

在電信乙太網路中提供高可用性及動態頻寬調整的 Triple Play 服務

張阜民¹ 鄭昆樺² 高勝助³

¹朝陽科技大學財務金融系

41349 台中市霧峰區吉峰東路 168 號

²中華電信南台灣服務中心

403 台中市市府路 37 號

³中興大學資訊科學與工程系

402 台中市國光路 250 號

摘要

隨著結合語音、視訊與數據的三合一 (triple play) 服務逐漸成熟, 如何建構一個具備穩定傳輸品質的服務網路架構, 是電信業者一直努力研究的課題。在本文中, 我們提出一個在電信乙太網路 (Carrier Ethernet) 下, 具備頻寬管理及高網路可用性的 Triple play 服務網路架構。此架構包含存取網路與 IP/MPLS (internet protocol/multiprotocol label switching) 核心網路。在存取網路中, 我們將匯集在一條實體乙太網路線路的 Triple play 服務, 利用虛擬網路 (virtual LAN, VLAN) 的技術將各服務虛擬隔離。為有效利用網路頻寬, 我們提出一服務限速結合監控管理的機制, 透過策略決策路由器 (policy decision router, PDR) 佈置, 動態調整各服務的限速, 讓使用者未使用的閒置頻寬得以有效利用, 並且讓各項服務品質獲得保證。為了提高網路的可用性, 我們在 PDR 的上鏈路中導入多機箱鏈路聚合 (multi-chassis LAG, MC-LAG) 機制, 以避免單一節點失效的問題。此外再經由多條虛擬專用區域網路服務 (virtual private LAN service, VPLS) 建立備援電路, 並導入雙向轉發檢測 (bidirectional forwarding detection, BFD) 第三層連通性測試機制, 讓我們能夠及早發現核心網路中斷處。並經由 node-level 與 pseudowire-level 保護機制的運用, 提供網路中斷快速回復的特性。為驗證所提架構的可行性, 我們進行許多的模擬實驗, 並比較傳統路由機制與所提的機制。模擬實驗發現, 目前常用路由資訊協定 (routing information protocol, RIP) 及開放式最短路徑優先協定 (open shortest path first, OSPF) 的收斂時間, 各需要 180 秒及 30 秒, 並無法滿足我們對於 Triple play 服務中斷快速回復的要求, 而我們所提之結合 BFD 與靜態路由協定的設定, 只要 1 秒就可以發現網路發生中斷處, 進而切換至備援路由。此外應用 MC-LAG 機制, 只要 2 秒就可將訊務移轉至另一個網路節點。因此藉由各種機制的運作, 本文提供滿足在電信乙太網路上穩定有效益的 Triple play 服務。

關鍵詞: 三合一服務, 電信乙太網路, VPLS, BFD



Providing High Availability and Dynamic Bandwidth Allocation for Triple Play Services over Carrier Ethernet

FU-MIN CHANG¹, KUN-HUA CHENG² and SHANG-JUH KAO³

¹*Department of Finance, ChaoYang University of Technology*

168 Jifong E. Rd., Wufong District, Taichung, Taiwan 41349, R.O.C.

²*Southern Taichung Service Center, Chunghwa Telecom*

37, Shihfu Rd., Taichung, Taiwan 403, R.O.C

³*Department of Computer Science and Engineering, National Chung-Hsing University*

250, Kuo Kuang Rd., Taichung, Taiwan 402, R.O.C

ABSTRACT

With the rapid growth of triple play (voice, video, and data) services, constructing a service network architecture with stable transmission quality is an urgent research topic. This paper proposes a triple play service network architecture with dynamic bandwidth management and high network availability over Carrier Ethernet. The proposed architecture consists of access networks and the IP/MPLS core network. In the access network, the traffic of triple play services in the same truck are virtually isolated using virtual LAN (VLAN) technology. To utilize the network bandwidth, a monitoring and control mechanism via a policy decision router (PDR) to dynamically adjust the bandwidth allocation for each service is adopted. To improve network availability, a Multi-Chassis Link Aggregation (MC-LAG) mechanism is introduced in the uplink route of PDR to prevent disconnection due to a single node failure. Establishing multiple VPLSs (virtual private LAN services) in the IP/MPLS core network and equipping a bidirectional forwarding detection (BFD) mechanism enables prompt discovery of the network disconnection. Through the application of both node-level and pw-level (pseudowire-level) protection schemes, a rapid network recovery can be facilitated. To verify the applicability of the proposed architecture, several experiments were conducted. Various routing mechanisms were tested since the discovery of route disconnection in the IP/MPLS core network is a complex and time-consuming task; for example, RIP requires 180 seconds while OSPF only requires 30 seconds to discover a network disconnection. A detection mechanism is developed by combining a static routing protocol and BFD mechanism. Using this mechanism, a disconnection in the IP/MPLS core network can be located in one second. Moreover, using the MC-LAG mechanism, the traffic can be redirected from an inactive node to the standby node in two seconds. The simulation results demonstrate that the architecture proposed in this study is suitable for triple play services.

Key Words: triple play, Carrier Ethernet, VPLS, BFD

一、緒論

隨著網際網路技術的快速發展，許多電信業者已經利用網際網路提供語音、視訊及數據傳輸等服務。目前透過專屬網路傳遞服務至用戶家中的運作方式，雖然可以確保各服務的服務品質，但專屬網路建置與維護成本太昂貴，造成消費

者無法享受較廉價的服務。因此，整合語音、視訊與數據等服務於單一網路傳遞的 Triple play 服務，已經成為次世代網路的重要應用。Triple play 服務在次世代網路中是由 IP 多媒體子系統 (IP multimedia subsystem, IMS) 所主導，舉凡服務的提供、信令的建立、服務品質的保證、記帳等都是 IMS



龐大系統中的子單元。但 IMS 是開放式系統，整合不同廠家所開發的 IMS 是一大問題，再加上功能相當複雜，所以開發進度相對落後，因此以 IMS 為基礎的 Triple play 服務一直未能推出 [18]。

目前國內大部份的電信業者，其核心網路已經提升為次世代網路或網際網路協定/多重協定標籤交換 (internet protocol/multiprotocol label switching, IP/MPLS) 網路，但用戶端接取技術仍舊是使用傳輸頻寬最高為 55.2 Mbps 的數位用戶迴路 (digital subscriber line, DSL) 技術 [16]，來提供 Triple play 服務。在 Triple play 服務中，以視訊的頻寬需求最大 [20]，一個標準解析電視 (standard definition TV, SDTV) 頻道的頻寬大約需要 3 Mbps，一個高解析電視 (high definition TV, HDTV) 頻道的頻寬則大約需要 15 Mbps，若有三台電視要收看不同的頻道就需要三台機上盒 (setop box, STB)，因此整個 Triple play 服務的總頻寬必然會大於 DSL 技術所能傳輸的最大頻寬，這也是國內網路電視 (IPTV) 服務業者針對單一用戶只提供一台 STB 的原因之一。為了解決此問題，近年來電信業者紛紛積極投入佈建電信乙太網路。其主要原因是由於乙太網路是近 30 年中最成功且佔有率最高的區域網路技術，目前幾乎所有的網路設備都將乙太網路視為標準介面。電信乙太網路的成本效益高，傳輸速率非常有彈性，最低 10 Mbps，最高可達 100 Gbps [10]。

在本文中，我們設計一個利用電信乙太網路為基礎，傳遞 Triple play 服務的機制。我們利用乙太網路作為用戶接取的介面，以虛擬網路 (virtual LAN, VLAN) 的技術將各服務虛擬隔離，達到在一條實體電路上同時提供 Triple play 服務。但我們發現，雖然乙太網路可以滿足 Triple play 服務對於頻寬的需求，但各服務對於網路品質的要求未必相同。我們嘗試利用 IEEE 802.1p [6] 所提出的機制將各種服務設定不同的優先順序，但經由實驗結果 (詳細結果列於第四節) 發現，此種方式並不適合 Triple play 服務。因此在本文中，我們在電信乙太網路中佈署策略決策路由器 (policy decision router, PDR)，利用限速 (rate-limit) 機制讓各項服務品質獲得保證。我們進一步觀察發現，雖然限速機制可讓 Triple play 服務的服務品質得到保證，但是大部份使用者對於視訊服務，並非 24 小時都在使用。為有效利用使用者未使用的閒置視訊頻寬，我們於策略決策路由器 (PDR) 設計一個回應時間報告 (response time reporter, RTR) 監控模組，定期偵

測使用者是否有在使用，在不違反服務水準協議 (service level agreement, SLA) 的原則下，動態調整各服務的限速，讓使用者申請的頻寬有效利用。

在另一方面，Triple play 服務大多是即時性的應用，一旦網路發生問題，若無法快速回復，勢必造成服務中斷。然而目前電信乙太網路並未制定完整而健全的營運管理維護 (operations, administration, and maintenance, OAM) 機制，雖然已經有一些電信乙太網路的 OAM 標準被定義出來，但是各家廠商對於標準的支援程度不一。在本文中，為使骨幹網路達到快速回復，我們在 PDR 所介接的上鏈路中導入多機箱鏈路聚合 (multi-chassis LAG, MC-LAG) 機制 [3]，分別與不同的邊界路由器 (border router, BR) 相連接，以避免單一節點失效。此外再經由多條虛擬專用區域網路服務 (virtual private LAN service, VPLS) [1] 建立備援電路，增加核心網路的高可用性。由於 VPLS 是屬於第二層的虛擬電路，一旦核心網路發生中斷將無從得知，因此需要透過路由協定來發現網路發生中斷。但由實驗結果發現 (詳細結果列於第四節)，透過路由協定發現中斷，需要一些收斂時間，而目前常用路由協定路由資訊協定 (routing information protocol, RIP) 及開放式最短路徑優先協定 (open shortest path first, OSPF) 的收斂時間並無法滿足我們對於 Triple play 服務中斷快速回復的要求。因此我們在 PDR 中，導入乙太網路 OAM 機制的雙向轉發檢測 (bidirectional forwarding detection, BFD) 第三層連通性測試機制 [2, 4]，經由 BFD 的偵測可快速發現骨幹網路發生中斷處，進而將訊務切換至其他正常的 VPLS 線路達到快速回復的要求。

