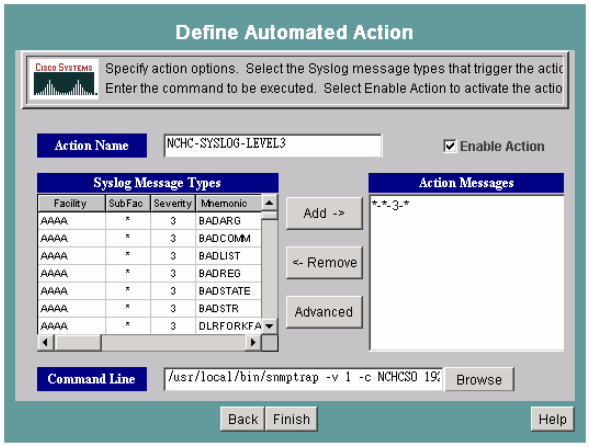
	SYSLOG	Analyzer	SNMP 網管
0	Emergency	同左	Critical
1	Alert	同左	Critical
2	Critical	同左	Major
3	Error	同左	Minor
4	Warning	同左	Warning
5	Notice	同左	Warning
6	Informational	不記錄	NA
7	Debug	不記錄	NA

如圖五，NCHC-SYSLOG-LEVEL 6 及 7 設定為關閉(以紅色顯示)，如此可以濾掉 Informational、及 Debug 等級的 SYSLOG，因為這些並不代表有問題，故不必送到 SNMP 網管主機進行錯誤處理。



圖五 ：Information、Debug 等級無需進行錯誤處理

舉 NCHC-SYSLOG-LEVEL3 為例子，再進行細部解說如圖六所示，所有等級為 3 的 SYSLOG，均要進行例外處理



圖六 ： 設定使用者自訂程序

自訂程序處理的指令範例如下:

```
snmpTraps -v 1 -c **********
192.168.3.1 .1.3.6.1.4.1.9.14.1.2 $D 6
300 "" .1.3.6.1.4.1.9.14.1.2.0.300 s $M
```

以上指令可以參考 net-snmp[4]的網頁，以得到進一步的說明。Ciscowroks2000 的 Automated Action 提供了變數$D 代表來源設備名稱(送 SYSLOG 的設備名稱)及$M 代表 SYSLOG 的內容。

