TWAREN 100G 整合式網管監控平台之規劃與建置

鄭欣恬
國家實驗研究院國家高速網路與計算中心
hsintien@narlabs.org.tw

摘要

台灣高品質學術研究網路 (TWAREN) 主要以提供台灣學研界一個高可靠度、高品質及高安全性的100G新骨幹網路傳輸品質為任務。因應TWAREN 100G新骨幹網路架構的建置與TWAREN 7x24小時網路維運中心 (NOC) 的網路監控和網路管理之需求，本文將說明以TWAREN網管維運人員的角度，設計並建置一套適用於新100G大型骨幹網路的「TWAREN 100G整合式網管監控平台」。平台具備資料視覺化之特色，提供NOC維運團隊最佳的骨幹網路維運之輔助工具，可達到提早發現和解決異常事件之目的，進而提升整體網路的服務品質。

關鍵字：網路監控、網路管理、資料視覺化。

Abstract

The primary goals of TaiWan Advanced Research and Education Network (TWAREN) are to provide a high reliability, high quality and high security 100G new backbone network for Taiwan's academic and research data transmission. In response to TWAREN 100G new backbone network infrastructure deployment, TWAREN 7x24 Network Operation Center (NOC) needs to monitor and manage the new 100G network. This article describes how to design and build a suitable 100G large backbone network INMS (TWAREN 100G Integrated Network Management System) from TWAREN NOC point of view. Platform with the characteristics of data visualization provide NOC operator the best NMS Tools. NOC operator can use this INMS to early detect and resolve the network anomaly event, and thus enhance the overall service quality of the network.

Keywords: Network Management, Network Monitor, Data Visualization.

1. 前言

台灣高品質學術研究網路[1] (TWAREN，TaiWan Advanced Research and Education Network) 主要的任務，是提供台灣學術和研究單位一個高可靠度、高品質及高安全性之 100G 骨幹網路。TWAREN 100G 國內骨幹網路架構如圖 1 所示，主要涵蓋臺北、新竹、臺中、臺南和中研院，共五個頻寬為 100G 的主節點 (Core Node)，每個主節點下接數個區域網路中心 (GigaPOP)，共十二個 GigaPOP 連接至骨幹雙主節點，頻寬各為 50G。每個 GigaPOP 再下接數個連線單位（包含各大學院校、研究單位等）。

圖 1 TWAREN 100G 國內骨幹網路架構圖

TWAREN 100G骨幹上的設備包含提供第一層服務的光設備、提供第二層和三層服務的骨幹路由交換器設備、小型交換器及伺服器，設備數量加總共達上百台。然而，目前市面上仍然沒有單一的一套網管軟體可以全面性的監控TWAREN 100G所有的網路設備，並且TWAREN監控到的告警事件必須要與國家實驗研究院國網中心 (NCHC) 的事件開單管理系統 (Remedy System) 整合，但現行的網管軟體亦沒有針對這部分做結合。

因應 TWAREN 100G 新骨幹網路架構的建置與 TWAREN 網路維運中心(NOC, Network Operation Center) 對新骨幹網路的監控和管理需求，TWAREN 網管開發團隊開始重新思考與評估資料的儲存方式，並規劃與建置新的 100G 資料庫與資料儲存架構，同時著重於設計與規劃更符合 100G 骨幹網路架構的監控平台。於 2016 年著手進行全新的一套「TWAREN 100G 整合式網管監控平台」(TWAREN 100G INMS, TWAREN 100G Integrated Network Management System) 之開發和建置。新平台具備資料視覺化 (Data Visualization) 之特色，讓網管維運人員在單一的平台上，即可同時監控和追蹤到視覺化和動態化的即時資料或歷史趨勢資料，亦結合自動化的預警、告警和開立事件單等機制，提供網管維運人員一個最佳的輔助維運之監控工具，以達提早發現和解決異常事件之目的，進而提升整體骨幹網路服務的品質。

