第二章 文獻探討

本節將針對論文主題之基本技術做研究探討，包括了：多重協定標籤交換相關技術的背景及運作原理分析【1,5,13,14】，並且說明了 VPN 技術的演進與目前新趨勢-MPLS VPN 相關技術的運作原理與設計的特點分析【3,6,7】，接著是對網路管理技術的概念簡介與現行常用網管工具 MRTG 的介紹【11,12,15,18,19】，最後導入以政策為基礎的網管系統(Policy Based Network Management, PBNM)架構的概念說明【3,4,9,10,16,20】，並瞭解 ISP 為企業客戶提供 VPN 服務商業化模式【17】，必需配合集中式以政策為基礎的網管系統才能提供具經濟規模的網路管理服務。

2.1 多重協定標籤交換技術

傳統網際網路運作的問題

傳統的網際網路是一個以 IP 為網路層的網路，其中是由很多的路由器把不同區段的網路連接起來，封包在一般的 IP 網路傳遞時，路由器的運作是以所謂的”Store and Forward”的運作原理，來做封包路由的選擇及轉送，所以當路由器收到一個封包時，會先儲存這個封包、再透過分析路由找到最佳路徑、最後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)，這樣是很沒有效率的，而且會耗用路由器大量的 CPU 處理能力及記憶體空間，也就是說會受限於 CPU 的運算速度，因此而限制了 IP 網路的傳送能力。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 以線上速度(Line Speed)來轉送封包到達目的地【13,14】。

2.1.1 MPLS 技術背景簡介

交換式路由器技術的發展

根據基本概念的不同，目前已知結合 IP 與 ATM 優點的技術發展趨勢可分成：Overlay Model 與 Peer Model 兩大類，但不論 ISP 所用的技術是那一類，對於 IP 網路的用戶而言，只需知道對方的 IP 位址，即可傳送資料到遠方用戶，並不需要知道中間的網路是用何種技術幫它傳送資料的。

Multi-Protocol Label Switching(MPLS)是由 IETF 所主導，希望融合目前世界上各種不同 IP 交換技術的優點，整合發展出來的一個網路標準。MPLS 技術規格中主要是參考了 Ipsilon 公司的 IP Switching、Cisco 公司的 Tag Switching、Toshiba 公司的 Cell Switch Router(CSR)、Cascade 公司的 IP Navigator 以及 IBM 公司的 Aggregate Route-Based IP Switching (ARIS)等各種 IP Switching 技術發展而來。然而 IETF MPLS Working Group(WG)制定 MPLS 的目的，是希望透過制定標準解決各家 IP Switching 技術間不相容的問題，並且希望透過收容各家 IP Switching 技術的優點，制定出更具彈性、擴充性及效率更高的 IP 交換技術。簡而言之 MPLS 技術是能提供一個兼具第二層快速交換的效能與第三層彈性路由選擇之優點，並且能廣為各方接受的標準化網路傳輸技術。MPLS 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 網路中的 Label Switching Router(LSR)會根據標籤(Label)值來做為轉送(Forwarding)封包的依據，不再需要解開第三層 IP Header 來看目的 IP 位址(Destination IP address)，是一種整合了類似 ATM 網路交換架構與網路層的路由機制的技術【13,14】。

2.1.2 Label 的格式與屬性

Label Header 的 Format 與各欄位的意義

Label Header 是一個 4Bytes、固定長度、具本地有意義的區別符號(Locally-Significant Identifier)等特質，其中有四個欄位分別是 Label=20bits、Experimental (Exp)=3bits、Bottom of Stack (S)=1bits、Time To Live (TTL)=8bits 請參考【圖 2-1】。其中 Label 這個欄位的值類似於在，ATM 網路中的 Virtual Path Identifier(VPI) /Virtual Circuit Identifier (VCI)或是 Frame-Relay 網路中的 Data Link Circuit Identifier(DLCI)參數的功能，用於識別封包轉送的路徑選擇，Exp 欄位的值則用於識別資料流的服務等級，也就是確保資料傳送的服務品質與當網路發生擁塞時判斷封包是否要丟棄的優先順序，S 這個欄位值則是用於判定各種 Label 堆疊(Stack)的順序與架構運作的先後，TTL 這個欄位與傳統 IP Header 中 TTL 欄位的功能相似，用於防止網路回圈(Loop)發生【7】。

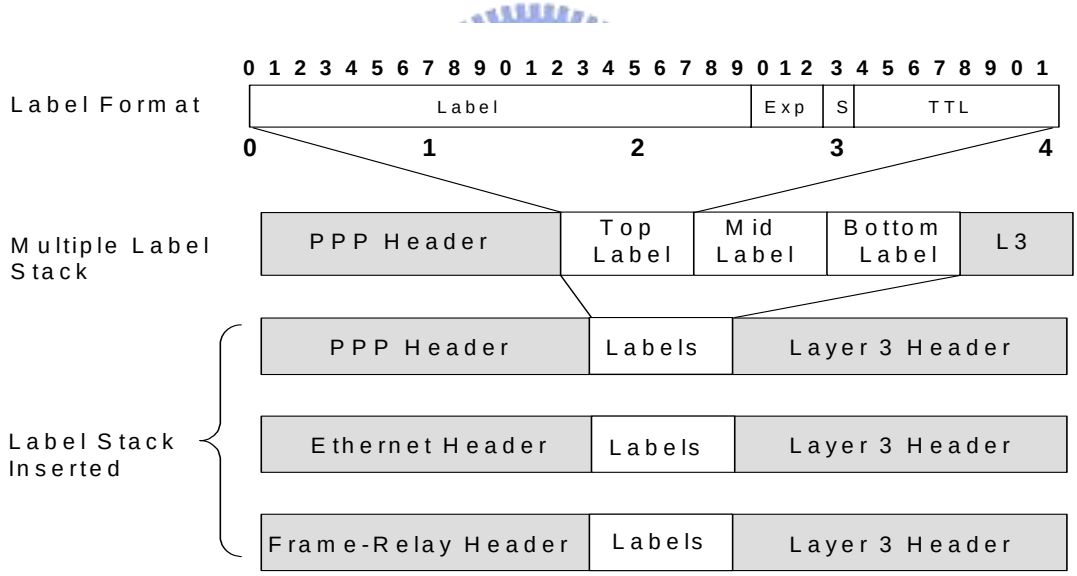
Label Header 的插入位置與 L2 Header 的修改

Label Header 的位置是在封包協定標頭的第二層資料鏈結層(Data Link Layer)與第三層網路層(Network Layer)之間，請參考【圖 2-1】。因為 MPLS 的

Label 是插在 L2 與 L3 之間，傳送的路由器必需有一些方法來分辨確認那一些封包有加上 Label？那些封包沒有加上 Label？因此在原先 L2 Header 中 Protocol type 欄位中，要定義新的指標值來標示那些已加上 Label 的封包做為區別，如果在區域網路上 L2 是 Ethernet Header，其中 ethertype 的欄位值為 8847 和 8848 表示此封包已被加上 Label，如果在廣域網路上 L2 是 PPP Header，其中 PID 欄位值為 8281 表示此封包已被加上 Label，如果在 Frame-Relay 網路上 L2 是 Frame-Relay Header，其中 SNAP 欄位值為 8847 表示此封包已被加上 Label【7】。

Multiple Label and Label Stack 的運作

MPLS Label Header 可在封包中插入多個，也就是在 MPLS 網路中的封包有攜帶 Multiple Label 的能力，請參考【圖 2-1】。根據不同的功能來區分主要有三種，分別是 VPN Label、IGP Label 及 TE Label，標籤堆疊(Label Stack)的運作是採後進先出(LIFO)的方式，而且 MPLS 路由器每次只處理 Label Stack 中最上層的 Label 以簡化運作模式【7】。



【圖 2-1】Label Stack 架構圖

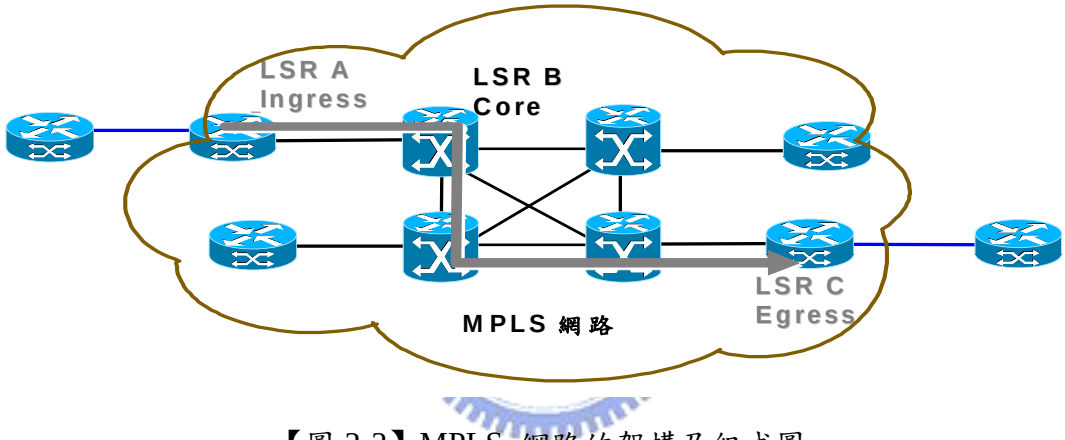
2.1.3 MPLS 網路的架構與組成

MPLS 網路是由多個具有標籤交換能力的路由器的 LSR 互相連結所組成，請參考【圖 2-2】。根據在 MPLS 網路內扮演角色的不同 LSR 可以分為三種類型：**Ingress LSR** 是負責將進入 MPLS 網路的 IP 封包貼上標籤(Push Label)，而 **Core LSR** 則是位於 MPLS 網路的核心，負責做標籤轉換(Label Swap)，最後

Egress LSR 是負責當 IP 封包要離開 MPLS 網路到一般 IP 網路時，負責去除標籤(Pop Label)。

Label Switch Path (LSP)

當封包從貼上 Label，到拿掉 Label 所經過的整個路徑稱之為 LSP，請參考【圖 2-2】。當封包進入 MPLS 網路開始傳遞前，MPLS 網路將開啟一條 LSP，它是一個邏輯的通道(Logical Tunnel)，位於第二層與第三層之間，通道之間各自獨立而且有安全性，類似於 ATM 或 Frame-Relay 網路的虛擬電路(Virtual Circuit)，由於有 LSP 使得 MPLS 網路能確保每一個 VPN 客戶都是獨立且有特色的，同時也能夠保證其傳輸的品質【7】。



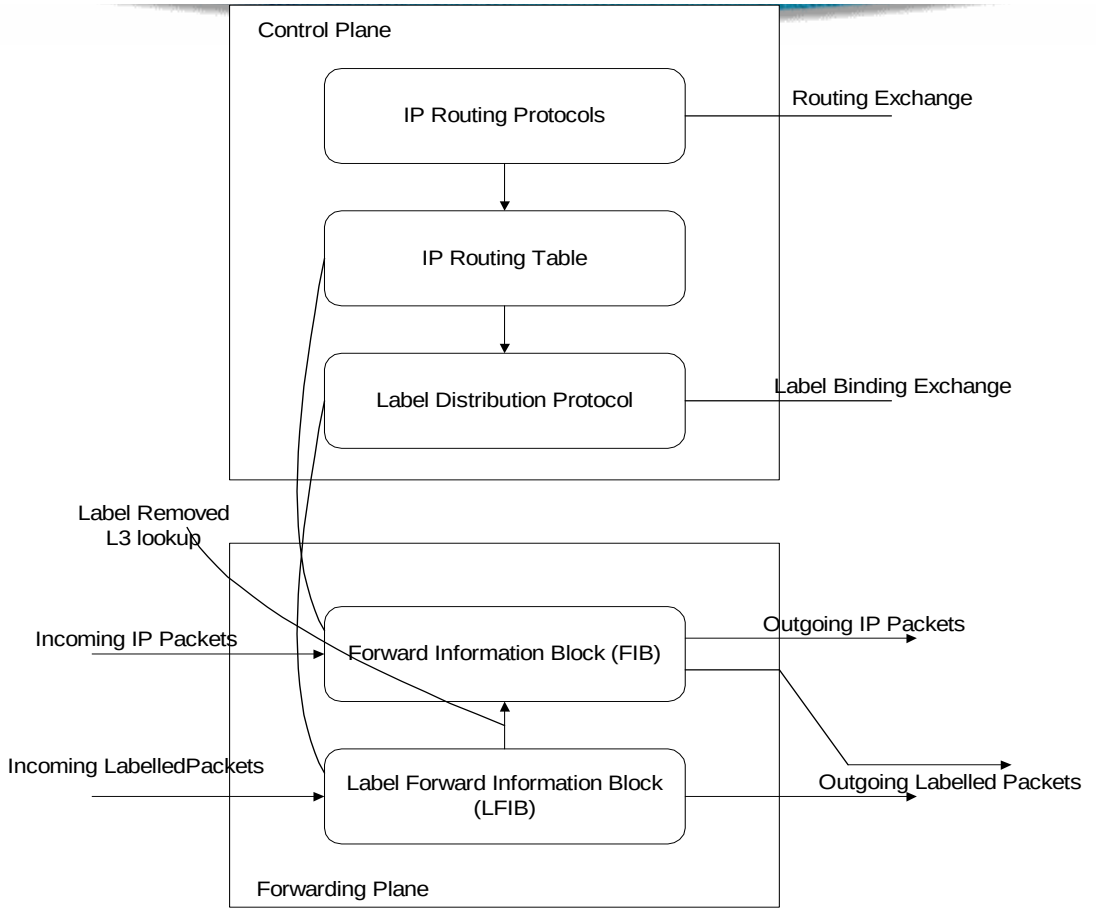
【圖 2-2】MPLS 網路的架構及組成圖

2.1.4 LSR 內部功能模組分析

LSR 有兩大功能模組，分別是控制模組(Control Module)與轉送模組(Forwarding Module)，請參考【圖 2-3】。控制模組中包括一般路由表的產生與維護，還有在 MPLS 功能方面，主要是負責 Label 資訊的產生及維護，此外在路由資訊的交換上主要靠路由協定(OSPF or RIP)來運作，而 Label information 的交換主要靠 Label Distribution Protocol (LDP)這個協定來運作。