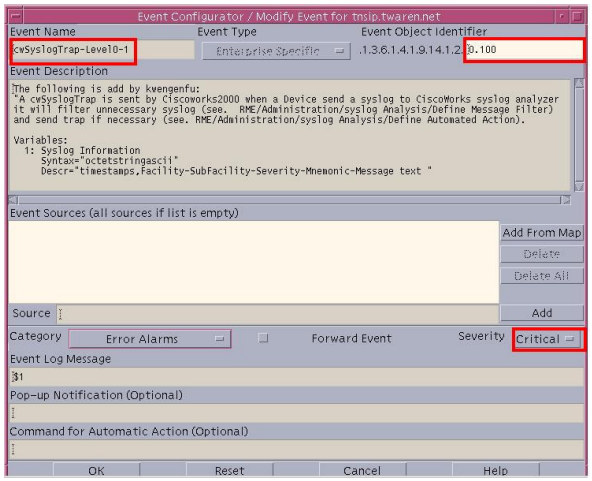
3.2.3 SNMP 網管主機-Level

如圖三所示，SNMP 網管主機可以粗分為三個部份，Traps Filter、Alarm Browser、Script。

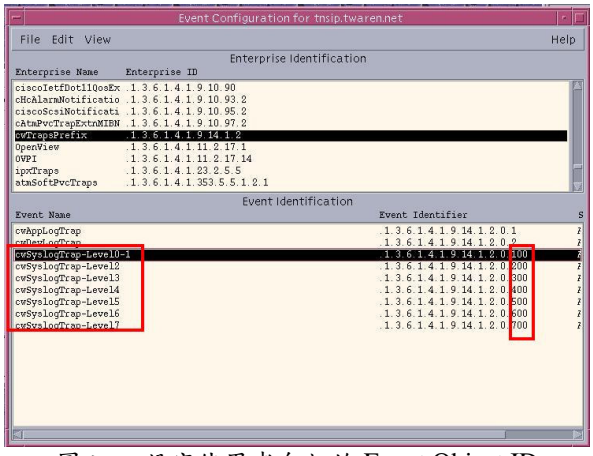
3.2.3.1 Traps Filter

於載入 CISCOWORKS-MIB[7]後，依圖七逐一建立各個不同的 SNMP Event Object ID。圖八為全部設定完成後的結果，過濾的方法可以經由設定 Source 來完成，本文中並沒有設過濾的條件，參考圖八，詳細設定請參考 HP 所提供的使用手冊[3]。

因為 SNMP 網管 提供 5 種重要性，但 SYSLOG 伺服器 所送來的有 7 種，所以需要適當的對應對應表可以參考表一。



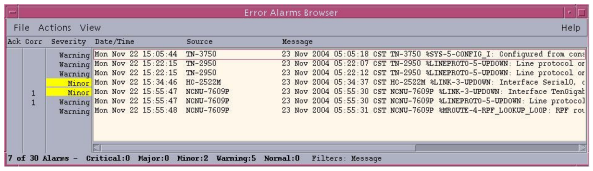
圖七 ： 設定一個使用者自訂的 Event Object ID



圖八 ： 設定使用者自訂的 Event Object ID

3.2.3.2 Alarm Browser & Script

在 Alarm Browser 中可以查到不同的 SYSLOG 已用不同的重要等級呈現，如圖九所示



圖九 : Alarm Browser

在圖九中，經過適當的 Event Correlation 可以將告警的數量減少依設備的 IP 或是事件的種類合併成同一個告警。

如同 Ciscoworks2000 Automated Action，在 SNMP 網管主機中，可以用 Script 自定使用者程序，由於這是 SNMP 網管主機的強項，故不再特別強調。

3.3 討論

3.3.1 合則二利的共生架構

在圖一中， 如果沒有 SYSLOG 伺服器，讀取 SYSLOG CISCO-SYSLOG-MIB 所產生的 SNMP Traps 也可以用於收集 SYSLOG，並利用 SNMP 網管主機的進階功能，達到依重要性的分類的功能。缺點是因 CISCO-SYSLOG-MIB SNMP Traps 所送的 Event OID 只有一種，需要依賴消耗 SNMP 網管主機自身的運算能力來讀取 SNMP Trap 的參數內容以達到相同的效果，對長期的維運而言，其所需要的維運技術和難度將會增加，對系統將是一種傷害。

如能配合使用 SYSLOG 伺服器的長處對 SYSLOG 先進行分析及過濾，可補 SNMP 網管主機之短處，依本文中所舉在 SYSLOG 伺服器端依重要性分類成 7 種 Event OIDs，即可以使網管主機在處理時不再需要依賴消耗 SNMP 網管主機的運算能力來讀取 SNMP Trap 的重要性的參數內容，長期而言維運難度也不會增加。同時 SNMP 網管軟體端有 5 種變化，以本文為例，最多可以有 7x5 種變化。例如以表一為例預設為 SYSLOG 的重要等級為 3(Error)者在 SNMP 網管中為 Minor 等級，如果符合特定條件的某項問題並不嚴重可以進行適當的降等調整成 Warning 以符合實監控的需求。

反之從 SYSLOG 伺服器的角度來看，SYSLOG 將所有的事件以 SNMP Traps 送到後方的 SNMP 網管主機，會使得在 SYSLOG 伺服器的 Event 處理工作變得很單純，僅需要將工作轉給後方的 SNMP 網管主機。而 SNMP 網管主機的長處剛好是處理各類事件使得 SYSLOG 伺服器在維運上也能受益。

