行政院所屬各機關因公出國人員出國報告書

（出國類別：實　習）

赴美國參加「網際網路交換設備技術」實習

報　告　書

服務機關：中華電信股份有限公司
國際電信分公司

出國人 職　稱：助理工程師　助理工程師　助理工程師

姓　名：李訓忠　劉義信　鄭睿夫

出國地點：美　國

出國期間：91.9.15～91.9.26

報告日期：92.2.26

系統識別號:C09200958

公 務 出 國 報 告 提 要

頁數: 22　含附件: 否

報告名稱:

赴美國參加網際網路交換設備技術實習

主辦機關:

中華電信國際電信分公司

聯絡人／電話:

／

出國人員:

李訓忠　中華電信國際電信分公司　網路處　助理工程師
劉義信　中華電信國際電信分公司　網路處　助理工程師
鄭睿夫　中華電信國際電信分公司　網路處　助理工程師

出國類別: 實習

出國地區: 美國

出國期間: 民國 91 年 09 月 15 日 -民國 91 年 09 月 26 日

報告日期: 民國 92 年 02 月 26 日

分類號/目: H6／電信　／

關鍵詞:　網際網路交換設備技術

內容摘要: 職等三人奉派赴美國參加「網際網路交換設備技術」實習，此次行程除參加「Advanced MPLS and VPN Solutions」的訓練課程及「New IP Solution and Technology」相關技術的研討外，同時實地參觀Cisco EBC(Executive Briefing Center)由Cisco相關人員針對VPNSC及MPLS VPN網路相關技術爲我們作說明及介紹。本報告共分爲四節：第一節：前言簡介本案出國的緣由及實習的行程。第二節：VPN基本概論第三節：MPLS VPN概論內容包括MPLS VPN基本概念、網路架構、MPLS網路中標籤交換、封包的傳送及MPLS VPN網路的運作原理。第四節：結論與心得

本文電子檔已上傳至出國報告資訊網

摘　　要

職等三人奉派赴美國參加「網際網路交換設備技術」實習，此次行程除參加「Advanced MPLS and VPN Solutions」的訓練課程及「New IP Solution and Technology」相關技術的研討外，同時實地參觀 Cisco EBC(Executive Briefing Center)由 Cisco 相關人員針對 VPNSC 及 MPLS VPN 網路相關技術為我們作說明及介紹。

本報告共分為四節：

第一節：前言

簡介本案出國的緣由及實習的行程。

第二節：VPN 基本概論

第三節：MPLS VPN 概論

內容包括 MPLS VPN 基本概念、網路架構、MPLS 網路中標籤交換、封包的傳送及 MPLS VPN 網路的運作原理。

第四節：結論與心得

目　　錄

一、前言

因應跨國企業客戶對IPVPN業務服務殷切的需求，本公司業務、工務及相關單位特別於91年5月成立IPVPN工作小組，工作小組除定期召開會議積極進行IPVPN市場規劃及IPVPN網路相關建設外，同時針對各單位工作進度定期追蹤及檢討。

此次實習乃為配合該項業務的推動及讓相關的技術維護人員對IPVPN網路中使用的MPLS技術有更進一步的研究及瞭解，以便日後能提供給客戶高品質的通信服務及IPVPN相關的技術諮詢。

本分公司依據「網路國際通服務系統擴充案」合約規定，核派網路處三中心李訓忠、劉義信及海衛處四中心鄭睿夫三人赴美國參加「Advanced MPLS and VPN Solutions」訓練課程及「New IP Solution and Technology」相關技術的研討。

實習日程如下:

(一)、九十一年九月十五日
去程：台北 – 美國

(二)、九十一年九月十六日至九月十九日共四天
「Advanced MPLS and VPN Solutions」訓練課程

(三)、九十一年九月二十日
參觀Cisco的Executive Briefing Center(EBC)

(四)、九十一年九月二十一日至九月二十二日
例假日

(五)、九十一年九月二十三日至九月二十四日共二天
「New IP Solution and Technology」技術的研討

(六)、九十一年九月二十五日至九月二十六日
返程：美國 – 台北

二、VPN 基本概論

所謂 VPN(Virtual Private Network)是指服務提供商(Service Provider)在其所提供的公眾網路上為企業客戶建構虛擬的專用網路，從客戶的角度來看，VPN 就像是客戶的一個專用網路。

服務提供商公眾網路的範圍包括公共骨幹網路和周邊相關設備，通信點彼此分離的 VPN 客戶透過客戶端設備連接到服務提供商的邊界設備，再經由服務提供商的公共網路架構其企業客戶的 VPN 網路。

傳統的 VPN 網路主要兩種架構的方式：

1)專線電路 VPN 或虛擬電路 VPN

採用虛擬電路 VPN 的方式(如 ATMPVC、FRPVC 等)，VPN 客戶的設備直接連接到服務提供商的邊界設備，由服務提供商負責建立 VPN 客戶通信點之間的虛擬電路連接，客戶對屬於自己 VPN 的通信點之間的路由進行自主的控制和管理。