LSR 的轉送模組，在接收到有 Label 的封包或一般的 IP 封包，其處理的方式會不同。當 LSR 接收到有 Label 的封包進入時，會去根據 Label 值去參考查詢 Label Forwarding Information Base(LFIB)的資訊，再決定選擇那一個 interface 轉送到下一個網路節點，反之如果接收到的是一般 IP 封包則會解開 L3 的 IP Header 根據 Destination IP 的值，去參考查詢 Forwarding Information

Base (FIB)的資訊，再決定選擇那一個 interface 轉送到下一個網路節點，所以當含有 Label 的封包與一般 IP 封包同時進入 LSR 時是不會互相影響的。同時也因為控制模組與轉送模組的分開運作，使網路上的資料傳輸功能與路由選擇功能可以獨立分開，增加了網路的彈性與效能【7】。

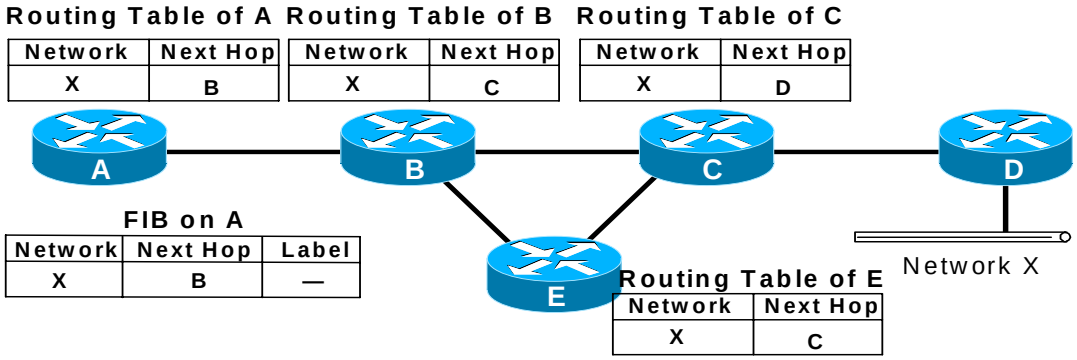


【圖 2-3】封包在 LSR 中的處理架構

2.1.5 Label 的指定與分配過程

(1) LSR Routing Table 的建立：

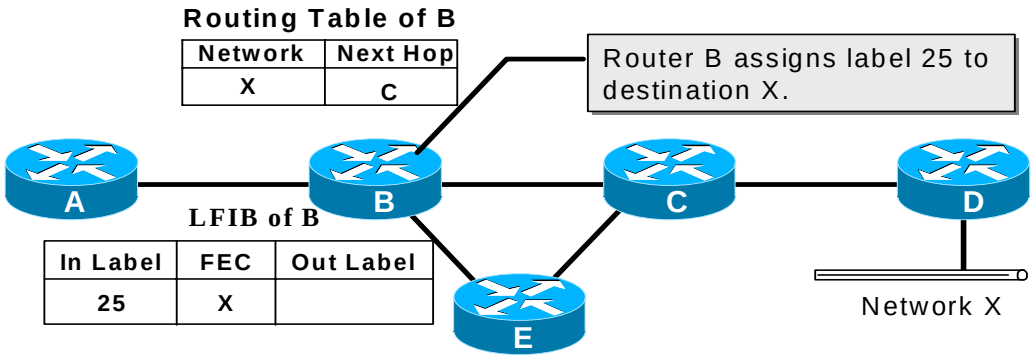
在 MPLS 網路中所有的 LSR 利用 Interior Gateway Routing Protocol (IGP)的路由協定來彼此交換路由資訊(Routing Information)，經過計算後建立自己的路由表(Routing Table)，請參考【圖 2-4】，並根據路由表的內容來建立自己的 Forwarding Information Base (FIB)，此時的 FIB 中並沒有 Label 的資訊【7】。



【圖 2-4】LSR 路由表建立的過程

(2) LSR Allocating Label 過程：

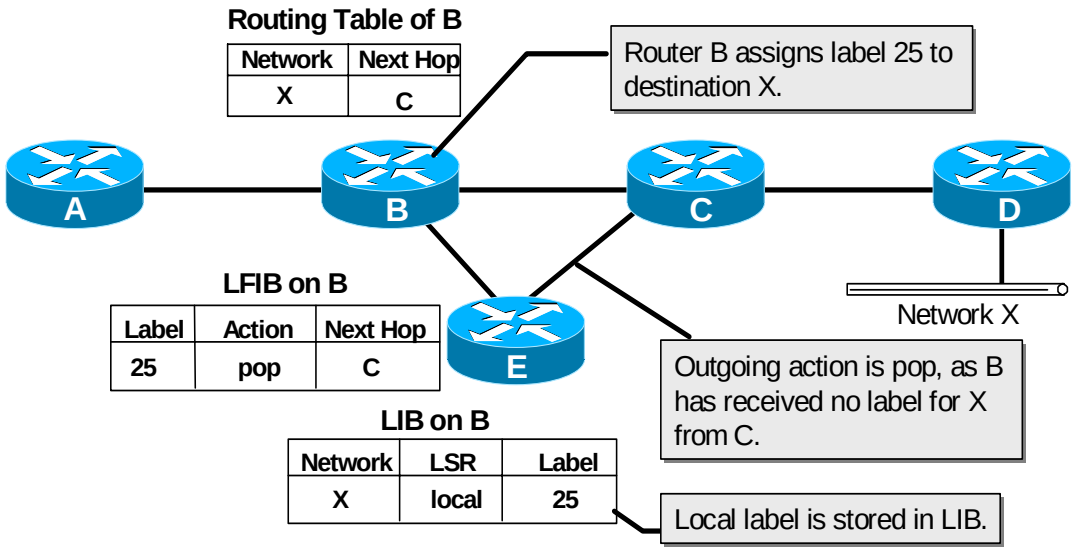
當 LSR 開始啟動 MPLS 功能時，會根據由 IGP 路由協定(如 RIP、OSPF)學來的路由表內容，對於使用相同處理方式、相同路徑、到達相同目的地(IP Prefix)的 Routing entry 做彙整(Aggregation)與分類的工作後，建立 Forwarding Equivalent Information (FEC) Table，並且自動將其各別的 FEC entry 分別指定一個特定的 Label 值(Local independent)與之對應，這個動作稱之為 FEC-to-Label Mapping，請參考【圖 2-5】。這種先彙整同類資訊再指定具代表性的唯一 Label 值，是為了節省 Label 值的使用與減少同類資料的重複儲存浪費儲存空間而設計，此外對於路由表內的路由資訊(IP Prefix)，如果是來自 Border Gateway Protocol(BGP)學來的，不會指定 Label 給他對應，因為 ingress Edge-LSR 只要針對 BGP Routes 的 Next-hop IP address，指定 Label 給它就可以轉送封包到 BGP routes 的目的地，這樣的設計不但可以減少骨幹路由器記憶體需求及 CPU 使用率(處理 BGP 路由更新)，同時可以使骨幹網路更穩定，不會受到網際網路異常路由資訊更動(Route Flaps)的影響【7】。



【圖 2-5】LSR Allocating Label 過程

(3) LSR 初步建立自己的 LIB 及 LFIB：

LSR 將前面步驟 Allocating 的 Local Label 資訊，儲存於 Label Information Base (LIB)和 Label Forwarding Information Base (LFIB)中，此時的 LFIB 中只有 local Label 的資訊並沒有 outgoing Label 的資訊，請參考【圖 2-6】，因為此時尚未起動 LDP 協定與鄰近的 LSR 交換彼此的 Label information。

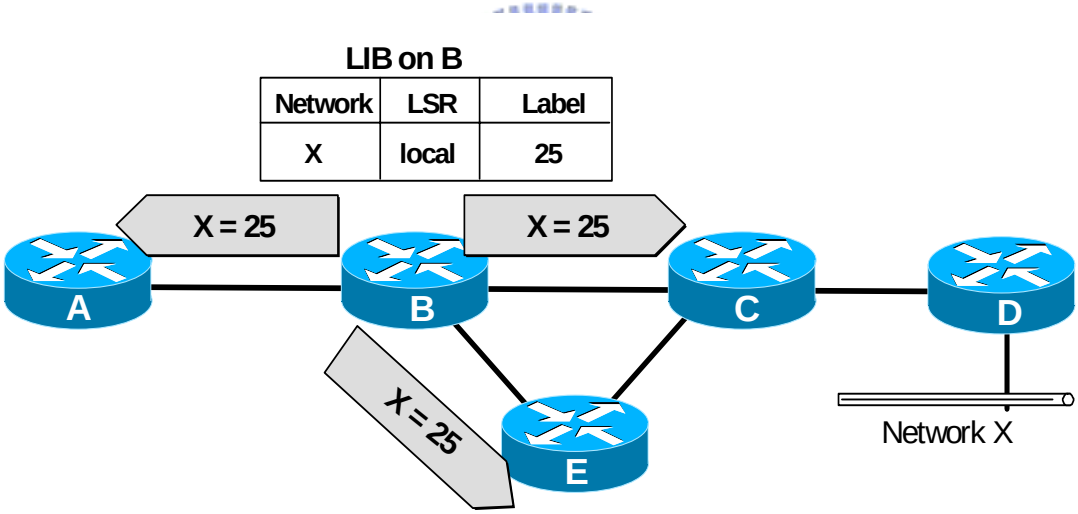


【圖 2-6】LSR 初步建立自己的 LIB 及 LFIB

(4) LSR Label Distribution 過程：

Local LSR 將他 Local assign 的 Label information 傳送給相鄰的 LSR，請參考【圖 2-7】，不論這相鄰的 LSR 是 Local LSR 的 Downstream 或 Upstream 都會傳送，而且 Label Distribution 靠的是相鄰 LSR 間要執行 LDP 這個協定，來互相交換彼此的 Label information，而 LDP 是 IETF 制定標準的 Label Binding Protocol。

另外談到 LDP 的特性，啟動 MPLS 功能設定的設備都會傳送或接收 LDP 協定的資訊，當然 LDP 協定會透過 Discovery 的方式去和鄰近的 MPLS Device 溝通，看對方是否有啟動 MPLS 功能及是否需要交換 Label information，而 LDP 是透過 UDP 協定的 Hello Packet 以 Multicast 方式去發現鄰近的 MPLS Device 是否存在，如果發現存在就利用 TCP 協定(TCP port=646)建立 LDP session 去交換彼此的 Label information【7】。

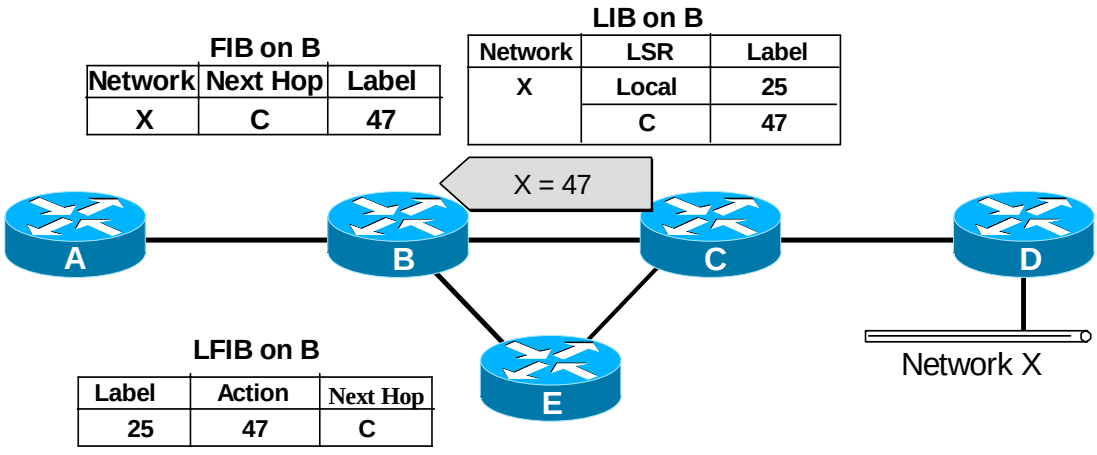


【圖 2-7】LSR Label Distribution 過程

(5) LSR 收到相鄰 LSR 送來的 Label 資訊做資訊的彙整過程：

每個 LSR 根據接收到相鄰 LSR 送來的 Label information 後，新增這些 Label 資訊於自己的 LIB 中，並根據路由表獲知的最佳路徑資訊，用來判定到某個目的網段 Network X 之 Next-hop LSR 是誰？並將其所送來的 Label 資訊，插入到 LFIB 的 outgoing Label 資料欄位中，做為主要轉送封包到 Network X 的最佳路徑，請參考【圖 2-8】，但是如果最佳路徑發生異常(斷

