建置於 TWAREN 之防災專屬網路架構設計及效能品質量測

古立其 李慧蘭 陳敏
財團法人國家實驗研究院國家高速網路與計算中心
{ lku, gracelee, minchen}@nchc.org.tw

摘要

台灣雨量豐沛，又位處於颱風地震頻繁的地區，因此防災防洪能力的提升刻不容緩。藉由新世代高速網路及各式嶄新的網路技術，使防災作業所需的各式觀測資料及各地防災水利單位能有效溝通傳遞，迅速對災情做出反應，則為防災能力提升至為重要的一環。本研究針對防災網路的獨特需求，以 VPN 技術搭配台灣高品質學術研究網路 (TWAREN) 骨幹，設計出高可靠性、高安全性的防災網路架構，並針對防災作業的網路特性設計適合防災網路的網路效能品質量測機制，以期能有效提升台灣防洪防災作業效率，使台灣防災作業品質藉由新世代的網路技術得以大幅提升。

關鍵詞：臺灣高品質學術研究網路、虛擬私有網路防災網路。

Abstract

Taiwan is a subtropical island with abundant rainfall and natural disasters. The key to the mitigation of the impact of the natural disasters is the ability to efficiently collect the disaster observatory data and to smoothly communicate among those disaster mitigation agencies. The introduction of the next generation network technology shows a very promising potential on this issue. This study aimed at designing and implementing a highly reliable and secure disaster mitigation network addressing the special needs of guaranteed quality under extreme conditions and disasters. A measurement method was developed to evaluate the performance of the disaster mitigation network in the way that matchs the unique characteristics of the disaster mitigation traffic.

Keyword: TWAREN 、 VPN 、 Disaster Mitigation Network。

1. 前言

台灣屬於亞熱帶海島型氣候，平均年雨量為 2470 mm，在山地的平均年雨量甚至高達 4892mm[1]。由於台灣地形陡峭，這些豐沛的降雨會在短時間內匯集到低窪的谷地及盆地，極易造成水患。台灣近幾年來山地開發過度，集中的降雨更可能直接沖刷缺乏植被保護的表土，造成大量土石沿著坡度滑動，形成土石流，造成更大的安全隱憂。面對水患和天災的威脅，隸屬於經濟部的水利署[2]成為事前防災，事後抗災的第一線單位。水利署在各縣市佈有河川局及水資源局，負責河川水位、水文觀測、雨量偵測、災區影像監控等工作。這些收集得來的第一手資訊則進一步匯整到水利署防災中心，以便對可能的災情迅速研判並做出適當的防災或抗災反應。

在此之前，水文及災情資訊的收集主要仰賴人工以電話回報。雖然有部份數位資訊透過網路送回資料庫儲存，但主要是做為事後數值分析之用，對即時的資訊取得幫助有限。以防災的角度而言，這樣的資訊收集模式不但過於被動、不夠即時，而且並不可靠。特別是當某個單位的電話線路已因為災情而斷線時，災情中心並不能立刻發現。此外這種資訊傳遞的方式所能傳達的資訊，不論種類或量都十分有限，大大限制了防災中心正確且快速針對災情做出反應的能力。因此建置一個可靠、安全並且高速的防災網路平台，實是刻不容緩。

2. 防災專屬網路之規畫與設計

2.1 防災專屬網路之特殊需求

由於天災發生時往往伴隨著停電、線路故障、道路橋樑受損、無線訊號不良等惡劣狀況，再加上防災作業的資訊傳遞需求往往在受災時高度集中，因此防災專屬網路必須具備以下特殊條件：

(1) 多重異質傳輸媒介互為備援

為免天災發生時，同一種類的傳輸通道同時失效，因此防災網路必須由多重異質的傳輸媒介所構成，並且互為備援，以確保在天災發生時的可靠性。

(2) 低傳輸延遲

由於水利署各河川局及水資源局遍佈全省各地，不僅數量眾多而且地理分佈十分零散，因此防災網路必須能確保傳輸的延遲時間低且一致，以使災情影像及視訊會議能獲得理想的品質。

(3) 高頻寬

防災網路的流量將高度集中發生在天災發生的期間，特別是天災發生的初期。而視訊的傳輸又具備 burst 的特性，因此防災網路必須擁有高頻寬的傳輸能力，以使天災發生時的資訊能準確的傳送至目的地。

