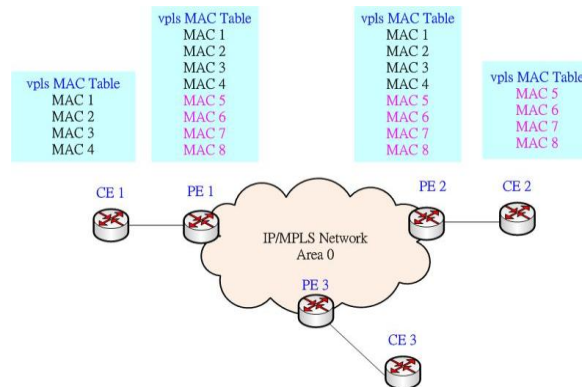


# PBB over H-VPLS 技術應用於多點 L2 VPN 服務

游幼蘋\*、陳俊瑋、徐浩然、朱煜煌  
中華電信研究院

**摘要** — Provider Backbone Bridge over Hierarchical Virtual Private LAN Service(PBB over H-VPLS)技術為第二層 L2 VPN(Layer 2 Virtual Private Network)服務所使用的方式之一，PBB over H-VPLS 可提供點對點 ELAN/EVP-LIN 或多點對多點 ELAN/EVP-LAN 的 L2 VPN 服務連接。本文將探討 PBB over H-VPLS 技術應用於多點對多點 L2 VPN 服務的特點；PBB over H-VPLS 技術除了保留原有 H-VPLS 網路的高擴充彈性與保護機制，同時兼具以下優點: (1)大幅減低服務供應商在 H-VPLS 網路下，中間階層 Provider Edge 路由器所需學習 MAC(Media Access Control)地址數量、服務電路與 PW(Pseudo-Wire)數量，(2)降低服務供應商所需建置之設備資源與後續維運成本。

要參考 RFC4762。



圖一：VPLS 網路

## 一、簡介

L2-VPN(Layer 2 Virtual Private Network)廣泛應用於一般企業用戶、銀行與校園網路，近年來網路技術朝向 MPLS(Multi-Protocol Label Switching) L2 VPN 發展，取代傳統第二層 ATM 與 VLAN Cross-Connect 技術。VPLS(Virtual Private LAN Service)為 MPLS L2 VPN 的一種類型，模擬了 IEEE 802.1D 橋接功能，具備多點到多點的連接與 MAC(Media Access Control)位址學習能力，可讓用戶從多個位置分散的服務據點，像在同一個 LAN 上面，互相交換資訊。當網路慢慢擴大後，VPLS 網路朝向階層式設計，即 H-VPLS(Hierarchical Virtual Private LAN Service)，如同將所有用戶放置在一個規模很大的區域網路，不能將客戶分類，位於中間節點的路由器除了必須學習所有用戶 MAC 位址外，服務電路與 Pseudo-Wire 數量也很高。

服務供應商佈建 H-VPLS 代替 VPLS 主要理由有二點，第一在大型網路情境下 PW 數量仍須 Full Mesh，若服務需要再擴充，也無法要求或超出此網路建置的規模，使得服務擴充彈性低。其二，無論是實體或邏輯拓樸的 PW 連接成 Full Mesh 較無效率，尤其是派送 Multicast 訊務。[1]

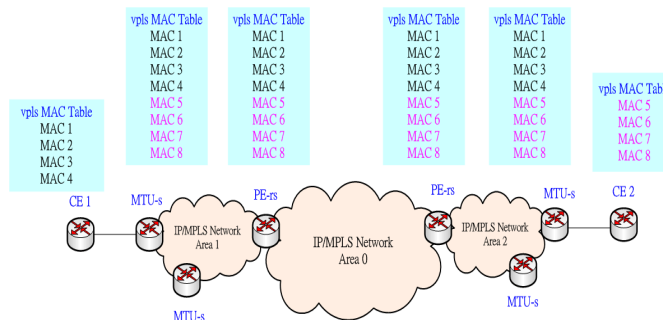
本文接著探討 VPLS、H-VPLS 與 PBB over H-VPLS 技術的特點，並對 PBB over H-VPLS 技術與應用詳細說明。在第三節將探討 PBB over H-VPLS 的 QoS(Quality of Service)設計與 OAM(Operation Administration and Maintenance) 查測機制，在第四節是結論。

