TANET 網路管理服務-sFlow 流量監測軟體研發

張耀中*,舒安平,李忠昇,李宇峰*,林志昇*,趙涵捷

國立東華大學電算中心, 國立東華大學資訊工程學系*
{changyc,schang,majorlee,eric,zslin,hcc}@mail.ndhu.edu.tw

摘要

有鑑於目前 TANet所廣泛使用之 NetFlow統計軟體，僅能運用於 Cisco 相關網路設備上，但許多網路設備如 Foundry、HP 所生產之設備，並不提供 NetFlow 格式之封包輸出，而改以 sFlow 格式之封包。因此，本文針對 sFlow 封包格式及其運作模式進行深入研究，撰寫 sFlow 之流量監測軟體，以提供學術網路上支援 sFlow 之設備進行流量統計分析，期望能為 TANet提供另一種網路管理服務機制。

關鍵詞：NetFlow, sFlow。

Abstract

For the network management tool “Netflow” using popularly on TANet is dedicated for Cisco equipments. The equipments of Foundry and HP do not support NetFlow but the format of sFlow. This paper is focus on studying the packet format of sFlow and the standard of sFlow to develop a new network management tool for TANet users. We anticipate this tool will provide another service for network management mechanism on TANet.

Keywords : NetFlow, sFlow.

1. 現有網路流量監控機制

目前常使用之網路流量監控機制有 MRTG、Netflow 等流量監控機制。MRTG(Multi Router Traffic Grapher)是一監控網路流量負載之工具程式，透過 SNMP 通訊協定由設備端得到相關流量資訊，以 PNG 格式之圖形，結合 HTML 網頁呈現方式顯示給使用者。MRTG主要的優點為:

- 可移植性：目前可以運行在大多數 Unix系統和 Windows 系統平台之上。
- 開放原始碼：MRTG是採用 PERL 語言編寫，可自行修改原始碼。
- 固定大小之系統日誌：MRTG 採用了獨特之演算法，其系統日誌大小固定。
- 性能：針對時間敏感部分使用 C 程式碼編寫，因此具有良好的性能與效能。
- PNG 格式圖形：圖形介面採用 GD 函式庫直接產生 PNG格式。
- 客製化網頁設計：MRTG所產生的 Web 頁面可以依照使用者需求設計。

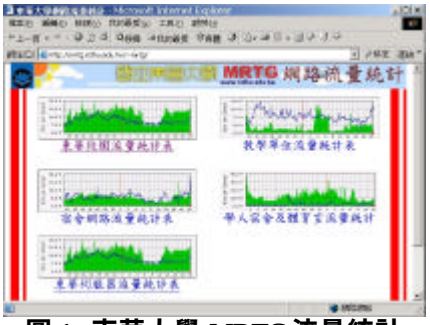

圖 1. 東華大學 MRTG 流量統計

另一套網路流量監控機制為 Cisco 所發展之 Netflow 技術，以搜集網際網路上流量(traffic)及分析軟體。它能幫助網路管理者做長期性監測並收集 Cisco 路由器指定位置之流量，並可在單一點位置對多點網路區段進行蒐集網路流量。

Netflow 之運作方式如下如圖二所示: Cisco Router 經由 flow-export function 將資料導出，在 Statistic PC 端之 Collector 模組接收由路由器所傳送來之 flow 資訊，並轉成原始資料儲存成檔案，傳送到統計分析之 PC 或工作站(Statistic PC)之 Analyzer 模組。

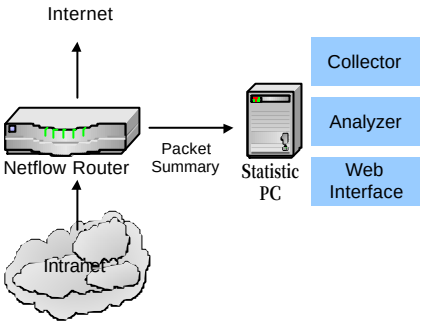

圖 2. NetFlow架構示意圖

分析模組(Analyzer)讀取 Collector 所集之原始 flow 資料加以分析統計，計算出所需求之資料，如 source_ip、destination_ip、flows 及 packets size 等資訊並產生相關報表，再將結果輸出到網頁供 web 介面查詢(圖三為東華大學之 NetFlow 流量統計)。