(4) 高度的安全要求

由於部份防災資訊具備機密性，而維持系統不被駭客侵害，同時也是保障整個防災

網路在天災發生時能可靠運作的必要條件，因此防災網路必須具備高度的安全性。

(5) 高品質的網路維運

防災網路必須具備良好的維運品質，主動發現並預防任何可能的問題，以確保在天災不預期發生時，防災網路永遠能成為防災作業啟動時可靠的平台。

一個理想的防災網路必須能滿足上述條件，才能確保在天災發生時，能有效的提供可靠的服務，使防災作業得以順利進行。

2.2 防災專屬網路之網路架構

本研究採用台灣高品質學術研究網路(TaiWan Advanced Research and Education Network; TWAREN)[3] 做為防災專屬網路的骨幹。TWAREN 具備極高的頻寬，而且在全省各地均有網路接取點 (GigaPOP) 可以提供連線服務，更可以視需要提供第六代網際網路協定 (IPv6)、群組廣播 (Multicast)、多協定標記交換 (MPLS/VPLS)、甚至光通道網路 (Lightpath) 的服務，非常適合防災網路所需的特性及未來持續擴充的需要。藉由租用 100 Mbps 至 1 Gbps 頻寬的都會型網路 (Metropolitan Area Network; MAN)，每個水利署單位均使用雙實體線路連上最近的 TWAREN GigaPOP，防災網路的實體連線即得以順利完成，如圖 1 所示。

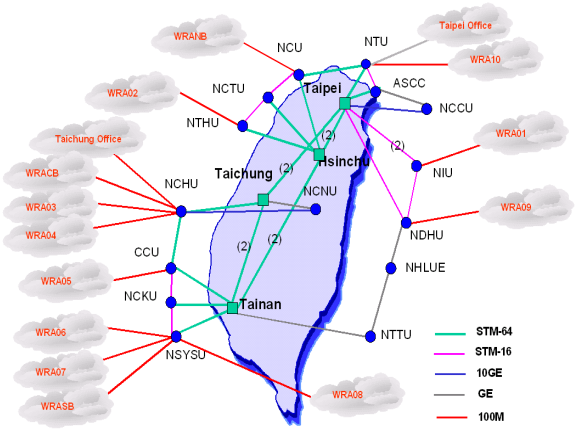

圖 1 防災專屬網路線路架構圖

為了達成防災網路所需的安全特性，我們使用在各個河川局所建置的防火牆建立 IPsec VPN 連線，如圖 2 所示。每個水利署的單位均建立兩個 IPsec VPN 通道，分別連往水利署台北辦公室及位於新竹國網中心機房的異地備援中心。數位化的水情資料即依此 VPN 通道送往台北辦公室的資料庫進行匯整，並同時備份至異地備援中心的資料庫中。視訊會議的資料則經由台北辦公室的 bridge server 轉接，再分送至目的地。同樣的 bridge server 亦在異地備援中心進行建置，當位於台北辦公室的主要 bridge server 失效時，即可以位於異地備援中心的備援主機取代。所有往返 Internet 的網路流量均經由位於台北辦公室的 proxy server，再循台北辦公室這個唯一與 Internet 相接的端點連入 Internet。在此架構下，所有的水利署單位均僅與台北辦公室及異地備援中心相連，彼此之間完全隔絕，而通往 Internet 的流量則分別經過各自的防火牆及台北辦公室的防火牆方與外界相連，最終得以確保整體防災網路擁有最高的安全保障。

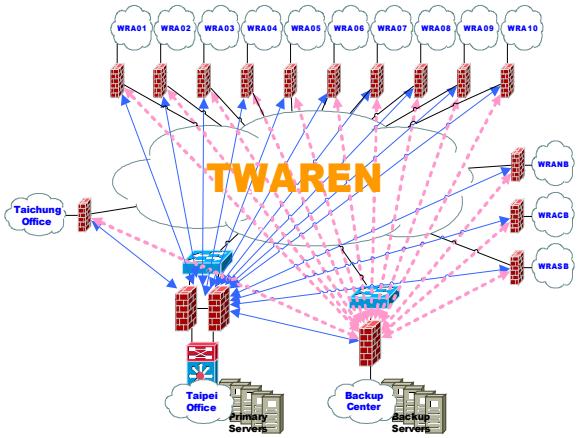

圖 2 防災專屬網路邏輯架構圖

各水利署單位除了使用 TWAREN 做為防災網路主要的傳輸平台外，也同時採用政府服務網路(Government Service Network; GSN)、GSN VPN、微波通訊系統 (Micro Wave; MW) 及衛星通訊系統 (VSAT) 進行異質傳輸媒介備援，如圖 3 所示。