2)基於客戶端設備的 VPN。

基於客戶端設備的(CE-Based)VPN，該 VPN 的功能全部落在客戶端的設備，客戶可以透過購買相對應的 VPN 設備或者在現有的路由器、閘道器甚至於 PC 上安裝相對應的 VPN 功能軟體就可以獨立構建的 VPN。VPN 的成員通信點之間通常是透過非信任的服務提供商的公網實現互連，所以一般客戶端設備的 VPN 都使用加密機制保護通信點之間跨服務提供商公網的通信流量。這個解決方案的最大缺點就是客戶需要購買、配置和維護昂貴的 VPN 閘道設備，同時也意味著需要高素質的網路管理人員對 VPN 閘道設備和整個 VPN 網路運行、安全進行有效的管理，採用加密機制也會對設備的轉發性能和網路的擴展性產生很大的影響。

隨著 IP 資料通信技術的不斷發展和新技術的湧現，許多設備製造商提出基於服務提供商(Service Provider-Based)網路的 VPN 解決方案。這種基於服務提供商網路的 VPN 解決方案受到了市場的廣泛關注，並且市場也呈逐年遞增的趨勢。基於網路的 VPN 解決方案允許服務提供商使用其 IP 公共骨幹網支持大量的 VPN 客戶，並且這種基於網路的 VPN 也具有比較好的擴展性和可管理性。服務提供商還可以結合 VPN 向客戶提供其他一些相關的 IP 增值業務(如 Internet 接入，防火牆，IP 服務品質(QoS)及 NAT 等)。

在 IP 網上建構 VPN 的優點：

■由於利用 IP 網路廉價和普遍的 WAN 通信資源，IP 網路上的 VPN 與傳統意義的 VPN 相比，通信費用更為低廉。

■IP 網路建構的撥號 VPN 可擴展能力強，用戶在家或出差到外地能夠透過 IP 網路接取公司內部的網路。

IPVPN 無論是對服務提供商或是對客戶都是一個新的商機，並且它將隨著網路技術(隧道技術、MPLS 技術等)的不斷發展，使其在安全性、可靠性方面更趨成熟。

IP 網路的流量控制與擁塞控制

在 IP 網路中，如果不對進入網路的流量進行控制，就會使網路某些單元(路由器或交換機)中的緩衝器出現溢出，從而引起 IP 資料封包的丟失，使網路產生擁塞。當網路出現擁塞時，網路就不能保證其性能目標，對於那些已經建立的資料流程，網路就不能實現與客戶間商定的服務品質(QoS)承諾。

爲了在 IP 網路中提供具有服務品質的業務，就必須對 IP 網路進行流量控制和擁塞控制，而這種控制是通過 IP 網路提供的資訊傳送能力(IP Transfer Capability，IPTC)實現的。

(1)確定頻寬(Dedicated Bandwidth，DBW)傳送能力

用於支援對時間延遲敏感的業務應用，其目標是完成各種確保品質的端到端通道的 IP 資料封包傳送。

(2)統計頻寬(Statistical Bandwidth SBW)傳送能力

用於支援對時間延遲沒有嚴格限制，但對資訊丟失率有一定要求的業務應用，這種傳送能力在網路中不進行 IP 資料封包的再分段，並且盡可能的確保所傳送 IP 資料封包的順序完整性。

(3)盡力而爲(Best Effort，BE)傳送能力

用於支援對時間延遲和資訊丟失率都沒有嚴格限制的業務應用，其目標是在有可用的網路資源情況下，盡力而爲的完成 IP 資料封包的傳送。網路對這種傳送能力不提供任何 QoS 承諾。

IP 網路的流量控制是網路正常工作時採取的一系列措施，使得網路避免出現發生擁塞的條件，從而避免造成網路的擁塞，這些措施包括：網路資源管理、接入允許控制、流量參數控制、非一致性 IP 資料封包的標記和 IP 資料封包的有計劃分流等。

IP 網路的擁塞控制是網路擁塞時採取的一系列措施，從而使得網路擁塞的強度、持續時間和擴散的影響減至最小，具體措施包括：標記 IP 資料封包的丟棄、非 QoS 承諾 IP 資料封包的丟棄等。在 IP 網路中對通過節點（或介面）IP 資料流程進行一致性檢測，可以將 IP 資料封包標記成三種顏色，即："紅色"、"黃色"和"綠色"。"綠色"的 IP 資料封包符合一致性要求，網路要嚴格提供 QoS 承諾；對於"黃色"的 IP 資料封包，網路在一定程度上給予 QoS 承諾，而對於"紅色"的 IP 資料封包，網路將不給予 QoS 承諾。當網路發生擁塞時將首先丟棄"紅色"的 IP 資料封包，如果網路擁塞還不能緩解的話，將繼續丟棄"黃色"的 IP 資料封包，直到網路擁塞解除為止。

三、MPLS VPN 概論

多重通訊協定標籤交換（Multi-Protocol Label Switching, MPLS）是一種在開放的通信網上利用標籤引導資料高速、高效傳輸的新技術，是由 IETF(Internet Engineering Task Force)所發展出來的網路標準。它是實現寬頻網際網路最熱門的技術；其目的是要提供一個更具彈性、擴充性及效率更高的 IP 層交換技術。

MPLS 是一種整合了標籤交換架構與網路層的路由機制的技術，最基本的概念是將進入 MPLS Network 的封包(Packet)配置一個固定長度的標籤(Label)，在 MPLS Network 中會根據標籤做封包的轉送(Forwarding)，由 Label 來決定封包在網路上的路徑，不會再看 Layer 3 的 IP Header。