線)，LSR 會根據存在於 LIB 中的其他替代路徑資訊做計算找出最佳替代路徑，並會即時更新在 LFIB 的資訊，使封包改走備援替代路徑【7】。



【圖 2-8】相鄰 LSR 送來的 Label 資訊做彙整的過程

2.1.6 MPLS 網路中封包運作原理

(1) Ingress LSR(Router A)：

IP 封包進入 MPLS 網路的第一顆 LSR 路由器稱為 Ingress LSR，當 IP 封包進入 Ingress LSR 首先會查看封包中的 Destination IP address，並且在 FIB 中查詢(lookup)是否有符合的 IP Prefix，請參考【圖 2-9】，如果有則進一步查看 FIB 中相對應的 Label 欄位其值為何？(例如：IP =X ，Label=25)，當封包從 Ingress LSR 送出時，會在此封包中插入 Label=25 的標示，再傳送出去。

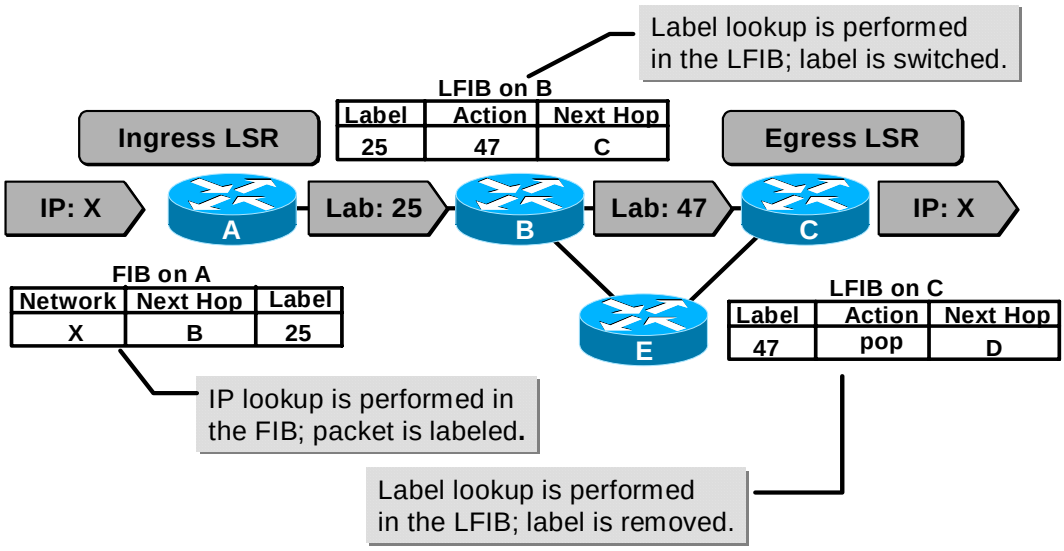
(2) Core LSR (Router B)：

當帶有 Label=25 的封包傳到 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)，所以封包中的 Label 快速的被置換(Label=25 →Label=47)並往下一個節點傳送出去。

(3) Egress LSR(Router C)：

當帶有 Label=47 的封包傳到 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)，所以封包中

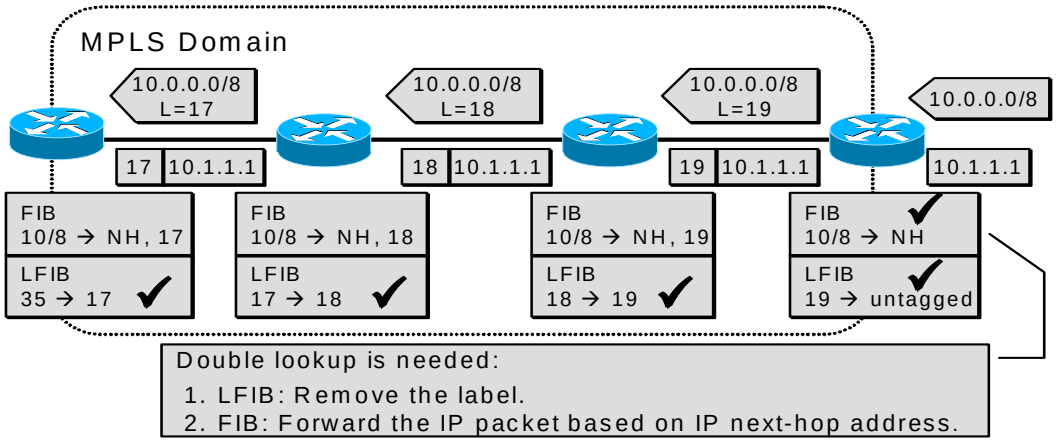
的 Label 被移除，此時已離開 MPLS 網路要再進入到一般 IP 的網路中，因此重新查看封包中的 Destination IP address 為何？並查看其 FIB 以決定封包要傳送的下一個網路節點【7】。



【圖 2-9】封包在 MPLS 網路中傳送的過程

MPLS 網路中 Egress LSR Double Lookup 的問題分析

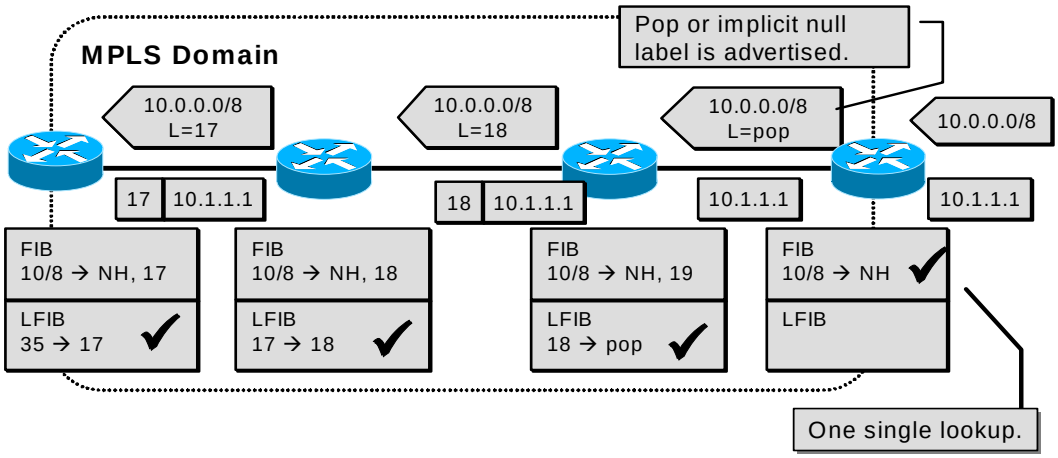
由於 Egress LSR 不但要查看 LFIB 中的資料以便移除封包中的 Label，而且還要查看 FIB 中的資料，才能決定將封包往 IP 網路的下一個節點傳送，這樣的作法會使 Egress LSR 的負擔太重，請參考【圖 2-10】，而且對於傳送有 Label 的封包，也不是最有效的方式。



【圖 2-10】MPLS 網路中 Egress LSR double lookup 問題

解決的方式為 Penultimate Hop Popping

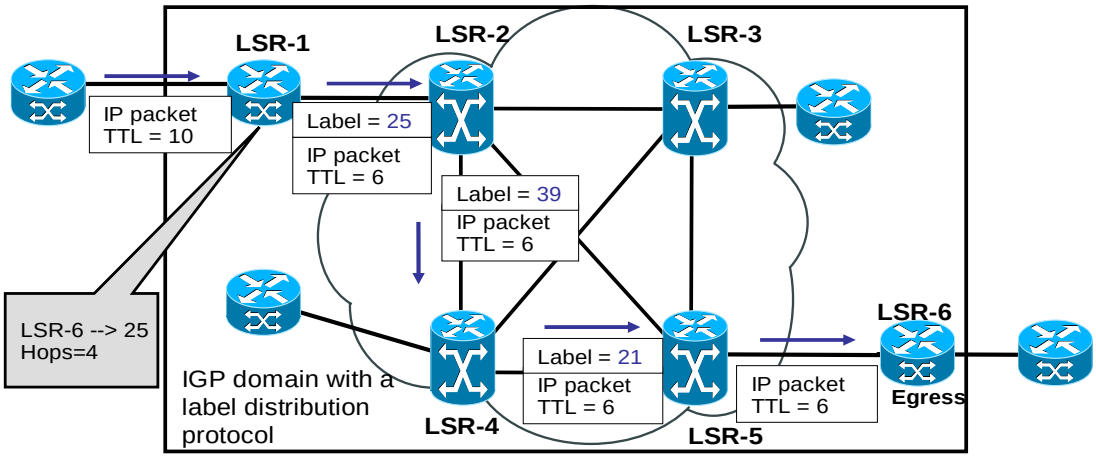
所以解決的方式就是在原來Egress LSR前一個節點就把Label移除，Egress LSR只要做IP lookup 的工作就好了，請參考【圖 2-11】，此種運作方式稱為Penultimate Hop Popping，因此Egress LSR必需透過LDP協定宣告***implicit-null*** label通知要求鄰接於Egress LSR上游的LSR(upstream neighbour of the egress LSR)，改變其LFIB內的outgoing Label欄位值為Pop【7】。



【圖 2-11】Penultimate Hop Popping 運作原理

MPLS 網路中防止 Loops 的機制

在 IP 的網路中，TTL 的值每經過一個網路節點就會減 1，這樣的設計是為了防止封包在網路中產生回圈(Loops)時造成封包無限制的被轉送，因此使網路資源被浪費。MPLS 網路也是用相似的機制，請參考【圖 2-12】，但是只有在 LAN 及 PPP 的環境中 MPLS Label Header 中才有 TTL 的欄位，然而在 ATM 的環境中沒有 TTL，他的運作方式是如果當進入 MPLS 網路前 IP Header 中的 TTL=0 時，封包會直接被丟棄不再進入 MPLS 網內，相反的如果 TTL>0，會在封包進入 MPLS LSP 前，將 IP Header 中的 TTL 的值先一次減去 LSP 會經過的網路節點總數後，再將剩下的值填入 TTL 欄位中，接者進入 MPLS 網路後，每經過一個節點都不會更動 TTL 的值，一直到封包離開 MPLS 網路再度進入 IP 網路時，TTL 才會再恢復每經一個網路節點就減 1 的機制【7】。



【圖 2-12】MPLS 防止 Loops 及 TTL 運作機制

2.1.7 MPLS 技術之應用

流量工程(Traffic Engineering)

隨著網路流量的增加，骨幹網路架構越來越龐大且複雜，因此而增加了網路管理者在維護骨幹網路的困難度，MPLS 流量工程(Traffic Engineering,TE)技術的出現，就是要減輕管理網路的複雜度，讓網路服務業能透過 MPLS TE 的功能，降低管理網路的困難度，更有效率的維護好骨幹網路，使網路骨幹頻寬能得到最大利用。傳統建立路徑的方法與 TE 的運作方式比較，傳統建立路徑的方法是每個路由器藉由 IGP 的路由協定交換彼此的路由資訊，根據路由資訊計算出最短路徑，但是最短路徑並不一定就是最佳路徑，也許還有可能是最擁塞的路徑，因此需要 TE 來幫忙做進一步判定。

目前 MPLS 有三種 Signaling Protocol：LDP、RSVP-TE、CR-LDP，只有後面兩個有支援 TE，此外 TE 的運作還需要有路由協定的配合，如 Interior Gateway Protocol (IGP)路由協定中的 OSPF 及 ISIS，有了路由協定的配合才能使 Signaling protocol 可以了解網路的變化，進一步做處理使網路運作達到最佳化。

在建立 TE 的路徑時，首先由 IGP 取得路由資訊，經由計算後取得一個最佳路徑，但此路徑不一定是最短路徑，但一定是最有效率最少擁塞的路徑，這種方法稱為 Constrained Shortest Path First (CSPF)。由於 MPLS 是透過 RSVP-TE 來建立路徑，RSVP-TE 是一種 Soft-state 的通訊協定，因此 RSVP-TE 可輕易的

根據目前網路狀態來調整路徑，使每條路徑得到最好效能。

Quality of Service (Qos)技術概念簡介

Qos 的技術可分為三種，第一種是 Predictive Qos，是用足夠的網路頻寬來達到 Qos，並無其他機制，適用於區域網路及校園網路，對於價格昂貴的廣域網路不適用。第二種是 Flow-based Qos，在網路上建立一條 end-to-end 的路徑 ，並在此路徑上預留頻寬，以保障服務品質 例如：ATM 網路的 Virtual Circuit (VC) 及 IETF 訂定的 InterServ 機制，是利用 RSVP 來設定路徑和預留該路徑的頻寬。最後一種是 Class-based Qos，是在進入網路的封包上 Mark 標籤，以區分其服務等級，並在網路的節點根據標籤的不同而做不同的處理，例如：IETF 訂定的 DiffServ 機制，利用 Mark IP Header 的 TOS 欄位【7】。

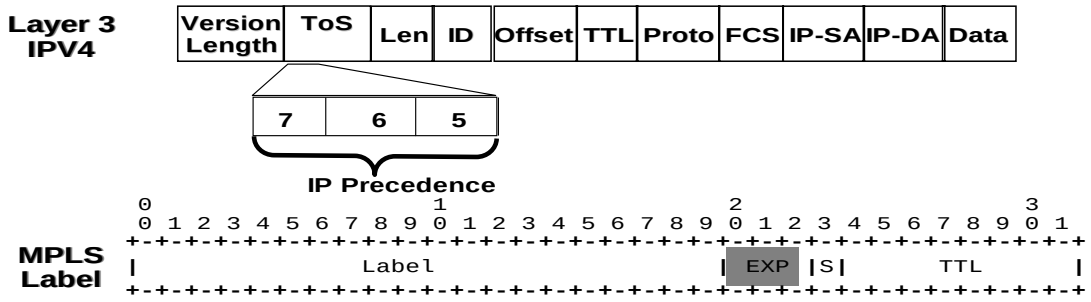
IETF 在 DiffServ 中建議了三種 Per-Hop Behaviors (PHB)第一種是 Best Effort (BE)，是指路由器不做任何品質保證，也不保證封包一定能送達目的地，第二種是 Expedited Forwarding (EF)，也就是優先權最高的一種等級，不論網路順暢或擁塞都能得到當初設定的速度，Delay time 和 Packet loss，不受網路其他流量的影響，保證設定的頻寬如私人專線一般，第三種 Assured Forwarding (AF)是優先等級介於 BE 和 EF 之間，在網路擁塞時，AF 等級的封包最小仍可使用到設定時的某個固定頻寬，而在網路順暢時則可能得到超過該設定速率的頻寬，也就是保證最小使用頻寬，網路順暢時可超用，另外網際網路上各種應用程式對 QoS 的需求差異是不同的，請參考【表 2-1】，因此我們在規劃 Qos 之前先要了解網路應用程式的種類再做政策決定。

