二、 NMS/SEVER設備網管監控延伸授權

基於ITU-T定義FCAPS精神設計的 IT 資源營運的安全平台

ISOinsight 基礎一具基於ITU-T定義FCAPS與OAM設計的網管系統，再經由其他模組與核心引擎加持晉級至 IT 資源營運的安全平台管理系統，基本FCAPS各項管理詳述：(1)**警報處理(Fault Management)** – 提供管理者在視窗下(瀏覽器)有效管理並顯示來自被管理設備(IP設備)的所有警報和事件（通過EMS SNMP Trap/Event Log/LINE/mail/SMS接收），並將所有事件顯示在警報瀏覽器中，讓系統管理者即刻了解系統運作健康狀態。(2)**組態管理(Configuration management)** – 維護網路設備組態配置管理功能，包括：1. 藉由SNMP或SSH/telent編輯script自動設備軟體版本檢測管控。 2. NMS所管理的IP交換器(手動加入或自動檢測加入)，NMS並提供自動版本偵測功能。3. IP交換器資產摘要與組管理，資產與設定組態加密保存,可自動備份、比較設定組態功能差異，遇有差異可設定告警。4. 提供TFTP伺服器儲存網路設備映像檔管理與設定。(3)**設備帳務管理(Accounting management)** –系統內建collector/probe 收集單元職司設備或裝置資料蒐集，含有被動與主動收集方式：Passive Sensor - 職司被動資料接收，手段包括：ARP listen/DHCP sniffer/syslog/Network traffic probe/Packet mirror。Active Scanner - 職司主動資料獲取，手段包括：SNMP/Ping/SSH/Telnet/TCP hello/Http method/WMI/NMAP/ AD logger等，collector/probe 收集資料後再藉由辨識精靈自動賦與設備種類與屬性及品牌、韌體版本、序號進行設備資產建構管理，網管紀錄儲存與查詢。(4)**效能管理(Performance management)** – 以Web GUI網管網路設備與介面管理，監控交換器即時與歷史圖像、當日/周/月/年趨勢流量圖形、IP流量管理。針對效能管理系統內建介面管理與流量管理之外，另外安排NPM網路流量效能管理授權，提供進階IP流量效能分析，啟動netflow/sflow/packet mirror 1:1刻度netflow針對組織與組織之間或client/server之間的效能分析與異常分析。 (5)**網路通信安全管理(Security management)** – 提供用戶帳號集中管理Radius/TACACS+服務器，可以進行管理員系統本身與納管設備管理身份AAA驗證授權及操作紀錄之外，系統本身通過NCC資通安全防護認證。

關鍵特色

- ●VLAN網段自動建構拓樸,建構完整IT網路運作的全貌
- ●內網骨幹與聯外電路介面流量儀表板
- ●資產自動的獲取，減輕IT人員大量工作負荷
- ●圖形介面：以滑鼠及鍵盤操作拓樸圖、流量圖、事件等網管拖放，平移和縮放，彈出菜單，工具欄操作介面
- ●設備介面效能(Tx/Rx,error,廣播,丟棄)臨界值告警、長期圖表
- ●設備資源使用(CPU,RAM,I／O) 臨界值告警、圖表
- ●VLAN內廣播臨界值監視、排行、及告警
- ●事件源與異常設備、行為的追蹤
- ●支援叢集運算高可用性、高延展性巨量資料網路
- ●VM虛擬主機管理, 支援VMware vSphere, vCenter API虛擬伺服器效能(CPU, memory)與資產管理
- ●NPM網路骨幹介面流量、組織IP群組流量監視整合

圖形化的直覺拓樸圖導引

滑鼠及鍵盤拖放方式(Drag & Drop)視窗圖形提供中英文Web 2.0介面多視窗拓樸圖、流量地圖、事件地圖編修，藉由這些圖形動態顯示直覺的導引管理員一目了然整體系統與網路資源可用性, 包括設備介面埠運作狀態、設定、燈號、流量警示、事件發生的位置與資產等。

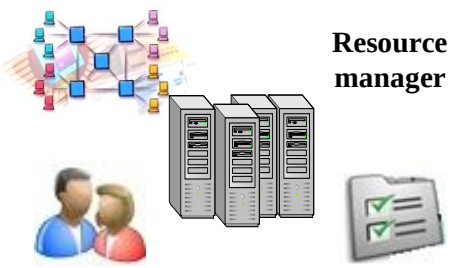
✓**向量拓樸圖** – 以台灣向量地圖顯示各個附屬邊緣運算/群組/路由器的地理位置與目前運作的狀態。

✓**拓樸圖** – 手動或自動收尋網路節點與裝置繪製、持續展示監控網路資源關聯與狀態, 包括layer 2/3 路由器、VLAN網段、IP 、交換器/介面/POE、主機等。這些關聯圖可以多個視窗方式來顯示不同群組設備的健康狀態、CPU%負載相關資訊。

✓**流量圖** – 以箭頭來表示網路骨幹介面上行與下行的流量資訊, 並以顏色及MRTG趨勢圖來表示目前流量離臨界值的狀態及當日的流量趨勢

✓**事件關聯圖** –自動持續監視網路節點之狀況與連結狀態，將網路設備以圖形(Icon)改變顏色變化來示警, 並直接可將事件相關聯, 協助管理員掌握事件發生的時間、內容、位置與處理的結果。並協助管理問題查找，如左上圖以拓樸圖提示問題來源, 並佐證相關環境資訊。

✓**儀表板** – 提供IP網路流量統計圖、服務儀表板、應用服務儀表板、機房設備與電路介面流量儀表板。



圖三. 2

資產、組織、拓樸管理

ISOinsight協助IT經理建構企業IT網路資源暨威脅監視的管理平台，提供『組織與網路』子系統協助管理者掌握企業行政組織與網路運作的關連，並提供企業IT運作設備資產即時報表、異動報表的資料庫管理，包括網路交換器、路由器、閘道器、伺服器、用戶主機等。而經由這些『基礎資料庫平台』便可以讓管理員透過『儀錶板』、『MAC/IP管理』、『流量及異常分析』等子系統來監視、控制、管理、追蹤Location tracking 網路行為與威脅防禦的管理，以幫助管理員稽核与管理網絡的安全。