行政院所屬各機關因公出國人員出國報告

＜ 出國類型 ： 實習＞

實習網際網路品質控制技術

服務機關 ： 中華電信股份有限公司　　網路處
出國人　 ： 助理工程師　　彭康韶
出國地點 ： 美國
出國期間 ： 民國 91 年 11 月 3 日至民國 91 年 11 月 16 日
報告日期 ： 民國 92 年 3 月 3 日

系統識別號:C09104748

公務出國報告提要

頁數: 46　含附件: 否

報告名稱:

赴美實習網際網路品質控制技術

主辦機關:

中華電信股份有限公司

聯絡人／電話:

姜學民／2344-5405

出國人員:

彭康韶　中華電信股份有限公司　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 11 月 03 日 -民國 91 年 11 月 16 日

報告日期: 民國 92 年 03 月 03 日

分類號/目: H6／電信　H6／電信

關鍵詞: MPLS,CoS,VPN,TE,RSVP,Diffserv,Traffic Engineering

內容摘要: 由於網際網路的快速成長，IP網路之建置非常普遍。在IP公眾網路(Public Network)平台上,我們進一步思考是否也能提供專屬私有網路(Dedicated Private Network)之服務,提昇附加價值。而MPLS（多重協定標籤交換，Multiprotocol Label Switching）技術在VPN (虛擬私有網路)服務上提供了建置選擇之一, 其主要效益在於功能的提昇並提供商業IP VPN之服務 。 提供VPN服務的供應商常常必須爲客戶提供某程度的QoS。MPLS VPN便利用Differentiated Service技術支援CoS，這些技術可以讓客戶的資料在進入服務供應商網路時，能夠根據各種管理政策--例如原始站址、應用型態等，來區分爲不同的等級。在此網路中，資料流的等級是根據表頭位元與不同的標籤來辨別，而路由器便是據此來決定佇列處理方式及CoS等級--如Precedence。 本次出國實習內容係針對MPLS相關技術,包含有VPN服務的建置、Traffic Engineering-RSVP及QoS 之Differentiated Service等議題進行深入之研究,對於本公司現在之IP VPN服務建置將提供有利之參考價值。

本文電子檔已上傳至出國報告資訊網

目錄

第一章前言

由於網際網路的快速成長，以及IP網路建置的普遍，對於IP網路新功能的需求與日俱增,而MPLS（多重協定標籤交換技術，Multiprotocol Label Switching）正為虛擬私有網路(VPN)以及資料傳輸工程(traffic engineering)，提供了多種支援功能。MPLS的主要效益在於功能的提昇並提供商業IP服務的MPLS提供了下列基本功能：

- □可擴充虛擬私人網路(VPN)支援
- □資料傳輸工程(traffic engineering)

提供VPN服務的供應商常常必須為客戶提供某程度的QoS。MPLS VPN便利用新的區分化服務(Differentiated Service)技術支援QoS，這些技術可以讓客戶的資料在進入服務供應商網路時能夠根據各種管理政策--例如原始站址、應用型態等，來區分為不同的類別。在此網路中，資料流的層級是根據表頭位元與不同的標籤來辨別，而路由器便是據此來決定佇列處理方式及QoS參數--如延遲或遺失。

本次出國實習內容係針對MPLS相關技術,包含有VPN服務的建置、RSVP-Traffic Engineering及QoS 之Differentiated Service等議題進行深入探討,下列各章為本次出國案之實習報告。

第二章 實習行程及課程

實習行程及課程

91/11/3(星期日) : 去程,飛往美國舊金山。

91/11/4~91/11/9 : 實習Introduction to QoS and Traffic Engineering Technology。
實習Introduction to Cisco Gigabit Switch Router Technology 。
實習Introduction to MPLS, QoS and Traffic Engineering Technology。
實習Introduction to Juniper Network Router Technology。

91/11/10(星期日) : 行程,飛往華盛頓DC。

91/11/11~91/11/12 : 實習Implementation of MPLS, RSVP, and QoS Technology。

91/11/12 : 行程,飛往紐約。(利用課後夜間行程)

91/11/13~91/11/14 : 實習Implementation of Traffic Engineering, and QoS Technology。

91/11/14~91/11/16 : 回程,飛回台北。

第三章 MPLS技術

3.1 MPLS基本技術

MPLS背後的主要設計概念在於使用一個以標籤置換技術(label swapping)為基礎的傳輸模型，該標籤交換技術可以與不同的控制模組相結合。每一個控制模組負責指派和配送一組標籤，以及維護其他相關的控制資訊。舉例而言，一個MPLS路由器大致包括：

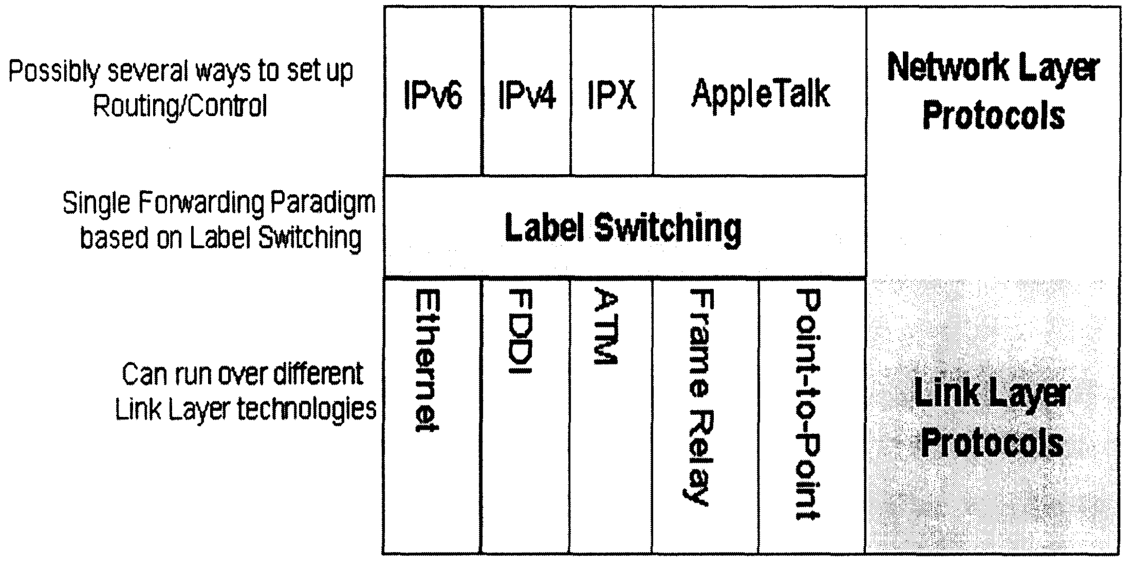
□ 使用傳統IGP路由通訊協定(諸如OSPF、IS-IS等)來建立路由表單，指派標籤路由，並使用標籤分配協定(Label Distribution Protocol, LDP)來分配標籤。