3.3.2 SYSLOG Analyzer 的功能

通常 SYSLOG Analyzer 的主要特性包括了

- 過濾不要的 SYSLOG
- 啟動使用者的自訂程序
- 提供 SYSLOG 報表
- 分散處理 SYSLOG

本文中介紹了分析和啟動自訂程序，針對這兩項功能再補充如下:

分析可以針對不同的欄位加以篩選，包括了類別、子類別、重要性(本文只有用這個來篩選)、助記憶元(Mnemonic)、樣式(Pattern)及設備名稱等，而又有許多萬用字元可以使用，如樣式可用*router* 來代表訊息內容中有 router 字樣的 SYSLOG，足見其字元比對的功能相當強大。

自訂程序提供了執行例外程序的最佳選則，在本文中使用 SNMP Traps 的方式，將整個程序的使用者自訂程序的執行的工作，巧妙的轉給專門負責處理事件的網管主機 SNMP 網管，經由系統所提供的變數使整個轉移的過程完全不需要程式化，而順利的和 SNMP 網管主機結合。

3.4 結論

成功的結合 SYSLOG 以及 SNMP Traps，使得整合前，資料重複和處理重要訊息的工作得以在整合以後解決。同時共生的架構使 SYSLOG 伺服器和 SNMP 網管主機可以相互受益。最後只支援 SYSLOG 的設備，也可以利用現有的機制自動與 SNMP 網管主機接軌，享受即時的事件的處理服務。

在解決資料重複的問題上，設備不再需要二份 SYSLOG 以不同的協定分送到 SYSLOG 伺服器和 SNMP 網管主機，而達到資料達減量的效果。在解決處理重要訊息的工作上，結合兩者的專長，使得處理重要訊息的工作可以分工進行由 SYSLOG 伺服器分析、過濾，由 SNMP 網管主機處理。

在彈性上，原本只有 CISCO-SYSLOG-MIB 所產生的一種 Event OID 可用，在本文中至少有 7x5 種變化提供彈性還不只如此。

思考負責前段工作的 SYSLOG 伺服器其維運工作也大為降低，原因是本由 SYSLOG Analyzer 所需處理，如 E-MAIL、簡訊傳送的工作，均改為以 SNMP Traps 直接交給負責後段工作的 SNMP 網管主機，而網管主機除了可傳 E-MAIL、簡訊之外，還可以進一步進行 Event Correlation 等複雜的判斷工作。

這項整合不但可利用到 SYSLOG Analyzer 的優點同時也利用到網管主機的處理使用者自訂程

序的長處，經由這項結合，只要是支援 SYSLOG 的設備均可以將 SYSLOG 送往 SYSLOG Analyzer 這個平台，而和後段的 SNMP 網管平台接軌，成功的結合了 SYSLOG 和 SNMP Traps 這兩種協定。

參考文獻

[1]C. Lonvick,Cisco System,”The BSD SYSLOG Protocol,”RFC3164. August 2001

[2] SYSLOG 伺服器 Using Resource Manager Essentials V3.3 , SYSLOG 伺服器 April 2001 Release CD One 4th Edition

[3]Hewlett-Packard Company., “Managing Your Network with HP SNMP 網管 Network Node Manager”,March 2001

[4]http://net-snmp.sourceforge.net/, “NET-SNMP”

[5]J. Case, M. Fedor, M. Schoffstall, J. Davin, ”Simple Network Management Protocol (SNMP)”,RFC 1157, May 1990

[6]Scott Mordock,cisco Systems, Inc.,” CISCO-CISCO SYSLOG-MIB : Cisco SYSLOG message MIB file” ,August 1995, LAST-UPDATED "9508070000Z"

[7]Teyao Chen, Cisco Systems, Inc.,” CISCOWORKS-MIB”, April 1995

[8] 符光恩，李進興，”SNMP 趨勢管理”，TANET2004 台灣網際網路研討會論文發表論文集，2004 年 9 月