【表 2-1】各種應用程式對 QoS 的需求

	Voice	FTP	ERP
頻寬需求	低~中	中~高	低
封包隨機丟棄的敏感度	低	中	高
封包延遲的敏感度	高	低	低~中
Jitter 的敏感度	高	低	中

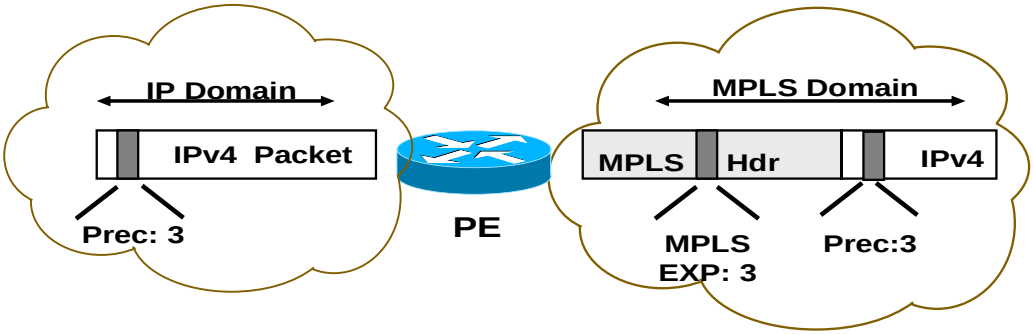
QoS Design 觀念，分成 Edge 端及 Backbone 端，Edge 端主要為接收傳送客戶資料，因此在 Edge 端利用 Class of Service 去 Classify Traffic Type，依此可針對不同 User 及給與不同 QoS 值(IP Precedence ToS)，請參考【圖 2-13】，並且限定 User 傳送最大頻寬，在 Backbone 方面並不適合去分類使用者的資料型態，在 Backbone 部份主要是針對不同 IP Precedence 值給與不同的 Queue Size 與 Drop Possibility 做為傳遞封包時的政策，在 IP 封包表頭欄位內有 1 個 byte 是專門定義 Qos 的稱為 Type of Service (TOS)，TOS 定義 3 個 bits(稱

之為 IP Precedence)去分成 8 個資料傳輸型態 0~7 越高者，表示資料越重要，在 MPLS Label 的資料型態中也有 3 bits 專門定義 Qos 的稱為 EXP (Experimental)。



【圖 2-13】IP precedence 與 MPLS Label EXP bit

因此當在 MPLS Edge Router 在 classify 不同資料型態及 User 資料時，給予不同的 IP Precedence 值，當進入 MPLS 環境後會其 MPLS Header 會自動複製 IP precedence 到 DSCP 的欄位中，因此 MPLS QoS 不須重新定義請參考【圖 2-14】，在 PE Router classify 不同資料型態及 User 資料時，給予不同的 IP Precedence 當進入 MPLS 環境後，MPLS QoS 繼承 IP Network QoS 參數以下主要說明 Cisco 所提供 QoS 機制，CAR 主要是在 Edge Router classify 及 set IP Precedence.依據上述 QoS 分別 Enable 在 MPLS P Router 與 PE Router 可提供客戶不同的需求，提供不同的傳輸服務，如 Gold Silver 等級，以滿足客戶需求【7】。



【圖 2-14】封包在 IP 網路與 MPLS 網路中被標示 QoS 等級

2.2 VPN 的新趨勢--MPLS VPN

2.2.1 VPN 技術簡介

虛擬私有網路(VPN)的定義

Virtual Private Network (VPN)，“虛擬私有網路”，簡單的說，就是指在公眾網路架構上所建立的企業網路，因此企業網路擁有與私有網路相同的安全、管理及效能等條件。所以 VPN 是原有[專線式]企業私有網路，可節省成本的替代方案。

虛擬私有網路(VPN)的種類

VPN 可以分成三大項目，分別為遠端存取(Remote Access)、Intranets 及 Extranets。遠端存取 VPN 乃是連結移動用戶(Mobile User)及小型的分公司，透過電話撥接上網來存取企業網路資源。Intranet VPN 是利用 Internet 來將固定地點的總公司及分公司加以連結，成為一個企業總體網路。而 Extranet VPN 則是將 Intranet VPN 的連結再擴展到企業的經營夥伴，如供應商及客戶，以達到協力廠商彼此資訊共享的目的。

企業 VPN 解決方案的種類如下：

私有網路(Private Network)：

以租用實體電路的方式，建立企業內點對點的通訊網路，頻寬使用效能低(通常不超過 50%)，須自行管理的封閉網路，總公司埠(port)密度高，建置成本昂貴。

L2 虛擬私有網路(Virtual Private Network)：

ISP 建置 X.25、Frame-Relay 或 ATM 的網路架構，以虛擬電路(Virtual Circuit)在實體電路上建立連線，達到 end-to-end VPN，連結可提供頻寬保證(CIR)，但不易替客戶建置完全網狀連結(Fully-Meshed)之網路架構，並且缺乏 Intranet，Extranet，Remote Access 的完全整合能力。

IP VPN：

IP 網路環境中結合通道技術(Tunneling)、加密技術(Encryption)、認證技術(Authentication)建立的虛擬私有網路。可輕鬆建置完全網狀連結(Fully Meshed)

容易擴充，並且具備 Intranet、Extranet 及 Remote Access 的完全整合能力。這種 VPN 的解決方案是透過 IP Tunnel 建立 VPN 連線，而 IP Tunnel 技術是將 Private IP 包在 Public IP 之後，但透過一個公衆網路連結，還是有安全的問題，因此利用 IP Security 機制將資料封包加密，以達到資料保密的功能。

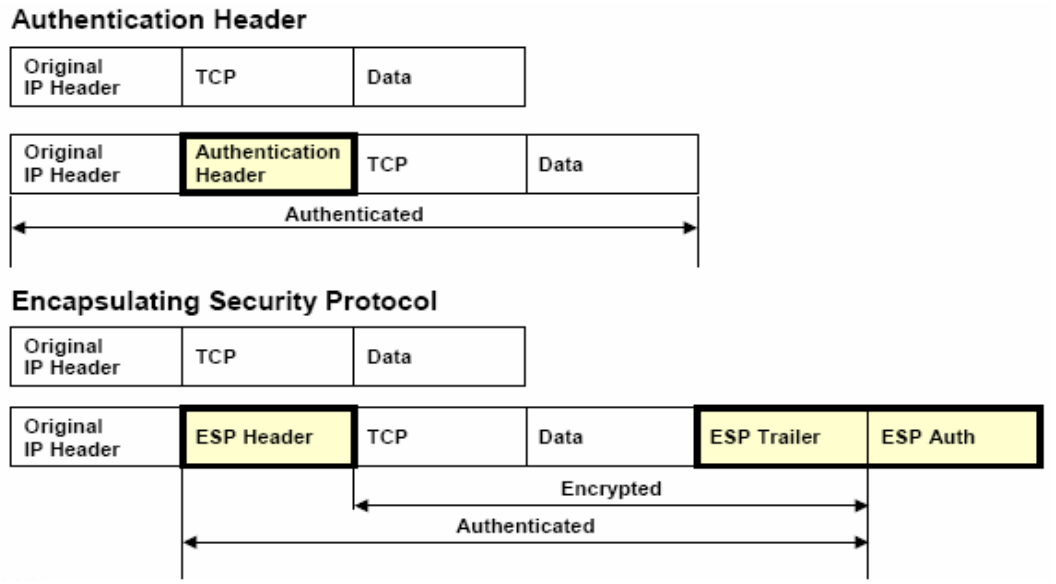
因此 IETF 在設計下世代 IPv6 時，即提出相關的安全保密架構，後來該架構才獨立為「網際網路層安全協定」(IP Security Protocol)，簡稱 IPsec【17】。IPsec VPN 的「安全」並不僅在於保證資訊的隱密（Confidentiality)，避免第三者「竊聽」到通訊內容，同時還確保網路傳送內容不被篡改破壞，亦即所謂資料的一致性（Integrity)；另外就是資料來源的驗證（Authentication)，確定資料並非來自公用網路上第三者所偽造。

IPsec 的安全協定

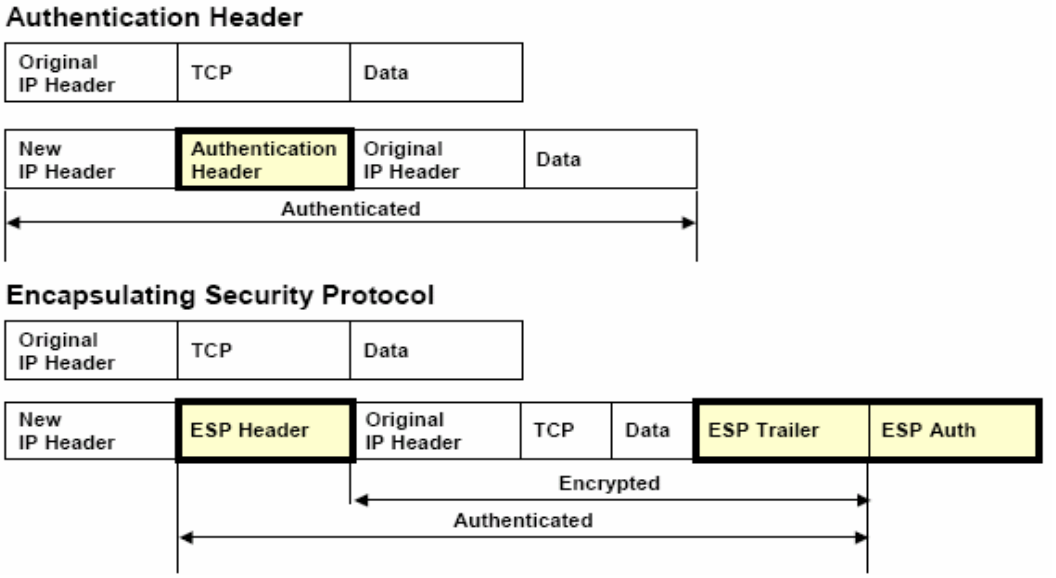
IPsec 提供兩種安全協定：AH(Authentication Header)與 ESP(Encapsulating Security Payload)，請參考【圖 2-15】【圖 2-16】。AH 主要透過 Hash function（例如 MD5 及 SHA-1）的技巧，提供封包來源的驗證、以及內容一致性的檢查，因此，一旦 IP 封包（包含 IP Header 及 Data Payload）在網路上遭人篡改或假造都可檢查出來。ESP 則可同時結合加密演算法（如 DES、3DES、或 AES）及 Hash function，對封包內容加密後即可不用擔心封包遭竊取，同時亦可有類似 AH 的驗證能力。但是 ESP 協定對於防篡改或造假的能力並不如 AH 強大，因此雖然 ESP 亦有類似驗證功能，仍不可完全取代 AH【17】。

IPsec 的封裝機制

對於 IPsec 如何與既有的 IP-based 網路結合，IPsec 提出兩種不同實作的封裝機制：Transport Mode 與 Tunnel Mode，請參考【圖 2-15】【圖 2-16】。前者即是所謂的 Host-to-Host 的封裝機制，亦即由連線兩端主機對其交換的 IP 封包以前段所述的 AH 或（及）ESP 做安全保護，兩通訊主機皆須實作有 IPsec。而後者，Tunnel Mode 則是所謂 Gateway-to-Gateway，其原理是通訊主機先將未保護的 IP 封包傳給具 IPsec 功能的 Security Gateway（通常是連接廣域網路的 Router)，Gateway 再將封包以 IPsec 保護、傳給遠端的 Gateway，對方在解除 IPsec 的保護機制後、再把還原後的 IP 封包轉送至真正的目的端主機【17】。



【圖 2-15】IPsec Transport Mode (AH and ESP)



【圖 2-16】IPsec Tunnel Mode (AH and ESP)

MPLS VPN 新趨勢

上述企業 VPN 解決方案在功能上都有一些不完美之處，傳統 VPN 都是建構在 L2 的 ATM 或 Frame-Relay 網路上，所以服務提供者需要建構其 L2 的骨幹網路。在 IP 網路越來越普遍的今天，實在不需再做此方面的擴充，另外在 L2 骨幹網路提供的 VPN 解決方案中，在建置及維護 Virtual Circuit (VC)方面是比較複雜的，同時如果要擴展 Extranet 網路時，會有相當的困難度。

然而 L3 的 IP VPN 解決方案，其安全和服務品質上在透過公衆網路時將無法確知效果，所以傳統 L2 及 L3 皆有其發展上的限制及問題，於是 MPLS

VPN 解決方案應運而生，其結合了 L2 及 L3 的優勢，只需目前 L3 的 IP 骨幹網路，即可以很容易的提供及建置客戶 Internet/Intranet/Extranet/Inter-AS VPN 完整解決方案，並且對客戶端來說設定更為簡易，同時透過 MPLS TE 及 MPLS Qos 的功能可進一步控制流量與保障傳輸的品質【7】。