本文提出在電信乙太網路中以 VLAN 方式匯集提供 Triple play 服務，利用乙太網路方式接取，存在比目前常見的 DSL 方式接取的優勢，例如有效改善最大電路頻寬的限制。相較於其他研究，如 Zhang 等人 [22] 利用被動光纖網路 (passive optical network, PON) 技術來提供服務，他們將 Triple play 服務分成不同的光波長透過同一條光纜傳送至用戶端，再透過不同的光纖網路單元 (optical network units, ONU) 將服務分離出來。這種方法和本研究有點類似，但是本研究建置成本相對低很多。而 Sotiropoulos [19] 發表利用 Common DiffServ 方法提供 Triple play 服務，他們利用 Queuing 的方法對服務進行分級。由於此篇論文是利用模擬軟體進行實驗，其接取方法仍為 DSL 技術，相對於本研究所使用的乙太網路接取技術，DSL 接取自然會面臨 DSL 速



率頻寬的限制。此外本文提出之 PDR 具有維持服務品質、動態頻寬調整及提供高可用性網路等多重功能,使其在電信乙太網路上提供穩定有效益的 Triple play 服務。

二、相關研究

乙太網路是近 30 年中非常成功且佔有率很高的區域網路技術,此外電信乙太網路的成本效益高,傳輸速率非常有彈性,最低 10 Mbps,最高可達 100 Gbps。在此節中,我們針對乙太網路技術、VPLS 及電信乙太網路的相關技術加以介紹。

(一) 乙太網路技術

乙太網路通訊協定是由全錄 (Xerox) 於 1973 年設計,當時的資料傳輸速率為 10 Mbps,現在使用的乙太網路傳輸速率為 100 Mbps 及 1000 Mbps,乙太網路正式定義在 IEEE802.3 標準。關於乙太網路架構標準則是定義在 IEEE802.1 之中。

1. 802.1Q (virtual bridged local area networks)

802.1Q [7] 是用來定義 VLAN 的標準規格,它在原來的乙太網路 II 訊框中位於 Source MAC 與 EtherType 間新加入一個大小為 4 bytes 的 TAG 欄位,如圖 1 所示。在 VLAN 網路中,不同的 TAG 就代表不同的區域網路,相同的 VLAN 在邏輯上可視為相同的地理區域,代表一個獨立的廣播領域,因此不同的 VLAN 網路可視為不同的廣播領域。一個 IP 子網域就是一個廣播領域,不同 IP 子網域之間互通需要透過第三層的設備轉送,因此在資料傳送時,VLAN 技術會比傳統的 LAN 更有效率。此外只有相同 TAG 值的封包才會往相同設定的通訊埠轉送,因此 VLAN 可以提高整體網路的安全性。在網路管理方面,管理者可將不同屬性的單位劃分成不同的 VLAN,增加了管理者的方便性。

TAG 欄位是由大小各為 2 bytes 的 TPID (tag protocol Identifier) 及 TCI (tag control information) 所組成,如圖 2 所示。TPID 標籤協定辨識碼長度為 16 bits,用來辨識是否為 IEEE 802.1Q 的訊框,其定義值為 0x8100,值得注意的

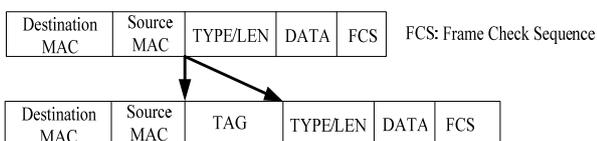


圖 1. 802.1Q Tag in Ethernet II frame

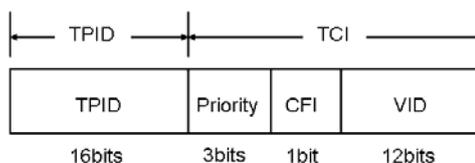


圖 2. 802.1Q Tag 欄位格式

是 TPID 完全相容於乙太網路 II 訊框中 TYPE/LEN。TCI 標籤控制資訊長度為 16 bits,它是由 Priority (3 bits)、CFI (canonical format indicator) (1bit) 及 VID (VLAN ID) (12 bits) 所組成。Priority 可定義使用者的優先權等級,詳細的分級標準定義在 802.1p 之中。CFI 用來標示訊框所攜帶的 MAC 位址是否為制式格式。VID 長度為 12 bits,其中 0 表示這個訊框不屬於任何 VLAN,而 FFF 則是保留不使用,且在實務上 VLAN 1 通常保留給網路管理使用,因此只有 4,093 個 VLAN ID 可供使用,所以不適合應用在服務業者的網路架構。

2. 802.1ad (provider bridges)

IEEE 802.1ad [8] 利用和 802.1Q 一樣的概念,在原本的 VLAN Tag 之前再加一個 VLAN Tag,並定義外層的標籤協定識別 (tag protocol identifier, TPID) 為服務標籤協定識別 (service-TPID, S-TPID),並將值改為 0x88A8,以和原本的 802.1Q 作區分。若只是單純的使用兩層以上的 VLAN Tag 又稱為 Q-in-Q。此 2 層的 VLAN tag 各別以 Service-Tag (S-Tag) 及 Customer-Tag (C-Tag) 作為區分。802.1ad 的訊框格式如圖 3 所示。Q-in-Q 又稱為供應商橋接器 (provider bridge, PB),代表服務供應商可以在網路上使用 VLAN Tag,將客戶的資料和服務供應商的資料區分開來,同時客戶也可以在其網路上使用 VLAN tag 區分內部的資料,而這兩種 VLAN Tag 不會互相衝突。服務供應商只需要看 S-Tag 就可以決定資料是那個客戶的資料,而在傳送到客戶端時,先將第一層的 S-Tag 移除,所以客戶只看到原本的 C-Tag。這樣子的作法,就可以將原本只限在 LAN 上面使用的 VLAN 設定,直接接到遠端網路,就如同是直接連接一般,而不需作修改,或是先轉換到 Layer3,直接以比較快速的 Layer 2 交換資料了。而若是兩個 VLAN ID 有重覆時,也可以利用 S-Tag 將之分開,互不干擾。這項技術目前在都會型的乙太網路中廣泛使用。

3. 802.1ah (provider backbone bridges)

由於 802.1ad 技術會讓 PB 在網路存取層位址 (medium



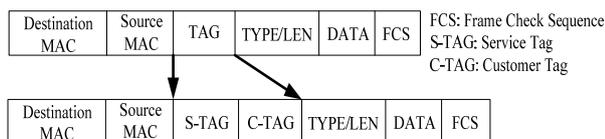


圖 3. 802.1ah Tag 欄位格式

access layer, MAC) 表格中保有用戶的 MAC 位址資料, 因此只要 PB 的網路規模過大, MAC 位址表格的維護就變成沈重的負擔。為解決此問題, 802.1ah [9] 標準, 在原來的 802.1ad 的訊框前面再增加 B-DA、B-SA、B-TAG 及 I-TAG 這些欄位, 如圖 4 所示。I-TAG 的功能有點類似 S-TAG, 不過 I-TAG 總共有 24bits, 相對於 S-TAG 的 12bits 有更大的擴展性, 也更適合在骨幹網路使用。此外 I-TAG 的另一個功能是隔離用戶端 MAC 位址資料, 在供應商骨幹網路橋接器 (provider backbone bridge network, PBBN) 中使用骨幹設備的 MAC 位址進行交換, 骨幹設備的 MAC 位址表格完全不用維護, 減少維護用戶端 MAC 位址表格的負擔。B-TAG 代表 PBBN 中的 VLAN ID, 同一 VLAN ID 中可以服務不同的 I-TAG, 增加系統使用容量, 此外 B-TAG 也可以應用在流量工程, 不同服務等級的用戶可以指配在不同的 B-TAG。

(二) 虛擬專用區域網路服務 (Virtual Private LAN Service, VPLS)

MPLS 網路提供第二層虛擬私人網路 (VPN) 服務的架構, 可分為虛擬專線 (virtual leased line, VLL) 與虛擬專用區域網路服務 (virtual private LAN service, VPLS)。VLL 是在 IP/MPLS 網路中提供乙太網路為基礎的點對點通訊的一種方法。而 VPLS 最主要的功能是将網路上分散的各點實現多點連接成一個 LAN 的架構。IETF 提出兩種標準來實現 VPLS: RFC4761 (BGP-based VPLS) [12] 及 RFC4762 (LDP-based VPLS) [13]。RFC4761 是利用 BGP 的 RR (route reflector) 方式來達到 signaling 及 auto-discovery, 但是 BGP-based 技術的缺點就是複雜。RFC4762 則是利用 LDP (label distribution protocol) 的方式來實現 signaling, 最大的好處就是簡單, 但是缺點是無法 auto-discovery, 需要手



B-DA: Backbone destination address B-SA: Backbone Source address
B-TAG: Backbone VLAN Tag I-TAG: Service Identifier

圖 4. 802.1ah Tag 欄位格式

動設定。由於 VPLS 各個交換器之間都要完全連接, 邊界的交換器也要負責處理用戶的 MAC 位址資料, 因此若網路規模太大, 此方式將會負擔太大。因此有人提出了階層式 VPLS (hierarchical-VPLS, H-VPLS) 架構 [5], 如圖 5 所示。H-VPLS 把原本的 VPLS 領域切割成多個領域, 各領域再透過虛擬線路 (pseudowire, PW) 建立透通, 如此可以大量減少核心網路的負擔。

(三) 電信乙太網路 (Carrier Ethernet)

1. MEF 定義之服務

都會乙太網路論壇 (metro ethernet forum, MEF) [15] 組織, 致力於電信級乙太網路標準化。該組織把乙太網路應用成點對點的連結, 所有的資料都透過乙太網路傳輸, 增加效率。如圖 6 所示, MEF 定義出三種電信級乙太網路的標準服務架構: E-Line、E-LAN 及 E-Tree。E-Line 特色就是提供點對點的連結, 有如在乙太網路中將任意 2 點利用虛擬電路相互連接, 如 VPN、遠距醫療照護或用戶連網服務等。E-LAN 特色就是提供多點對多點的連結, 各介接節點如同在一個 LAN 互連, 適合應用於大型機構與各分支機構互連。E-Tree 是 E-LAN 的變型, 同樣適合多點對多點的連結, 一般應用於多媒體傳輸網路, 其樹狀架構的根部正好可以用於頭端, 只要一份資料從頭端發佈位於底部的各節點就可以收到, 非常適合用於廣播網路。