H-VPLS 將原 VPLS 網路做階層化網路設計，以減少 PW 連接成 Full Mesh 的數量，同時提升網路擴展性，將 PE 路由器分成 MTU-s(Multi-Tenant Unit switch)與 PE-rs(Provider Edge Routing/Bridge)路由器兩階層，MTU-s 是靠近用戶側 PE，PE-rs 則是網路側 PE，如圖二所示。MTU-s 將會學習到所有用戶的 MAC 地址，同理 PE-rs 也是如此；但 PE-rs 會連接多個的 MTU-s，PE-rs 所學習的 MAC 地址的數量會遠高於 MTU-s，因此 PE-rs 路由器功能之考驗，在於學習 MAC 地址數量，以及用戶 MAC 地址對服務電路之儲存與處理程序能力[2]。

## 二、PBB over H-VPLS 技術

### 2.1 VPLS、H-VPLS 與 PBB over H-VPLS 架構簡介

VPLS 技術為多點 MPLS(Multi-Protocol Label Switching) L2 VPN 服務所使用的技術，架構如圖一，PE(Provider Edge Router)為服務供應商網路中之邊緣路由器，屬於服務供應商的邊緣節點，用來與 VPN 用戶之 CE(Customer Edge Router)路由器進行連接；CE 路由器為 VPN 用戶網路中之邊緣路由器，用於與服務網路之 PE 路由器介接。PE 之間使用的 MPLS LSP/PW 傳送路徑建立，是採用 Full Mesh 方式，LDP VPLS 系統標準主

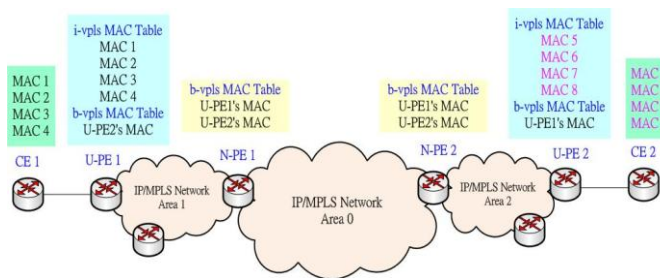


圖二：H-VPLS 網路

PBB(Provider Backbone Bridge) 802.1ah 技術又稱 MAC-in-MAC，屬於 OSI 第二層 (Layer-2; L-2) 網路技

術，將網路區分為服務供應商骨幹領域(Backbone Domain, B-Domain)領域與用戶領域(Service Domain I-Domain)，透過服務供應商與用戶之間明顯分界，實現網路分層能力。在服務供應商領域中，網路交換是依據服務供應商來源與終端地址包裝後，利用終端 Provider Edge 的 MAC 地址為傳送至遠端 Provider Edge 設備，因無須學習用戶 MAC 地址，使中繼設備得以大幅減少 MAC 地址的儲存與處理程序。

PBB over H-VPLS 技術架構為將原 H-VPLS 網路引入 PBB 技術，H-VPLS 網路的 MTU-s 服務將進一步分成 I-Domain VPLS(I-VPLS) 與 B-Domain VPLS(Backbone VPLS)兩部分，其中 I-VPLS 只負責學習用戶 MAC 地址的工作，B-VPLS 負責學習 MTU-s 與 PE-rs 的 MAC 地址，如圖三所示。PE-rs 只有 B-VPLS 服務僅須學習 MTU-s 來源的 MAC 地址，不須學習用戶端 CE MAC 位址。



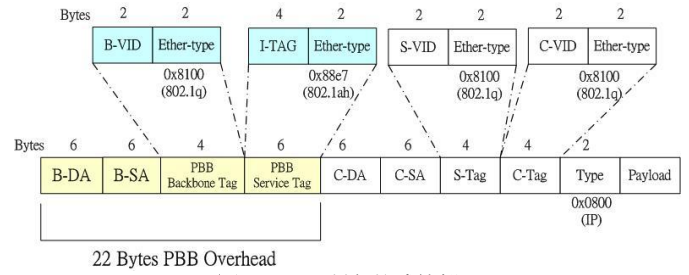
圖三：PBB over H-VPLS 網路

PBB over H-VPLS 技術應用在點對點與多點對多點 VPN 服務的主要特色在於展現網路擴展能力與高彈性擴充應用服務，並提供單純化的端點供裝維運，以及完整的 OAM 障礙查測功能。

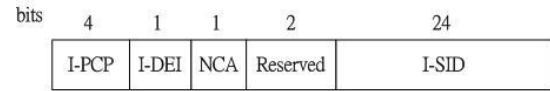
## 2.2 PBB 封包格式

PBB 封包封裝方式即原有乙太網路封包再加入 PBB Overhead，可清楚畫分用戶端和服務供應商的界線，用戶端為傳統乙太網路格式，PBB Overhead 則為服務供應商範圍，PBB 將用戶 MAC 地址封裝在服務供應商 MAC 位址內，實現用戶隔離，如圖四所示。