傳統 IP Network 的運作方式：
封包(Packet)在一般的 IP Network 傳遞時，路由器的運作是以所謂的 "Store and Forward" 的程序來作封包路由的選擇及轉送，所以當路由器收到一個封包時，會先儲存該封包、分析路由、轉送封包到下一個適當的路由器，而當此路由器又收到下一個封包要傳送到相同的目的地時，它必須重覆執行相同的程序(儲存、分析、轉送)，這樣的處理方式是很沒有效率而且會耗用路由器大量的 CPU 處理能力及記憶體空間，此外傳統的路由器是以軟體的處理方式轉送 IP 封包，而 MPLS 的技術則是引用與 ATM 交換技術類似的標籤交換(Label Switching)技術，簡化了路由器的轉送功能直接利用 Switching Fabric 來轉送封包到達目的地。

MPLS 市場的發展大約分爲三個階段：

- 第一階段(2000-2002 年)
  原有技術和設備繼續發展，但 MPLS 設備開始進入市場，現有高端設備將作軟体升級來提供 MPLS 功能，以與新入網的 MPLS 設備互連互通。
- 第二階段(2003-2006 年)
  MPLS 設備以其優良的性能迅速佔領市場，其特點爲原有設備不再發展，MPLS 設備從骨幹網延伸到客戶終端。全面實現 MPLS 技術

的各項標準化協定。

■第三階段（2007 年以後）：

MPLS 技術與光纖傳輸交換技術融合在一起，提供性能更爲優良的高效能服務。

MPLS VPN 專門術語

◆P-Network

P-Network(Provider Network)是指服務提供商(Service Provider)所控管的骨幹網路。

◆C-Network

C-Network(Customer Network)是指 VPN 客戶端的網路，一般是指客戶端區域網路及相關的設備。

◆CE router

CE router(Customer Edge router)屬於 C-Network 的一部份。

CE router 的 interface 透過實体連線和服務提供商的 PE router 介接。

◆PE router

PE router(Provider Edge router)屬於 P-Network 的一部份。

PE router 的 interface 透過實体連線和客戶網路端的 CE router 介接。

◆P router

P router(Provider Core router)屬於 P-Network 的一部份。

◆Border router

所謂邊際路由器(Border router)，顧名思義是指該路由器是用來和另一個服務提供商的 MPLS VPN 網路作介接。

◆Route-target

Route-target 由 64 bits 所組成，服務提供商會針對不同的 MPLS VPN 客戶設定不同的 Route-target。

Router-target 分為 Route-target import 及 Route-target export。

◆VPN-IPv4 addresses

VPN-IPv4 addresses 由 64 bits 的 RD(Route Distinguisher)和 32 bits IP address 所組成。

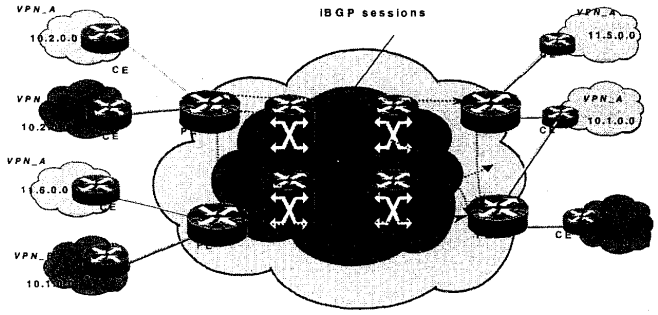
◆VRF

VRF 是指 VPN Routing and forwarding，在 MPLS VPN 網路的 PE router 針對不同的 VPN 客戶均會有各自的 VRF table。

◆VPN-Aware network

所謂 VPN-Aware network 是指一個服務提供商的骨幹網路，同時該骨幹網路已啟動了 MPLS VPN 的功能，並能夠提供 MPLS VPN 的相關服務給其所屬的 IPVPN 客戶。

MPLS Network 的組成



MPLS VPN 骨幹網路是由多個具有標籤交換能力的路由器 LSR(Label Switching Router)互相連結所組成，根據在 MPLS 網路內扮演角色的不同，LSR 可分為：

1)PE router(Edge LSR)

PE router 又稱為 Edge LSR(Edge Label Switching Router)，依其在 MPLS 網路中所扮演的角色可再區分為：

❶ Ingress LSR：Ingress LSR 負責將進入 MPLS 網路的 IP Packet 貼上標籤(Push Label)。

❷ Egress LSR：當 Packet 要離開 MPLS 網路到一般 IP 網路時，Egress LSR 負責去除標籤(Pop Label)。

PE router 和客戶端的 CE router 直接連接，並利用 EBGP、OSPF、RIPv2 或 static route 中任一種 Routing Protocol 和 CE router 互相交換路由資訊(Routing Information)。

骨幹網路中的 PE 和 PE routers 間利用 MP-iBGP 互相建立 iBGP session 並交換 VPN 的相關資訊，該 VPN 相關資訊包括 connected sites、VPN-IPv4 addresses、 Extended Community 及 Label。

2)P router(Core LSR)

P router 又稱為 Core LSR，Core LSR 位於 MPLS 網路的核心，負責做標籤轉換 (Label Swap)。

P router 和 PE router 間運行 IGP(Interior Gateway Protocol)，換句話說 P 和 PE routers 間使用相同的 IGP，例如 OSPF routing protocol。