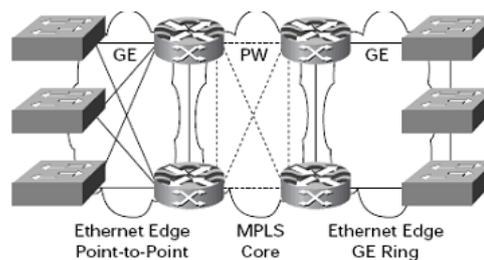


圖 5. H-VPLS 架構

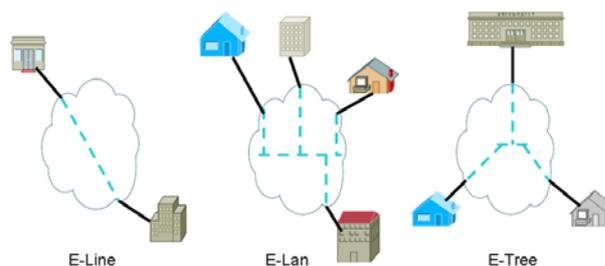


圖 6. MEF 定義之服務架構圖



2. 營運、管理與維護 (operations, administration, and maintenance, OAM)

營運管理和維護 (operations, administration, and maintenance, OAM) 分為兩個主要領域：障礙管理及效能監控。障礙管理的目的在確保網路發生障礙時可以回報給電信業者，以進行適當的處置。障礙管理內容可分為障礙偵測、障礙確認、障礙隔離及障礙通知。效能監控內容又分為訊框遺失評量、訊框延遲及訊框延遲變動。因乙太網路的設計源由是為應用於校園網路，並非以電信網路為設計目標，所以其 OAM 功能不若電信網路這麼嚴謹且完整 [14]。目前乙太網路 OAM 的標準正陸續制定中。在障礙偵測方面，IEEE 802.1ag 與 ITU-T Y.1731 的標準透過持續性核對訊息 (continuity check messages, CCM)，達到支援障礙偵測的功能。這些功能可使終端設備偵測服務是否有干擾中斷的情形。透過 CCM 週期性地運作，從來源傳送至目的端。若兩終端未在指定時間內收到 CCM，表示服務發生問題。在障礙確認方面，IEEE 802.1ag 與 ITU-T Y.1731 標準透過迴路訊息 (loopback messages, LBM) 與迴路回覆 (loopback reply, LBR)，支援障礙確認的功能。在開始設定或已偵測到障礙時均可使用，以確認在兩終端間是否發生障礙。在障礙隔離方面，IEEE 802.1ag 與 ITU-T Y.1731 的標準透過連結追蹤訊息 (linktrace messages, LTM) 與連結追蹤回覆 (linktrace reply, LTR)，來隔離發生障礙的設備。在障礙通知方面，ITU-T Y.1731 標準是透過警告指示信號傳送障礙通知。

在訊框遺失評量方面，ITU-T Y.1731 標準透過 CCM 模式經由寄發傳送和接收計數器，以雙向進行方式來計算訊框遺失的狀況。遠端計數器所分析出的結果，可和發訊原地的訊框製造量比較，導出訊框遺失的比率。在訊框延遲方面，ITU-T Y.1731 標準亦藉由延遲管理模式，使用時間戳記方式來計算訊框延遲。接收端可將算出的延遲時間導入整個網路做為參考，但是需要每個服務終端的時脈同步化。另外延遲管理訊息和回覆功能亦可被應用在計算雙向訊框延遲上面，這種方法不需要時脈同步化便可進行。在訊框延遲變動方面，ITU-T Y.1731 標準藉由追蹤訊框延遲管理計算訊框延遲變動程度。

三、系統架構與運作流程

本文所提出的系統網路架構，如圖 7 所示，是由用戶接取網路及核心網路所連接組成。用戶接取網路使用的是

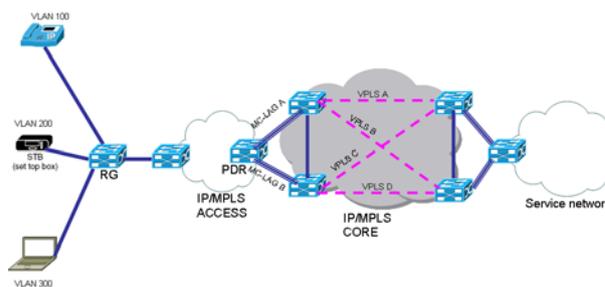


圖 7. 系統網路架構圖

IEEE802.1ad 技術，核心網路則是以 IP/MPLS 網路為主。我們透過策略決策路由器 (PDR) 的佈置，將此二網路連接起來。PDR 至用戶端的家用閘道器 (residential gateway, RG) 為電信乙太網路的環境，PDR 至服務網路之間則為 IP/MPLS 的網路。在所提出的系統網路架構中，PDR 扮演重要的角色，它由動態頻寬調整單元及快速回復單元所組成。接下來，我們介紹此二單元的組成及運作流程。

(一) 動態頻寬調整單元及運作流程

動態頻寬調整單元的功能除了將不同的服務分成不同 VLAN 及引用不同的限速外，還要定期偵測用戶端頻寬利用的情況，動態的調整各服務的限速。此單元由 VLAN 模組、Rate-Limit 模組、RTR 模組及 TRAP 模組所組成。VLAN 模組負責將電信乙太網路所匯集過來的 VLAN 進行解析，檢查各乙太網路 II 訊框之 TPID 是否為 0X8100，再將接收到 Customer VLAN 封包封裝上一層服務供應商使用的 Service VLAN 往下傳送，如此就能將服務封包送達其所屬的服務 VLAN。Rate-Limit 模組的功能是限制各種服務速率符合 SLA 要求，在本文我們以 VoIP 服務、IPTV 服務及 HIS (high speed internet) 服務分別代表 Triple play 服務的語音、視訊及 data 服務，並設定 VoIP 服務、IPTV 服務及 HSI 服務的頻寬分別為 128 Kbps、30 Mbps 及 20 MBps。

RTR 模組負責對各項服務進行 IP 層的連接性偵測，依據 Triple play 服務需求設定不同的 RTR 參數，只要符合策略設定即發出 TRAP 訊息。RTR 模擬定期偵測圖及偵測參數表分別如圖 8 及表 1 所示。在本文中，我們設計 4 種 RTR 偵測參數，偵測類型為 ICMP，timeout 時間依據各服務的要求分別設定為 150 ms、5 s、100 ms，偵測頻率是每 5 秒偵測一次，連續 3 次失敗 (RTR A、B、C) 或成功 (RTR D) 則發出 TRAP 訊息。在此 4 種 RTR 偵測參數中，RTR A 所代表的服務應用為 VoIP，由於 VoIP 服務所使用的頻寬不



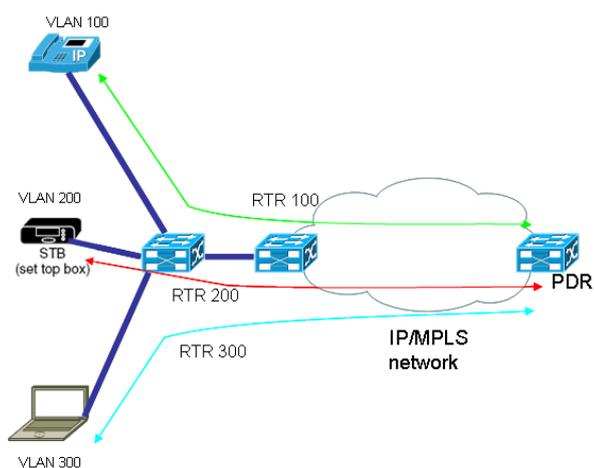


圖 8. RTR 定期偵測

表 1. RTR 偵測參數表

RTR 類型	測試頻率	測試類型	Timeout	TRAP 條件
RTR A (偵測 VoIP LAD)	5 秒	ICMP	150ms	失敗
RTR B (偵測 HSI GW)	5 秒	ICMP	5s	失敗
RTR C (偵測 IPTV STB 關機)	5 秒	ICMP	100ms	失敗
RTR D (偵測 IPTV STB 開機)	5 秒	ICMP	100ms	成功

高，且 VoIP 服務需隨時正常使用，因此不適合調整 VoIP 的頻寬。RTR B 代表的服務應用為 HIS，因為在一般的應用中數據傳輸頻寬的變動量較不固定，因此閒置的頻寬可調整供數據傳輸使用。RTR C、D 所代表的服務應用是 IPTV，因為 IPTV 服務並不是 24 小時都在使用，因此 IPTV 服務未使用時的頻寬將釋放給 HSI 服務使用。在另一方面，由於 IPTV 服務開機使用時，要將頻寬保留給 IPTV 服務使用，因此本文設計 RTR D 來偵測 IPTV 開機使用。另外，TRAP 模組則是負責接收 RTR 模組所送出之 TRAP 訊息及進行對應之策略設定。

動態頻寬調整單元流程，如圖 9 所示。首先 PDR 會判斷是否收到 VoIP 服務 RTR 測試失敗的 TRAP 訊息。若收到此訊息，代表 VoIP 的服務目前中斷，因此流程轉向 Case1 (Case1 代表 VoIP 服務中斷，VoIP 服務的頻寬可以被其他服務使用)。若沒有收到此訊息，表示 VoIP 服務正常。由於 VoIP 服務的頻寬不高，所以可以忽略不使用，因此 Case1 只將狀態設定為 True。HSI 判斷式是判斷是否收到 HSI 服務 RTR 測試失敗的 TRAP 訊息為條件。若沒有收到此訊息，