□ 一套資料傳輸工程模組，可以透過網路明確地設定特定標籤交換路徑，以達到資料傳輸工程之目的。

□ 一套VPN模組，可以使用MP-iBGP路由通訊協定建立VPN專屬的路由標籤，並分配等同於VPN路由的標籤。

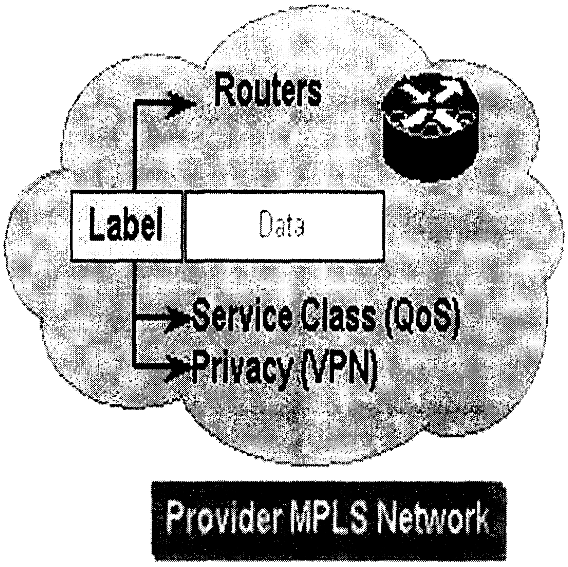
由於MPLS允許不同的模組使用不同的標準來指派封包標籤，它可以根據封包IP表頭(header)的內容分別傳送封包。此一特性對於傳輸工程(traffic engineering)和支援VPN等功能是很重要的。

3.1.1Multi-Protocol:Both Above and Below:

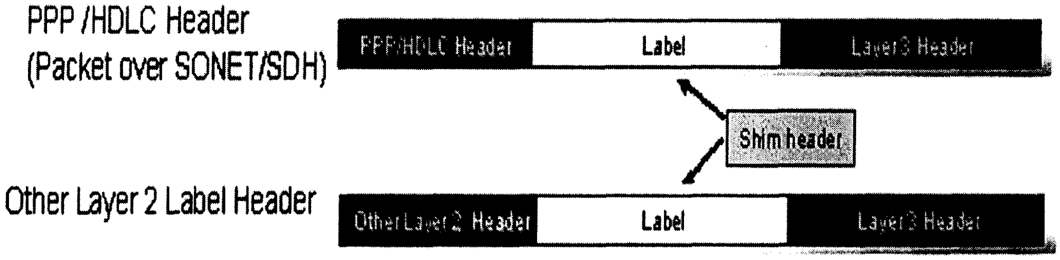

Possibly several ways to set up Routing/Control
Single Forwarding Paradigm based on Label Switching
Can run over different Link Layer technologies
IPv6
IPv4
IPX
AppleTalk
Network Layer Protocols
Label Switching
Ethernet
FDDI
ATM
Frame Relay
Point-to-Point
Link Layer Protocols

3.1.2 MPLS Labels: Destination and Service Attributes:

- Labels are the key
- Interoperability of MPLS routers
- Indicates service attributes without per-hop decisions:
  - –Service Class
  - –QoS
  - –Privacy (VPN)
  - –Switching
    - •traffic engineered paths

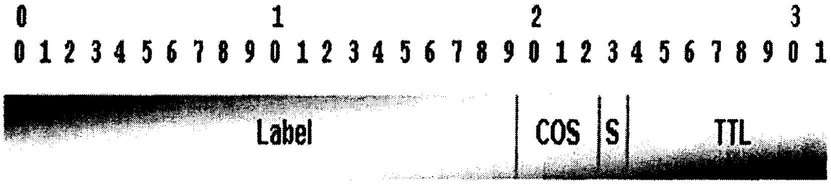


- MPLS Labels:

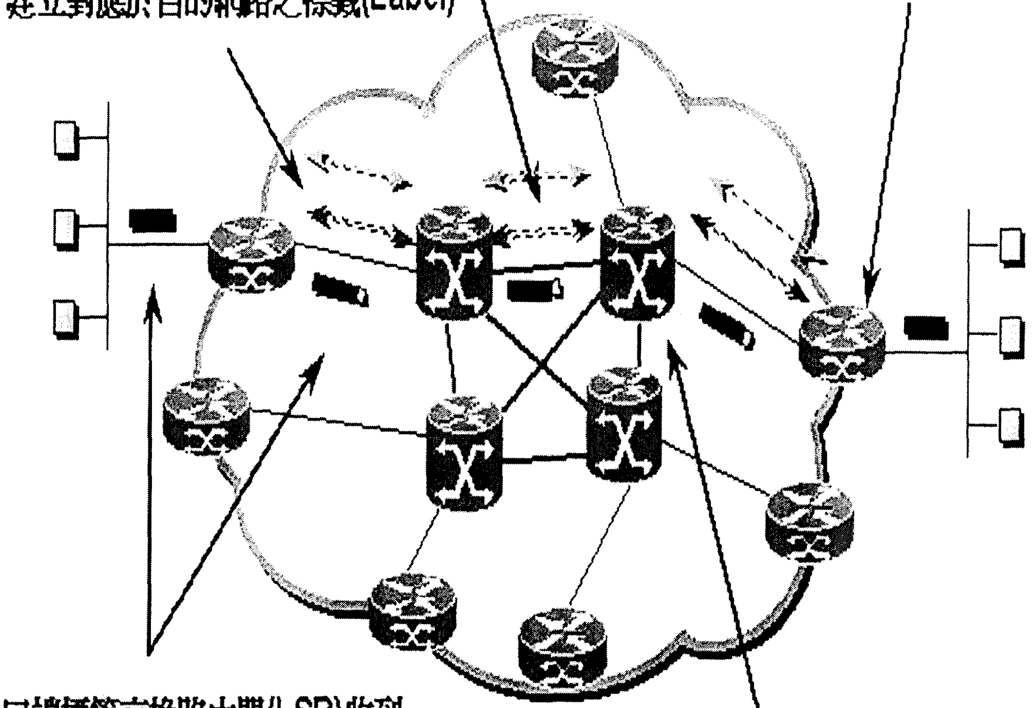


- Label Header:

Label = 20 bits
COS = Class of Service, 3 Bits
S = Bottom of Stack, 1 Bit
TTL = Time to Live, 8 Bits



3.2MPLS Operation



1a. 以現用之路由協定 (e.g. OSPF, IS-IS)
建立目的網路之路由表

4.出口端標籤交換路由器(LSR),移除標籤,遞送封包

1b. 啓動Label Distribution Protocol (LDP)
建立對應於目的網路之標籤(Label)

2. 入口端標籤交換路由器(LSR)收到封包後,進行網路層加值服務及貼標籤之動作

3.標籤交換路由器(LSR)以標籤置換方式 進行封包交換

3.3 MPLS VPN網路

3.3.1 MPLS VPN服務之優點:

MPLS的應用中，對網路服務供應商具有強大潛在利益的就是對VPN服務的支援。在VPN上採用MPLS對於VPN的建置是一個具有吸引力的替代方案，可以依客戶決定來取代ATM、訊框中繼(Frame Relay)、固接虛擬電路(permanent virtual circuits, PVC)，或是互相連結路由器的各種通道。

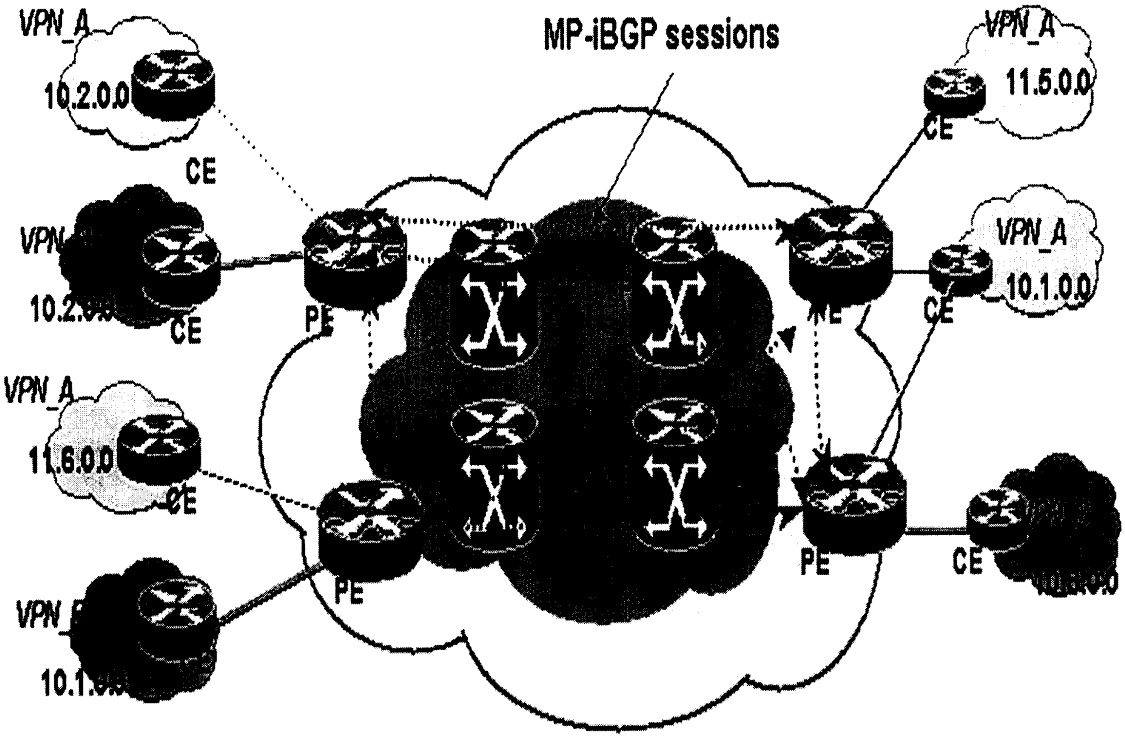
使用MPLS VPNs具有許多以PVC為基礎模組的優勢。顧客可以自行選擇他們的定址方式，而不一定會與其他客戶或服務供應商重覆。每一個客戶可以確保資料除了在客戶的VPN網站中傳送外，不會傳送到任何其他地方，因此資料通常不太需要加密，這一點和許多資訊傳輸方式不同。不過，不同於PVC模組，MPLS VPNs模組是可以隨著節點和客戶的增加來進行擴充的。MPLS同時也支援VPN網路上「any-to-any」的通訊模式，而毋需在網路服務供應商的網路上加裝固接虛擬電路(PVC)或是交換式虛擬電路(SVC)。對每一個MPLS的VPN的客戶來說，供應商的網路可以說提供了一個私人IP骨幹，讓客戶可以存取到自身企業中的其他節點，但不是任何其他客戶的節點。

就客戶的觀點而言，MPLS VPN模組的主要優勢是在許多的情況下，此起PVC模式路由(routing)部份則大幅地簡化。MPLS VPN的客戶一般可以使用服務供應商的骨幹作為公司所有節點的預設路徑，而毋需透過由許多PVC組成的複雜拓撲虛擬骨幹來管理路由器。