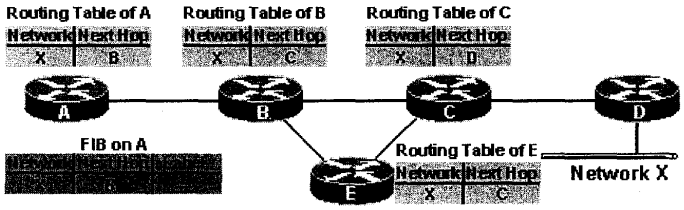
對 P router 而言，不需要運行 BGP(Border Gateway Protocol)，它也沒有 VPN routing information。

Label Assignment and Distribution 的過程

(1) LSR Routing Table 的建立

在 MPLS 網路中所有的 LSR 利用 routing protocol 來交換路由資訊，建立自己的 IP routing table，並根據 routing table 建立自己的 FIB (Forwarding Information Base)，此時的 FIB 中並沒有 Label 的資訊。

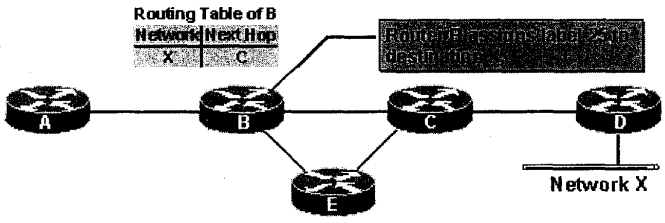
(1) LSR Routing Table 的建立



(2) LSR Allocating Label 過程：

當 LSR 路由器開始啟動 MPLS 功能時，會根據由 IGP(如 RIP、OSPF)學來的 routing table 內容，對於使用相同處理方式、相同 path、到達相同目的地 IP subnet 的 routing entry 做彙整(aggregation)及分類後 Assign Label。

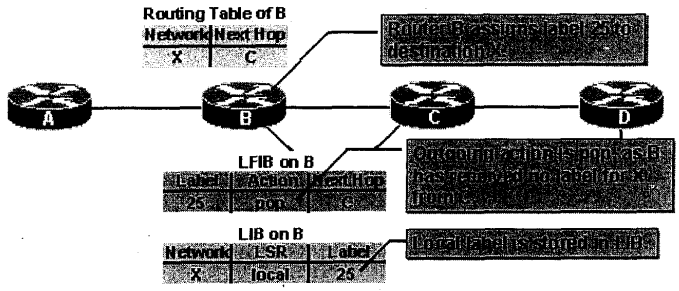
(2) LSR Allocating Label 過程



(3) LSR 初步建立自己的 LIB 及 LFIB：

將前面步驟 Allocating 的 local Label 資訊儲存於 LIB(Label Information Base)和 LFIB(Label Forwarding Information Base)中，此時的 LFIB 中只有 Local Label 的資訊並沒有 outgoing Label 的資訊。

(3) LSR 初步建立自己的 LIB 及 LFIB

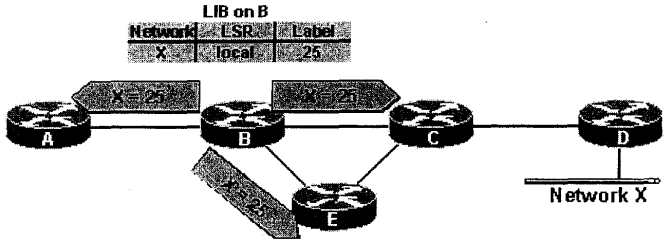


(4) LSR Label Distribution 過程：

LSR 將 Local Label 資訊傳送(Distribution)給相鄰的 LSR，不論這相鄰的 LSR 是 local LSR 的 downstream 或 upstream 都會傳送，而 Label Distribution 是藉由相鄰的 LSR 間執行 LDP(Label Distribution Protocol)的協定來互相交換彼此的 Label 資訊。

MPLS Device 會 send/receive LDP，LDP 是用 UDP(User Datagram Protocol)去 discovery neighbors，並和 Neighbors 作溝通確認對方是否有啟動 MPLS 的功能，若 neighbors 有啟動 MPLS 的功能則用 TCP (Transmission Control Protocol)去交換彼此 Label information。

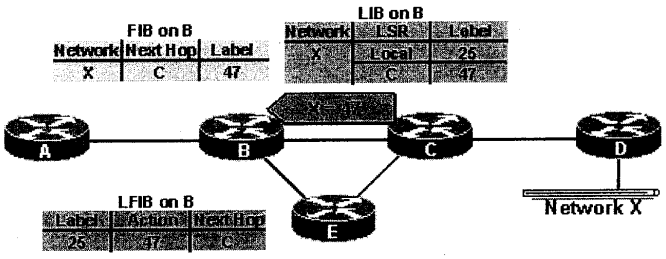
(4) LSR Label Distribution 過程



(5) LSR 收到相鄰 LSR 送來的 Lable 資訊後彙整過程：

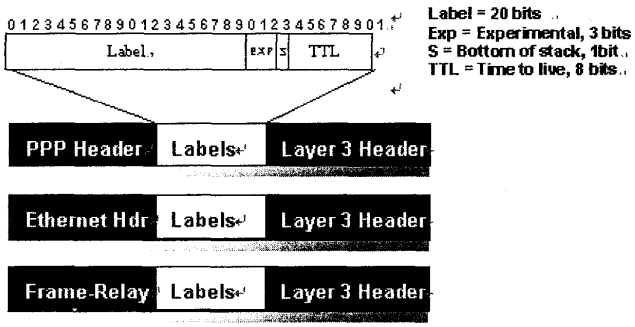
最後每個 LSR 根據接收到相鄰 LSR 送來的 Label 資訊後，新增這些 Label 資訊於自己的 LIB 中，並根據 routing table 得到的最佳路徑，獲知到某網段的 Next-hop LSR 所送來的 Label 資訊，插入到 LFIB 的 outgoing Label 資料結構中。