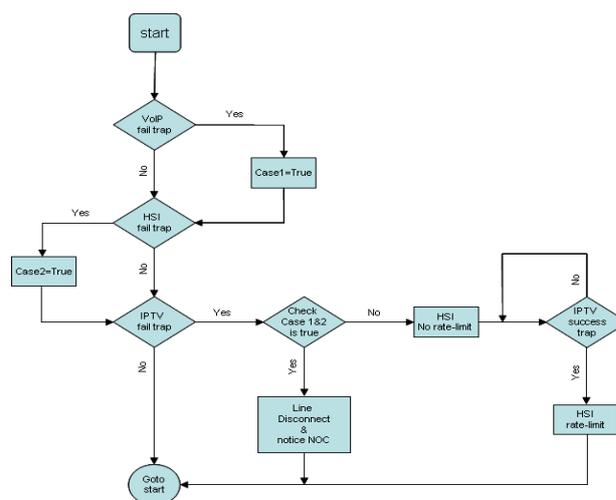


圖 9. 動態頻寬調整單元流程

表示 HSI 服務正常。若收到此訊息，表示 HSI 的服務中斷，因此流程轉向 Case2。Case2 代表 HSI 服務中斷，表示其頻寬已閒置，但是 VoIP 及 IPTV 所需頻寬固定，所以 Case2 將狀態設為 True。

IPTV 判斷式以是否收到 IPTV RTR 測試失敗的 TRAP 訊息為條件。若沒有收到此訊息，表示 IPTV 服務正常。若收到此訊息是表示 IPTV 的服務中斷或是 STB 關機。若 Case1 和 Case2 的狀態同時為 True，表示同時收到三種服務 RTR 測試失敗的 TRAP 訊息，就代表實體線路中斷，此時需通知網路服務中心處理。若 Case1 和 Case2 的狀態不是同時為 True，則表示只有 IPTV 中斷，因此 IPTV 的頻寬目前處於閒置狀態，所以頻寬可以釋放出來提供 HSI 服務使用，處理控制將 HSI 改成不限速率。接著流程轉向是否收到 IPTV RTR 測試成功的 TRAP 訊息，由於收到此 TRAP 訊息就表示 IPTV 的 STB 已開機準備收看節目，因此處理控制將 HSI 速率限制調回原來的申請速率。

(二) 快速回復單元

快速回復單元的主要功能是提高網路可用性，它由 LAG 模組、VPLS-PW 模組、BFD 模組及 PATH-SELET 模組所組成。高可用性是電信級乙太網路必要的條件，一般而言可由 node level redundancy 及 pseudowire level redundancy 兩方面來提高網路可用性。node level redundancy 的目標就是預防設備故障失效，常見的技術就是同時建立 2 台相同的設備透過 hot-standby 的方式相互備援。但此方法無法預防網路中任一電路失效造成服務中斷，因此就需要 pseudowire level redundancy 合併使用，才能提供高可用性的服務網路。



在本文中，我們分別從此兩方面來提升網路可用性。

LAG 模組負責 node level redundancy，我們採用多機箱鏈路聚合 (multi-chassis link aggregation, MC-LAG) 實體保護方式，避免骨幹單一節點失效。LAG 是 IEEE 802.3ad 定義的標準 [11]，LAG 就是將兩台對接設備之間的多條連線群組成一條虛擬的連線，透過鏈路聚合控制協定 (link aggregation control protocol, LACP)，動態新增電路頻寬至群組內。但是如果只建立一條 LAG，將無法解決單點失效的問題，因此必須對不同的兩個設備各建立一條 LAG，透過 LACP 將這兩個 LAG 群組成一個主要 LAG，如圖 10 所示。在此架構中，一個接取網路的邊界設備中都會同時存在 Active-LAG 及 Standby-LAG，同一時間只會使用一條 LAG，另一個 LAG 做為備援使用，當 Active-LAG 中斷時會自動改由 Standby-LAG 接手，以主要 LAG 的觀點來看是完全不受影響。

VPLS-PW 模組負責 pseudowire level redundancy，我們依據表 2 的建立原則，於核心網路建立 4 條 VPLS PW 至服務網路，如圖 11 所示。在此環境中，同一時間只有一條 Active PW 提供服務，若網路發生變化可迅速切換至 Standby PW，因此使用多條 PW 可提高網路可用度。以圖 12 為例，當 BR2 發生故障，此時 VPLS C、D 將受影響而中斷，但仍有 VPLS A、B 可連通至服務網路。圖 12 另一個情形是說明當 VPLS D 中斷時，還有 VPLS A、B、C 可連通至服務網路。

BFD 模組應用乙太網路 OAM 機制的 BFD 第三層連通性測試機制，定期偵測網路品質，其偵測參數如表 3 所示。BFD 機制利用 Liveness Detection Interval 來判定網路是否中

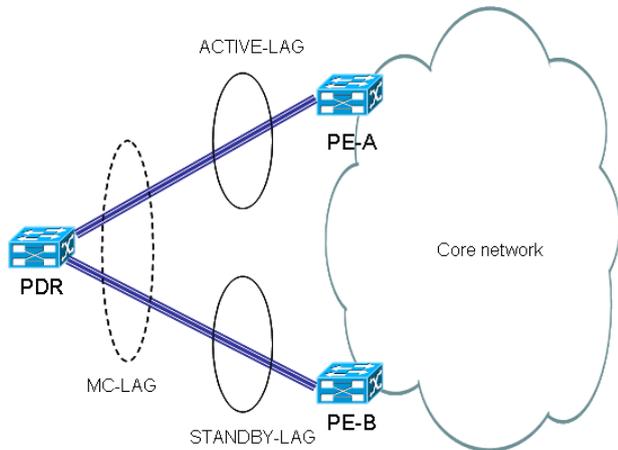


圖 10. MC-LAG 表示圖

表 2. VPLS PATH 建立規則表

	node-level protection (節點層保護)	pw-level protection (虛擬線路層保護)
VPLS PATH A	Active (現行)	Active(現行)
VPLS PATH B		Standby(備援)
VPLS PATH C	Standby (備援)	Active(現行)
VPLS PATH D		Standby(備援)

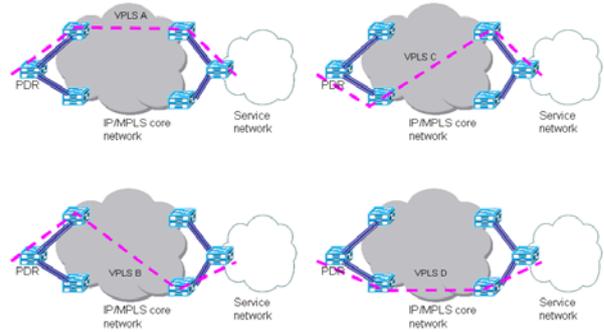


圖 11. VPLS 分散建立之上鏈電路

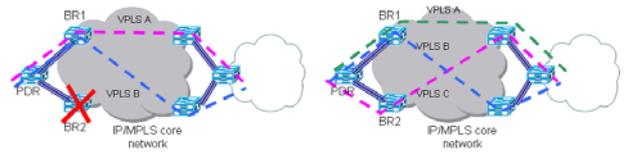


圖 12. MC-LAG 與 VPLS 架構快速回復網路

表 3. BFD 偵測參數表

Router (路由器)	A	B
Configured Transmission Interval (ms) (設定的傳輸區間)	100	100
Configured Receiving Interval (ms) (設定的接收區間)	100	100
Negotiated Transmission Interval (ms) (協商的傳輸區間)	100	100
Detection Multiplier (偵測乘數)	3	3
Liveness Detection Interval (ms) (存活偵測區間)	300	300

斷。在表 3 中，Liveness Detection Interval 是 300 ms，一旦 ROUTER A、B 偵測時間大於 300 ms，代表 A、B 之間中斷。此參數值是由 ROUTER A、B 事先設定溝通後所決定。以表 3 為例，ROUTER A、B 所設定的 Transmit 及 Receive Interval 都為 100 ms，經過溝通之後產生 Negotiated Interval



為 100 ms。在 BFD 機制中，因考量網路傳遞因素，會增加參數 Detection Multiplier，將 Negotiated Interval 與 Detection Multiplier 相乘後得到 Liveness Detection Interval。

PATH-SELECT 模組的功能是根據 BFD 機制測試結果，選擇資料傳送的路徑。為了維持強化上鏈電路的穩定度，同時間只會有一條 VPLS PW 扮演 Uplink 的角色。PATH-SELECT 模組會依 VPLS A B C D 的順序判斷其網路是否連通，當某一 VPLS 經由 BFD 機制測試成功，則所有資料會經由該 VPLS 傳送和接收。若全部的 VPLS 均測試失敗，則表示核心網路中斷。動態頻寬調整單元與快速回復單元各模組之 pseudo code 如圖 13 所示。

四、系統效能模擬分析

為驗證所提出系統架構的可行性，我們於中華電信的實驗室建立系統模擬環境。此模擬環境是由 1 部 Cisco Catalyst 3550 及 2 部 Juniper ERX1440 寬頻服務路由器組成實驗網路。在此環境中，Cisco Catalyst 3550 擔任 RG 的角色，介面包含 48 port Fast Ethernet 及 2 port Gigabit Ethernet，其功能是提供一個 trunk（多重實體連線結合成單一邏輯連線的技術）與 PDR 介接，Triple play 服務經由此 trunk 進入 RG，再透過 VLAN 方式轉送到對應的通訊埠提供服務。在另一方面，我們利用 Juniper ERX1440 的虛擬路由器的功能來建構核心網路，每部 ERX1440 寬頻服務路由器擁有 1 個 PDR 及 2 個橋接路由器，每部 ERX1440 的介面為 2 張 2 port GE 卡及 2 張 8port FE 卡，系統模擬環境及實驗 IP 機線配置表，如圖 14 和表 4 所示。

```

Module VLAN
Input = packet_incoming // check incoming packet
IF TPID = 8100 // check TPID is 802.1Q
THEN get VID // get VLAN ID
ELSE drop packet
END

Module rate-limit
IF rate-limit = yes
THEN
set vlan.voip = 128Kbps // voip 128Kbps
set vlan.IPTV = 30Mbps // IPTV 30Mbps
set vlan.HSI = 20Mbps // HSI 20Mbps
ELSE
set vlan.voip = 128Kbps // voip 128Kbps
END

Module RTR
IF RTR.trap = true // RTR test fail
THEN trap to trap module // send trap to trap module
ELSE return module RTR
END

Module Trap
IF Trap.VOIP & Trap.IPTV & Trap.HSI = 1
THEN notice NOC line disconnect
ELSEIF Trap.IPTV=1
THEN set rate-limit = no
ENDIF

Module LAG
Set LAG=link group (node1,node2)
END

Module VPLS-PW
Set VPLSA = node.active + path.active
Set VPLSB = node.active + path.standby
Set VPLSC = node.standby + path.active
Set VPLSD = node.standby + path.standby
END

Module BFD
IF BFD session state = up
THEN PATH-select module
ELSE next BFD session state
END

Module PATH-select
IF BFD session state is up = 1
THEN forward via BFD session
ELSEIF compare all BFD's cost
THEN forward via lowest cost BFD
ENDIF