本文共分五章節，在以下各章節將說明如何規劃與建置一套適用於監控 TWAREN 100G 新的大型骨幹網路之整合式網管監控平台。在第二章中，將說明歷年 TWAREN 網管開發團隊所自行開發的各時期 TWAREN 整合式網管監控平台的特色和差異比較。第三章為系統設計，將說明本系統之架構，以及本系統的監控項目與其監控目的。第四章為系統實作與展示，將展示本系統的實作成果。第五章將說明結論與未來展望。

2. 歷年自行開發的 TWAREN 整合式網管監控平台 (INMS) 之說明

TWAREN 舊骨幹網路架構時期，為提供 TWAREN 用戶高品質的網路服務，TWAREN 網路維運中心 (NOC) 的網管開發團隊於 2007 年自行開發第一套 TWAREN 整合式網管監控平台 (INMS) [2]，如圖 2 所示，為第一代監控平台的首頁畫面。平台主要負責監控舊 TWAREN 整體骨幹網路上的所有網路設備之即時狀況，包含提供第一層服務的光設備、提供第二層服務的骨幹交換器設備，以及提供第三層服務的骨幹路由設備、小型交換器和伺服器等，並且提供異常告警事件的自動告警通知與自動開立事件單之自動化功能。

爾後，於 2010 年進行平台的全面改版與功能的升級，如圖 3 所示，為第二代監控平台的首頁畫面。平台除了新增操作使用功能的權限控管機制外，亦新增更多監控項目，讓整個 TWAREN 舊骨幹網路的監控更加完善及全面性。此平台在監控與管理 TWAREN 骨幹網路上已穩定地運行多年，於 2016 年 TWAREN 100G 新舊骨幹電路移轉期間，亦同步且穩定地持續運行在監控 TWAREN 舊骨幹網路設備與電路上，並且能即時偵測出網路之異常問題，即時發送告警通知，提供 TWAREN 網路維運人員可靠的訊息，以更準確地掌握事件狀況並進行後續之處理及追蹤。