(5) LSR 收到相鄰 LSR 送來的 Lable 資訊做資訊的彙整過程



MPLS Label 的 Format

Label 是一個 4Bytes、固定長度、locally-significant identifier 類似在 ATM 網路中 VPI(Virtual Path Identifier)/VCI(Virtual Circuit Identifier)或是 Frame-Relay 網路中的 DLCI(Data Link Circuit Identifier)，Label 是被插入於 Packet 的第二層資料鏈結層(Data Link Layer)與第三層網路層(Network Layer)Header 之間。



Packet 在 MPLS 網路中傳送的過程

Ingress LSR(Router A)：

IP Packet 進入 MPLS 網路的第一顆 LSR 路由器稱為 Ingress LSR，當 IP Packet 進入 Ingress LSR 首先會查看 Packet 中的 Destination IP address，並且在 FIB 中 lookup 是否有符合的 IP network，如果有則進一步查看 FIB 中相對應的 IGP Label(interior Label)欄位其值為何？(例如：IP = X，Label=25)，當 Packet 從 Ingress LSR 送出時，會在此 Packet 中打上 IGP Label=25 的標示，再傳送出去。

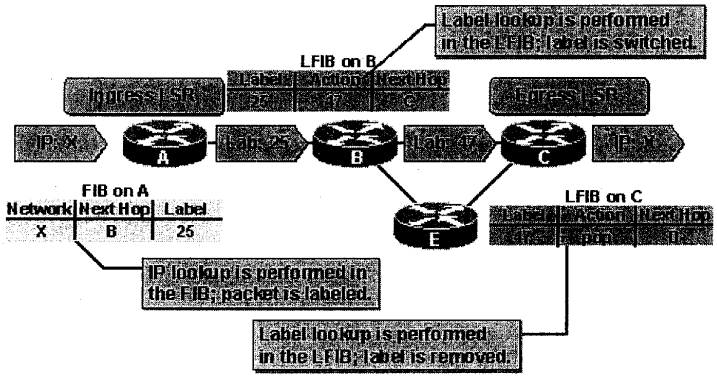
Core LSR (Router B)：

當帶有 Label=25 的 Packet 傳到 Router B 時，Router B 會查看(lookup)他的 LFIB 的資料，看看是否有 Inbound Label=25 的 entry，如果有則再查看此 entry 中 Outgoing Label 的欄位值為何？(例如 Outgoing Label=47)，所以 Packet 中的 Label 快速的被置換(Label=25⇨Label=47)並往下一個節點傳送出去。

Egress LSR(Router C)：

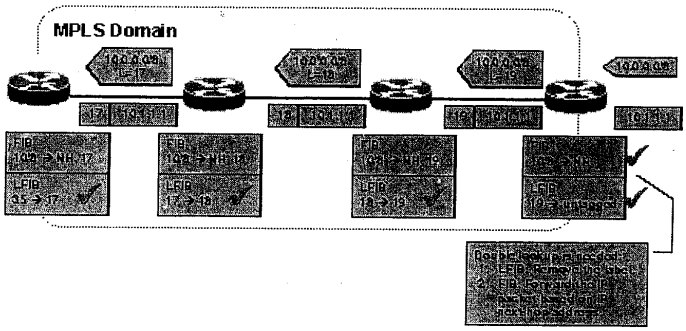
當帶有 Label=47 的 Packet 傳到 Router C 時，Router C 會查看(lookup)他的 LFIB 的資料，看看是否有 Inbound Label=47 的 entry，如果有則再查看此 entry 中 Outgoing Label 的欄位值為何？(例如 Outgoing Label=Pop)，所以 Packet 中的 Label 被移除，此時已離開 MPLS 網路再進入到 IP 的網路中，因此重新查看 Packet 中的 Destination IP address 為何？並查看其 FIB 以決定 Packet 要傳送的下一個節點。

以上所述僅為 IGP label，IGP label 為第一層的標籤(又稱為 interior label)，該標籤主要是用來指引 BGP 的 next hop。第二層的標籤為 VPN Label(又稱為 exterior Label)，該 Label 也是由 Ingress LSR 貼上，packet 在 MPLS 骨幹網路傳送過程中一直保留，該標籤主要是告知 egress LSR 經由那一個 outgoing interface 將該 packet 轉送到目的地的。