```

圖 13. 系統模組功能 pseudo code 表示圖

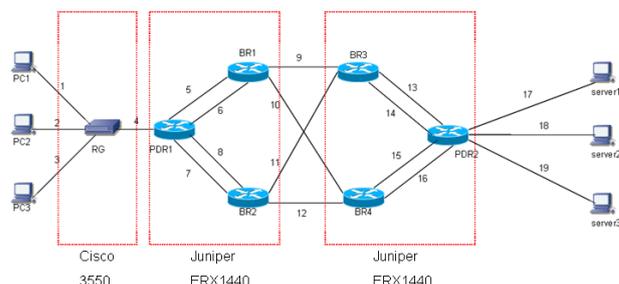


圖 14. 模擬網路架構圖

在此實驗環境中，首先我們比較 IEEE 802.1p 的優先順序策略（CoS）與利用限速策略的方式，哪一種機制較適合於提供 Triple play 服務；接下來我們比較靜態頻寬限制策略與我們所提出的動態頻寬調整策略的效能表現。此外我們模擬單一節點失效的情境來測試 MAC-LAG 是否具備避免單一節點失效的能力。在另一方面，我們分別利用靜態路由協定偵測、動態路由協定偵測與我們所提出的 BFD 機制，來測試與比較這三種策略在偵測電信乙太網路中發生電路中斷或設備故障時，進而切換至備用路由達到服務不中斷的表現，最後針對我們所提出的機制作系統效能的測試。

（一）優先順序策略與限速策略的比較

在優先順序策略的實驗部份，由於 Cisco Catalyst C3550 在 802.1p 的優先順序策略只支援 2 種分級：正常順序與高優先順序，因此我們設定 2 種分級來進行實驗。為模擬 VoIP 服務，我們在 trunk 端限制速率在 50 Mbps，由 server1 與 PC1 互相傳送 128 Kbps 之流量；為模擬用戶收看 2 個 HD 之 IPTV 服務，我們同時由 server2 往 PC2 傳送 30 Mbps 之 UDP 流量；為模擬高速上網，我們由 server3 與 PC3 互相傳送 20 Mbps 之 UDP 流量。我們進行兩個實驗：實驗一設定 IPTV 服務與 VoIP 服務為高優先順序，高速上網為正常順序；實驗二設定 VoIP 服務為高優先順序，IPTV 服務與高速上網為正常順序。優先順序策略實驗分級表，如表 5 所示。

在實驗中，我們使用 iperf [17] 效能測試軟體，測量 bandwidth 及 jitter。圖 15 為優先順序策略實驗的結果。由圖 15(a)(b) 可發現雖然 voice 跟 video 服務均設為高優先順序，但是兩者之間會互相影響，所以 jitter 均顯示不穩定。由圖 15(c)(d) 可發現，若將 video 改成正常順序時，實驗結果顯示 voice 已經較為穩定，但是 video 還是呈現不穩定的狀態。

在限速策略的實驗部份，我們於 PDR1 導入限速策略，



表 4. 實驗 IP 機線配置表

編號	左端介面	左端 IP	右端介面	右端 IP	VLAN	備註
1	PC1	192.168.101.1/24	RG-F0/1		101	
2	PC2	192.168.102.1/24	RG-F0/17		102	
3	PC3	192.168.101.1/24	RG-F0/33		103	
4	RG-G0/1		PDR1-G1/0			限速 50Mbps
	RG-G0/1.101		PDR1-G1/0.101	192.168.101.254/24		
	RG-G0/1.102		PDR1-G1/0.102	192.168.102.254/24		
	RG-G0/1.103		PDR1-G1/0.103	192.168.103.254/24		
5	PDR1-F12/0.20	192.168.20.1/30	BR1-F12/4.20		20	VPLSA
6	PDR1-F12/1.30	192.168.30.1/30	BR1-F12/5.30		30	VPLSB
7	PDR1-F12/2.40	192.168.40.1/30	BR2-F12/6.40		40	VPLSC
8	PDR1-F12/3.50	192.168.50.1/30	BR2-F12/7.50		50	VPLSD
9	BR1-G2/0		BR3-G2/0			MPLS core
10	BR1-G4/0		BR4-G2/1			MPLS core
11	BR2-G2/1		BR3-G4/0			MPLS core
12	BR2-G4/1		BR4-G4/1			MPLS core
13	BR3-F12/4.20		PDR2-F12/0.20	192.168.20.2/30	20	VPLSA
14	BR3-F12/5.40		PDR2-F12/1.40	192.168.40.2/30	30	VPLSB
15	BR4-F12/6.30		PDR2-F12/2.30	192.168.30.2/30	40	VPLSC
16	BR4-F12/7.50		PDR2-F12/3.50	192.168.50.2/30	50	VPLSD
17	PDR2-F1/0	172.16.30.254/24	server1	172.16.30.1/24		測試 voice
18	PDR2-F1/1	172.16.31.254/24	server2	172.16.31.1/24		測試 video
19	PDR2-F1/2	172.16.32.254/24	server3	172.16.32.1/24		測試 data

表 5. 優先順序策略實驗分級表

Priority	實驗一	實驗二
High	Voice (PC1) Video (PC2)	Voice (PC1)
Normal	Data (PC3)	Video (PC2) Data(PC3)

於介面 G1/0.101 限速 128 Kbps 來模擬 VoIP 服務的頻寬；於介面 G1/0.102 限速 30 Mbps 來模擬用戶申請 2 個 HD 的 IPTV 服務；於介面 G1/0.103 限速在 20 Mbps 來模擬高速上網。Jitter 是影響即時性服務品質的重要因素之一，有些服務供應商已經在服務水準協議（service level agreement, SLA）註明 jitter 最大不能超過 10 ms [21]，如表 6 所示。由圖 16 的實驗結果可看出，在 PDR 導入限速策略時，各項服務間不會互相影響，頻寬測試結果也都符合設定的要求，jitter 均在 3 ms 以下。

(二) 靜態頻寬限制與動態頻寬調整之比較

在限速策略的實驗中，雖然各項服務間不會互相影響，

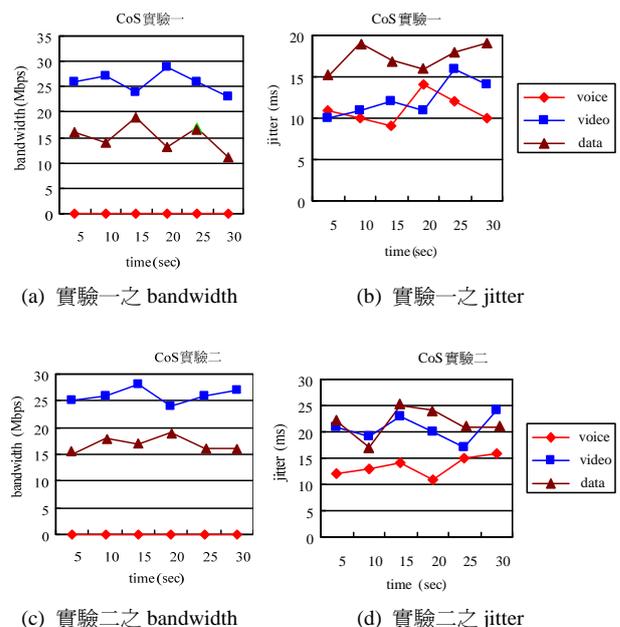


圖 15. 優先順序策略實驗

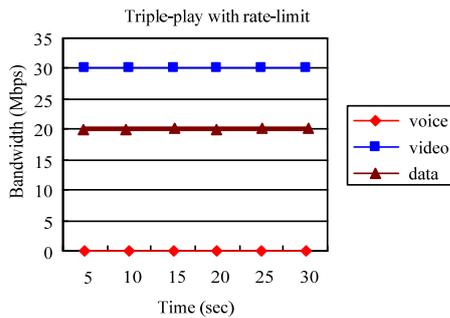


表 6. 各服務提供商服務水準協議之 jitter 最大值

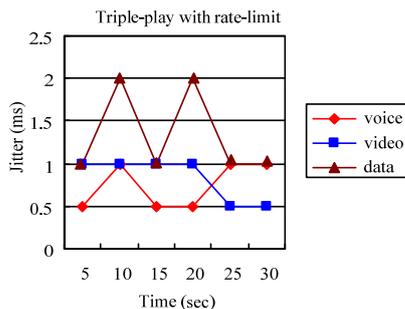
服務提供商	服務水準協議 (SLA) jitter 最大值
Qwest	2ms
Viterla	1ms
Axiowave	1ms
Verio	10ms(0.5ms average)
Internap	0.5ms

表 7. RTR 偵測參數表

RTR 偵測	RTR 1	RTR 2	RTR 3	RTR 4
偵測類型	ICMP	ICMP	ICMP	ICMP
Timeout	150ms	5s	5s	200ms
頻率	5s/round	5s/round	5s/round	5s/round
Trap	失敗	失敗	失敗	成功
Triple play	VoIP	HSI	IPTV	IPTV