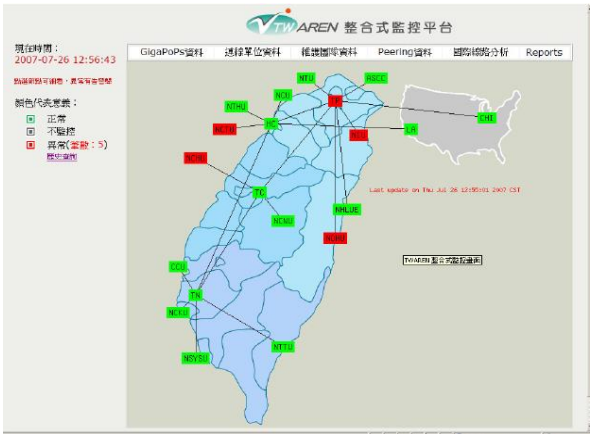

圖 2 第一代 TWAREN INMS 的首頁畫面

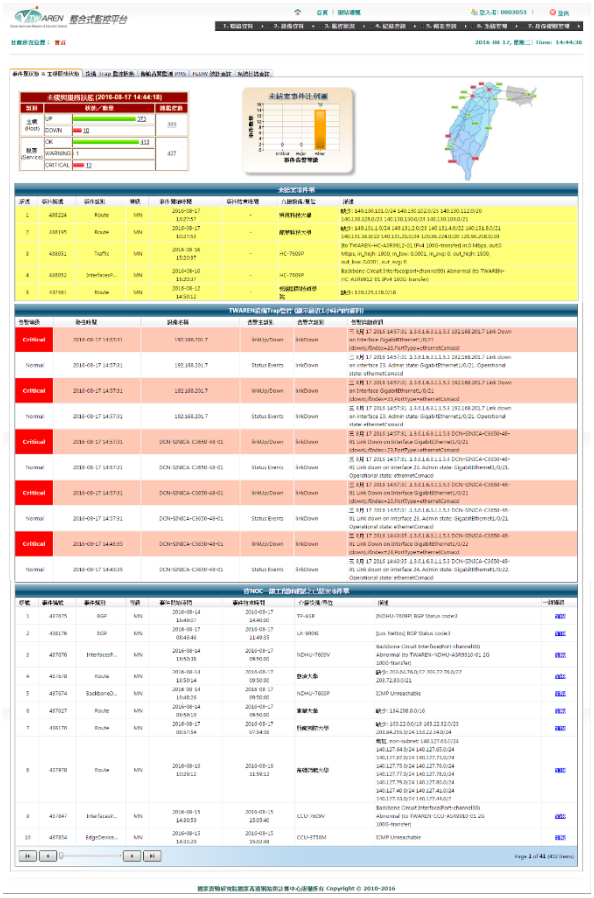

圖 3 第二代 TWAREN INMS 的首頁畫面

因應 TWAREN 100G 新骨幹網路架構的建置和 TWAREN NOC 24 小時不間斷的網管監控需求，於今年 TWAREN 網管開發團隊著手開發與建置一套符合 TWAREN 100G 新骨幹網路架構的 TWAREN 100G 整合式網管監控平台(TWAREN 100G INMS)。

表 1，將針對 TWAREN 網管開發團隊歷年和目前所開發與建置的 TWAREN 整合式網管監控平台，進行平台特色與差異化的比較和說明。

表 1 歷年 TWAREN 整合式網管監控平台的比較

比較	第一代 INMS	第二代 INMS	新 100G INMS
監控項目	(1) 國內電路品質狀態 (2) 網路設備效能狀態 (3) GigaPOP 機房環境溫度狀態 (4) 連線單位狀態 (5) VPLS VPN 狀態 (6) 伺服器設備狀態	新增以下監控項目： (1) GigaPOP RPM 設備的電流供電狀況 (2) 骨幹設備和局端設備的存活狀況 (3) 國際電路品質狀態	新增以下監控項目： (1) 100G 所有網路設備的即時存活狀況監控（包含骨幹設備、局端設備、機房電設備和溫控設備等） (2)TWAREN 主節點和各 GigaPoP 設

		(4) TANet 骨幹電路狀態	備的總電流與電壓之供電狀況
監控資料呈現方式	靜態即時(每五分鐘為監控的最小單位)。	靜態即時，新增提供部分靜態歷史報表。	動態視覺化的即時資料和歷史趨勢報表。
平台特色	(1) 以 Web 為基礎的設計，不需要於使用者端安裝任何網管軟體。 (2) 單一整合的監控平台，全面性的監控 TWAREN 所有的網路設備，且可自動化的整合系統告警事件與事件開單管理系統。	除承接第一代的特色外，新增以下特色： (1) 平台 Dashboard 新增整合 Nagios、Trap、NetFlow 和 SysLog 等資訊查詢。 (2) 平台新增監控功能和操作使用功能的權限控管機制。	除承接第一代和第二代的特色外，亦強化監控資料和告警事件的視覺化和動態化之呈現效果，以及更友善的使用者操作介面。

3. 系統設計

本章共包含兩節。3.1 節將描述本系統之架構；3.2 節將說明本系統主要的監控項目及其監控目的。

3.1 系統架構

本系統的系統架構，如下圖 4 所示，NE (Network Element) 區塊代表 100G 網路設備，包含光傳輸網路交換設備 (ROADM, OLA)、路由器 (ASR)、乙太網路交換器 (Nexus 5672, Catalyst 3650)、網路設備之供電設備 (SMR, PRM) 及伺服器等。TWAREN 100G INMS 區塊為本系統主要的元件，共區分成三大部分，分別為網管監控主機 (NMS)、資料庫和前端的網頁伺服器。網管監控主機分成四大模組，主要負責網管監控資料的探測 (Probe)、分析 (Analyze)、紀錄收集 (Log Collect) 和事件處理 (Event Trigger) 之任務，共有兩台主機互為備援。網管監控資料的探測是利用 SNMP、Command Line Interface (CLI)、Trap 和 NetFlow 等技術來進行。本系統資料庫採用 MariaDB，架構為 Cluster 設計以達到高容錯及高可用性。前端監控網站則是以 Web 為基礎的一套監控平台，以 ASP.Net 程式設計語言進行開發，並搭配 D3.js[3]、Highcharts[4]、Bootstrap[5] 和 CSS3[6] 等視覺化的開發工具，呈現視覺化和互動式的網頁監控畫面。網管維運人員即是透過此前端 Web 伺服器介面以掌握目前整體網路狀態，並進行相關事件的追蹤及處理。