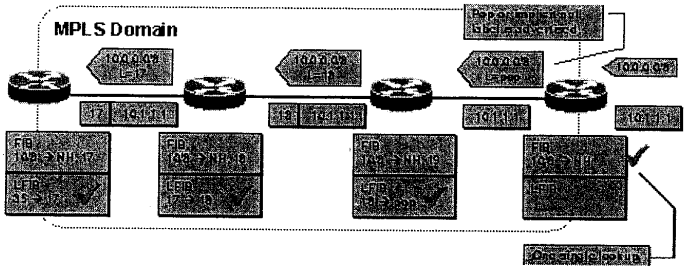
MPLS 網路中 Egress LSR double lookup 的問題

由於 Egress LSR 不但要查看 LFIB 中的資料以便移除 Packet 中的 Label，而且還要查看 FIB 中的資料以決定將 Packet 往 IP 網路的下一個節點傳送，這樣的作法會使 Egress LSR 的負擔太重，而且對傳送有 Label 的封包也不是最有效的方式。

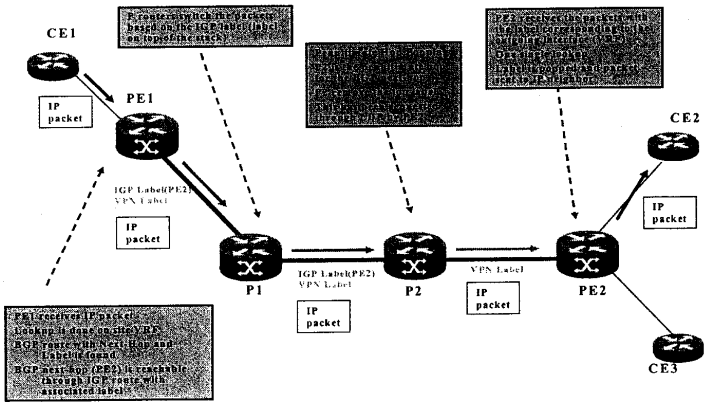


Penultimate Hop Popping

解決 Egress LSR double lookup 問題的方式就是在原來 Egress LSR 前一個節點就把 Label 移除，最後一顆 Router 只要做 IP lookup 就好了，此種運作方式稱為 Penultimate Hop Popping。



Packet Forwarding and Penultimate Hop Popping



1)PE1 router 收到 CE1 傳送的 IP 封包後，根據 Destination IP 從 VRF table 找出 BGP next hop 的路由，並在該 IP 封包貼上 2 層標籤後將該封包轉送至 P1 router。

PE1 貼上的 2 層標籤分別 IGP label 及 VPN label。

◆ IGP label

IGP label 為第一層的標籤(又稱為 interior label)，該標籤主要是用來指引 BGP 的 next hop，以上圖為例 BGP 的 next hop 為 PE2，在 MPLS 骨幹網路內封包的轉送是透過 IGP label 來完成。

◆ VPN label

VPN label 為第二層的標籤(又稱為 exterior label)，該標籤主要是告知 egress PE router 經由那一個 outgoing interface 將該 IP 封包轉送到目的地的 CE router。

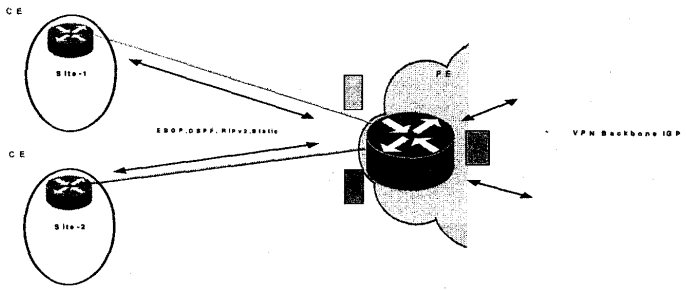
2)P1 router 收到封包後，根據 IGP label 將該封包轉送至 P2 router。

3)Penultimate Hop Popping

Penultimate Hop 負責將第 IGP label 拿掉，對 BGP next hop(PE2)而言，P2 router 是倒數第二(Penultimate)的 router，故 P2 router 收到 P1 router 轉送的封包後，保留 VPN label 而將 IGP label 拿掉並轉送該封包至 PE2 router。

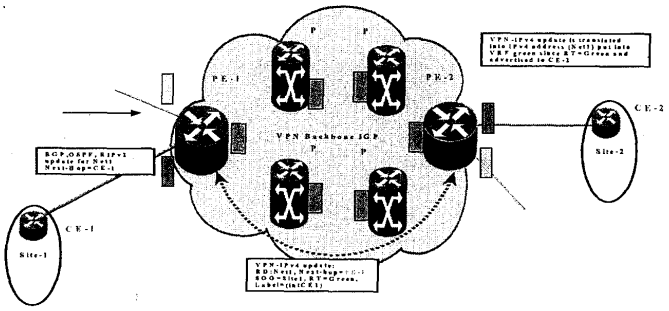
4)PE2 router 收到該封包後，根據 VPN label 找出該 IP 封包要送到目的地須透過那一個 outgoing interface，然後將 VPN label 拿掉後再將該原來 CE1 router 傳送的 IP 封包傳送到目的地(CE2 router)。

VRF and Global Routing table



PE router 收到 CE router 路由資訊後，將該客戶的路由資訊存放 PE router 內該客戶個別的 VRF table(VPN Routing Forwarding table)，因每個 VPN 客戶在 PE router 均有各自單獨的 VRF table，故 MPLS VPN 允許不同的 VPN 客戶在 LAN 端使用相同的 private IP address。
至於 PE router 經由骨幹網路 IGP 學到的路由資訊資訊則存放在 Global routing table。