其中 PBB Overhead 包含一個 I-TAG 欄位，I-PCP(Instance Priority Code Point)為標示決定此用戶傳送優先等級，I-DEC(Instance Drop Eligibility Indicator)為標示用戶優先丟棄欄位，NCA(No Customer Address)為標示無用戶端位址，I-SID(Interface Service Instance Indicator)為標示介面服務範例，長度為 24-bits，可提供高達  $2^{24}$  (16777215)個服務範例，即此網路內可容納  $2^{24}$  個用戶，如圖五所示[3]。



圖四：PBB 封包格式範例



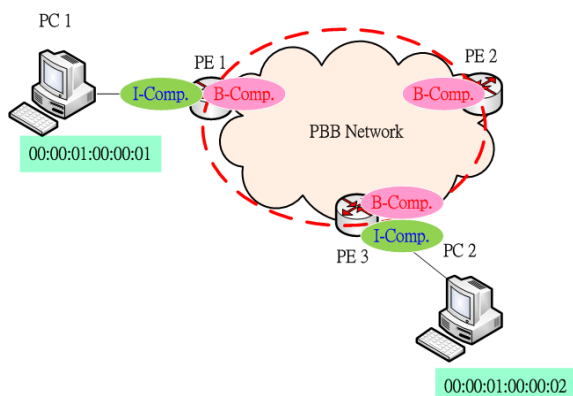
I-PCP : Instance Priority Code Point  
I-DEC : Instance Drop Eligibility Indicator  
NCA : No Customer Address  
I-SID : Interface Service Instance Indicator

圖五：I-TAG 封包格式

## 2.3 802.1ah PBB 工作原理

PBB 的 BEB(Backbone Edge Bridge)角色包含 I-Component 與 B-Component 兩種功能。I-Component 的功能包括將用戶端網路至服務供應商網路的 MAC 地址映射功能，與從服務供應商網路至用戶端網路 MAC 地址映射功能兩部分。從用戶端網路至服務供應商網路的 MAC 地址映射功能說明如下，當 BEB 設備收到用戶端封包後，I-Component 首先查詢目的端用戶 MAC 地址映射表，以確認用戶封包到服務供應商網路之目的端端點，即封包格式的 B-DA 欄位；然後再封裝用戶封包，同時將 I-TAG 加入封包中，以交給 B-Component 處理。倘若 I-Component MAC 表還沒學習到目的端用戶 MAC，或用戶訊務為廣播、群播服務時，此時 I-Component 會採用特別的 MAC 地址，其 MAC 地址格式是 01-1E-83-nn-nn-nn，以進行訊務群播至遠端 BEB 設備，其中 nn-nn-nn 位址格式為 24bits I-TAG 轉為 16 進位。從服務供應商網路至用戶網路 MAC 地址映射功能說明如下，經由 I-TAG 查訊後，BEB 的 B-Component 移除 PBB 封裝後，封包送至 I-Component，I-Component 依據 CE MAC 表將封包轉發至目的用戶網路。

B-Component 為 I-Component 與所有服務供應商網路 PE 的橋梁，在用戶網路往服務供應商網路方向，首先根據 I-TAG 於用戶封包中插入 PBB Backbone TAG 欄位，即尋找對應的 B-VLAN，再將封包送至特定 B-VLAN 服務供應商網路中轉發。在服務供應商網路往用戶網路方向，直接移去 PBB Backbone TAG 欄位，交由 I-Component 處理，如圖六所示[4]。



圖六：802.1ah PBB 網路學習與轉送行為範例

I-Component 對應至特定的 B-Component，是由供裝系統指定，B-Component 如何對應至 I-Component，則是依據 I-TAG 欄位之 I-SID，同一個用戶所有的 I-Component 之 I-SID 皆相同。

PBB over HVPLS 技術亦採用上述 802.1ah 工作原理，唯一差別是將 B-Component 對應到具備有 MPLS Traffic Engineer 機能的 H-VPLS 架構中，以 B-VPLS 取代原有的 B-VLAN 的觀念，搭配已商用化成熟的 H-VPLS 技術傳送 B-Domain 封包至骨幹網路中。

PBB 的 Overhead 會使得頻寬使用率下降一點，一般情況來說乙太網路皆以長封包為主，以實體 1Gbps 頻寬計算，PBB Overhead 相較於 Multi-Segment 技術封包格式，理論計算相差約為 1.1%(約 11Mbps)左右，實測值與理論值相近。