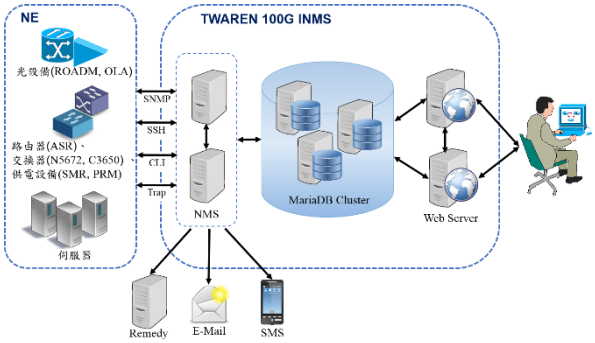

圖 4 系統架構圖

3.2 系統的監控項目

本系統的監控項目之定義與設計，除參考第二代 TWAREN 整合式網管監控平台的網管監控項目外，並依據 TWAREN 100G 整體骨幹網路的新架構，調整與新增必要的監控項目。系統亦針對各項監控項目訂定相關的臨界值 (threshold)，當監控值超過設定的臨界值時，就會觸發對應的處理動作，包含郵件通知、簡訊通知或開立事件單紀錄。以下共分七大類的監控類別，並針對各項監控項目和監控目的加以說明。

(1) TWAREN 100G 國內與國際電路品質的監控

「國內與國際電路的流量監控」：當骨幹介面流量異常增加時，可能代表網路遭受攻擊，將進一步進行 Netflow 分析。當流量異常減少時，可能代表線路斷線，將立即進行線路品質查測。

「國內與國際電路界接介面狀況監控」：確保電路正常運作，並穩定地提供 TWAREN 骨幹連線服務。

(2) TWAREN 100G 骨幹網路設備效能和存活狀態的監控

「設備 CPU 和 Memory 效能監控」：監控設備之 CPU 和 Memory 使用量，確保及早發現設備是否超載運作，進而影響網路整體運作。

「設備 Power Supply 效能監控」：確保及早發現設備是否電源模組異常或故障，造成設備異常，進而影響網路整體運作。

「骨幹設備、局端設備、機房電源設備與溫控設備存活狀態監控」：監控 TWAREN 100G 各類設備之存活性，以掌握與確保所有 100G 網路設備的正常運作。

(3) TWAREN 100G 主節點和區網中心的相關監控

「GigaPOP 機房環境溫度監控」：機房溫度升高將直接影響網路設備的運作。當機房溫度異常時，將按照 SOP 通知各 GigaPOP 管理人員進行第一時間的處理。

「主節點 SMR 和 GigaPOP RPM 設備的供電狀況監控」：因 100G 設備由 SMR 及 RPM 進行直流供電，若 SMR 或 RPM 發生故障，將會造成 100G 設備無法正常運作。此監控可確保 TWAREN 100G 設備供電穩定度，並確保設備可以正常供電運作。

(4) TWAREN 100G 各連線單位的相關監控

「路由狀況監控」：為維持國內研網路由秩序，與連線單位約定彼此交換路由，並提供 Internet2 路由轉訊服務給連線單位，故監控連線單位的路由內容。

「連線單位流量狀況監控」：可以了解連線單位的使用量，並可作為連線單位線路斷線 (如流量為零) 或遭受網路攻擊 (如流量滿載) 之參考依據。

「連線單位WAN Port IP Ping狀況監控」：可以確保連線單位連至TWAREN骨幹之間線路品質狀況(如斷線或線路品質不佳等)，以確保TWAREN連線單位之連線品質。

(5) TWAREN 100G VPLS VPN 監控

「VPN Client 界接介面狀況即時監控」：針對每一個 VPLS VPN 客戶，為提供良好之網路品質供計劃研究使用，此監控乃針對每個 VPN Client 界接 Port 進行監控。