(a) 使用限速策略之 bandwidth



(b) 使用限速策略之 jitter

圖 16. 限速策略實驗

頻寬測試結果也都符合設定的要求，但頻寬使用就不是那麼有效率。在此實驗中，我們比較靜態頻寬限制與動態頻寬調整的效能表現。在動態頻寬調整部份，我們透過在 PDR 佈置 RTR 定期偵測機制，偵測服務是否處於閒置狀態。若服務閒置時，便將該服務的頻寬釋放出來供其他服務使用；一旦閒置的服務要上線使用時，也會被 RTR 偵測機制發現而將其頻寬還原保留。

RTR 偵測參數表，如表 7 所示。我們在 PDR1 上分別設定 3 組 RTR 偵測：PC1、PC2 及 PC3，分別使用 iperf 軟體於 server 端測試頻寬使用狀況。為模擬 video 關機的狀況，實驗中將 PC2 網路線拔除，5 秒後 RTR 送出 Trap 訊息，此時 PC3 的頻寬會增加至 50 Mbps。之後再把 PC2 的網路線接回，模擬 video 開機，此時 PC3 的頻寬限回 20 M。如圖 17 所示，RTR 偵測到 video 關機後送出 Trap 訊息，PDR，

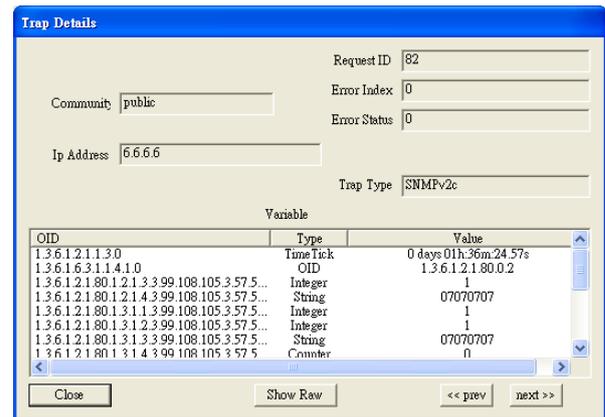


圖 17. Trap receiver 接收到之 trap

根據頻寬調整策略進行頻寬調整，由圖 18 可看出在第 20 秒時 data 之頻寬變大，在第 40 秒時 PDR 偵測到 video 開機因此將速率設回原設定值。相較於圖 16 的靜態頻寬限制而言，動態頻寬調整對於使用者所申請的頻寬是有比較好的使用效益。

(三) Node-level 保護機制

為測試 MAC-LAG 是否具備避免單一節點失效的能力，我們在 PDR1 及 PDR2 利用靜態路由的設定方式設定四條不同的 VPLS，並在 PC 端量測 PC 端至 server 的 ICMP 封包來回時間。在此實驗中，我們將 BR2 關掉來模擬節點故障，此時 VPLS C、VPLS D 將會因為節點故障而從路由表中消失，此時再測量 PC 端與 server 間是否快速回復正

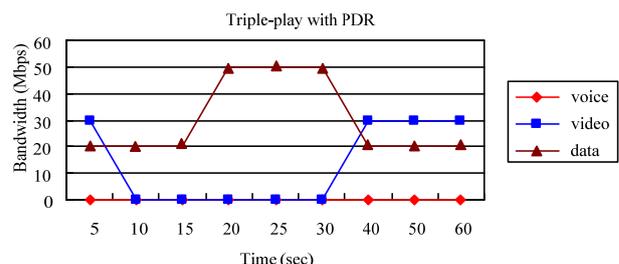


圖 18. 動態頻寬調整實驗



常。圖 19 及圖 20 分別代表 BR2 故障前後靜態路由的情況。從此二圖比較後可看出，當 BR2 發生故障後，PDR 會發現與 BR2 間的鏈結中斷，因此會在路由表中將下一點為 VPLS C 及 VPLS D 的路由移除。

由於 BR2 是實際與 PDR1 介接，在乙太網路設備中下一節點故障失效，其對接 port 會偵測得知而變成 down，其相關路由資訊也會從路由表中移除，從圖 21 我們可以發現在第 5 秒 BR2 發生故障後，第 7 秒受影響的電路馬上恢復正常，本實驗證明 MC-LAG 是可以達到 node-level 的保護能力。

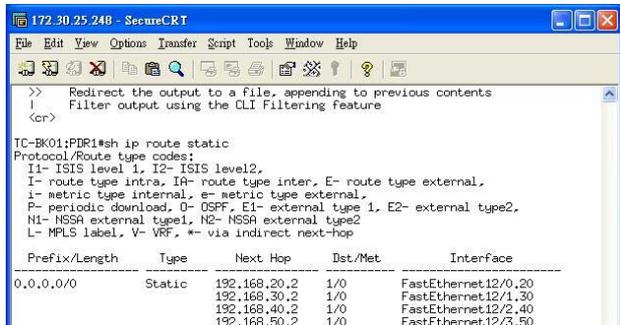


圖 19. BR2 故障前靜態路由圖

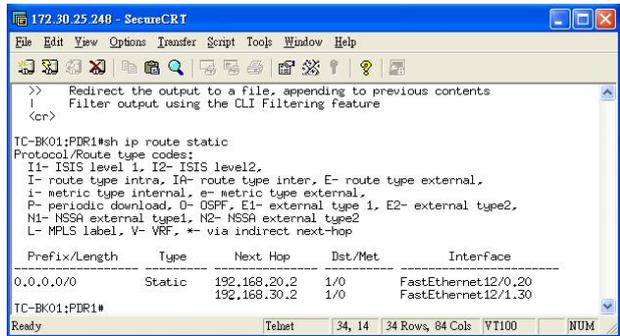


圖 20. BR2 故障後靜態路由圖

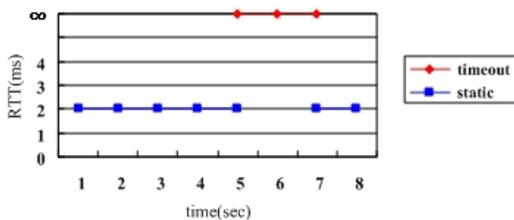


圖 21. 模擬 BR2 故障電路復原圖

(四) 虛擬線路層 (Pseudowire-level) 保護機制

在此節中，我們分別利用靜態路由協定偵測、動態路由協定偵測與我們所提出的 BFD 機制，來測試與比較這三種策略在偵測電信乙太網路中發生電路中斷或設備故障時，進而切換至備用路由達到服務不中斷的表現。

1. 靜態路由協定

本項實驗在 PDR1 及 PDR2 上使用靜態路由設定的分別設定四條不同的 VPLS，實驗時在 BR3 的介面 G2/0 將其關閉，模擬電信乙太網路中某條電路中斷影響到一個 VPLS。分別由 PC 往 server 端量測 ICMP 的 RTT。由圖 22 及圖 23 可發現在實驗時將 BR3 的介面 G2/0 關閉後，於 PDR1 及 PDR2 上所呈現的 default route 還是 4 條並未發現 VPLS A 已經中斷，但是由圖 24 可發現經由 VPLS A 的訊務從第 15 秒開始已經中斷。使用靜態路由設定，除非是相連節點故障或是對接電路中斷才會使得 routing 消失，否則中間網路中斷或失效是不會知道的，因此靜態路由協定無法滿足快速回復的需求。

2. 動態路由協定

為驗證於 PDR 的 uplink 若是使用動態路由的方式設

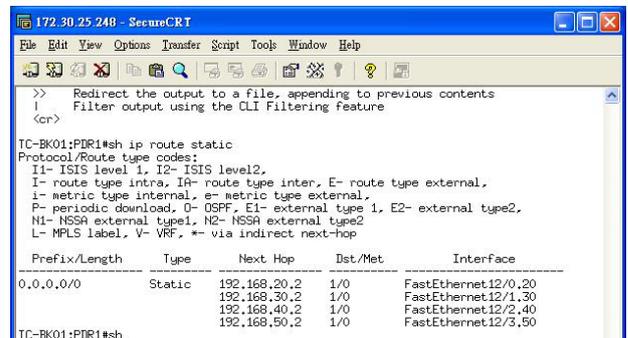


圖 22. VPLS A 中斷後 PDR1 之路由圖

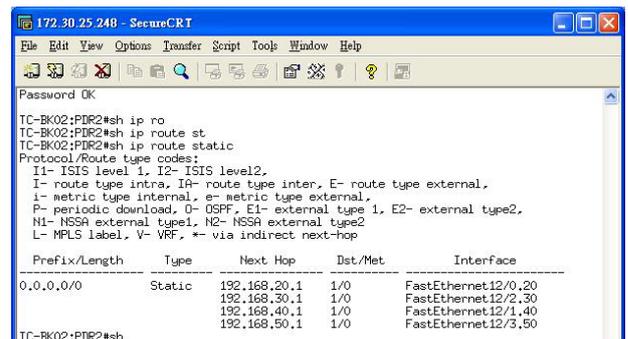


圖 23. VPLS A 中斷後 PDR2 之路由圖



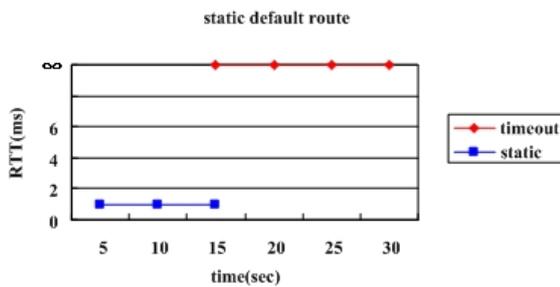


圖 24. 經由 VPLSA 之 RTT 測試圖

定，是否有能力偵測電信乙太網路中發生電路中斷或設備故障，進而切換至備用路由達到服務不中斷的效果，我們分別使用 RIP 及 OSPF 進行測試。首先分別在 PDR1 及 PDR2 設定 RIP，透過 4 條 VPLS 交換路由資訊，在 BR3 的介面 G2/0 將其關閉，模擬電信乙太網路中某條電路中斷影響到一個 VPLS，分別由 PC 往 server 端量測 ICMP 的 RTT。由圖 25 及圖 26 的圈圈處比較可發現，將 BR3 的介面 G2/0 關閉後，RIP 可以查覺 VPLS A 發生中斷，因此於 PDR1 及 PDR2 上所呈現的 default route，192.168.20.1 及 192.168.20.2 的路由資訊已經被去除。另外我們在 PDR1 及 PDR2 設定 OSPF，透過 4 條 VPLS 交換路由資訊，在 BR3 的介面 G2/0 將其關閉，模擬電信乙太網路中某條電路中斷影響到一個 VPLS，分別由 PC 往 server 端量測 ICMP 的 RTT。由圖 27 及圖 28 的圈圈處比較可發現，將 BR3 的介面 G2/0 關閉後，OSPF 可以查覺 VPLS A 發生中斷，因此於 PDR1 及 PDR2 上所呈現的 default route，192.168.20.1 及 192.168.20.2 的路由資訊已經被去除。