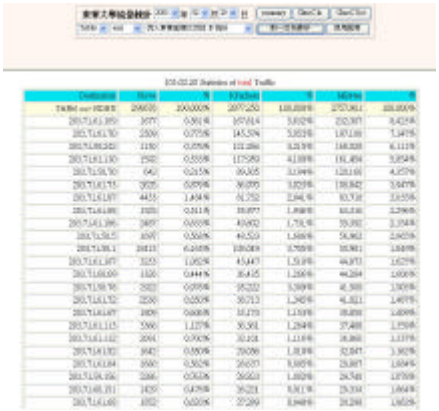

圖 3. 東華大學 NetFlow流量統計

2. sFlow網路流量監控機制

交換路由器（Switch Router，又稱 Layer 3 Switch）是 IP 網路環境中資料封包的交通中心，亦是最佳的流量分析資料來源。上節所提及之 MRTG 及 NetFlow網路流量分析機制均可使用在 Layer3之 Switch 或 Router 上，提供網路管理者圖形化之流量監測機制。

有鑒於網路流量分析已不再侷限於流量統計資料，同時也必許考量到網路上其他相關之訊息：如 Layer2-Layer4 封包解析資訊及額外之 IP 封包解析資訊(如 Route Table、Next Hop Address、Source and Destination AS、Destination AS Path 等相關資料)之分析與統計。目前，Foundry 與 InMon 所制定之 sFlow 架構，已成為網路設備業界公認的標準（RFC3176），有鑒於中華電信與東森寬頻之骨幹採用 Foundry 產品，無可避免的，SFlow 之格式封包輸出問題也會是 TANet未來需了解與運用的方向之一。

2.1 sFlow 架構

sFlow 的主要功能是監測 Switch 上每一個 IP 封包，並解析其 Header 所帶之屬性值，如 Source and Destination IP Address，Protocol and Port Number、AS Number、Interface、VLAN 等相關資訊。sFlow 匯整上述資訊成為一筆筆 "Flow Entry"資料，每隔一段固定時間，或累積到一定的數量，輸出給需要這些資訊之分析系統。此技術規範了 Sampling Mechanisms(取樣機制)，使用 sFlow Agent 來監測網路流量。同時，sFlow MIB 負責控制 sFlow Agent 運作及使用 sFlow Agent 來傳送 Sample Data(取樣資料)至資料收集端，即所謂的 Central Data Collector，如圖 4 所示。

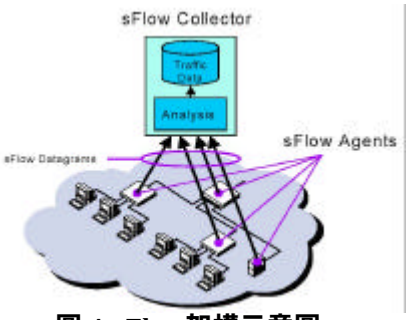

圖 4. sFlow架構示意圖

在設計 sFlow 此種監測架構及取樣技術時主要是考量提供網路上高速監測系統之能力，主要的特點有:

- 在 Gigabit 或更高速之網路精確監測網路流量。
- 提供單一節點控制所有 sFlow agent 之運作及接收監測資料能力。
- 製作 sFlow agent 時不需耗費大量系統資源。

sFlow 監測系統包含了內嵌在 Switch Router 或是 Gateway 之 sFlow Agent，負責將所收集之 sFlow 資料傳送至中央資料收集器，並交由 sFlow Analyzer 作分析運算。使用 Sampling 技術來擷取網路裝置之流量統計資料，利用 SFLOW MIB 來收集及控制 sFlow Agent 之監測資料，產生 sFlow Datagram 並將網路流量相關資訊傳送至 sFlow Analyzer 供查詢及分析結果。

2.2 sFlow取樣技術

sFlow 取樣技術是當封包到達 Interface 時，先決定是否過濾此封包。若此封包沒有被濾除時，網路裝置上的 Switching 或 Routing 機制會將目的地之 Interface 值指定給封包，此時再決定是否取樣此封包。利用一個計數器來決定是否取樣此封包，若計數器值為 0 時取樣此封包，而不論是否取樣，Total_Packets 紀錄所有能被取樣之封包的總數量，如圖 5 所示。