### 三、 PBB over H-VPLS 應用於多點 L2 VPN 服務

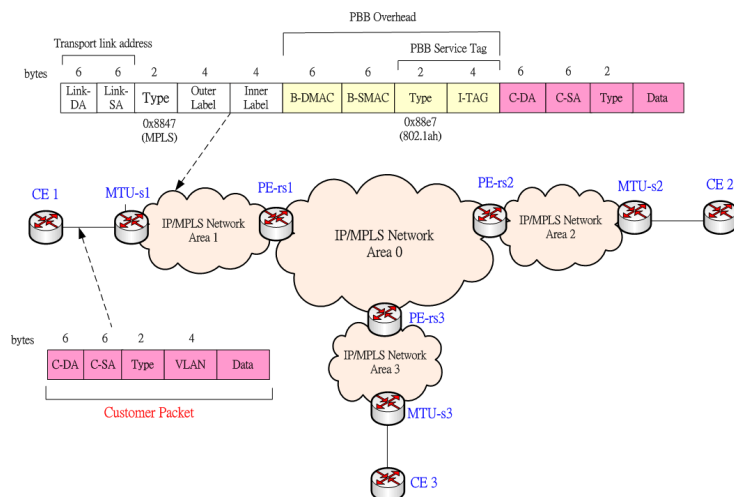
#### 3.1 應用架構說明

MPLS L2 VPN 的應用分為 VPLS 與 VLL(Virtual Lease Line)兩種，MPLS 提供兩種控制協定 LDP(Label Distribution Protocol)和 RSVP-TE(Resource Reservation Protocol-Traffic Engineering)，用來建立 MPLS 隧道路徑。MPLS L2 VPN 封包格式有兩層標籤，外層標籤為 LDP 或 RSVP-TE 所建立之 Tunnel，內層標籤由 T-LDP(Target- Label Distribution Protocol, RFC4762)或是 BGP(Border Gateway Protocol, RFC4761)建立，其用途為 PE 間辨識不同 VPN 用戶[5]。

PBB over H-VPLS 應用架構與封包格式如圖七所示，所有的 PE 架構出階層式 MPLS 跨區網路架構，其中 MTU-S 為面對用戶端之路由器，所有的 PE-rs 則組成骨幹網路，CE1、CE2 與 CE3 為用戶網路的路由器，各個 CE 與 MTU-s 介接使用的封包格式，利用 VLAN ID 來識別用戶。以 CE1 往 CE2 方向為例，從 MTU-s1 由 I-Component 至 B-Component 經由 PIP(Provide Instance Port)機制，PBB Overhead 而經過 B-Component VPLS 技術之後加入 MPLS 兩層標籤後，送至 MPLS 網路經由 PE-rs 傳送到遠端 MTU-s2，MTU-s2 依據 I-TAG 欄位之

I-SID 分辨 VPN 用戶，此架構之 PBB Overhead 不包括使用 PBB Backbone TAG 欄位，其原因為從 MTU-S 開始已使用 VPLS 技術達成一個 B-Component 橋接領域，不需要 PBB Backbone TAG 欄位再區分其他橋接領域[6]。

CE1 與 CE2 之用戶封包為標準乙太網路封包格式，經過 MTU-s 後，封裝成 MPLS 格式，並加入 PBB Overhead 總計 18bytes。



圖七：PBB over H-VPLS 網路應用架構

當兩組不同用戶傳遞多點電路，若遠端 MTU-s 節點不為某一用戶服務建立點時，廣播、未知及群播類型封包仍會複製到遠端 PE 節點，經過 I-SID 確認後決定是否轉送至對應的 I-Component 或丟棄該封包，考量避免 B-Domain 內的廣播、未知及群播訊務泛洪(flooding)太多，可透過標準 802.1ak MRP(Multiple Registration Protocol)的 MMRP(Multiple MAC Registration Protocol)技術將泛洪抑制及最佳化，有效提升網路頻寬資源。

#### 3.2 QoS(Quality of Service)設計

MTU-s 用戶側負責所有服務用戶 QoS 管控，將依據用戶所申請的服務等級依照優先權值進行分類、排程與上下行速率限制，服務包含語音、上網、VPN、MBH(Mobile Backhaul)與視訊服務等。

B-Component VPLS 在規劃上具備未來網路與服務擴充彈性，視網路規模大小決定是否規劃 PBB Backbone Tag，相同客戶性質規劃同一個 B-Component VPLS，如大專院校或銀行業，或規劃成金銀銅三種等級客戶群分別在同一個 B-Component VPLS。若單一客戶有多組 VPN 據點在同一實體路徑時，可利用網綁速率集縮，使客戶共享最大頻寬，例如公司分部彙集至總部。