IPv4 路由更新

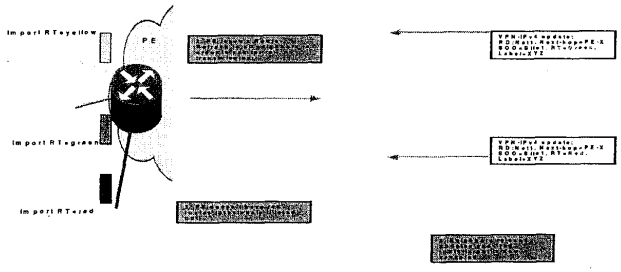


PE-1 router 經由 EBGP、OSPF、RIPv2 或 static route 收到 CE-1 router

的 IPv4 update 後，將該 IPv4 update 轉換成 VPN-IPv4 並根據該客戶在該 PE 上的原來 VRF 設定來指配 SOO(Site of Origin)、RT(Route-target)及 Label，並將該路由更新訊息經由 MP-iBGP 傳送給骨幹網路內的其他 PE routers。

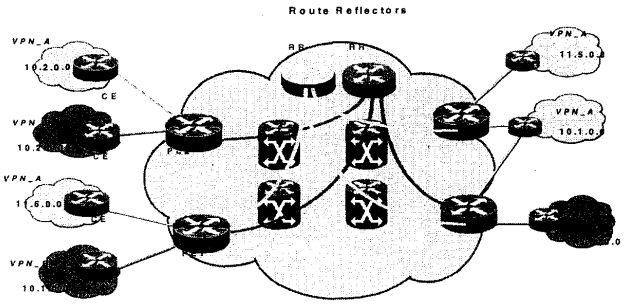
PE-2 router 收到該更新路由後根據 RT 的相關設定來判斷並更新屬於同一群組 VPN 客戶的 VRF table，並將該 VPN-IPv4 update 轉換成 IPv4 address 然後傳送給 CE-2。

VPN-IPv4 路由更新(Route Refresh)



上圖中，當 PE router 新增加 import RT=red 後，因原來並無"red" route-target 相關的路由資訊，故會向所有的 neighbors 發出路由更新(Route Refresh)的要求，neighbors 收到該路由更新的請求後會將 VPN-IPv4 updates 送至該 PE router，PE router 進而完成了 VPN-IPv4 路由的更新。

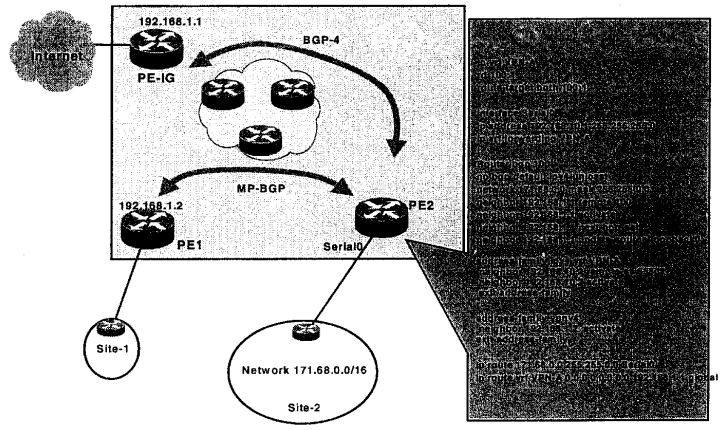
MPLS VPN Route Reflector

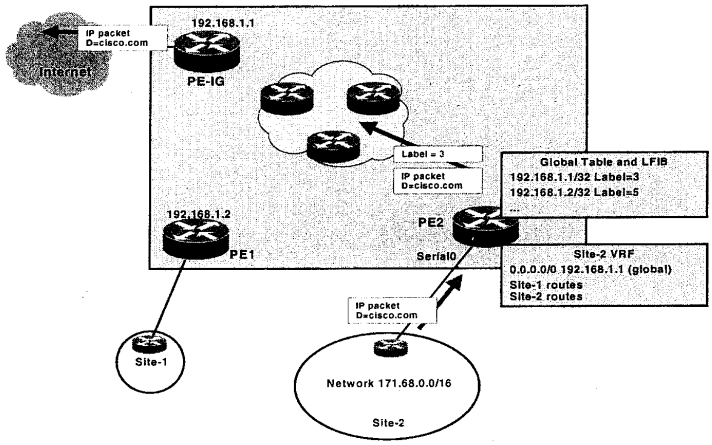


在 MPLS VPN 網路 PE 和 PE router 間彼此須透過 MP-iBGP 互相建立 iBGP session 以便交換 PE routers 間的 VPN routing information，這種 fully mesh 的 iBGP session 將使所有的 VPN-IPv4 routes 氾流(flooding)至每一個 PE router，因而每一個 PE router 均會收到很多和自己本身無關的 VPN-IPv4 route，同時對於大型 VPN 網路或需要增加新 PE router 時，PE routers 間 iBGP session 的建立所需的相關設定將較為繁複，為讓網路中參數的設定單純化，一般在大型 VPN 網路中大都採用 Route Reflector 方式。