MPLS VPN同時也可以藉由彈性的管理政策來建置Extranet。舉例來說，A公司可能想要讓B公司連結到其某個主機，它可以利用傳送一個路徑至B公司的那個主機來完成，而A公司的其他網路仍然限制開放給B公司。

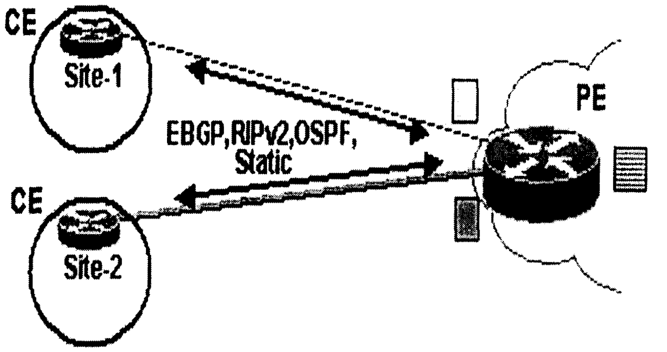
3.3.2 MPLS VPN Connection

(1)



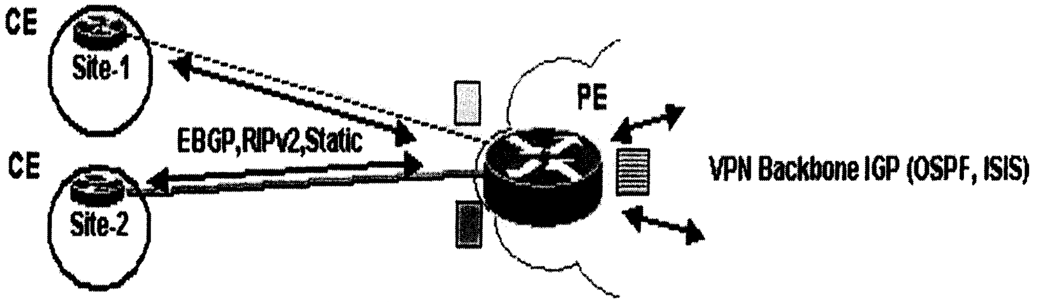
- The VPN backbone is composed by MPLS LSRs:
  - PE routers (edge LSRs). P routers (core LSRs).
- PE routers are faced to CE routers and distribute VPN information through MP-BGP to other PE routers:
  - VPN-IPv4 addresses, Extended Community, Label
- P routers do not run BGP and do not have any VPN knowledge.
- P路由器(LSRs) 為MPLS網路之核心路由器.
- PE路由器以MPLS方式與核心路由器(P)銜接, 同時以一般簡單 的IP 方式連接客戶路由器(CE).
- P and PE 路由器以(IGP如OSPF,IS-IS)路由協定共享相同之網路路徑訊息.
- PE路由器之間以MP-iBGP 方式fully meshed.

2)



- PE and CE routers exchange routing information through: EBGP, RIPv2, OSPF, Static routing
- CE router run standard routing software

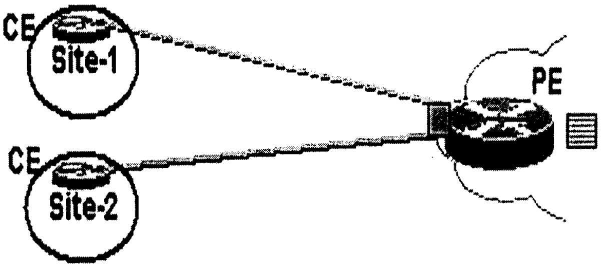
3)



PE routers maintain separate routing tables:

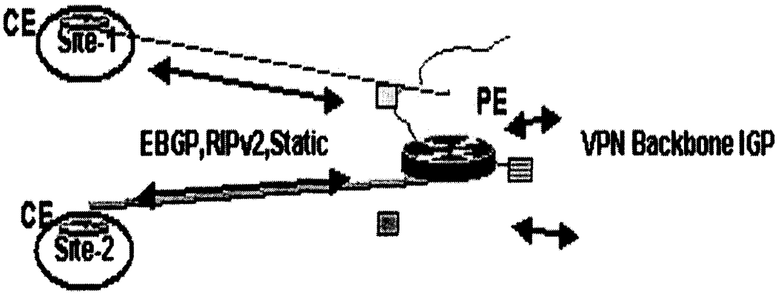
- The global routing table: With all PE and P routes. Populated by the VPN backbone IGP (ISIS or OSPF) .
- VRF (VPN Routing and Forwarding):
  - Routing and Forwarding table associated with one or more directly connected sites (CEs).
  - VRF are associated to (sub/virtual/tunnel)interfaces.
  - Interfaces may share the same VRF if the connected sites may share the same routing information.

(4)



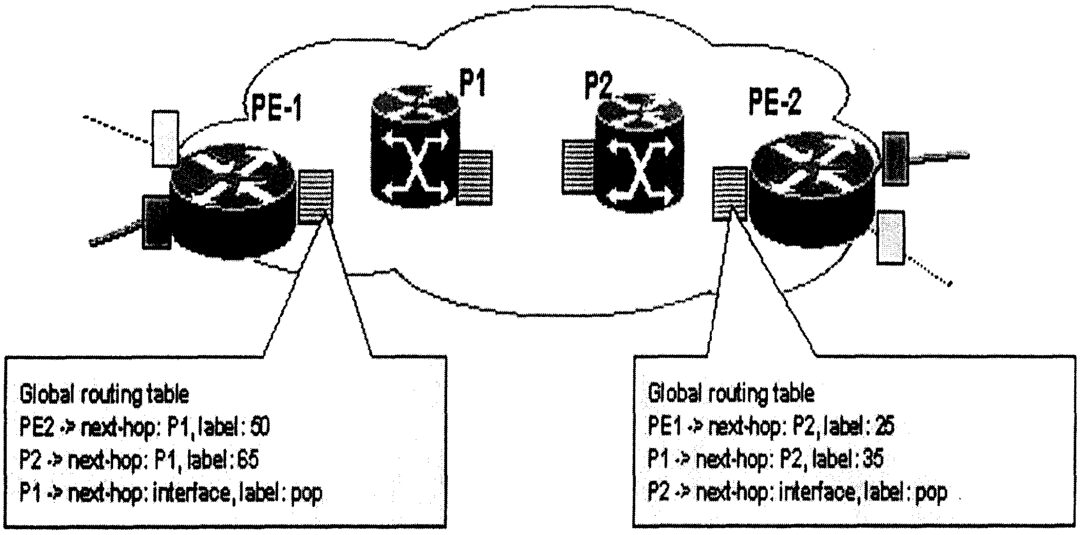
- Different site sharing the same routing information, may share the same VRF.
- Interfaces connecting these sites will use the same VRF.
- Sites belonging to the same VPN *may* share same VRF.

