網路監控系統如何進行設備傳輸管理

張潯福

影像監控網路設備管的傳輸管理事實上說起來是一件屬於IT網管的工作，與安防監控系統的本質原本並無太多直接關係，但包含後台的軟體管理在內，從監控及其它門禁報警等安防系統進入人工智慧數位化的架構後，我們在網路監控工程上再也無法與網路設備及網路傳輸管理這項工作劃清界線。

網路監控基本功-先瞭解監控應用網路設備

網路監控設備與網路管理優劣是影響網路整體執行成效的最大關鍵，也是影響網路監控系統效能最大的因素。何謂網路管理？簡單的說就是提升網路整體效率、可以簡單的做好路架構，讓IP監控設備IP CAM、NVR、Server及負載平衡設備、管理工作站、管理軟體及HuB、Switch及Router等設備可以透過網路管理工具即時瞭解網路運作的情形與效率，與維持高效能的表現，以保障網路傳輸品質這些工作都是安防監控網路管理環節，但要做好這些工作就必須要先透徹的瞭解網路設備的功用及運作功能，還有更重要的網路傳輸上的OSI網路七層協定應用原則及管理，首先讓我們先來瞭解網路管理基本設備有那些；一般應用於監控系統的網路設備大致上分為二類；一是區域網路使用的設備，也就是在監控上俗稱的內網架構設備。另一種是廣域網路設備，監控應用上也稱之為外網或跨網域網路架構設備，這二類設備產品分別也下列型式及功能：

一、LAN區域網路設備（Lan Network Equipment）

1. 中繼器（Network Repeater）：是一種用來增強網路傳輸訊號，以延伸訊號傳輸距離的裝置。由於每一種監控設備傳輸界面都有其最長傳輸距離的，一旦超過該距離，訊號即會衰減而無法辨識。因此必須透過網路訊號中繼器來加強訊號，以利影像或控制資料的傳輸延長。
2. 橋接器（Network Bridge）：這是一種屬於不同區域子網路接續連接的設備，它可以連接多個實體上分離的監控不同區域網路，使整個監控系統網路看起像是單一的運作網路。網路橋接器可以增加網路的可靠性、安全性及效率，是監控系統中網域與網域之間連接設備中最單純的設備。
3. 集線器（Hub）：在監控乙太網路中用來連接區域網路上所有IP監控的設備。這裡包含IP攝影機DVR或有像伺服器等。但接埠中；當監控設備中其中二個連接到集線器接埠上進行資料互相傳輸時，其它連接在其上的電腦工作站或監控設備便不能同時進行資料傳輸的工作。另外各監控設備及電腦工作站連接的設備可以形成星狀拓樸的區域網路，如此可以能擴充網路的節點，是監控系統上區域網路常見的網路設備。
4. 交換式集線器（Switching Hub，簡稱交換器）它的功能和集線器大致相同，也是用來連接區域網路上的監控設備。但交換器和集線器最大不同之處，在於交換器的任

意兩個連接埠在進行設備資料相互傳輸時，其它的連接埠也可同時間進行影像或資料傳輸的工作。此種交換技術可以讓頻寬給多個網路設備共享，線路交換與包封交換技術是兩種最基本的交換技術；在大型監控網路中，交換技術是必備的運用技術，而此種交換器就為交換技術而生的網路設備。

二、WAN廣域網路設備（Wan Network Equipment）

1. 路由器（Router）：它是一種提供資料傳輸路徑選擇的裝置，它可以連接多個不同架構的網路，並根據內部的路由表為資料封包選擇最佳的傳輸路徑，使資料能夠快速地送達目的地。屬於不同網域的網路連接一種設備，用在監控上可為不同監控子系統連網所應用。其基本功能是依照網路協定的標準，交換動態的路徑資訊，以決定送達目的地的最短路徑。路由器也可以視為區域網路與廣域網路之間的橋樑。
2. 閘道器（Gateway）：這是用來連接不同類型的子網路,讓使用不同通訊協定的網路，能夠相互傳送與接收訊息的裝置，屬於網路連接設備的一種，主要的功能是監控系統應用上，連接二個不同網域的異質網路，將傳輸的資料依網路協定做轉換的處理。一般而言，閘通道被視為一個網路的節點，在網路的組態上，同時也歸屬於多個相連的網路。