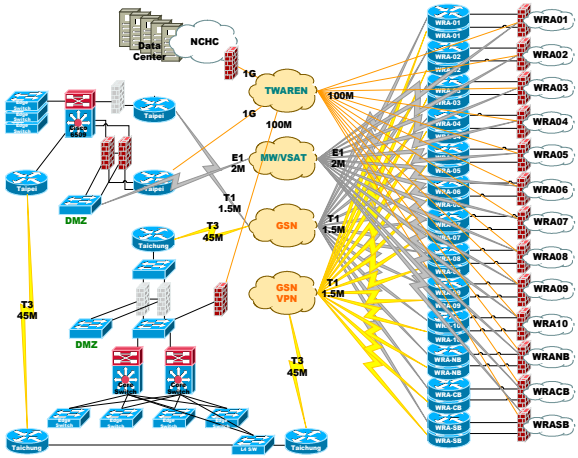

圖 3 防災專屬網路的多重異質備援邏輯示意圖

其中 TWAREN 及 GSN 連線分別為不同上游、不同線路供應商、實體線路各異的光纖網路，而微波系統及衛星通訊系統則分別為使用微波站及衛星居中傳遞的通訊媒介。此四種不同的傳輸媒介不論是實體的傳輸路徑或是傳輸的方式均彼此不同且獨立運作，因此具備極高的異質備援特性，大幅提高了防災網路在天災中的可靠性。

防災網路的維運工作則交由 TWAREN 網路維運中心 (Network Operation Center; NOC) 所提供的 24 小時網路維運服務協助負責。除了提供網路的流量統計外，還有專人負責線路故障偵測及告警，

確保防災網路能保持在最佳狀態，隨時在天災發生時提供最可靠的服務。

藉由防災網路所採用的多重異質備援、高頻寬的連線、就近接取 TWAREN GigaPOP、完全隔離的邏輯網路架構設計以及全天候的網路維運服務支援，確保了防災網路能在最惡劣的條件下，成為防災工作可靠的平台。

3. 網路效能品質量測

防災網路所承載的網路流量組成，與以 TCP 為主要傳輸協定的一般商業網路有很大的不同。防災網路的主要流量來自各水利署單位間的高畫質視訊會議系統及各地的災情影像觀測站。這些視訊的網路流量採用的是架構於 UDP 上的即時傳輸協定 (Real-time Transport Protocol; RTP)，相對之下數位水文觀測資料庫系統所使用的 TCP 傳輸僅佔極小的部份。由於 UDP 網路傳輸不具備 TCP 的錯誤重傳、循序抵達特性，而網路視訊的品質卻極易受到封包遺失 (Packet Loss) 及非循序抵達 (Out of Order Delivery) 的影響而劣化，因此在現今網路設備均以 TCP 為主要考量的情況下，發展適當的方法檢測防災網路的 UDP 效能，便成為檢驗防災網路是否符於所需的重要課題。在本研究中，我們選用了 iperf[5]及 tptest[6]兩個工具來進行 UDP 的有效最大傳輸頻寬及非循序抵達封包比例的量測，並同時併用 ping 工具來進行網路品質的長時間追蹤。

3.1 iperf

Iperf 為 NLANR 所開發的 OpenSource 網路效能量測工具，同時支援 IPv4 及 IPv6，並能進行 TCP 及 UDP 兩種協定的頻寬量測。在目前 UDP 網路效能量測工具相對缺乏的環境中，iperf 是一個可靠、準確、跨平台而且使用容易的優秀工具。

Iperf 使用 Server-Client 的架構，在單向測試中由 Client 端向 Server 端傳送指定速率的 UDP 流量，由 Server 端回報實際接收到的資料量、平均速率、非循序抵達封包比例等測試結果。Iperf 亦提供雙向測試模式，即 Client 端及 Server 端都同時開啟一通訊埠接收對方傳來之 UDP 流量，同時以另一通訊埠向對方傳送 UDP 流量。然而在先前的實驗中發現，iperf UDP 雙向模式的行為及其結果與本研究所需不同，因此本研究採用的方法為同時在待測線路兩端的主機中執行 Server 及 Client 模式的 iperf，以 ssh 的方式遙控兩端 Client 模式之 iperf 同時向對方的 Server 模式 iperf 進行單向 UDP 測定，亦即同時使用兩個相反方向的單向 UDP 測定來構成一個實質的雙向 UDP 流量測試。