採用 Route Reflector 的方式，每一個 PE router 只須和 Route Reflector router 建立 iBGP session，PE routers 彼此間則不須再互相建立 iBGP session，至於 PE routers 間的 VPN routing information 則由 Route Reflector router 來處理，這種方式不僅解決了 VPN-IPv4 routes 氾流的問題，同時簡化了網路參數的設定使 MPLS VPN 網路擴充更具彈性。

MPLS VPN 客戶 Internet 需求





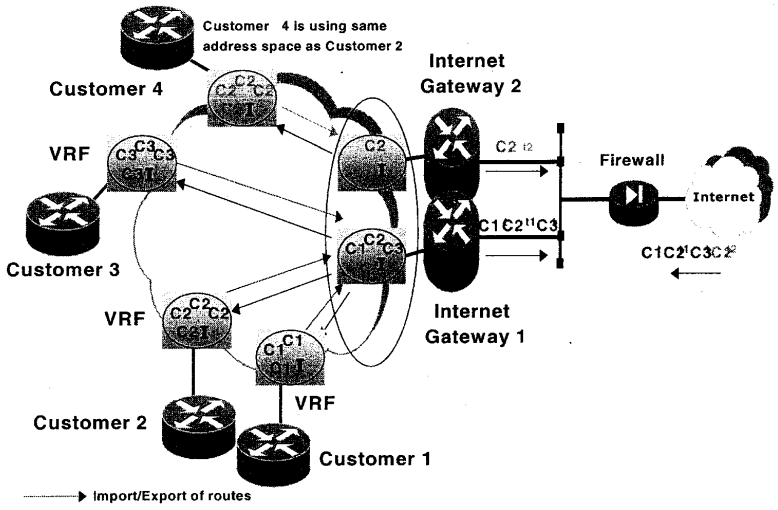
上圖中 MPLS VPN 客戶除 site1 及 site2 間 Intranet VPN 需求外，同時亦有 internet 的需求，PE2 router 除和 PE1 router run MP-iBGP 外，同時和 PE-IG(PE-Internet Gateway)間 run BGP。

PE2 router 上 site2-VRF routing table 除有 site1 及 site2 路由外，同時亦有 default route 指向 PE-IG，封包在送往 site1 router 及 PE-IG 所貼上的

IGP label 亦不同。

上圖中 PE2 router 收到 site2 傳送的 IP 封包後，知道該 IP 封包目的地並非在 intranet 網路內而是要到 internet 的 cisco.com 網站，根據 default route 得知該封包須送往 PE-IG router，故 PE2 router 將封包貼上 3 號標籤(IGP label=3)後送往 PE-IG router，PE-IG 收到該封包後根據 destination IP 並參照 IPv4 routing table 將該封包經由 Internet 網路送至 cisco.com 網站。

Intranet/Internet Conversion



MPLS VPN 每個 VPN 客戶在 PE router 均有各自單獨的 VRF table，故 MPLS VPN 允許不同的 VPN 客戶在 LAN 端使用相同的 private IP address。

MPLS VPN 客戶有 Internet 需求時須將 private IP address 轉成 public IP address，這個動作就是一般所謂的 NAT(Network Address Translation)，

NAT 可由客戶或由網路服務提供商來作。

上圖中 VPN 客戶 Customer 2 及 Customer 4 使用相同的 private IP address，該 2 個客戶除了公司 Intranet VPN 的需求外且均有 Internet 的需求。因 2 個客戶使用相同的 private IP address，若 NAT 工作是由網路服務提供商來作，此時網路服務提供商須使用 2 個不同的路由器 (Internet Gateway1、Internet Gateway2)分別為這 2 個客戶作 NAT 的動作，然後再經由 Firewall 和 Internet 網路連接，以達到 Intranet/Internet Conversion。

四、結論與心得

此次奉派赴美國實習並參加 MPLS VPN 及相關技術的訓練，職等三人對於 MPLS VPN 運作原理及相關技術有了更深一層的認識與瞭解，相信對於日後在 IPVPN 網路相關的維護工作及提供跨國企業客戶技術諮詢服務有相當大的助益。

本出國報告主要內容包括 VPN 基本概論及 MPLS VPN 概論，MPLS VPN 概論從一開始介紹 MPLS 基本概念、MPLS VPN 專門術語、網路架構及各個不同角色 LSR 的運作方式、MPLS Label 的 format 及相鄰 LSR 之間如何交換彼此的 Label Information，另外更舉例說明封包在 MPLS 網路中從 Push(加上)Label，一直到離開 MPLS 網路前 Pop(去除)Label 的詳細過程，最後則探討 MPLS Route Reflector 及 Intranet/Internet Conversion。

MPLS 的主要優點是減少了網路複雜性，相容現有的各種主流網路技術，使網路的總體成本降低，在提供 IP 業務時能確保 QoS 和安全性，具有流量工程能力。MPLS 的實用價值在於它能夠在像 IP 這樣的無連接型網路中創建連接型業務，此外，MPLS 能解決 VPN 擴展問題和維護成本問題，MPLS 技術是目前最具競爭力的通信網路技術。因此，MPLS 被認爲是當今資料網路領域內最有前途的網路解決方案之一。另外一方面在通信需求上 VPN 被認爲是 21 世紀網路中最重要的應用之一，MPLS 順應了這種需求，這是 MPLS 未來發展的巨大動力也是它佔領市場的一個保證。