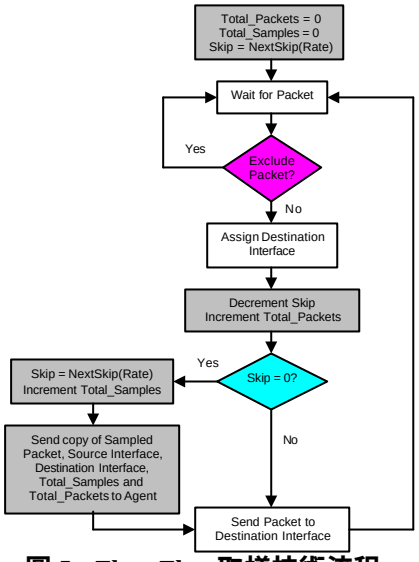

圖 5. sFlow Flow取樣技術流程

sFlow Agent **採用兩種取樣技術來進行網路流量監測(圖** 6 **所示)：**

- Statistical packet-based sampling of switched flows.
- Time-based sampling of network interface statistics.

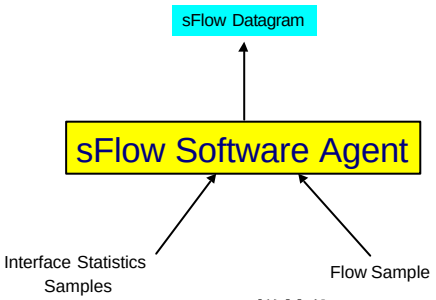

圖 6. sFlow取樣技術

Sampling of switched flows

所謂 Flow **是指由一** Interface **所收入之所有封包，經過** Switching **或是** Routing **模組傳送至另一個** Interface **之過程。取樣技術必須能夠保證在一個** Flow **之中所有封包都有相同之取樣機率；同時每個** Flow **之封包也能有相同取樣機率，以保證取樣後的流量能夠代表整體網路流量。**

Sampling of network interface statistics

此種取樣方式所採用週期性有效率之 Polling **方式來對網路設備作精準的流量資料統計。因系統效率及整體架構擴充成長考量，**sFlow **採用** Polling Interval **之方式來排程** sFlow Agent **監測網路流量。**sFlow Agent **將上述兩種取樣方式整合使用將所監測到的網路流量資料封裝於** sFlow Datagram**中，然後傳送給** sFlow Analyzer **作後續之分析處理。**

2.3 sFlow運作模式

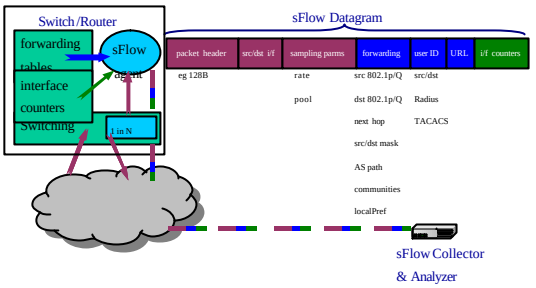

圖 7. sFlow Flow Datagram流程

sFlow **運作模式如圖** 7 **所示。首先** sFlow agent **將** sFlow Datagram**送出，接著由** sFlow Collector **及** Analyzer **來進行** sFlow Datagram **之蒐集及分析。**sFlow Collector **使用** InMon Technology **公司提供一免費命令列模式工具「**sflowtool**」，可用來擷取由** sFlow Agent **所送出之** sFlow **封包，並產生出文字型態輸出資料，供許多分析程式（如** tcpdump、ntop、snort **等）來進行資料分析。**sflowtool **所產生之文字格式資料如下所示：**

```
startDatagram
================================
  datagramSourceIP 203.72.80.2
  datagramSize 1404
  unixSecondsUTC 1045623538
  datagramVersion 2
  agent 203.72.80.2
  sysUpTime 154616000
  packetSequenceNo 630271
  samplesInPacket 9
  sampleSequenceNo 577684
  sourceId 0:25
  sampleType FLOWSAMPLE
  meanSkipCount 512
  samplePool 295774208
  dropEvents 0
  inputPort 25
  outputPort 2147483648
  packetDataTag INMPACKETTYPE_HEADER
  headerProtocol 1
  sampledPacketSize 64
  headerLen 64
```