在另一方面，由圖 29 及圖 30 可發現 RIP 需要大約 180 秒的收斂時間，OSPF 需要約 30 秒的收斂時間。雖然 RIP 及 OSPF 都有透過由路協定知道電信乙太網路中有電路發生障礙，而把受影響的 VPLS 從路由表中剔除，不過這些收斂時間還是無法滿足即時應用的需求。

3. 雙向轉發檢測 (bidirectional forwarding detection, BFD) 機制

此實驗是在驗證於 PDR 的 uplink 使用靜態路由結合 BFD 定期偵測的方式是否有能力偵測電信乙太網路中發生電路中斷或設備故障，進而切換至備用路由達到服務不中斷的效果。我們在 PDR1 及 PDR2 上使用靜態路由方式設定 4 條不同的 VPLS，同時在這 4 條預設路由上啟動 BFD 偵測機制，在 BR3 的介面 G2/0 將其關閉，模擬電信乙太網路中

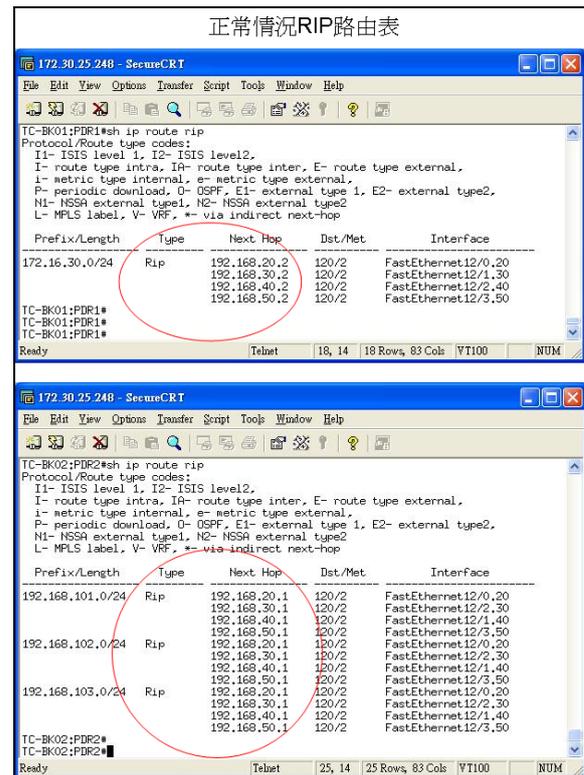


圖 25. VPLS A 中斷前之 RIP 路由圖

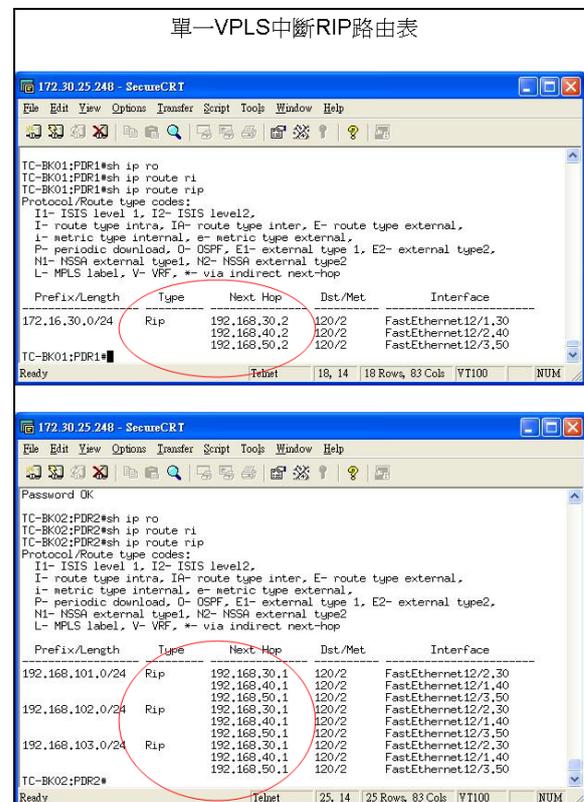


圖 26. VPLS A 中斷後之 RIP 路由圖



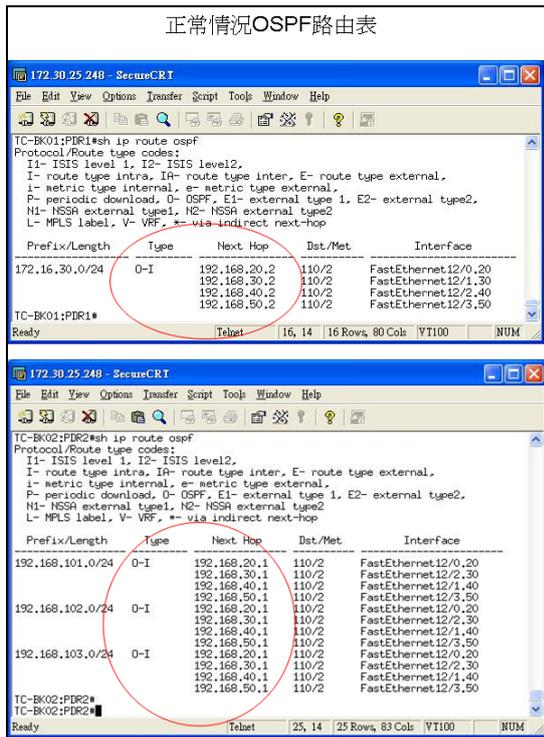


圖 27. VPLS A 中斷前之 OSPF 路由表

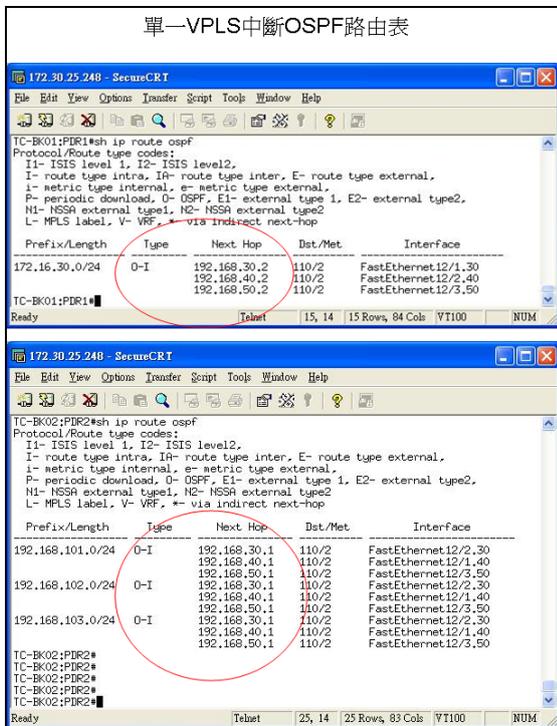


圖 28. VPLS A 中斷後之 OSPF 路由表

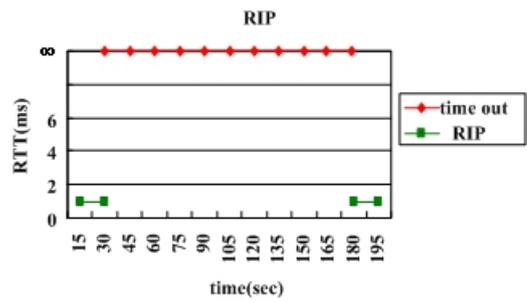


圖 29. 使用 RIP 快速回復圖

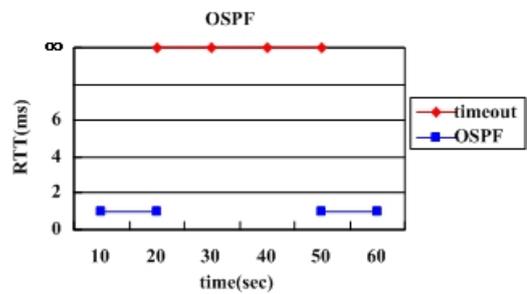


圖 30. 使用 OSPF 快速回復圖

某條電路中斷影響到一個 VPLS，分別由 PC 往 server 端量測 ICMP 的 RTT。由圖 31 及圖 32 比較之後可看出，當 VPLS A 發生中斷後，透過 BFD 偵測可立即發現 VPLS A 中斷，進而將路由剔除。由圖 33 可以發現透過 BFD 偵測機制只會讓網路中斷 1 秒，充分表現出 BFD 快速收斂的能力。

(五) 系統效能測試

我們針對所提出的機制進行系統效能測試。我們 Server1 與 PC1 互相傳送 128Kbps 之 UDP 封包模擬 VoIP 服務，Server2 往 PC2 傳送 30Mbps 之 UDP 封包模擬 IPTV 服務，Server3 往 PC3 傳送 20Mbps 模擬高速下载服務，此三種服務分別使用 iperf 軟體量測 jitter 值。我們在第 15 秒時進行 VPLS 中斷實驗，實驗結果如圖 34 所示。從圖 34 可看出，jitter 有明顯增加但是約略都在 6 ms 以下。在第 25 秒時進行單一節點故障實驗，由圖 34 可發現 jitter 最多增加至 8 ms，但仍是屬於正常可使用的範圍。