「VPN full-mesh ping 監控」：針對每一個 VPLS VPN 客戶，為提供良好之網路品質供計劃研究使用，此監控乃針對每個 VPN 之雙向私有連線進行連通性 PING 檢測。若 100%則代表網路品質良好。

(6) TWAREN 100G 國內外互連網監控

為維持國際研網路由交換秩序，當國際研網失連或交換路由筆數異常，將造成連線單位無法透過 TWAREN 存取研網資源，此監控乃針對與國際研網介接之 BGP 狀態及交換路由筆數進行監控。

(7) TWAREN 100G 伺服器監控

監控 TWAREN 對外服務伺服器的存活性及服務，以確保 TWAREN 對外服務伺服器之可用性。

4. 系統實作與展示

本章節的成果展示，將針對 TWAREN 100G INMS 主要的平台功能，分以下四節加以說明。

4.1 首頁即時監控畫面

基於安全性考量，使用者在進入本監控平台時必須經由權限認證，具有被授權身份的使用者方能登入。本系統提供使用者登入平台的畫面，如圖 5 所示。

圖 5 系統登入畫面

當使用者認證成功後，即能登入平台首頁的即時視覺化監控畫面，如下圖 6 所示。使用者可以於首頁監控畫面上分別查看到視覺化的「TWAREN 100G 骨幹網路即時監控狀態」，以及圖表化的「截至今日累計未結案事件統計圖」、「設備存活狀態統計圖」和「截至今日累計未結案事件單」等即時資訊。

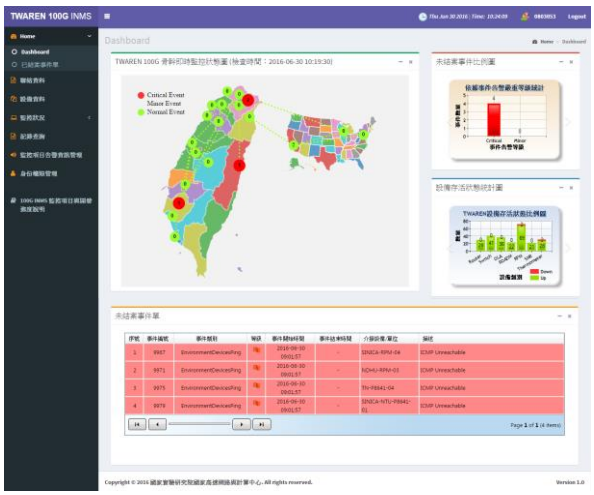

圖 6 首頁即時監控畫面

爲使網管維運人員可清楚瞭解和掌握骨幹網路的狀況，平台首頁的視覺化「TWAREN 100G 骨幹網路即時監控狀態」呈現方式採以階層式概念設計。第一層以每一個區網中心 (GigaPOP) 為主體，第二層則為查看各個GigaPOP詳細的即時監控項目之狀況。如上圖6「TWAREN 100G 骨幹網路即時監控狀態圖」所示，當監控項目有出現異常狀況時，所有異常事件皆歸屬於其所屬的GigaPOP，因此視覺化圖像上的GigaPOP圓點內將會顯示即時的異常事件總數量，並且依據事件的嚴重等級，呈現不同的顏色狀態和閃爍提示效果，以及發出告警聲響。系統亦會依據各監控項目定義的事件嚴重等級和異常累計發生的時間，針對各項監控項目自動發送告警通知（包含E-Mail通知、簡訊通知和自動開單至Remedy事件管理系統）給特定對象（包含一線或二線維運工程師、國際電路維護商等）。

針對上圖6「TWAREN 100G 骨幹網路即時監控狀態」視覺化動態圖的每一個GigaPOP之狀況，

可點擊特定的GigaPOP (如圖7，以東華大學為例)進一步了解詳細監控狀況，包含機房溫度、設備狀態、連線單位狀態和電路狀態等監控資訊，以及了解各監控項目設定的臨界值資訊。當異常發生亦會同時呈現正常狀態基準值及相關所需處理資訊，讓網管維運人員能更快速地處理異常事件。