透過分析由sflowtool**所產生之**sFlow**文字格式資料可分析出許多相關的資訊：**

- Protocols
  - ♦ Packet headers
  - ♦ Ethernet/802.3
  - ♦ IP/ICMP/UDP/TCP
  - ♦ IPX
  - ♦ Appletalk
- Layer2
  - ♦ Input/Output interface
  - ♦ Input/Output Priority

- ♦ Input/Output VLAN
- Layer3
  - ♦ Source subnet/prefix
  - ♦ Destination subnet/prefix
  - ♦ Next hop
- BGP 4
  - ♦ Source AS
  - ♦ Source Peer AS
  - ♦ Destination AS
  - ♦ Destination Peer AS
  - ♦ Communities
  - ♦ AS Path

3. sFlow流量監測軟體研發

由於網路流量資料十分龐大且變異性高，因此需要經由適當整理儲存後才能進行統計分析。運用網路資料庫儲存流量資料，其考量及優點如下：

- 透過已設計好之資料表，使資料處理人員易於瞭解資料內容。
- 資料處理人員可以利用標準之資料庫 SQL 語言，進行查詢及分析。
- 可利用資料庫 Client/Server 之特性，client 端統計分析程式較易於撰寫，（例如可利用 PERL，PHP 或 Delphi 等程式語言進行撰寫）。

透過網路資料庫來儲存 sFlow 流量資料，以期達到提升搜尋速度、計算速度及線上即時流量查詢之功能：

- 使用者介面簡易清晰， 讓使用者清楚瞭解目前網路頻寬及使用狀況。
- 以最基礎 IP 單位進行通訊協定以及流量之監控，進而進行應用及管理。
- 提供使用者進行監控區段中所有 IP 所? 生之行? ，如特定 IP 流量監控、特定單位流量監控、特定組織流量監控等。
- 監測各種通訊協定的傳輸流量，如；WWW、FTP、SMTP、DNS、NEWS、PROXY、OTHER 和 TELNET。
- 提供歷史資料之報表，讓管理者輕鬆掌握每階段所需要之不同要求。

3.1 sFlow流量監測軟體架構

sFlow 流量監測軟體架構如圖 8 所示，分為四個部分，分述如下：

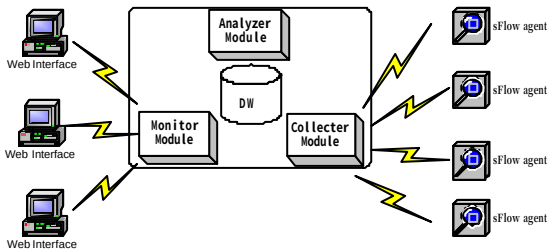

圖 8. 流量監測軟體架構

- 流量蒐集模組 Flow Collector Module

  此模組利用 sflowtool 公用程式及 撰寫 perl 程式 進行流量蒐集，收集 sFlow 流量資料之設備(如 Foundry 之 Router 或 Switch 等設備)，並將 sFlow agent 收集之流量資料(Flow Records) 傳送至資料倉儲 Data Warehouse 儲存流量資料。此外，根據設定，將 sFlow 的原始資料(Raw Data)儲存，以方便日後追蹤及回溯分析。

- 資料倉儲 Data Warehouse

  此模組負責儲存所有來自流量蒐集模組 Flow Collector Module 及流量分析模組 Flow Analyzer Module 所計算產生的資料，並接受來自流量分析模組 Flow Analyzer Module 及流量監測模組 Flow Monitor Module 之資料擷取請求。此設計必須考量資料倉儲中資料表儲存架構，以容納網路流量資料。

- 流量分析模組 Flow Analyzer Module

  此模組主要針對流量蒐集模組 Flow Collector Module 傳送過來之 sFlow 資料作運算與分析，使用者透過流量監測模組 Flow Monitor Module 所提供之 Web 介面去傳送欲監控之條件，依據所設定之條件過濾 sFlow 輸出之流量資料，將符合監控條件(Filter)流量資料作分類與統計，並將分析結果存入資料倉儲 Data Warehouse。使用者可以透過流量資料監測模組 Monitor Module 從資料倉儲 Data Warehouse 裡讀取監控條件(Filter)之即時流量圖。