(5)



- The routes the PE receives from CE routers are installed in the appropriate VRF.
- The routes the PE receives through the backbone IGP are installed in the global routing table.
- By using separate VRFs, addresses need NOT to be unique among VPNs.

(6) IGP and label distribution in the backbone



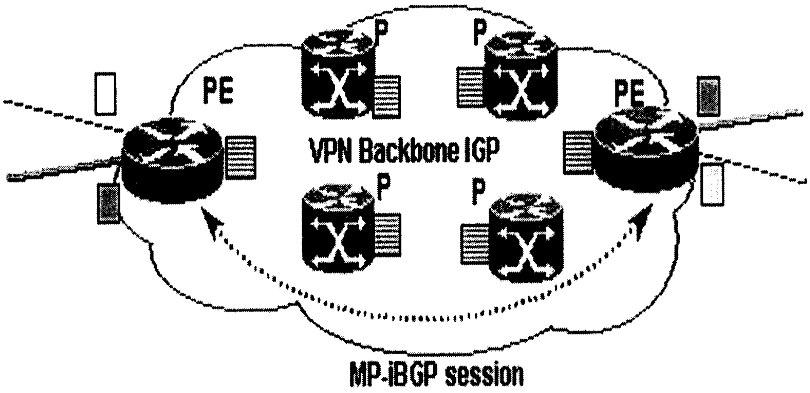
Global routing table
PE2 -> next-hop: P1, label: 50
P2 -> next-hop: P1, label: 65
P1 -> next-hop: interface, label: pop

Global routing table
PE1 -> next-hop: P2, label: 25
P1 -> next-hop: P2, label: 35
P2 -> next-hop: interface, label: pop

- All routers (P and PE) run an IGP and label distribution protocol
- Each P and PE router has routes for the backbone nodes and a label is associated to each route
- MPLS forwarding is used within the core

(7)

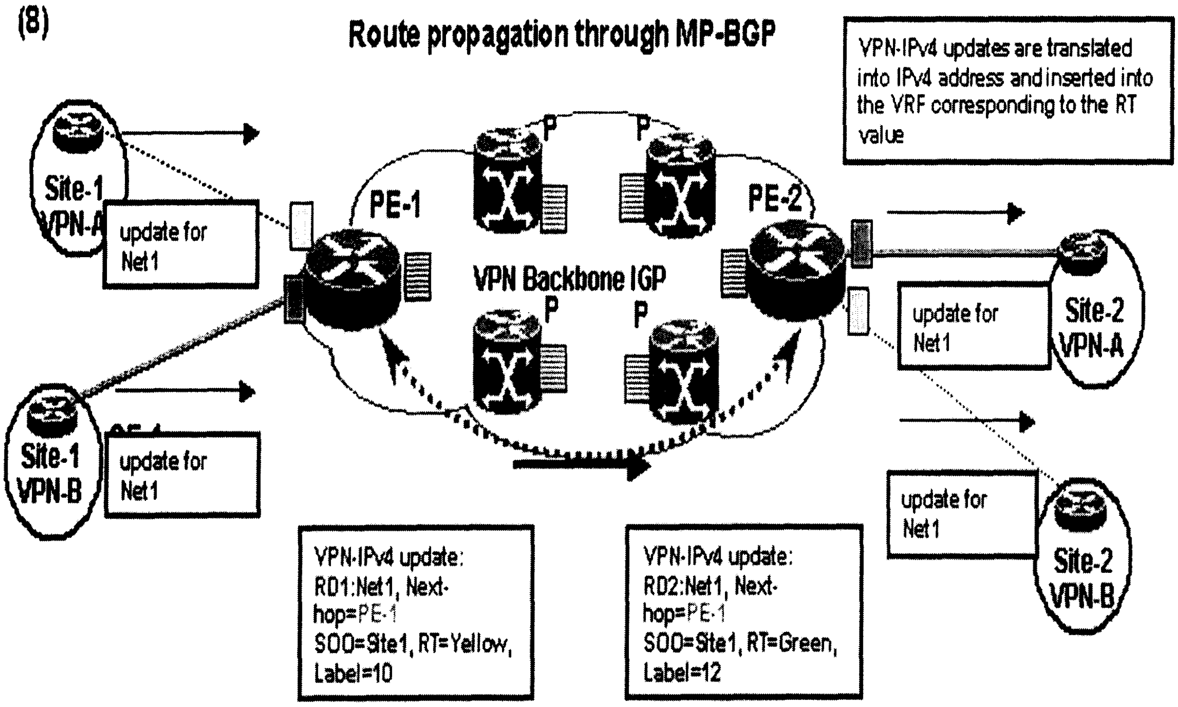
Addresses overlap



- Multiple routing tables (VRFs) are used on Pes. Each VRF contain customer routes. Custome addresses can overlap. VPNs are isolated
- MP-BGP is used to propagate these addresses between PE routers.
- VPN services allow customer to use the same address space, Address overlap, isolate customer VPNs.
- MPLS-VPN backbone MUST distinguish between customer addresses, Forward packets to the correct destination.
- BGP always propagate ONE route per destination. What if two customers are using the same address ?BGP will propagate only one route - PROBLEM !!! Therefore MP-BGP will *distinguish* between customer addresses.
- When routes are received (through MP-BGP) by remote PE routers, What is the routing table (VRF) the route has to be put in ? When packets have to be sent to destinations using the same address, How the PE will route packets with identical destination addresses ?