3.2 tptest

在先前的實驗中發現，iperf 所回報的非循序抵達封包比例與本研究所需不同。在視訊會議及影像觀測系統中，接收到的視訊資料會直接送入影像解壓縮模組中進行畫面的解壓縮及繪製。一旦資料未循序到達，即順序較後的封包比順序較前的封包先到達時，所有順序被超越的較前封包即使事後依然抵達，亦會因為資料對解壓縮模組而言已經過時，而被解壓縮模組直接丟棄，形成對解壓縮模組而言的實質封包遺失。這同時也是 tptest 對未循序抵達封包的判定方式，因此本研究選用 tptest 進行防災網路的未循序抵達封包比例測定。

Tptest 最初為 Swedish ICT-commission 所發展的網路測試工具，後來轉化為 Sourceforge 的開放軟體專案之一。其使用較為複雜，且穩定度較差，因此雖然 tptest 亦具備 UDP 流量的測定能力，在本研究中僅用於未循序抵達封包比例的測定。

3.3 實驗環境及測試方法

為了確保整體網路平台的品質及效能合於防災作業的要求，本研究在完成建置的水利署防災專屬網路實際環境中進行網路的測試及驗證。由於本網路平台已上線使用，為避免干擾相關作業的運作，因此本研究避開各連線單位至水利署台北辦公室的主要線路，選擇架構相同的各連線單位至異地備援中心的備援線路進行各項測試，其架構如圖 4 所示。

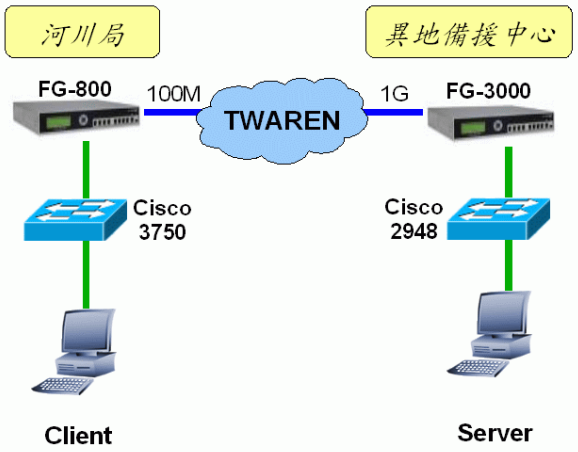

圖 4 防災專屬網路測試架構圖

Server 端置放於異地備援中心機房內，Client 端則攜帶至受測之水利署連線單位，各與防災專屬網路防火牆後之交換器連接。其配備及作業系統重要設定如表 1 所示。

由於筆記型電腦 CPU 時脈較低，進行網路傳輸時來自網路卡的中斷(Interrupt)處理負荷較大，往往排擠位於 User Space 的 iperf 所能獲得的 CPU 時間，造成 iperf 送出的有效流量受限，因此在 Client 端啟動 Kernel 的 Device Polling 機制，並加大系統 sysctl 變數 kern.polling.each_burst 至 50、並將 kern.polling.burst_max 加大至 300，系統處理頻率 HZ 則設為 1000，以確保 CPU 時間能在 Kernel 及 User Space 中合理分配，使 iperf 能達成的實際

輸出頻寬達到最高。兩端 iperf 的參數如下：
Server: iperf -u -s -w 196k
Client: iperf -u -c Server_IP -w 196k -t 30 -b 流量

每次測試時先以預定的流量進行 3 秒之預測試，隨即進行兩次 30 秒之正式測試，並將兩次測試之封包遺失率結果取平均值，做為該流量下之封包遺失率結果。為免影響水利署單位之正常作業測試頻寬定為 10 Mbps、20 Mbps、30 Mbps、40 Mbps、50 Mbps、70 Mbps、90 Mbps 共七段。