- 流量監測模組 Flow Monitor Module

  運用 PHP 程式撰寫，透過網頁介面提供使用者一個標準化 Web 型式之系統存取操作界面，以執行監控及查詢之動作。透過此監測模組，使用者可隨時隨地透過網頁瀏覽器登入系統，並可自行定義流量資料的過濾條件與監控範圍，連結流量分析模組 Flow Analyzer Mod 至資料倉儲 Data Warehouse 擷取倉儲資料，並產生即時性之 HTML 報表及流量圖。

3.2 sFlow流量監測軟體研發

流量蒐集模組 Flow Collector Module 區分成兩部分研發(圖 9 所示)：

- 第一部份採用 sflowtool 公用程式，擷取由 sFlow Agent 所送出之 sFlow 封包，並產生出文字型態之輸出資料。

- 第二部分撰寫 PERL 程式，將所收集之

sFlow 封包 Row Data 傳送至資料 Data Warehouse 之中儲存。

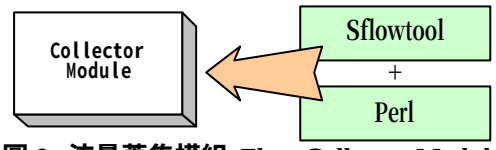

圖 9. 流量蒐集模組 Flow Collector Module

資料倉儲 Data Warehouse 研發：

主要以 MySQL 資料庫為考量，分別接收流量蒐集模組 Flow Collector Module 所收集得到之 sFlow 封包，以及接受流量分析模組 Flow Analyzer Module 及流量監測模組 Flow Monitor Module 之運算與分析(圖 10)。

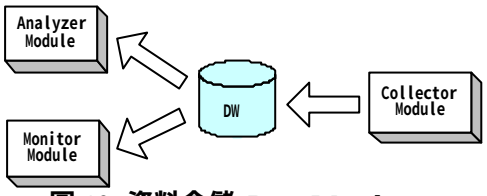

圖 10. 資料倉儲 Data Warehouse

以 MySQL 資料庫為考量主要特性有：

- **以 C 及 C++ 寫成，並使用 GCC 2.7.2.1 來測試，使用 GNU 自動偵測來增加移植性。**
- **用戶端可以用 C，C++，JAVA，PERL，TCL 等多種語言來存取資料庫。**
- **支援多重處理器，取得多個處理器資源，以增加資料庫存取效率。**
- **可執行於各式平台及作業系統。**
- **所有經過網路傳送的密碼，都經過加密處理。**
- **可使用工具程式(Isamchk)，用以檢查並達成最佳化及修正表格等功能。**

流量分析模組 Flow Analyzer Module 研發：

針對流量蒐集模組 Flow Collector Module 傳送過來的 sFlow 資料作運算與分析，使用者可以透過流量監測模組 Flow Monitor Module 所提供之 Web 介面去傳送欲監控之條件給流量分析模組 Flow Analyzer Module，依據使用者所設定的條件過濾 sFlow 輸出的流量資料，把符合監控條件(Filter)的流量資料作好分類與統計，並將結果存入資料倉儲 Data Warehouse 裡。

監控之條件參數包含：

- AS Number。
- IP **區段**(IP Block)。
- **主機**(Host)。
- **介面**(Physical Interface)。
- **應用層協定**(Application Protocol and Port Number)。
- VLAN。

流量監測模組 Flow Monitor Module 研發：

透過網頁介面提供使用者一個標準化的、Web 型式之系統存取操作界面，以執行監控及查詢之動作(圖 11)。

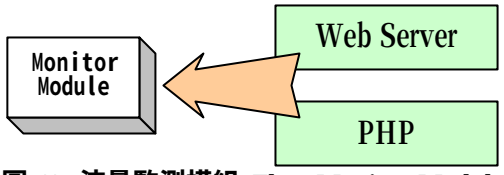

圖 11. 流量監測模組 Flow Monitor Module

使用 PHP 來製作網頁介面之考量：

- **PHP 是一種伺服端**(server-side)，**跨平台**(cross-platform)**之 HTML 嵌入式直譯式語言**(HTML embedded scripting language)。
- **以模組**(module)**的形式和 Apache 伺服器結合。**
- **提供多種連結資料庫的介面，如 MySQL，mSQL，PostgreSQL，Sybase ，Informix，InterBase。**