傳統的 IP VPN 的缺陷

傳統的 VPN 一般建基於 PPTP、L2TP 或 IPSec 等加密協定之上。而幾種協定當中又以 IPSec 最為先進。客戶端只要裝了對應的客戶端程式(client program)，就可以享受 IPSec 提供強而有力的加密及認証服務。IPSec 雖然安全，但對於一般使用者來說，要安裝客戶端程式卻不是一件簡單的事情。首先，你無法知道對方是使用何種系統，需要何種客戶端程式(甚至乎有沒有相應客戶端程式)；其次，是企業與客戶未必是長期合作伙伴關系，要別人安裝客戶端程式未必容易：其三，IPSec 很可能會受網絡設定影響而導致連線失敗。換言之，安裝 IPSec 的客戶端很可能要修改網絡設定，以迎合 IPSec 的需要。

另外一般 IP VPN 網路的缺點在於無法確保通訊品質，因此在面臨資料大量傳輸或即時影音的傳遞需求時，可能由於網路環境不佳影響資料傳輸品質，以 MPLS (Multi-protocol Label Switching)技術為主的 MPLS VPN 便在此趨勢下逐漸成為當紅的應用。 MPLS 是由 Cisco、Ascend 與 3Com 等大廠主導推動，並由 IETF (Internet Engineering Task Force)通過。MPLS 是以標籤交換(Label Switching)為主的機制，在資料封包上加上一個標籤(Label)，整合 OSI 第三層的網路路由與第二層的標籤交換作業，縮短了資料封包因路由計算所造成的延遲時間，更適合即時資訊或影音資料的傳遞。MPLS 也支援多種傳輸協定，在第二層支援 Ethernet、Token Ring、FDDI、ATM、Frame Relay 與點對點傳輸(Point-to-point Links)；在第三層則支援 IPv4、IPv6、IPX 與 AppleTalk 等。

MPLS VPN 與傳統的 IP VPN 比較

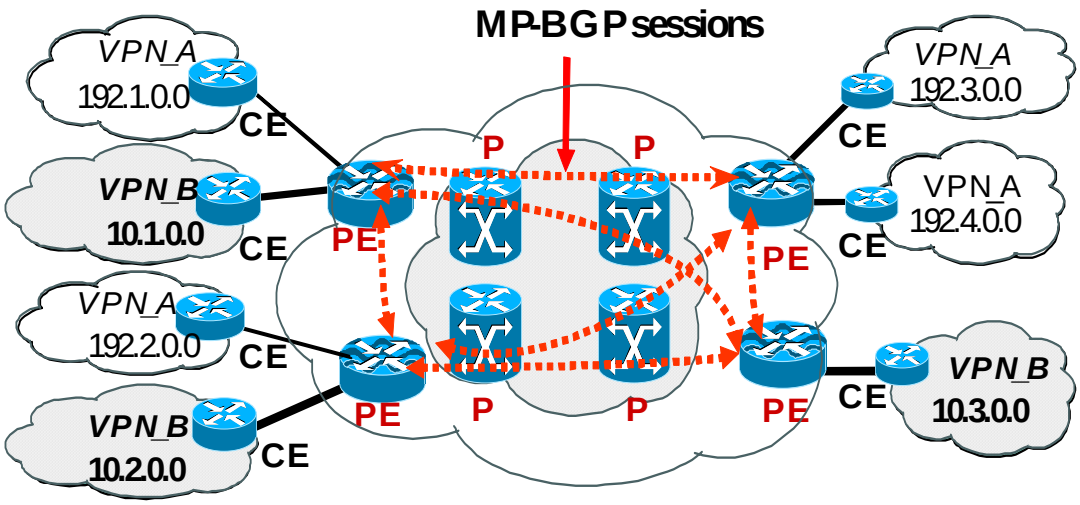
MPLS VPN 與傳統的 IP VPN 相比較最大的差異來源在於網路基礎架構的不同，在骨幹網路部分，傳統 IP VPN 通常是利用公共的網際網路進行資料傳輸，但 MPLS VPN 則大多以網路服務商的專屬網路為主，相對地減低資料外洩或被竊取的可能性。另一方面，由於在 MPLS VPN 上網路服務商可以依需求提供不同服務品質保證(Quality of Service, QoS)，解決了傳統 IP VPN 成本低廉但缺乏服務品質保證的缺點，因此在 VPN 技術的應用上，MPLS VPN 逐漸受到青睞。

事實上，除了由網路服務供應商所提供的 VPN 建置服務之外，許多防火牆與路由器製造商亦在產品中提供 VPN 服務的功能。然而，這樣的解決方案相對成本也稍高，因為企業必須自行購置硬體設備與建構網路環境。 就具有利用寬頻網路以進行即時線上會議、語音、資料存取或其它加值服務需求的企業而言，由於對於網路傳輸品質有更高的要求（如封包遺失率、影像延遲情況等），因此 MPLS VPN 較傳統 IP VPN 更能滿足需求。在 MPLS VPN 的解決方案部分，由於需建置一核心網路，目前則多由網路服務供應商負責，配合如 Cisco、Nortel 與 Juniper 等廠商的設備進行建置。然而，對用戶而言，隨著 IP 網路頻寬的提高，許多應用如即時影音、線上會議與語音通訊等，亦可因頻寬改進而在傳統 IP VPN 上獲得良好的品質。特別是，當 MPLS VPN 與傳統 IP VPN 在價格上的差異逐漸拉近時，用戶對於傳統 IP VPN 與 MPLS VPN 比較的關鍵將在於網路服務提供商所提供的整體服務品質與水準，例如是否能在跨國營運的需求中，提供可信賴的網路品質與連線服務，尤其目前許多台商均有跨兩岸三地進行企業營運往來的需求，網路服務供應商所提供的加值服務與可靠度將更為重要【7】。

2.2.2 MPLS VPN 技術介紹

MPLS VPN Connection Model

MPLS VPN 的網路區是由多個 LSR 及 Edge Label Switch Router (ELSR)所互相連結組成的，請參考【圖 2-17】，其中 LSR 位於 MPLS 網路區的內部核心(Core Network)，所以簡稱為 **P Router** 負責做更換標籤(Label Switching)的工作，而 ELSR 位於 MPLS 網路區的邊緣部分以連接客戶端 Router，所以簡稱為 **PE Router**，主要是負責將客戶端要進入 MPLS VPN 網路的封包加上 VPN Label 或是將要離開 MPLS VPN 網路要到對點客戶端網路的封包去除 VPN Label。而位於客戶端的 Router 我們簡稱為 **CE Router**。PE Router 與 P Router 間是屬於 MPLS 的區域，而 PE Router 與 CE Router 之間是屬於 IP 的區域，PE Router 與 PE Router 間必須建立 Full-Mesh 的 MP-BGP session，透過 MP-BGP 轉送與交換各節點 VPN 客戶的路由資訊(VPNv4 Routes)【7】。



【圖 2-17】MPLS VPN Connection Model

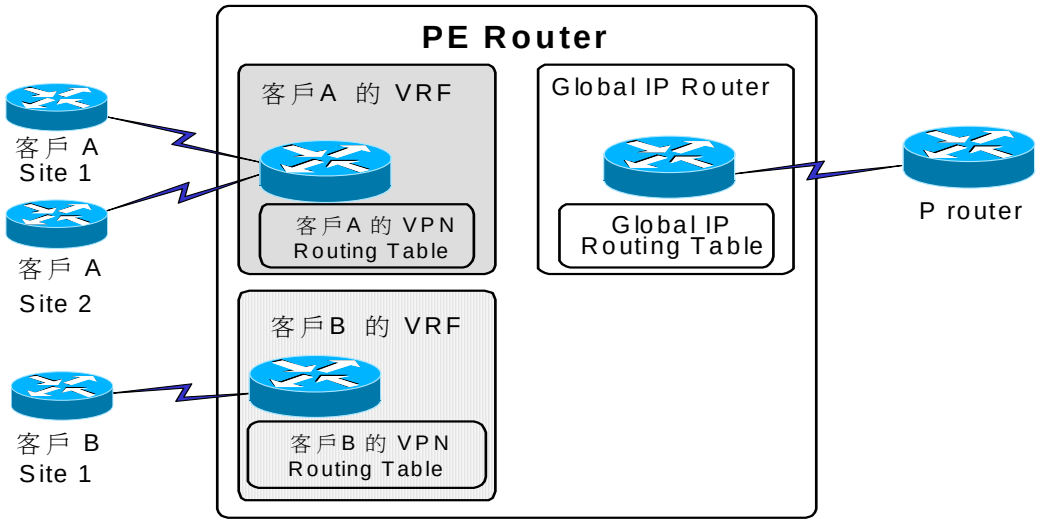
PE Router 維護兩份獨立的路由表

(1) Global Routing Table：

和骨幹網路透過 IGP 交換彼此的路由資訊，包含了所有 PE Router、P Router 的路由(Routes)。

(2) VRF(VPN Routing & Forwarding)：

每個 VPN 客戶可設定屬於自己的 VRF Table，Table 內儲存著 VPN 客戶端的路由(Routes)資訊，而且每個 VPN 客戶的路由資訊是各自分開獨立的，請參考【圖 2-18】，也就是說 PE Router 會根據設定不同 VRF 名稱的 VPN 客戶，切割一個獨立的空間，存放此 VPN 客戶的 Routing Table，這個各自獨立的 VPN 客戶 Routing Table 和 PE Router 本身網際網路的 Global IP Routing Table 是分開的，彼此不會互相影響【7】。

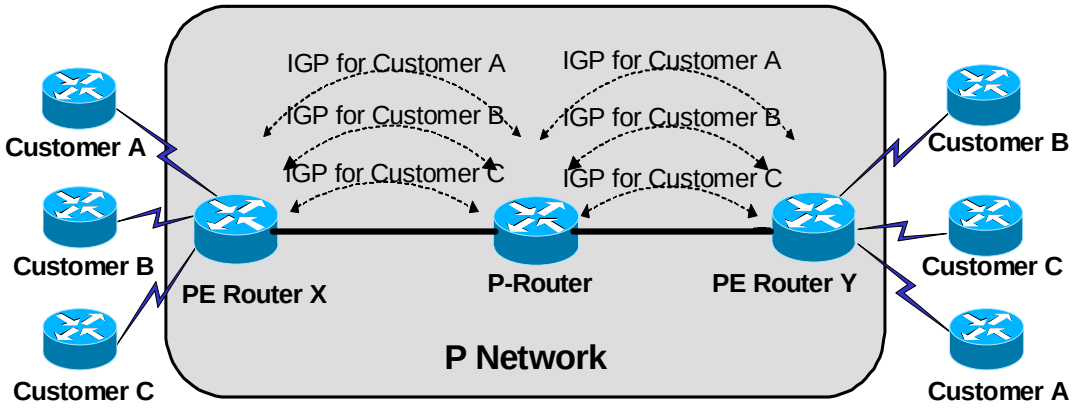


【圖 2-18】PE Router 有兩種互相獨立的 Routing Table

MPLS VPN 客戶路由資訊如何交換之研究

分散在各地的PE Router如何交換VPN客戶的路由資訊

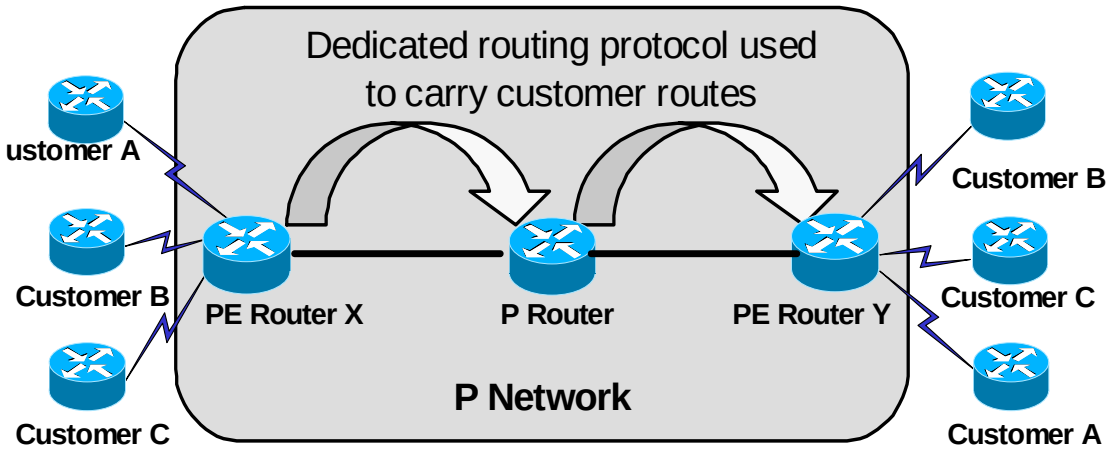
解決方案 1 請參考【圖 2-19】，對於每個客戶獨立執行一個 IGP 的路由協定，來攜帶客戶的 VPN 路由資訊通過骨幹 P Router 到達另一節點的 PE Router 交換彼此資訊，但它的缺點是不具擴充性(not scalable)，而且 P Router 需要擁有所有 VPN 客戶的路由資訊浪費 P Router 記憶體資源【7】。