除上述二種網路設備之外，當然因應監控應用的網路設備還會有以下這些部份：

三、其他網路傳輸設備（others Network equipment）

1. 光數據機（Fiber Modem）：用來連接通信設備與監控設備，由於監控設備收發的是數位訊號，而通信設備傳送的是類比訊號，數據機必須要做這兩種訊號之間的轉換，才能讓監控設備或電腦訊號透過數據機及通信線路來傳送。
2. 終端伺服器（Terminal Server）：它主要是用做為大型監控主機與工作站，可以讓多人同時使用；因此數據機才可以連接上終端伺機器，提供多通訊路由，讓遙遠的數據機可以撥接建立連線。
3. 網路卡（Eathernet Card）：用來連接監控設備與電腦工作站與網路的連結，網路卡上有代表設備的實體位址。網路卡控制電腦工作站在網路上使用傳送訊號的方式。

以上都是我們在網路監控工程上經常且容易遇上的一些網路傳輸設備，對這些設備的使用瞭解江會大大助益於安防工程商在數位網路監控上的應用與管理工作，要做好網路設備的傳輸管理，除設備認知外對於網路管理的須求也必須略知一二，才不致於完全依賴IT人員來掌控系統網路管理，接下來我們就先來瞭解監控網路管理的需求有那些？

監控系統在網路傳輸管理的需求分析

監控系統在網路傳輸管理上的需求其實不多，主要在監控系統接入網路環境和核心網路環境時會存在比較大的差異，對於IT網管系統的要求相應存在一定差別，從監控應用的角度分析，目前的接入監控設備的網路管理設計應該至少滿足下列要求：

1. 實用化：網管系統的功能要依據監控用戶對網路運行維護的實際需求，與網路實際情況和具體管理工作緊密結合，不追求大而全的方式。

2. 高效性：能及時有效地發現網路傳輸運行中的故障並對其進行定位，以節省網路的運行維護成本，提高網路的運營質量。
3. 可擴展：網路的管理內容、管理方式是變化發展的，因此，網管系統的建設是持續、長期的，網管的建設應該注意可擴展性，保證在網路的規模擴大、網路的業務增長、網路的管理變動時，網管系統在較少的調整下仍然可以適用。

一個進步的監控網路傳輸管理解決方案應該具有高性價比、實用性、多設備集中統一管理的特點。在通過友好的人機界面可實時高效的掌握設備的運行情況，隨時查看網路設備，並對其故障進行處理。通過數據庫管理系統，可以對各設備的告警信息，狀態信息和性能信息進行統計、匯總、分析，為設備維護人員實時進行設備集中監控，盡快查找故障原因，保障網路正常運行，提高工作效率，提供了先進的手段。

監控網路架構下如何做好傳輸管理

網路傳輸等管理議題經常在監控工程與網管人員之間討論不休，例如網路效能不佳影響監控系統整體動作、網路頻寬不足造成影像延遲或劃片張數不足、還有影像封包丟失現象產生等等問題，如何了解到網路是否發生過這些現象，有沒有方法可以將網路的運作狀態予以透明化，也困擾著大家。

本文中將會以網路傳輸穩定度的觀念來建立起一套量測網路是否健全運作的方法，透過網路穩定與健康度指標的訂定，IT網管人員可以隨時知道監控網路現在運作的效率是否正常，當問題發生時候可以透過各項網路效能趨勢圖形了解到確實問題發生在哪個網段、甚至於在那一個網路介面或節點，若問題發生在特定的控制接埠，系統應該可以直接設定該埠跳開以讓使用者繼續正常存取網路監控資訊，要做到網路傳輸管理與問題排除，避免整體網路崩潰；此時就要進行更深入的網路傳輸問題分析，可以透過網路設備的自動產生的補捉（Trap）及系統日誌（System log）訊息，進行更深入的分析；如此可以將網路管理制度與標準化，降低網路除錯時間，提升網路整體傳輸的使用度。

不同的監控設備要進行通訊時候，必須要透過網路來傳遞網路封包，而建構網路必須透過網路設備將這些網路連結起來；當網路上的交易或者檔案傳輸上發生了問題，就會變得非常難以分析出問題產生在哪個地方，究竟是Client的電腦設定問題，或者是監控伺服器端的負載過重，而單憑直覺就只能說網路又當掉而已。

網路傳輸管理獲得所有的異常發生時間點大都是過去式，應用系統產生異常或者無法連線，大都會歸咎於網路的問題，而在異常發生當時的時間點，究竟網路上有沒有發生任何異常行為，可能沒有任何一人可以知道；假設當網路頻寬不足、發現大量的不正常異常流量時候、出現超乎大量的廣播封包，若能即時通知相關人員作準備或預防，也可以大幅降低IT系統不正常運作而帶來給內部或外部客戶不方便。

其實這些問題可以透過具有網管功能之網路設備來協助解決這些問題，這些網管型的網路設備都會提供SNMP、System log、Trap功能來強化網路管理，透過這些標準網路管理協定幫助，我們可以蒐集到更多相關網路運作的情況以及當時可能異常發生真正原因。