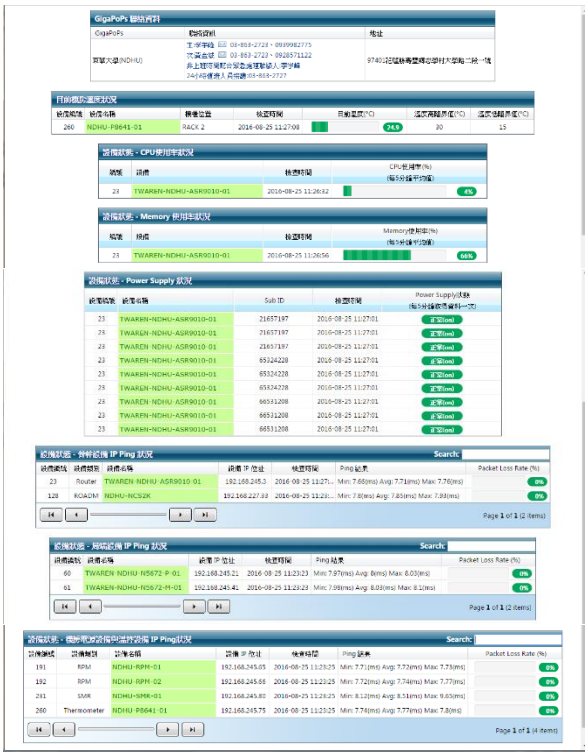

圖 7 東華大學各監控項目之即時監控狀態畫面

4.2 異常事件紀錄的追蹤與查詢畫面

針對持續發生中或已結束之異常事件，平台亦支援事件追查和匯出資料功能，如圖 8 所示，方便網管維運人員隨時掌握、追蹤、分析或統計事件的處理進度與狀況，以便清楚了解目前已處理和待處理的事件單類別及數量等資訊。

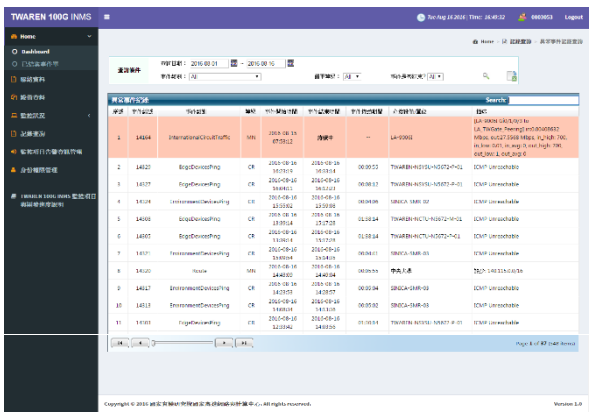

圖 8 異常事件紀錄查詢畫面

4.3 監控項目的即時監控畫面

平台主要的監控項目共有七大類，分別為國內及國外電路狀態、設備狀態、GigaPOP 狀態、連線單位狀態、VPLS VPN 狀態、Peers BGP 狀態及伺服器狀態等。所有監控項目的即時監控資料都是每五分鐘即時更新一次。即時監控畫面，如下圖 9 的機房環境溫度狀況和下圖 10 的國內骨幹電路介面流量狀況所示。由畫面可以清楚了解每一監控項目其目前監控的正常、異常和不告警數量，以及其統計的監控總數，維運人員可以從視覺化的畫面快速地查看到呈現紅色的異常事件，再依據判斷或 SOP 進行後續的分析、查修或報修等事項。