(8)

Route propagation through MP-BGP



VPN-IPv4 updates are translated into IPv4 address and inserted into the VRF corresponding to the RT value

VPN-IPv4 update:
RD1:Net1, Next-hop=PE-1
SOO=Site1, RT=Yellow, Label=10

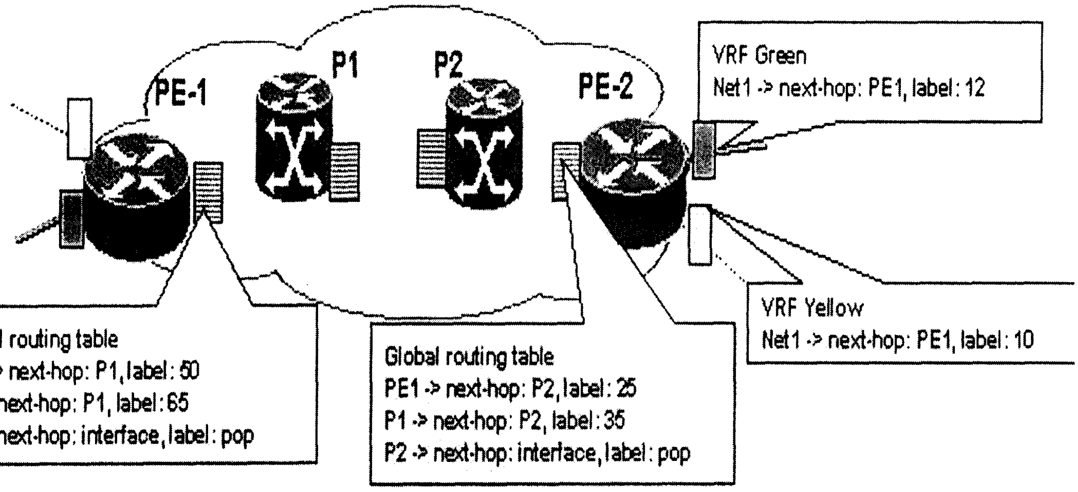
VPN-IPv4 update:
RD2:Net1, Next-hop=PE-1
SOO=Site1, RT=Green, Label=12

- MP-BGP assign a RD to each route in order to make them unique,In order to propagate them all. MP-BGP assign a Route-Target in order for remote PEs to insert such route to the corresponding routing table (VRF). Route-Target is the colour of the route.
- When a PE router receives a MP-BGP route it does: Check the route-target value. If such value is equal to the one intended to be used in a particular routing table the route is inserted into it. The label associated with the route is stored and used to send packets towards the destination .

- VPN-IPV4 address:
  - Route Distinguisher
    - 64 bits. Makes the IPv4 route globally unique . RD is configured in the PE for each VRF. RD may or may not be related to a site or a VPN
  - IPv4 address (32bits)
- Extended Community attribute (64 bits):
  - Site of Origin (SOO): identifies the originating site.
  - Route-target (RT): identifies the set of sites the route has to be advertised to .
- Any other standard BGP attribute
  - Local Preference、MED 、 Next-hop 、 AS_PATH 、 Standard Community ...
- A Label identifying:
  - The outgoing interface. The VRF where a lookup has to be done (aggregate label). The BGP label will be the second label in the label stack of packets travelling in the core.
- The Extended Community is used to:
  - Identify one or more routers where the route has been originated (site): Site of Origin (SOO)
  - Selects sites which should receive the route: Route-Target

3.3.3 MPLS VPN forwarding

(1)



VRF Green
Net1 -> next-hop: PE1, label: 12

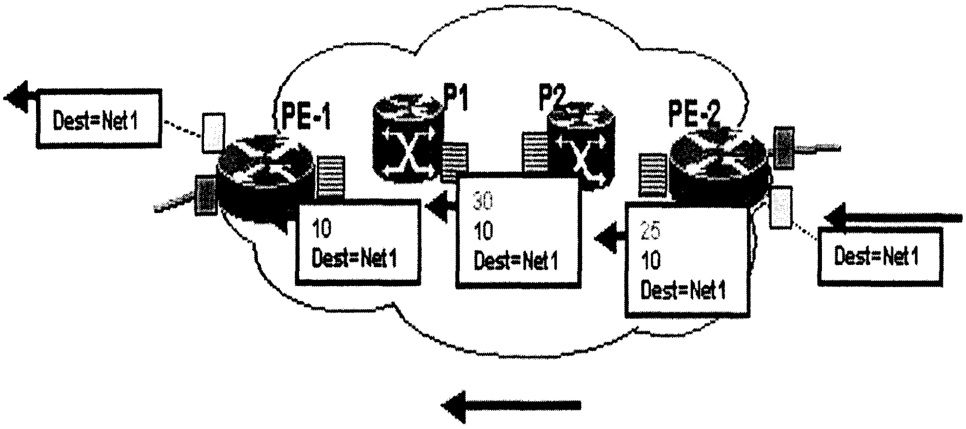
Global routing table
PE2 -> next-hop: P1, label: 50
P2 -> next-hop: P1, label: 65
P1 -> next-hop: interface, label: pop

Global routing table
PE1 -> next-hop: P2, label: 25
P1 -> next-hop: P2, label: 35
P2 -> next-hop: interface, label: pop