【圖 2-19】每個客戶獨立執行一個 IGP 的路由協定

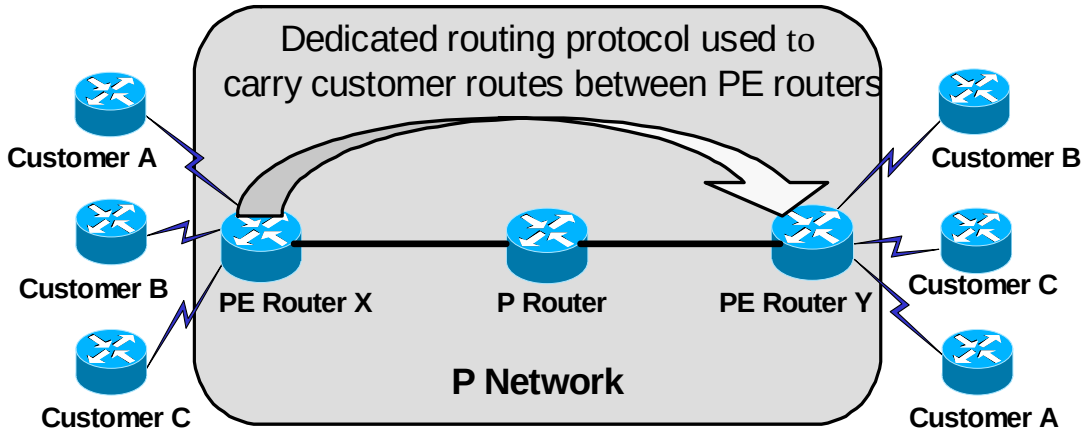
解決方案 2 請參考【圖 2-20】，執行一個路由協定，攜帶所有客戶的 VPN 路由資訊通過骨幹各節點的 P Router，最後到達另一節點的 PE Router 交換彼此資

訊。但是其缺點是 P Router 需要擁有所有客戶的路由資訊，造成資源的浪費【7】。



【圖 2-20】專有路由協定經骨幹各節點攜帶客戶的路由資訊

解決方案 3 請參考【圖 2-21】，是執行一個路由協定，攜帶所有客戶的 VPN 路由資訊(routing information)，直接和另一節點的 PE Router 交換彼此資訊，並在骨幹中利用 MPLS label 來交換 PE Router 間的封包。其優點為 P Router 不再需要擁有客戶的路由資訊，而且可以達成具有擴充性(Scalability)的目的【7】。



【圖 2-21】PE Router 間透過專有路由協定攜帶客戶路由資訊

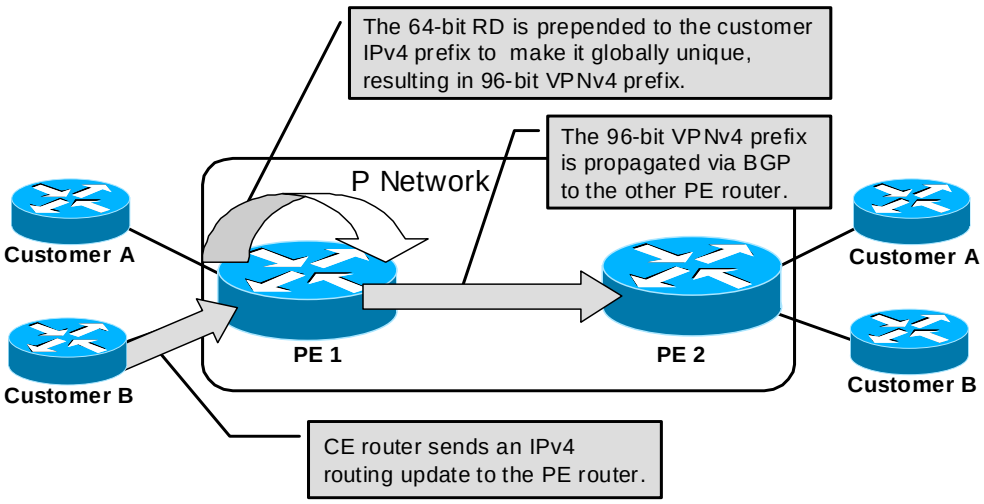
在這三種方案中以第三個方案最好有效率且最節省資源，但是要選用那一種路由協定來攜帶及交換 PE Router 間客戶 VPN 的路由資訊？尤其是 VPN 客戶的路由資訊是很多的，而唯一能攜帶大量路由資訊的路由協定就只有 BGP，而且 BGP 也可以直接在 PE router 間交換 VPN 客戶的路由資訊，而這種專門用

來交換分佈於各點 VPN routes 的路由協定稱為 Multi-Protocol Border Gateway Protocol (MP-BGP, RFC2283)【7】。

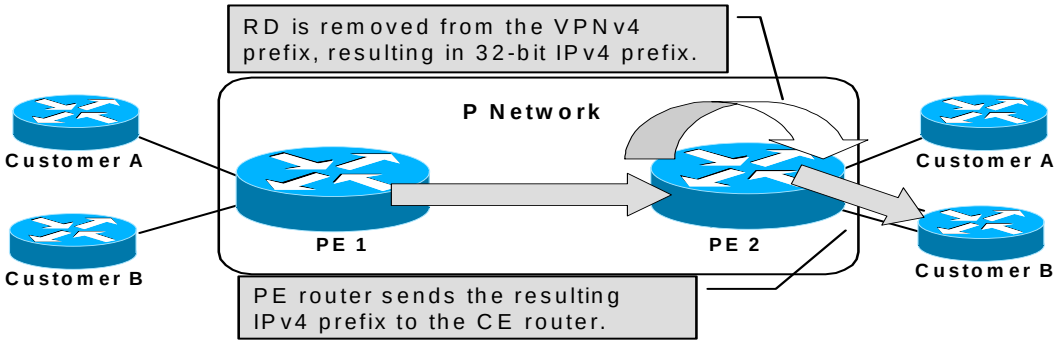
2.2.3 MP-BGP 的特殊屬性運作原理

Route Distinguisher(RD)值簡介

在企業 VPN 中，有很多的情況都有 IP 重覆使用的問題，如果有兩個 VPN 客戶使用了相同的網段，那要如何在使用單一路由協定(BGP)下的 PE Router，區分是不同的客戶的網段，因此在 MP-BGP 路由協定中加入一些新的屬性(Attribute)，將原來客戶的路由資訊延伸附加 RD 這個屬性值，使其客戶的路由資訊是唯一的。RD 是一個長度 64bits 的數字，附加於 IPv4 位址的前面使其達到絕對唯一(global unique)，這樣組合長度為 96bits 的位址表示法稱為 VPNv4 (RFC2547bis)，運作的方式請參考【圖 2-22】【圖 2-23】。這種 VPNv4 的位址表示法，只用於 PE Router 之間藉由 BGP 路由協定來交換，而這種 BGP 路由協定能支援除了 IPv4 位址表示法外的其他位址表示法(VPNv4)我們稱之為 MP-BGP。所以在一個簡單的企業 VPN 架構中，每個客戶都需要有一個 RD 值，藉以區分每個客戶【7】。



【圖 2-22】加入 RD 值的運作原理



【圖 2-23】去除 RD 值的運作原理

Route Targets (RT)值簡介

Route Targets 是額外附加在 VPNv4 BGP routes 的新屬性，用來表示所屬 VPN 之所有 VPN routes，例如某一個客戶端的節點可能需要參與或加入一個以上的 VPN，而 RD 值無法顯示出要參與或加入那些 VPN，所以需要一個新的屬性值來顯示出這個 VPNv4 routes 所屬的 VPN，RT 這個屬性值就是用在 MPLS VPN 結構中，支援複雜的 VPN 型態而設計的(draft-ietf-mpls-bgp4-mpls-01.txt)。Route Targets 是利用延伸原本 BGP communities 這個屬性來使用，我們稱這個屬性為 Extended communities。為了更彈性的規劃客戶的某個節點可以加入一個以上的 VPN 群組，而新增了 RT 這個屬性，由 RT 值來決定某個節點是否要和另一個節點網路互通，這個概念類似於區域網路的 VLAN。所以可是用 RT 值來控制路由資訊的分佈(Controlling route distribution)【7】。

RT 值如何運作

Export route targets：

表示其加入成為那一個 VPN 的成員，也就是說當客戶的 routes 被轉換成 VPNv4 時會再附加這個屬性。

Import route targets：

每個 MPLS VPN 客戶的 VRF 都可選擇要收入什麼樣的 routing 進入這個 VPN 客戶的 virtual routing table。

2.2.4 MPLS VPN 封包實際運作狀況分析

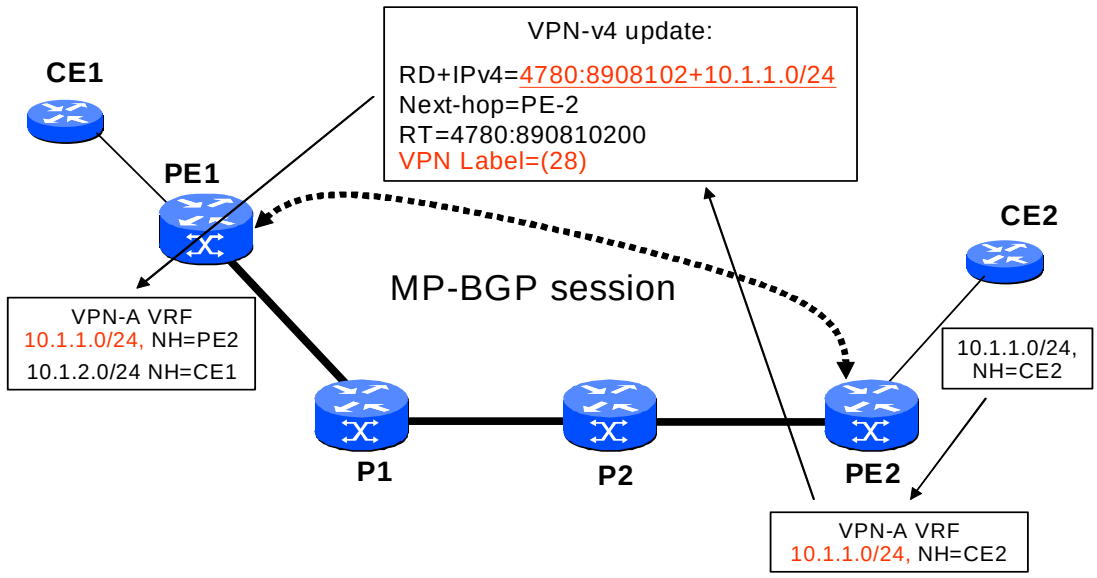
MPLS VPN 客戶端路由資訊建立及交換的過程如下【7】。

(1) IP網路路由與MPLS功能啟動：

在 IP 網路中利用 Routing Protocol (例如 IGP)交換各個 Router 的 Routing information。然而當啟動 MPLS 功能時，網路中的 PE Router 和 P Router 間利用 LDP 來交換彼此的 Label Information，並且在封包傳遞前就已決定 PE1 到 PE2 的 LSP 路徑。

(2) MPLS VPN 網路的建立：

利用 MP-BGP 的路由協定來攜帶及交換不同 PE router 間的客戶 VPN routes 請參考【圖 2-24】。PE2 將收到 CE2 的 MPLS VPN routes(10.1.1.0/24) 放入 VRF VPN-A 中，並將此 VPN routes 加上 RD 值組成 VPNv4 的格式 (Format)，另外再加上 RT 值，VPN label 等屬性值以 MP-BGP 的協定傳送給 PE1 Router，PE1 Router 收到來自 PE2 Router 的 VPN-v4 update 將其中的 IP Prefix 取出放入 VRF VPN-A 的 Routing Table 內並且告知(advertised to)CE1。



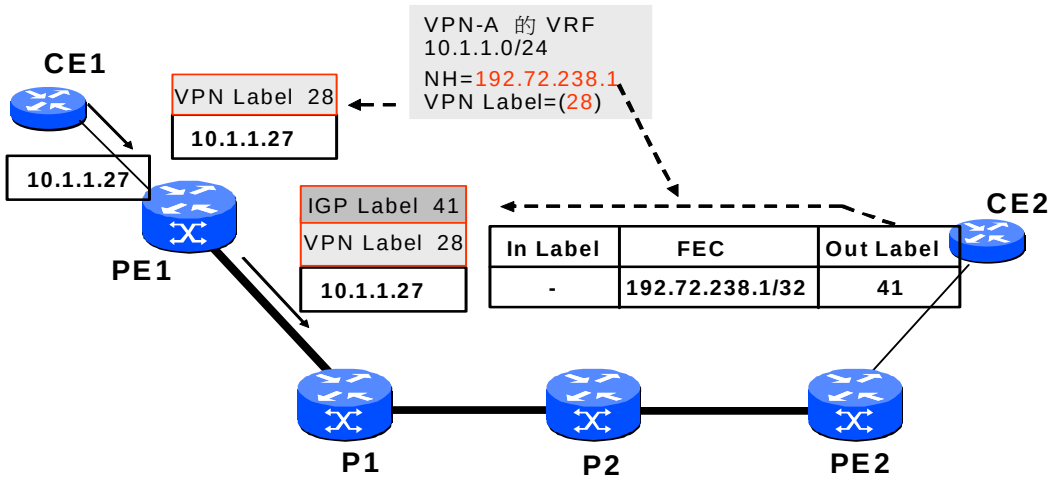
【圖 2-24】MPLS VPN 客戶路由資訊透過 MP-BGP 的交換過程

MPLS VPN 客戶端封包傳遞的過程

(1) PE1 將進入MPLS網路的客戶端封包加上VPN Label及IGP Label：

當 PE1 收到來自 CE1 的 IP packet ，得知封包的 Destination IP 是 10.1.1.27 立刻查詢 VPN-A 的 VRF Routing Table，發現要到 10.1.1.0/24 的 Next-hop IP 是 192.72.238.1，而且要在 IP Header 的前端加上 VPN Label 以