#### 3.3 OAM(Operation Administration and Maintenance)查測機制

PBB over H-VPLS 架構下之多點查測方式相同於以往端對端之查測方式，採甲與乙兩端點，若以網路多點方式進行，將增加網路上較多頻寬，如圖八所示。

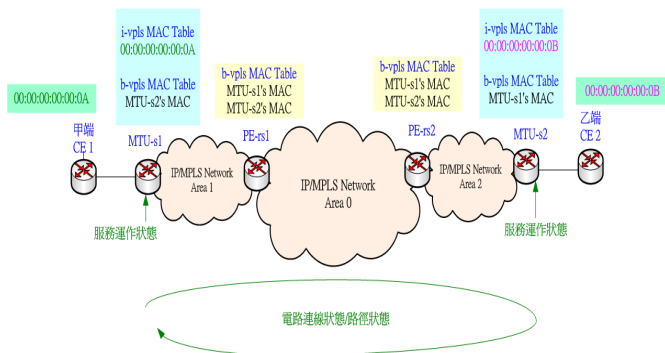
端對端電路查測包含近端與遠端 MTU-s 設備之 VPLS 服務運作狀態、端對端電路連線狀態與端對端路徑狀態。CE 設備會學習到用戶端所有 MAC 資訊，

MTU-s 設備在 I-Component 學習到用戶端所有 MAC 資訊，B-Component 則學習到遠端 MTU-s 設備的 MAC 資訊，而 PE-rs 設備只會學習到所有 MTU-s 設備的 MAC 資訊。

端對端電路連線狀態查測類似 Ping 的觀念，有兩種應用方式，第一種為先查詢到遠端 MTU-s 上用戶的 MAC，在近端 MTU-s 利用 MAC 折回測試，確認從近端 MTU-s 至遠端 MTU-s 回應狀況並同時可以知道兩端 RTT(Round-Trip Time)的時間。

第二種應用方式為直接於甲端 MTU-s 埋入一個測試用的 MAC，例如 00:00:00:00:00:0A，然後於乙端 MTU-s 埋入一個測試用的 MAC，例如 00:00:00:00:00:0B，兩端皆進行 MAC 折回測試，確認端對端的回應狀況。類似 LAN 的環境，於電路連線狀態查測第一步必須確定測試用的 MAC，用戶端沒有被使用，如此即時性的查測建議測試用 MAC 埋入時間不需太長，以免佔用 MAC Table，完成端對端電路連線狀態查測後，最後進入端對端路徑狀態查測。

端對端路徑狀態查測類似 Traceroute 的觀念，利用 MAC 追蹤路徑測試，確認近端 MTU-s 至遠端 MTU-s 路徑，包含所經過的 MTU-s 與 PE-rs 資訊，同時也包含 RTT 的時間，可依據 RTT 的時間來了解端對端網路狀態。



圖八：端對端電路查測

在 PBB over H-VPLS 架構之查測流程中，首先判斷甲乙兩端服務運作狀態是否正常，包含服務建立與 MPLS 之 LSP 狀態，若狀態皆判斷運作正常，則往下一步確認端對端電路連線狀態與路徑狀態。

## 結論

PBB over H-VPLS 用於多點 L2 VPN 服務其目的除了保留原有 H-VPLS Traffic Engineering 與保護機制的好處外，另外可以減低 Network-facing Provider Edge 路由器學習用戶端 MAC 地址與虛擬電路(Pseudo-Wire)數量，以多組 I-SID 對應於 MTU-s 側 PW 來識別不同用戶點對點與多點服務，避免 H-VPLS 技術下，單一用戶於 PE-rs 須建立一組 PW 的供裝行為模式，如此可大幅提高 PE-rs 與骨幹網路收容用戶服務電路的數目，降低設備建置與維運成本。

## 參考文獻

- [1] Zhuo Xu, "Designing and Implementing IP/MPLS-Based Ethernet Layer 2 VPN Service", 2010.
- [2] F. Balus and Ali Sajassi, "Extensions to VPLS PE model for Provider Backbone Bridging", IETF Internet draft, Sept. 2009, work in progress.
- [3] IEEE 802.1ah, "Virtual Bridged Local Area Networks, Amendment 6: Provider Backbone Bridges", June 12th, 2008.
- [4] Weijia Zhu, "Designs of PBB Interoperating with H-VPLS based on MPLS Network", IEEE 2010.
- [5] 游幼蘋、陳美君、王井熙, "VPLS技術應用於上網服務", 全國電信研討會, 2010.
- [6] IETF L2VPN Working Group, "Extensions to VPLS PE model for Provider Backbone Bridging", July 2010; <http://tools.ietf.org/html/draft-ietf-l2vpn-pbb-vpls-pe-model-02>