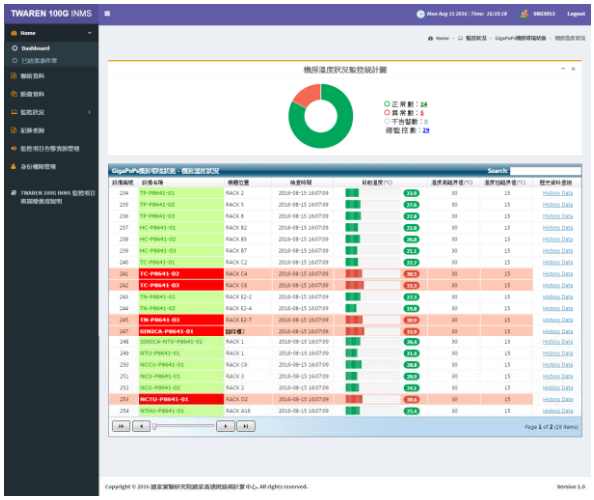

圖 9 GigaPOP 機房環境溫度狀況的即時監控畫面

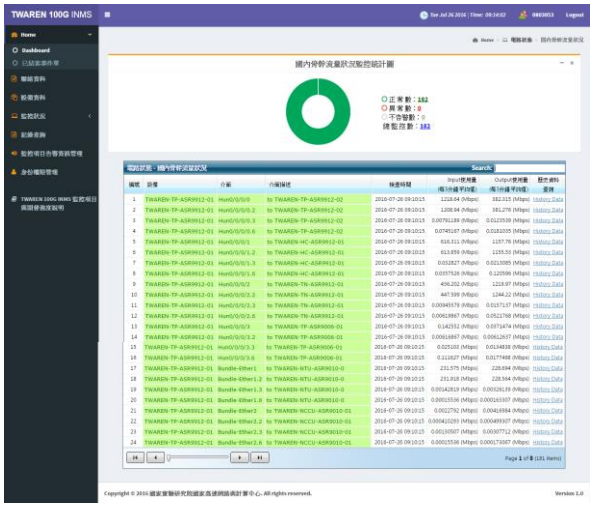

圖 10 國內骨幹電路介面流量狀況的即時監控畫面

4.4 監控項目的視覺化歷史資料查詢畫面

平台除了提供視覺化和動態化的即時監控資料查看與追蹤外，亦提供視覺化的歷史資料動態趨勢報表之查詢。歷史資料均以每五分鐘為最小的單位呈現，讓維運人員可以針對異常事件進行歷史資料的追蹤和分析，更明確地釐清問題點，以進行後續

的查修或通報等事項。下圖 11 是由上圖 9 機房環境溫度狀況即時監控表內，點選欲查詢的特定機房環境溫控設備（以點選圖 9 科技大樓 (TRTC) 為例）之視覺化歷史趨勢報表圖。視覺化的歷史趨勢圖除了依據查詢的起、迄日期呈現資料趨勢圖外，亦會在圖上呈現此類監控項目的高、低臨界值，讓追蹤異常點時更加快速。如圖 11 所示，可明顯地從趨勢圖上觀察到 2016 年 07 月 21 日下午 14 點 21 分時， TRTC-P8641-01 溫控設備其 sensor 測量到的 TRTC 機房溫度高於高臨界值，此時，網管維運人員將按照機房溫度異常的 SOP 通知各 GigaPOP 管理人員進行第一時間的處理。

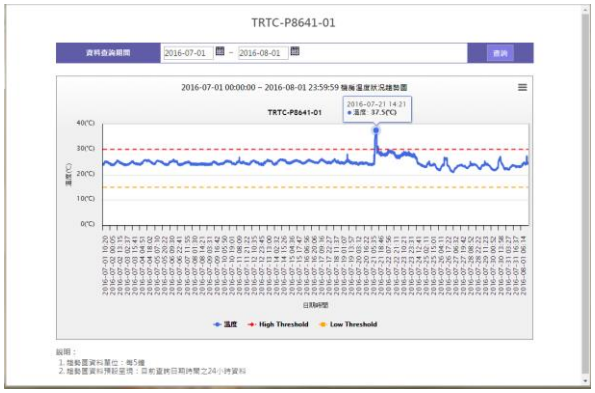

圖 11 科技大樓機房溫度視覺化歷史資料查詢畫面

圖 12 和圖 13 則是由上圖 10 國內骨幹電路介面流量狀況的即時監控表內，點選欲查詢的特定骨幹電路介面（以點選圖 10 表內的台北主節點與東華大學 (NDHU) 之間 50G 電路介面流量為例）之視覺化歷史趨勢報表圖。依據欲查詢之起、迄日期的選擇，可查看到日（如圖 12 所示）、週、月（如圖 13 所示）、季或年等不同時間區間的趨勢報表，讓歷史資料的查詢更具彈性。透過趨勢圖的查詢可追蹤到，當骨幹介面流量異常增加時，可能代表網路遭受攻擊，網管維運人員將進一步進行 Netflow 分析。當骨幹介面流量異常減少時，可能代表線路斷線，將立即進行線路品質查測。