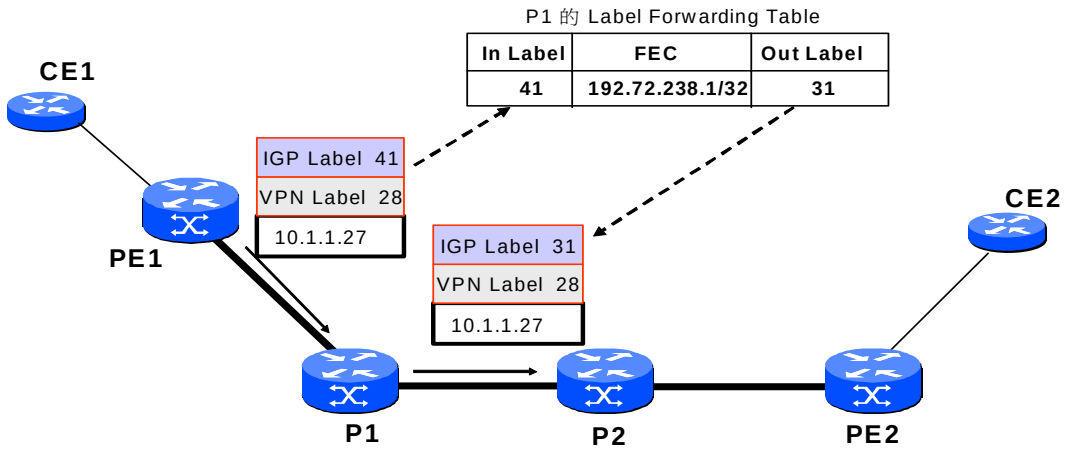
區別是來自不同的 VPN 客戶，請參考【圖 2-25】。另外再根據 Label Forwarding Table 可以查出要到 Next-hop IP 192.72.238.1 要使用 IGP label=41 才能 Forwarding 到 MPLS 的網路中，所以在 VPN Label 的前端再加上 IGP Label，這樣才能順利的依循著之前定好的 LSP 將 Packet 送達 PE2【7】。



【圖 2-25】PE1 將進入 MPLS 網路的封包加上 VPN 及 IGP label

(2) 在MPLS網路中P Router負責做Label Swap：

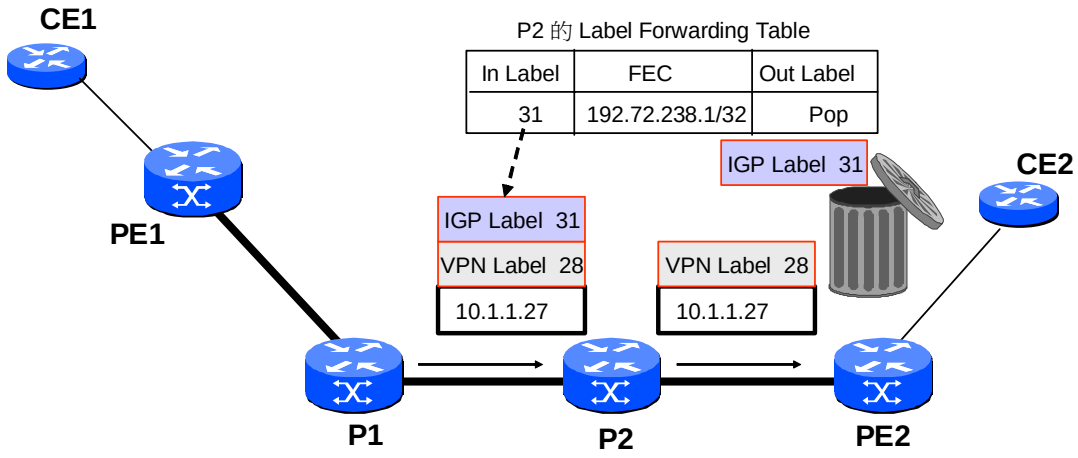
當 P1 Routers 收到來自 PE1 的封包時，請參考【圖 2-26】，首先查看封包最外層的 Label Header 也就是 IGP Label 其值為 41，再根據本身的 Label Forwarding Table 得知，凡是 In 的 IGP Label=41 之封包，要送出 P1 Router 到下一個節點 P2 時，要將 IGP Label 41 置換成 31 再送出封包【7】。



【圖 2-26】MPLS 網路中 P Router 負責做 IGP Label Swap

(3) Penultimate Hop Popping：

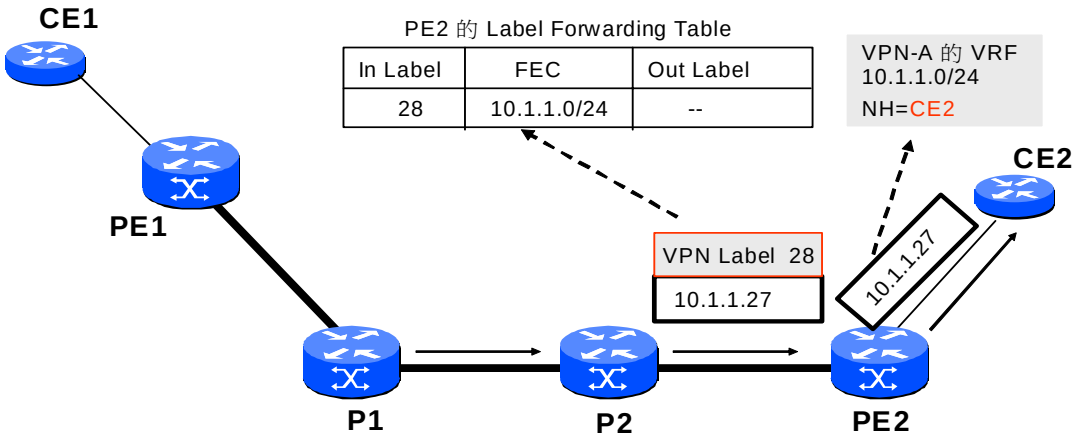
在 PE1 到 PE2 的 LSP 路徑中 P2 是 penultimate hop 的角色【7】，他會收到來自 PE2 透過 LDP 協定的通知說要把封包中外層的 IGP Label 先拿掉，以減輕 PE2 工作的負擔，詳細過程請參考【圖 2-27】。



【圖 2-27】Penultimate Hop Popping 運作原理

(4) PE2 負責去除VPN label並送到所屬VPN客戶的interface：

當 PE2 收到來自 P2 的封包，先查詢得知其 VPN Label =28，並得知此 VPN Label=28 相對應的 VRF 為 VPN-A 這個客戶，進一步得知要將封包送往屬於那個 VPN-A 客戶的 interface，因此 PE2 的工作程序是 One single lookup、VPN Label 被去除(popped)並將封包送往 CE2，詳細過程如【圖 2-28 】。



【圖 2-28】PE2 負責去除 VPN label 並轉送封包到所屬的界面

小結：

MPLS VPN 很容易建置(provisioning)，而且有最佳化的路由交換機制，同時 RD 的設計可以避免不同 VPN 客戶 IP 位址重覆使用的問題，另外 RT 值的加入可規劃複雜型式的 VPN 架構例如 Extranet 的應用，是其他企業 VPN 解決方案所無法做到的。

2.3 網路管理技術

2.3.1 網路管理簡介

網路管理四大模組

網路管理四大模組分別是組織模組、資訊模組、通訊模組、功能模組【11,12】。

- ✓ 組織模組(Organization Model)：網管系統的組成元件包括 Manager、Agent、Managed Object，各組成元件的功能及關係如下，Manager 負責傳送 request 給 agents 並且監控 alarms，Agent 這個元件負責從網路元件收集資訊並回覆給 Manager，Managed object 這個元件被 agent 管理及擁有。

- ✓ 資訊模組(Information Model)：SMI(Structure of Management Information)，Syntax and Semantics，定義網管資訊架構，提供共同的管理資訊儲存架構，MIB(Management Information Base)定義網管資料庫及資料物件，提供通用的網管資料物件。

- ✓ 通訊模組(Communication Model)：定義網管通訊協定，以作為 Manager 與 Agents 間交換網管訊息的標準。

- ✓ 功能模組(Functional Model)：包括有五項分別是組態管理、故障管理、品質管理、安全管理、計費管理。

網路管理五大功能

網路管理共分為五大功能【11,12】分別是組態管理、故障管理、品質管理、計費管理、安全管理等五項，請參考【圖 2-29】。

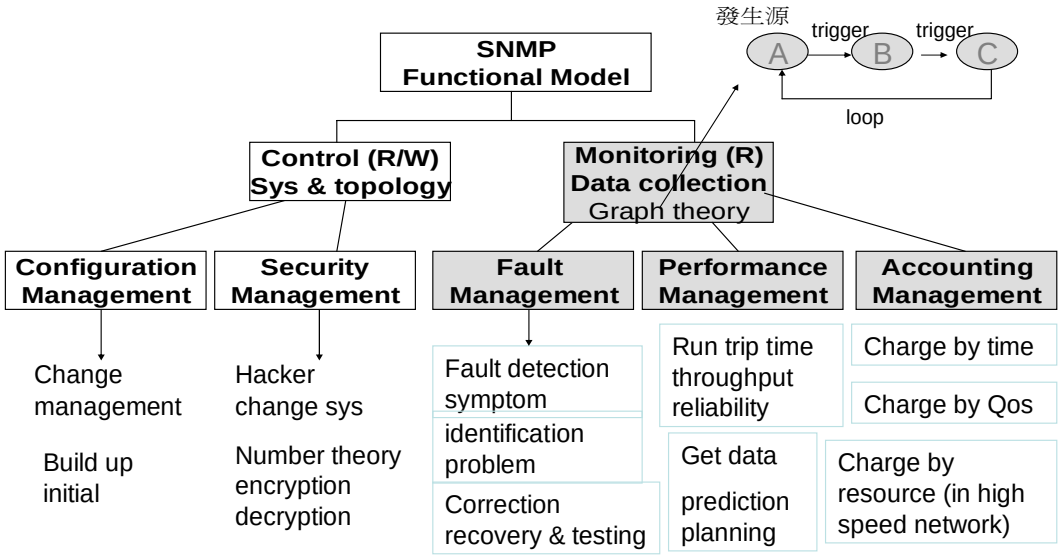
- ✓ 組態管理(Configuration Management)：提供收集、鑒別、控制來自代理的資料並將資料提供給代理的一組功能。這些資料主要包括軟硬體的運行參數和條件、路由控制、備份操作條件等。透過組態管理，還可以靈活地分配線路資源，提供各種出租業務。

- ✓ 故障管理(Fault Management)：提供對住處網路及其運行環境的異常情況進行動態檢測、故障隔離和修復的一組功能。包括監視告警、故障定位、故障校正、測試及故障控制等。這些操作能迅速地甄別出問題所在以及性能是否降低，必要時啟動診斷、修理、測試、恢復、備份等控制功能。

- ✓ 品質管理(Performance Management)：提供[預防性]的故障管理，傳輸效能的判別指標有延遲時間(Response Time)、傳輸正確率(Accuracy)、流量使用率(Throughput & Utilization)。

- ✓ 計費管理(Accounting Management)：提供測量網路中各種業務的用量並確定使用成本的一組功能。包括資產管理、帳單管理、計費管理、收費與資金管理、處理和報告的過程。計費管理的計費方式有物理線路出租計費、傳輸帶寬和時間計費、收視時間計費、節目內容計費、節目內容計費、資訊服務計費等。

- ✓ 安全管理(Security Management)：功能有三個方面的含義，首先是保證管理事務處理的安全，這些功能涉及到網路管理的各個層次，包括系統之間、系統與客戶之間、系統與內部用戶之間的認證、訪問控制、資料保密性、資料完整性和可用性等。其次，要保證整個傳輸網和管理網的安全，對非法使用網路資源的情況進行處理。第三，組織上的安全管理。安全管理對以上每一種管理功能的實現都是密切相關和重要的。



【圖 2-29】網路管理五大功能模組

2.3.2 網路管理協定 SNMP

SNMP是使用在TCP/IP網路環境裡的管理通訊協定，可用來監控網路上的設備狀況、效能、組態管理、統計分析與安全計費。SNMP共有SNMP v1、SNMP v2及SNMP v3三種版本，而目前的網路設備大多只支援SNMP v1的版本。在RFC（Request For Comment）的文件中，共有RFC1155、1212、1213、1157四份基礎文件組成SNMP v1—RFC1155文件描述定義了以TCP/IP為基礎的管理訊息庫（MIB）內的被管理端物件（object）的結構與辨識規格，RFC1212文件描述定義產生MIB模組必要的格式（format），RFC1213文件描述定義以TCP/IP為基礎的管理訊息庫（MIB-II），在使用網路管理通訊協定時必須要遵守的管理資訊；RFC1157文件就是簡易網路管理協定，描述了管理端與被管理端之間連繫溝通與訊息交換的資料格式與意義。

SNMP通訊協定組態，顯示了每個被管理端皆必須要執行SNMP、UDP、IP以及相關網路通訊協定（如Ethernet、FDDI、X.25）。而主機的部份除了前面所提到的各項通訊協定之外，也可能會需要提供FTP、HTTP等服務，因此TCP協定也會被執行。另外，代理者處理程序（Agent Process ）則會負責解譯SNMP訊息與代理者的MIB控制【12,15】。