表 1 測試主機配備及設定比較表

	Server	***Client***
硬體機種	HP DX2000 MT	IBM T42
作業系統	Fedora Core 5	FreeBSD 6.2
系統設定	預設值	ifconfig em0 polling sysctl kern.polling.each_burst=50 sysctl kern.polling.burst_max=300

3.4 測試結果

Iperf 的測試結果如圖 5 所示。當雙向 UDP 流量達到 70 Mbps 及 90 Mbps 時，UDP 封包的遺失率仍幾乎為零 (實線及實心圓點)。即使在雙向 UDP 測試中開啟 Access Grid 視訊會議系統，產生額外的 1-30 Mbps 實際視訊 UDP 流量時，雙向 70 Mbps UDP 流量測試中的封包遺失率仍僅為 0.64%，而在雙向 90 Mbps UDP 流量測試中亦僅為 2.4% (圖中虛線及空心圓點)。

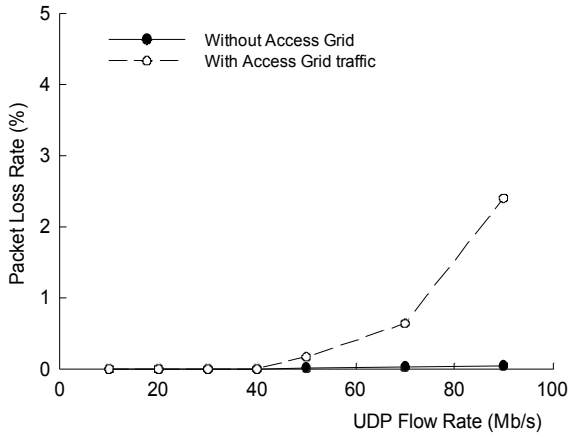

圖 5 雙向 UDP 流量與封包遺失率關係圖

所有測試中，封包幾乎均觀察不到非循序抵達的現象 (未在圖中顯示)。此結果顯示，本研究所建置完成的防災網路非常符合目前防災作業的需求。

4. 結論

本研究所完成的水利署防災專屬網路具備高度的異質備援能力，確保了整體系統在天災中的最高可用性，而水利署各單位間的網路架構完全隔離、配合單一 Internet 出口的設計，亦使安全性得到良好的保障。藉由本研究所提出的量測方式，網路效能亦在實際的環境中，以近似於防災作業實際網路特性的方式得到驗證。最後通過 TWAREN NOC 的 24 小時監控維護，本防災網路平台得以隨時保持在最佳待命狀態。

防災網路的建置提供了經濟部水利署水患災害防治與通報的平台，其架構於端點對端點的 IPsec VPN 上，但隨著防災作業的逐漸精緻化，未來在此平台上必然會導入更多新式的防災資訊收集機制，並隨之產生日漸可觀的網路頻寬需求。Palmieri[7]在其研究中提出，MPLS VPN 在 Gigabit 等級以上的光網路中將擁有比 IPsec VPN 更佳的效能，因此未來我們亦希望利用 TWAREN 骨幹建置 MPLS VPN，利用 TWAREN GigaPOP 路由設備建置 MPLS edge router(PE)，可以大幅減低硬體設備與人力維護成本。MPLS VPN 提供服務品質保證 (QoS)，可以大幅提升超級視訊格網(AG)的網路品質和穩定性。

效能品質量測工具已完善應用於 IPsec VPN 的環境中，待未來 MPLS VPN 建置完成後，可以有效的開發一套整合性的網路效能品質量測工具，以驗證大量視訊串流流量下的網路服務品質。

參考文獻

[1] The statistics of Taiwan climate from year 1971 to 2000, http://www.cwb.gov.tw/V5/climate/statistic/avg.htm , last viewed on Jul 6, 2007.

[2] Water Resource Agency, http://www.wra.gov.tw/ , last viewed on Jul 6, 2007.

[3] TWAREN, http://www.twaren.net/english/ , last viewed on Jul 8,2007.

[4] GSN, http://gsn.nat.gov.tw/eng/index.html , last viewed on Jul 8.2007.

[5] NLANR, Iperf, http://dast.nlanr.net/Projects/Iperf/ , last viewed on Jul 8, 2007.

[6] TPTEST, http://tptest.sourceforge.net/ , last viewed on Jul 8, 2007.

[7] Palmieri, F., "VPN scalability over high performance backbones evaluating MPLS VPN against traditional approaches", vol 2, pp 975-981, ISCC 2003 Proceedings, 2003.