3.3 sFlow 流量監測軟體

當支援 sFlow 之網路設備送出 sFlow 格式之流量資訊至 sFlow Collector 時，sFlow Collector 系統每十分鐘抓取一次 raw data 資料並進行轉換格式後寫入資料庫，以供網頁介面之流量資料查詢。網頁查詢介面提供網路管理者查詢功能，查詢某一天或當天即時流量統計及以 IP 為單位之流量排名統計，並且可依據特定服務或埠號(Port)作流量統計排名分析。進一步可以針對 IP 連線服務埠號作流量之排名分析與比較，以得知各種服務之流量。

由實際線上數據(圖 12 所示)顯示，當 IP 之流量特別大時，利用滑鼠點選功能進一步查詢其服務流量排名，由圖示可得知此 IP 埠號為 6677 之服務流量異常，此即為 peer-to-peer 的服務埠號，進而得知此 IP 之使用者行為而作處理。

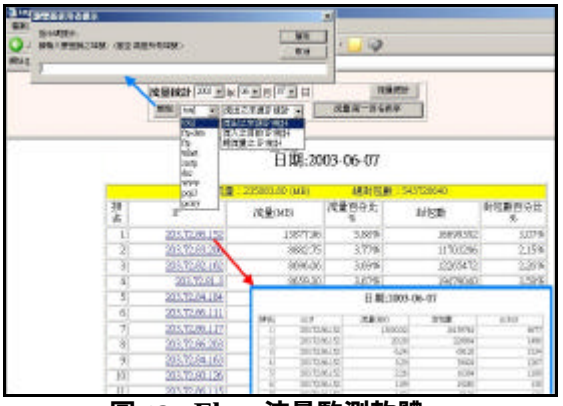

圖 12. sFlow 流量監測軟體

4. 結論與推廣應用

目前，Foundry 與 InMon 所制定之 sFlow 架構，已成為網路設備業界公認的標準（RFC3176)。基於下列幾點：中華電信與東森寬頻之骨幹採用 Foundry 產品；國家高速電腦中心與交通大學、中央大學以及中正大學等針對 Foundry 產品進行網路架設與連線測試；工研院、長庚大學、大仁技術學院及吳鳳技術學院所採用之 Foundry sFlow 網管系統等原因，sFlow 之格式封包將會是 TANet 未來需了解與運用的方向之一。因此，本文針對 sFlow 封包格式及其運作模式進行深入研究，，並研發 sFlow 流量監測軟體之系統架構，包含流量蒐集模組、資料倉儲、流量分析模組及流量監測模組等，以提供學術網路上支援 sFlow 之設備進行流量統計分析。

未來，本中心所撰寫之 sFlow 流量監測軟體將交由花東地區使用 Foundry、HP 等相關網路設備之 TANet 連線單位包含花蓮師院、台東師院、宜蘭縣網中心等，進行驗證與測試。待測試完成後推廣至所有 TANet 連線單位。並將此軟體提授權給 TANet 連線單位，期望為 TANet 提供支援 sFlow 設備另一種網路管理服務機制。

誌謝

本文研究經費由教育部電算中心之創新服務計劃補助，東華大學電算中心同仁共同規劃執行。

參考文獻

[1] MRTG 相關資料
http://people.ee.ethz.ch/~oetiker/webtools/mrtg/

[2] sFlow 相關資料http://www.sflow.org/

[3] 東華大學 MRTG 流量統計網址
http://mrtg.ndhu.edu.tw/~mrtg/

[4] 東華大學 NetFlow 流量統計網址
http://netflow.ndhu.edu.tw/

[5] Cisco NetFlow 網址
http://www.cisco.com/warp/public/732/Tech/nmp/netflow/index.shtml

[6] RFC 3176 “InMon Corporation's sFlow : A Method for Monitoring Traffic in Switched and Routed Networks”

[7] InMon Corp. “Traffic Monitoring Using SFLOW” www.inmon.com