VRF Yellow
Net1 -> next-hop: PE1, label: 10

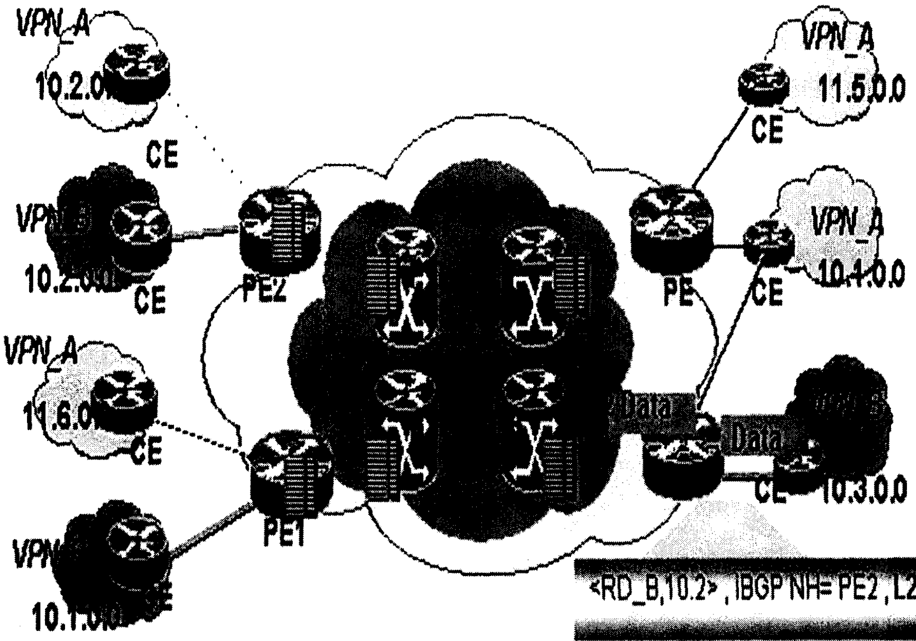
- PE routers store two kind of labels in their LFIB
  - Labels learned through the LDP protocol and assigned to IGP routes.
  - Labels learned through MP-BGP and assigned to VPN routes.
- In the global tables, PE routers store IGP routes and associated labels
  - Label distributed through LDP/TDP
- In the VRFs, PE routers store VPN routes and associated labels
  - Labels distributed through MP-BGP

(2)



- In the global tables, PE routers store IGP routes and associated labels:
  - Label distributed through LDP.
- In the VRFs, PE routers store VPN routes and associated labels:
  - Labels distributed through MP-BGP.

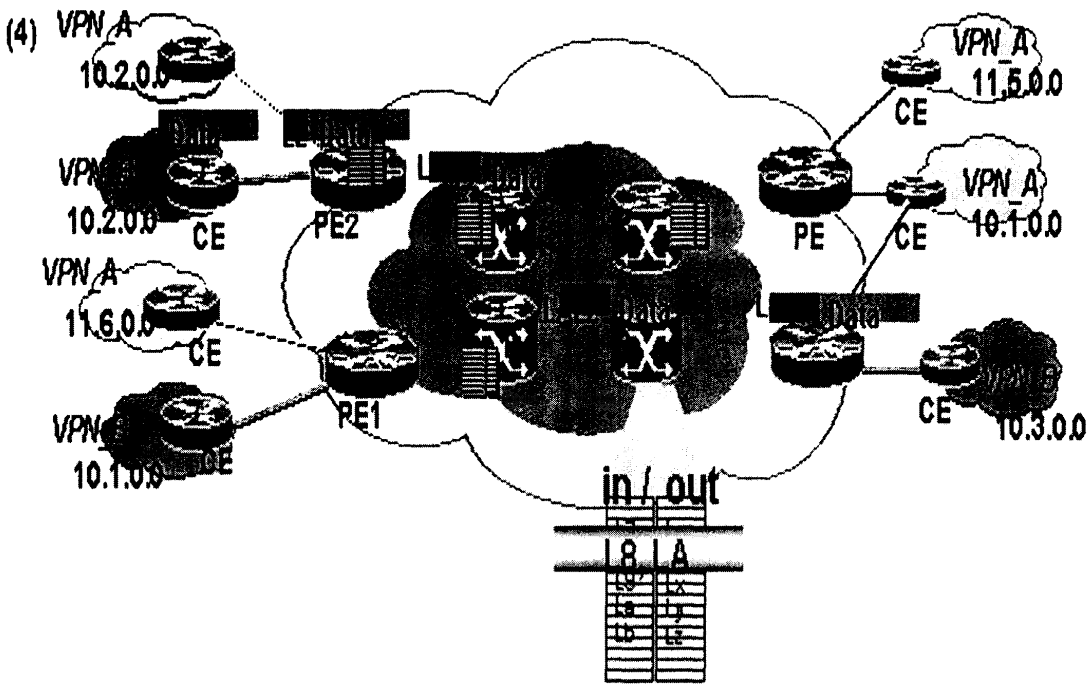
(3)



<RD_B,10.2> , IBGP NH= PE2 , L2 L8

<RD_B,10.1> , iBGP next hop PE1	L1	L7
<RD_B,10.2> , iBGP next hop PE2	L2	L8
<RD_B,10.3> , iBGP next hop PE3	L3	L9
<RD_A,11.6> , iBGP next hop PE1	L4	L7
<RD_A,10.1> , iBGP next hop PE4	L5	L8
<RD_A,10.4> , iBGP next hop PE4	L6	L8
<RD_A,10.2> , iBGP next hop PE2	L7	L8

- Ingress PE receives normal IP Packets from CE router
- PE router does "IP Longest Match" from VRF , find iBGP next hop PE2 and impose a stack of labels:
  exterior Label **L2** + Interior Label **L8**



- All Subsequent P routers do switch the packet . Solely on Interior Label.
- Egress PE router, removes Interior Label. Egress PE uses Exterior Label to select which VPN/CE to forward the packet to. Exterior Label is removed and packet routed to CE router.
- MPLS-VPN uses TWO labels for each packet going to a VPN destination
- The top label is the LDP one: Derived from an IGP route, Corresponding to a PE address (exit point of a VPN route), PE addresses are MP-BGP next-hops of VPN routes
- The second label is the MP-BGP label: It corresponds to the VPN route and identify the outgoing interface or routing table to be used in order to reach the VPN destination
- The MP-BGP label allow to use duplicate (overlap) addresses between VPNs
- Forwarding from the PE to the CE router is done based on the label value. Not the IP address which can be identical for different VPNs
- Overlapping address and traffic isolation between VPNs is done through MPLS forwarding
- MPLS nodes forward packets based on the top label
- P routers do not have BGP (nor VPN) knowledge, no VPN routing information, and no Internet routing information