五、結論

目前電信業者正積極發展電信乙太網路，相信這也是影響未來網路的架構。在本文中，除了介紹許多電信乙太網路的知識和標準外，也利用這些標準提出一個以電信乙太網路



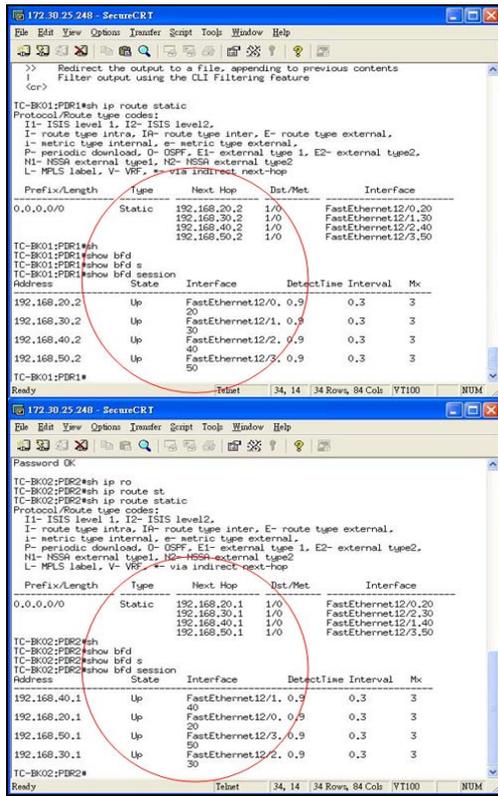


圖 31. VPLS A 中斷前之 BFD 靜態路由圖

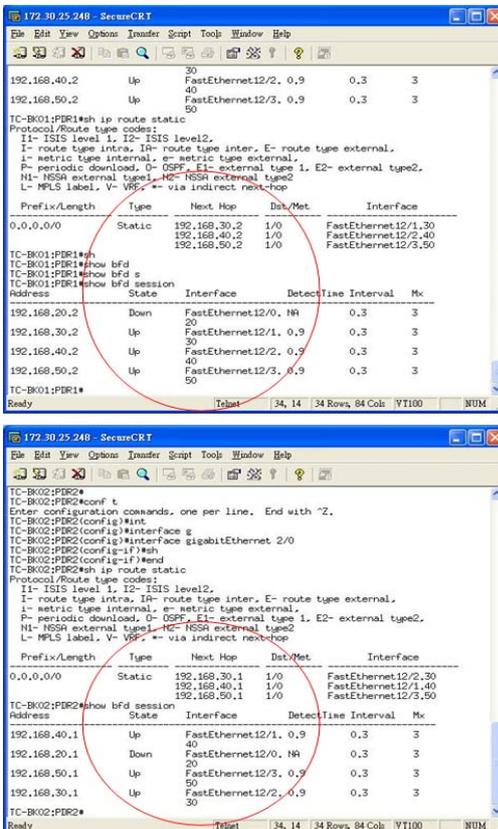


圖 32. VPLS A 中斷後之 BFD 靜態路由圖

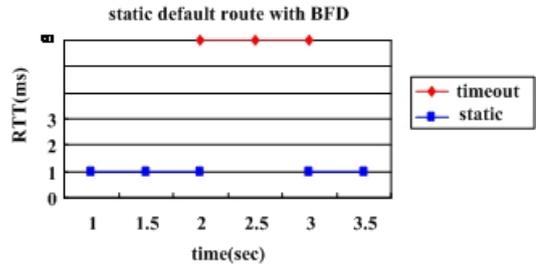


圖 33. 使用 BFD 快速回復圖

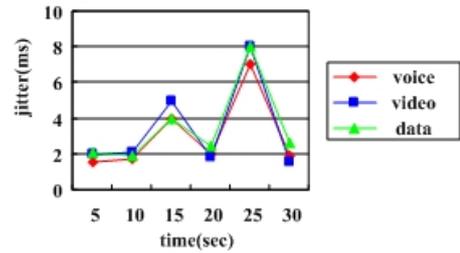


圖 34. 全系統測試之 jitter 量測圖

環境為基礎的 Triple play 服務架構。透過本文的實驗結果證明，雖然在乙太網路環境中頻寬已不是問題，但各項服務頻寬若不進行控管，其服務品質將會互相影響。因此提出於 PDR 佈置速率限制策略，保持 Triple play 服務的品質。除此之外，為有效利用頻寬，本文在 PDR 啟用 RTR 機制，透過定期偵測機制判斷頻寬是否閒置進而動態調整。在另一方面，由於在乙太網路環境中虛擬電路的兩端設備，無法得知中間發生障礙或斷線，因此必須透過其他方式才能得知。本文分別以靜態路由協定及動態路由協定為偵測的方法，實驗結果只有動態路由協定才有辦法明確知道中間網路發生障礙，但是以收斂時間最短的 OSPF 來說也需要 30 秒，對於服務網路而言是無法達到要求的。因此，本文透過在 PDR 上啟用 BFD 偵測機制，偵測中間網路是否中斷。實驗結果顯示只需要 1 秒就可以完成收斂，雖然 BFD 目前還是草擬階段，但是實驗結果證明 BFD 已經可以成為 layer 3 架構中快速收斂的解決方案。

本文所使用的 BFD 機制是屬於乙太網路 OAM 中的障礙偵測。由於 BFD 需要設定偵測對方的 IP 位址，因此屬於 layer 3 的偵測機制，其缺點是只要是針對 IP 的各項 DoS 攻擊，都有可能讓 BFD 誤判為線路中斷，即使虛擬電路完全正常無中斷，也可能讓服務無法正常使用。因此，未來希望提出一個類似 BFD 的偵測機制，卻是運作在 layer 2 的偵測



機制。以 ARP 為例，事先設定好虛擬電路兩端的 MAC 位址，而 layer 2 以上的封包經過特殊定義，透過定期詢問對方 MAC 的方式判斷網路是否中斷，這樣的偵測機制或許會比 BFD 安全、有效率。

參考文獻

1. Aguirre-Torres, L., G. Rosenfeld, C. Syst and C. A. San Jose (2006) High-availability in multipoint to multipoint Ethernet for the delivery of triple play services. Optical Fiber Communication Conference, San Jose, CA.
2. BFD Working Group (2008) *Bidirectional Forwarding Detection (bfd)*. Retrieved May 20, 2009, from <http://www.ietf.org/html.charters/bfd-charter.html>
3. Bocci, M., I. Cowburn and J. Guillet (2008) Network high availability for Ethernet services using IP/MPLS networks. *IEEE Communications Magazine*, 46, 90-96.
4. Gabor, A. F., V. Dobrota, K. Steenhaut and T. Blaga (2008) Preliminary implementation of bidirectional forwarding detection. 11th International Conference on Optimization of Electrical and Electronic Equipment (OPTIM). Brasov, Romania.
5. Hsu, C. W., F. S. Choi, W. S. Lai, T. C. Hou and W. L. Shyu (2006) *Hierarchical Interworking of Draft Kompella and Draft Lasserre Approaches for VPLS*. 2006 Workshop on High Performance Switching and Routing. National Chung Cheng University, Taiwan.
6. IEEE 802.1 Working Group (1998) *802.1D MAC Bridges*. Retrieved May 20, 2009, from <http://www.ieee802.org/1/pages/802.1D.html>.
7. IEEE 802.1 Working Group (2006) *802.1Q- Virtual LANs*. Retrieved May 20, 2009, from <http://www.ieee802.org/1/pages/802.1Q.html>.
8. IEEE 802.1 Working Group (2006) *802.1ad- Provider Bridges*. Retrieved May 20, 2009, from <http://www.ieee802.org/1/pages/802.1ad.html>.
9. IEEE 802.1 Working Group (2008) *802.1ah - Provider Backbone Bridges*. Retrieved May 20, 2009, from <http://www.ieee802.org/1/pages/802.1ah.html>.
10. IEEE 802.3 Ethernet Working Group (2007) *IEEE P802.3ba 40Gb/s and 100Gb/s Ethernet Task Force*. Retrieved May 20, 2009, from <http://grouper.ieee.org/groups/802/3/ba/index.html>.
11. IEEE 802.3 Working Group (2000) *IEEE P802.3ad Link Aggregation Task Force*. Retrieved May 20, 2009, from <http://www.ieee802.org/3/ad/index.html>.
12. Kompella, K. and Y. Rekhter (2007) *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*. RFC 4761, Internet Engineering Task Force (IETF), Washington, D.C.
13. Lasserre, M. and V. Kompella (2007) *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*. RFC 4761, Internet Engineering Task Force (IETF), Washington, D.C.
14. McFarland, M., S. Salam and R. Checker (2005) Ethernet OAM: Key enabler for carrier class metro Ethernet services. *IEEE Communications Magazine*, 43, 152-157.
15. MEF (2001) *The Metro Ethernet Forum*, Retrieved February 20, 2009, from <http://metroethernetforum.org>
16. Mikoczy, E., D. Sivchenko, B. Xu and V. Rakocevic (2007) IMS based IPTV services: Architecture and implementation. Proceedings of the 3rd International Conference on Mobile Multimedia Communications, ICST, Brussels, Belgium.
17. NLANR/DAST (2007) *Iperf*. Retrieved March 18, 2009, from <http://iperf.sourceforge.net/>.
18. Rahrer, T., R. Fiandra and S. Wright (2006) *Triple-play Services Quality of Experience (QoE) Requirements*. TR-126, DSL Forum, Fremont, CA.
19. Sotiropoulos, G. P., D. K. Styliaras, E. A. Kosmatos, C. A. Papagianni, N. D. Tselikas and I. S. Venieris (2006) Triple play service simulation and packet scheduling performance evaluation. International Conference on Digital Telecommunications, National Technical University (NTUA), Greek.
20. Valcourt, S. A. (2007) *DSL—from A to V and Back Again*. Second International Conference on AccessNets, Ottawa, Ontario, Canada.
21. Voip-Info.org (2005) *Maximum Jitter in SLAs*. Retrieved March 12, 2009, from <http://www.malico.com.tw/voip-info/wiki/view/QoS.html>.
22. Zhang, N., M. Xu, R. Liao, H. Yoshiuchi, Y. Ji and G. Saren (2006) A service-classified and QoS-guaranteed triple play mode in FTTH network. First International Conference on Communications and Networking in China, Beijing, China.

收件：100.01.05 修正：100.02.15 接受：100.05.03