網路管理系統的組成元件

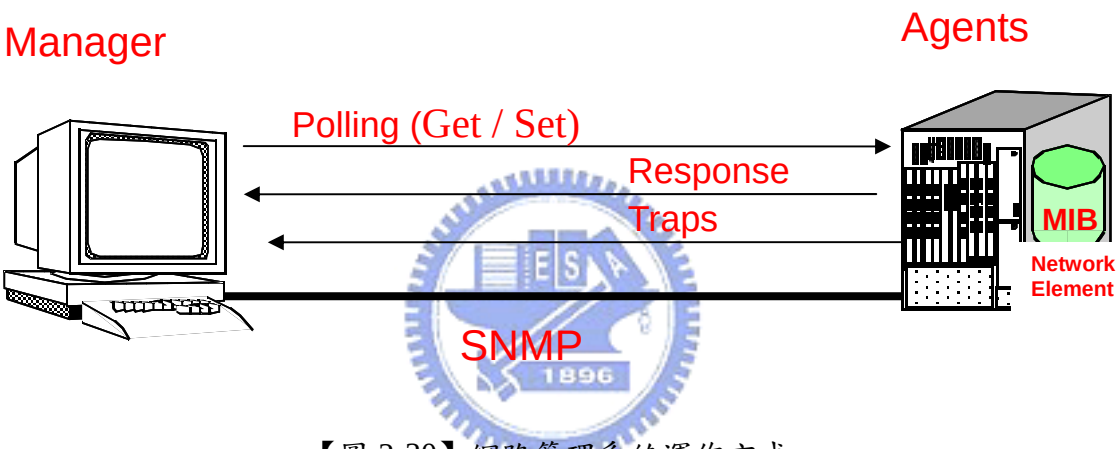
- ✓ 網路管理工作站(Manager)：執行網路管理系統，為一獨立管理平台，負責處理來自被管理端所傳送的資訊。

- ✓ 被管理端與網管代理者（Agent）：「負責即時、連續的擷取網路上的資訊」，等候管理端的要求（Request），將蒐集的資訊送回，並當設備發生問題時，主動傳回訊息（Trap）。被管理端可為router、switch、 HUB、Host 等設備，並在其上安裝Agent 軟體以便負責資料蒐集的工作。

- ✓ 管理訊息庫（MIB）：Network Element中有許多資源需要被管理，SNMP的做法是將這些需要被管理的資源定義成物件藉由被管理端物件的抽象概念（Abstractions）（如資源、屬性）表現在管理端介面上，如果被管理端是一部網路設備，則被管理端就會具有網路位址、封包流量、臨界值等的屬性表現。所有抽象資訊的總集合稱為MIB，管理者可透過Agent看到這些資訊。另外SMI則定義了Management Agent 內MIB中物件存在的資料結構或物件的類別。

✓ 網路管理通訊協定

管理端與被管理端之間的溝通，必須要靠一種標準的共通性語言—兩者均執行相同的SNMP通訊協定。SNMP包含了下述兩項主要功能，管理者可利用這些功能即時取得與瞭解被管理端的狀況，請參考【圖2-30】。(1)Polling：利用定時的Polling機制(Get or Set Agent Object)，以獲知網路系統的現況，並通知Agent處理網路問題，Polling 的使用，使得SNMP保持簡單的特質，Manager可控制Polling 的頻率，以限制網管資訊流量，Polling-based網管協定可管理的Agents數目有限。(2)Trap：利用traps, Agent可以主動將網路問題通知Manager, traps只有在重大錯誤發生時才傳送，而且traps的訊息通常很小，除非網路系統剛建置完成，否則traps的數量不會太大。



【圖 2-30】網路管理系統運作方式

另外我們還可以利用RMON（Remote Network Monitoring）網路管理資料交換機制，將網路上所有使用者的資料傳輸狀況蒐集起來，再結合資料庫的功能，分析出每位使用者或是每個組織的網路使用狀況，這麼一來，我們就可以依照這些網路使用資訊做後續的管理工作或是專業建議【12,15】。

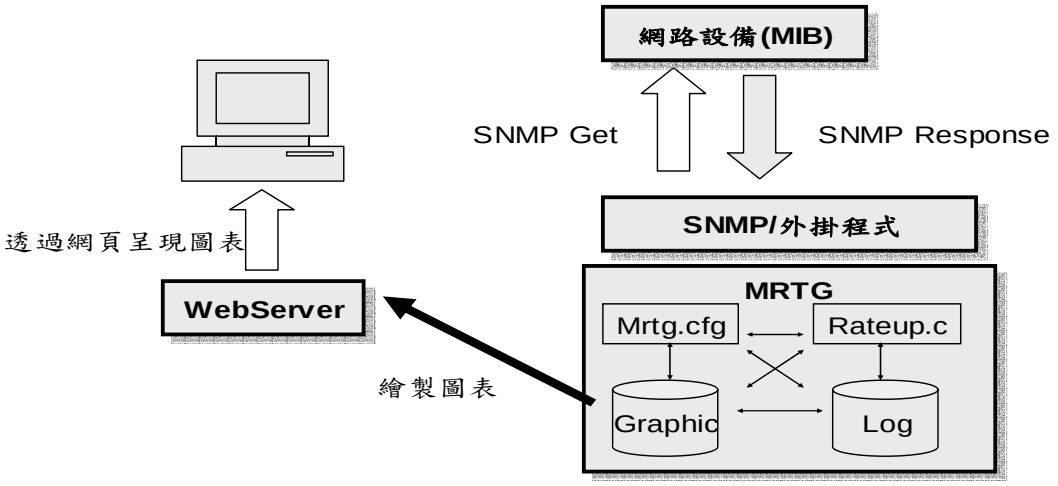
2.3.3 網管工具簡介

MRTG (Multi Router Traffic Grapher)

MRTG 是一套網路流量統計軟體，是透過 SNMP 的協定，向網路設備詢問相關的資料後，網路設備傳遞數值給 MRTG 程式，然後 MRTG 再繪製成網頁上的圖表，請參考【圖 2-31】，MRTG 網管技術的優點是(1)可同時監控多個設備或主機(2)以網頁圖形方式呈現簡單明瞭(3)消耗極少的系統資源(4)可及時監控(5)加掛自己寫的程式後，就可以偵測 CPU 或者是 RAM 或是其他資訊。

MRTG 為使用 Perl 程式寫成的，並且使用到 zlib 、 gd 及 png 的函式庫（zlib 用來繪製圖表、gd 用來壓縮圖表），且由於 MRTG 乃使用 SNMP 協定，並且最後是以 HTTP 的網頁型態輸出成圖表，因此需要確定 Linux 主機中已經含有下列的套件：Perl (perl-5.0xx 以上)，zlib (zlib-1.1.3-xx 以上)，gd (gd-1.3.xx 以上) libpng，httpd，net-snmp。

MRTG 的運作方式如下，Mrtg program 是一支perl 程式，為整個MRTG tool 的主程式。Mrtg.cfg 是一支config 檔，主要的是作為各項參數的設定。Mrtg.cfg file 內包含許多的option，這些option 可以幫助我們作MRTG 內部的各項設定，其中一項為Router 的指定，MRTG 可以透過SNMP protocol，利用crontab 的設定，於每一固定的時間間隔，取得Router於這一段時間間隔內MIB中某網路狀態參數的累積值，且將取回的值存於log檔案內，隨時間變化而update。Rateup.c是作資料update的程式。最後統計資料是以HTML檔儲存，可以利用web browser呈現出來【15,18,19】。



【圖 2-31】MRTG 網路管理技術運作方式

2.3.4 以政策為基礎的網路管理

技術的緣起與目的

自有網路以來，網路管理者一直扮演重要的角色，網際網路的流行風潮帶動了網路規模的大幅成長，網路使用者的數目大幅增加，連接至網路的網路設備數目與種類劇增。加上現今網路上提供的各種的應用服務，使得網路使用者

對網路傳輸頻寬的需求變大，對於網路傳輸品質與資料傳輸的安全性要求也跟著提高。

面對的這樣一個網路環境，一般網路管理者很難同時擁有管理這個複雜多變的網路環境所需的各項知識與技能，Policy-based 網路管理技術於是因應而生，成為最最新的網路管理概念。希望藉由此一技術，使得管理者不需要逐一地去設定所有網路設備組態，而是由管理者制定某些有意義的網路政策(Policy)，交由 Policy-based 網路管理系統執行，系統將依據其所訂政策內的規則與條件(Rules)，自動執行網路資源管理服務，例如對所管轄的網路設備進行相關組態設定、頻寬等級管理或安全管理等服務。

Policy-based 網路管理技術除了解決前述問題外，它也提供了有別於傳統網路管理的完整系統運作的技術架構(Policy-based Framework)，其中包含了所有網路系統資源控管所需的作業程序及通訊協定，同時也滿足企業既定的政策目標。此外 Policy-based 網路強調的是一個系統化的網路管理系統，而非單純的網路設備組態設定與管理，希望藉由 Policy-based 網路管理架構，直接將企業領導者所制定的政策目標以網路管理政策方式來表現進而透過 Policy-based 網路管理系統的運作，將網路管理政策分配至整個網路系統執行。

從應用面來看，除了網路管理最基本的網路設備設定管理(Configuration Management)需求，網路服務品質保證(QoS)及網路安全服務(例如 VPN)會是最可能直接應用 Policy-based 技術的兩種網路服務，依據網路服務性質，說明了 Policy-based 技術可能應用在網際網路的各個層面【9,10,20】。

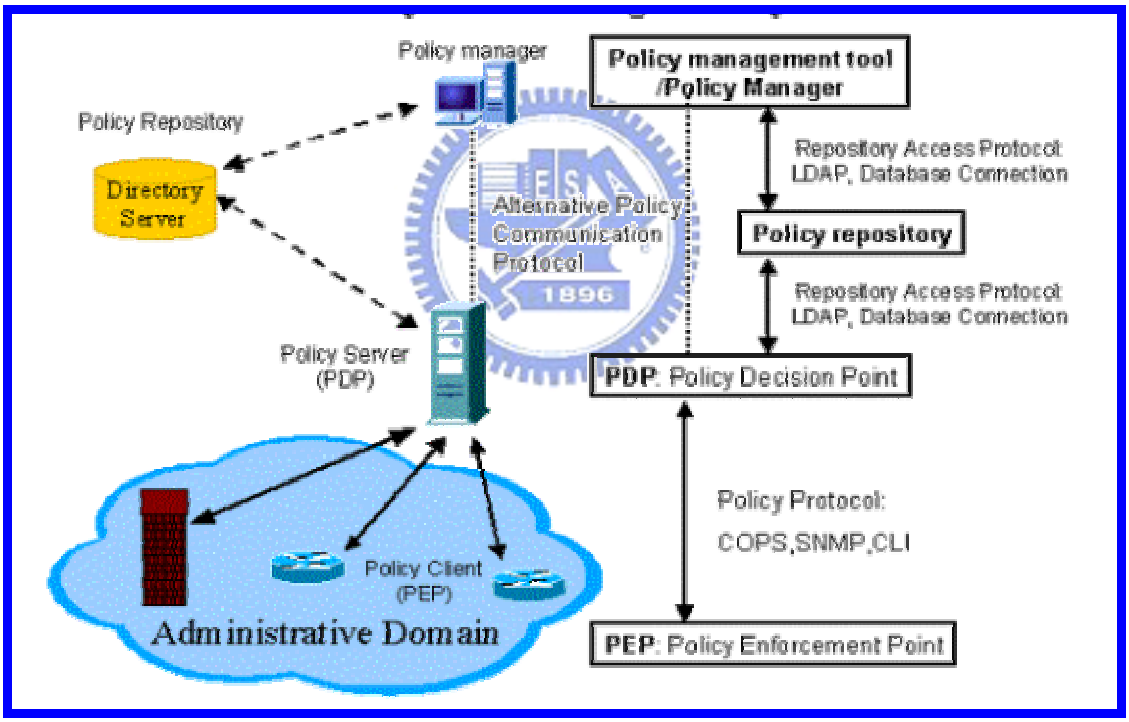
以政策為基礎的網管技術架構

綜合 Distributed Management Task Force (DMTF)與 Internet Engineering Task Force (IETF)這兩組織提出的 Policy-based Network，這裡以【圖 2-32】的階層式系統架構來說明 Policy-based 網路管理系統，並且說明管理系統中四大階層的功能與彼此間採用的通訊協定。

首先 Policy Management Manager (PM)提供管理者編輯、修改 Policy 資料的應用系統，通常會透過一個容易使用的管理界面來編輯網路政策，並將編輯好的 Policy 資料轉成一定格式，存於 Policy Repository 中。Policy Repository (PR)是 Policy 儲存機制，可以是一個目錄系統，或是資料庫系統，主要用來提供管理者儲存已編輯完成的網路政策資料(Policy)，及其他系統相關的網路設備資訊

或設定參數等資料。Policy Decision Point (PDP)通常也稱為 Policy Server，是整個系統的決策中心，負責依管理者所設定的政策，分配網路管理政策至 Policy Enforcement Point (PEP)，以達到管理需求【20】。

Policy Enforcement Point(PEP)則是接受 Policy 管理的設備，可能是路由器、Switch、防火牆等網路設備，這些接受 Policy 管理的設備(PEP)的組合，就是一個 Policy Administrative Domain。以上階層式系統架構中每一個階層都是獨立的子系統，各個階層均可透過一定的管理協定來互相溝通，如 PM 和 PR 間是用 Lightweight Directory Access Protocol (LDAP)的目錄方式來傳遞資訊，PDP 和 PEP 用 Common Open Policy Service (COPS)作業協定來傳輸資料。Policy 資料則過各種資料定義格式，在每個階段間轉譯，最後以標準的 Policy 資料定義格式，例如 Policy Information Base(PIB)或 Management Information Base(MIB)存在於接受 Policy 管理的網路設備(PEP)上【20】。



【圖 2-32】Policy-based 網路管理系統架構