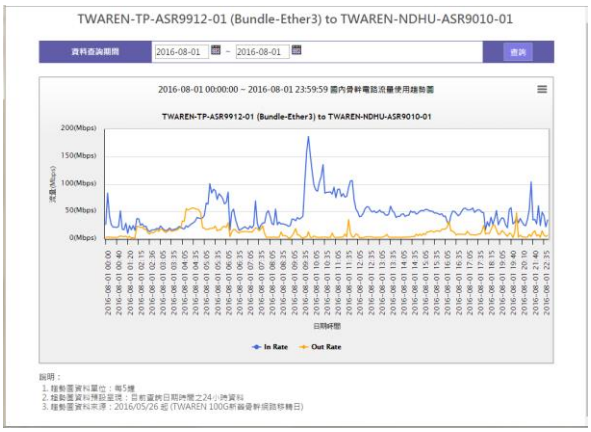

圖 12 TP 至 NDHU 50G 電路介面日流量報表畫面

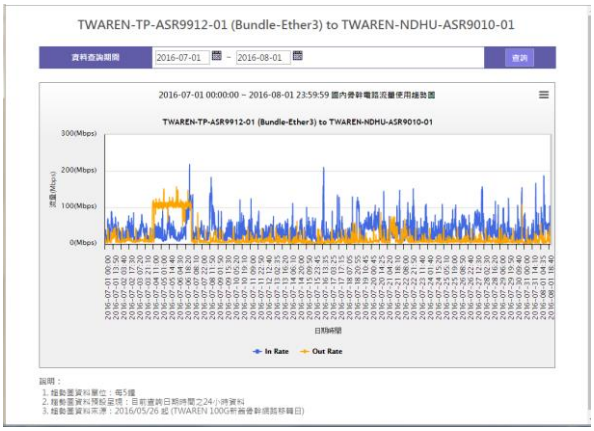

圖 13 TP 至 NDHU 50G 電路介面月流量報表畫面

5. 結論與未來展望

TWAREN 100G 整合式網管監控平台 (TWAREN 100G INMS) 是 TWAREN 網管開發團隊所開發的一套多功能的視覺化網路監控與網路管理系統。此平台強調資料的視覺化呈現，以及即時異常事件的偵測和告警，是 TWAREN 維運團隊用以監控與管理 TWAREN 100G 新骨幹網路之最佳的輔助工具。網管維運人員透過此單一整合式的視覺化監控平台，即可便捷地操作及使用介面的功能，並快速地掌握和追蹤整體骨幹網路的狀況，達到提早發現異常事件和解決異常事件之目的，提升維運的效率，同時提升整體網路的服務品質。

本系統未來發展方向將著重於配合 TWAREN 100G 新骨幹網路架構的頻寬或電路之調整，同步地進行平台監控項目的調校和擴充，以及平台操作功能的強化，並以準確且即時地提供異常告警資訊為首要目標，輔助 TWAREN 維運團隊持續地提供高品質且穩定的臺灣學術研究網路供 TWAREN 用戶使用。

參考文獻

[1] NCHC, TaiWan Advanced Research and Education Network, http://www.twaren.net/.

[2] 曾金山、劉德隆，「台灣高品質學術研究網路整合式監控平台之設計與實作」，TANET2007 臺灣網際網路研討會論文集。

[3] D3.js – Data-Driven Documents, https://d3js.org/.

[4] Highcharts, http://www.highcharts.com/.

[5] Bootstrap, http://getbootstrap.com/.

[6] CSS3, http://www.w3schools.com/css/css3_intro.asp.