在網路傳輸環境中，透過OSI 7 Layer模型分工傳輸方式，而透過標準SNMP MIBs可以蒐集第二、三層網路傳輸運作情況，選擇採用第二、三層做為網路健康度監控指標的目的在於在網路傳輸過程中，最後都需要透過OSI第二層的方式將網路框架做適當的切割，以便適應在不同的網路實體架構下進行傳輸，對於網路架構與實體設備上是否發生的問題，透過此一方式來觀察是最恰當不過的。

我們需要了解到每個網路介面（Interface）的相關運作效能，這些項目包括了：網路介面的流進/流出流量、封包、廣播封包、錯誤封包、忽略封包，這些項目使用數量多寡會影響到使用這台網路設備上全部使用者運作效能，情況嚴重下會擴展到整個企業網路的運作效能，這份文章也會探討每個項目影響層面有多大，問題可能發生在哪個點，要做哪些應對處理措施，日後要如何避免這些問題再度發生。

網路傳輸管理可以透過以下各項效能指標讓我們對問題做更清楚分析：

1. 是否有網路攻擊行為發生？
2. 網路整體設備的頻寬是否足夠？
3. 是否有封包遺失現象產生？
4. 網路應用程式傳送時間變慢？
5. 網路伺服器及主設備的CPU使用率是否過高？
6. 是否可以提升整體網路可用度與降低網路當機次數？
7. 是否可以及早發現網路上潛在問題，避免更大的網路異常發生？
8. 是否可針對過去歷史訊息進行分析，快速找出網路問題？
9. 是否有警訊提醒機制，當異常發生時可及早預防？
10. 可以訂定網路效能指標，訂出傳輸管理效能標準。

具體改善監控網路設備與傳輸管理四法則

以上是十個針對網路設備與傳輸管理的執行問答措施做法，當我們決定開始要針對現行網路環境開始進行管理與監控時，並不是僅要購買或者從網路上隨便抓取一套網管軟體直接安裝起來就可以開始進行網路管理的，我們需要作事前的規劃與準備，而且了解到我們管理需求是要這些軟體幫助我們解決哪些問題，從網路協定OSI 7層架構來看，是要做到全面性網路協定分析，做好網路傳輸流量統計與分析方面，另外還有應用程式服務的可用度監控等等，才能落實監控工程上網路，設備與傳輸管理工作。這部份還有4個方法可以協助做好上述10個系統檢測問答，這四種乙太網路管理的程序方法是：

1. **選擇具有網管功能的設備：**為了要能夠更詳盡了解網路上運作情況，最佳方式就是透過具有網路管理功能的網路設備，監控網路設備運作效能與各種產生自網路設備上的錯誤或異常訊息，避免網路因為這些異常事件持續發生而導致網路整體效能嚴重降低，甚至產生網路無法正常運作或癱瘓情況發生。
2. **對每台監控及網路設備進行時間校正：**為每台網路設備進行時間校正對於網路管理工作上是非常重要的，而且這也是大多數廠商在幫客戶架設網路設備而不會主動做的工作，由於中高階的網路設備在遇到網路上有異常或衝突情況發生時候，都會有系統記錄System log產生，這些記錄都會儲存在網路設備本機，降低問題除錯複雜度；所以網路設備一定有時間校正設定機制。
3. **啟動網路設備SNMP管理功能：**接下來工作就是要進行啟動各網路設備的網管通訊協定功能，這裡建議要啟動三項支援網管使用的通訊協定：SNMP，SNMP Trap，System log。當啟動了這三項網管通訊協定功能，網管主機便可以讀取這些系統或設備上效能資料，並且接收所有的訊息與事件，找出問題發生的原因與來源，並改善這些問題。
4. **開始收集各項設備穩定與健康度：**在此我們定義的監控系統網路穩定與健康度是由兩項指標所組成，第一個是網路運作效能，第二個是網路設備的CPU使用率。特別是CPU的使用率高低會嚴重影響到整體網路運作的效能，故需要將此列入網路傳輸穩定與健康度觀察項目。

最後本文要說明的是網路設備與傳輸的管理工作本來就不是電信弱電工程商專業的部份，筆者也是抱著小心謹慎的態度來探討這些問題，期盼讀這先進多予指導指正。同時也引用很多先進前輩的說法及經驗在內，希望透過這些內容可以讓有心在電信監控系統作上更精進於網路管理工作，也讓電信廠商碰到的監控網路設備管理的問題解決與系統應用有所啟發，共同為監控網路管理工程貢獻所知所學。