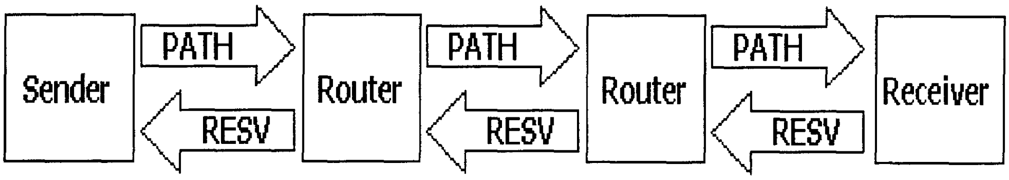
第四章 RSVP – Traffic Engineering

5.1 RSVP基本概念

- Generic RSVP - Internet standard for reserving resources
- Generic RSVP uses a message exchange to "reserve" resources across a network for IP flows
- A generic QoS signaling protocol
- An Internet control protocol
  - Uses IP as its network layer
- Originally designed for host-to-host
- Uses the IGP to determine paths
- RSVP is not
  - A data transport protocol
  - A routing protocol
- RFC 2205

5.1.1Basic RSVP Path Signaling:

- Simplex flows
- Ingress router initiates connection
- "Soft" state
  - Path and resources are maintained dynamically
  - Can change during the life of the RSVP session
- Path message sent downstream
- Resv message sent upstream



•Other RSVP Message Types:

♦PathTear

◈Sent to egress router

♦ResvTear

◈Sent to ingress router

♦PathErr

◈Sent to ingress router

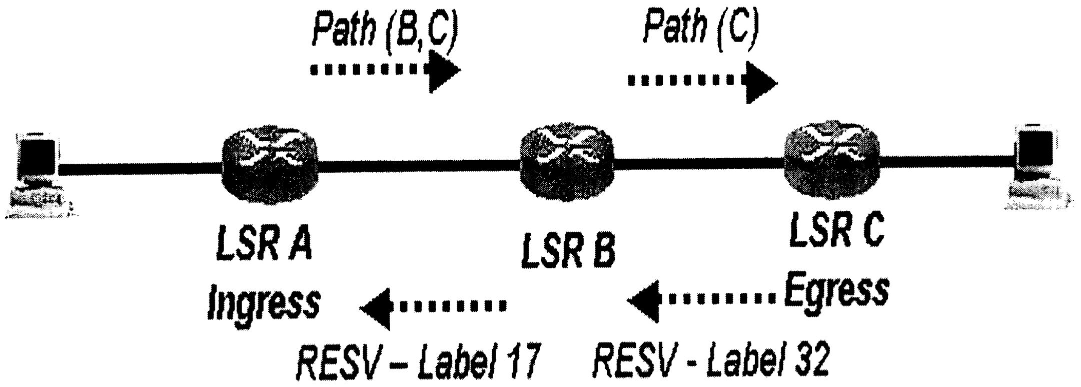
♦ResvErr

◈Sent to egress router

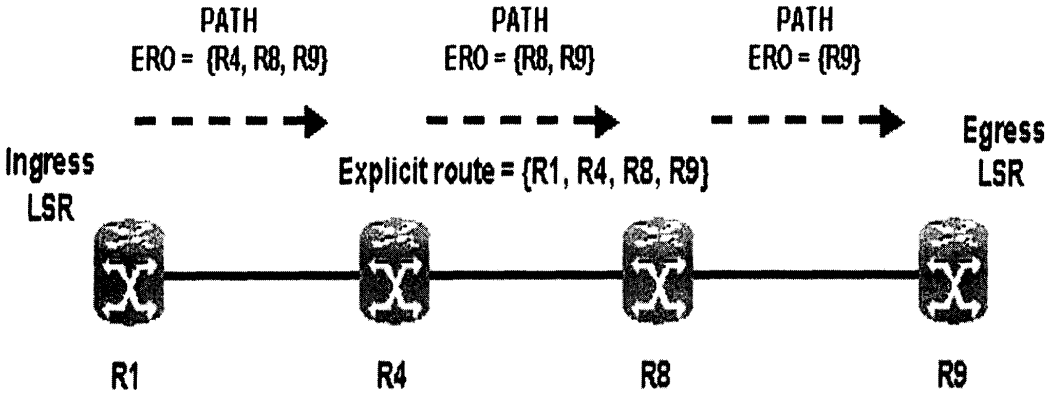
♦ResvConf

5.2 RSVP –TE (RSVP with Traffic Engineering Extensions)概念

- RSVP-TE uses IP Datagrams (UDP at the edge) between LSR peers to send messages
  - –No TCP session maintenance
- RSVP-TE- a mechanism for establishing explicitly routed LSPs
  - –An Explicit Route is a Constrained Route
- Extensions added to support establishment and maintenance of LSPs
  - –Maintained via "hello" protocol
- Used now for router-to-router connectivity
- Includes the distribution of MPLS labels



- Ingress LSR initiates connection
- 'Soft' state
  - Path and resources are maintained dynamically
- Path messages sent downstream
- Resv messages sent upstream
- Ingress LSR consults TED to determine path
- RSVP –TE support downstream-on-demand label allocation *only*
- LSR does Connection Admission Control (CAC)
- Each LSR process the RESV using received label for outgoing traffic associated with this LSP
- RESV allocates resources at each LSR
- When ingress LSR receives the RESV the LSP is established



- Establish state and request label assignment
- R1 transmits a PATH message addressed to R9
  - Label Request Object
  - ERO = {strict R4, strict R8, strict R9}
  - RRO = {ingress LSR IP add, store and add IP hop addr}
  - Session Attributes: Priority, preemption, and fast reroute
  - Flow_Spec: Request bandwidth reservation

5.3 RSVP –TE Message Objects

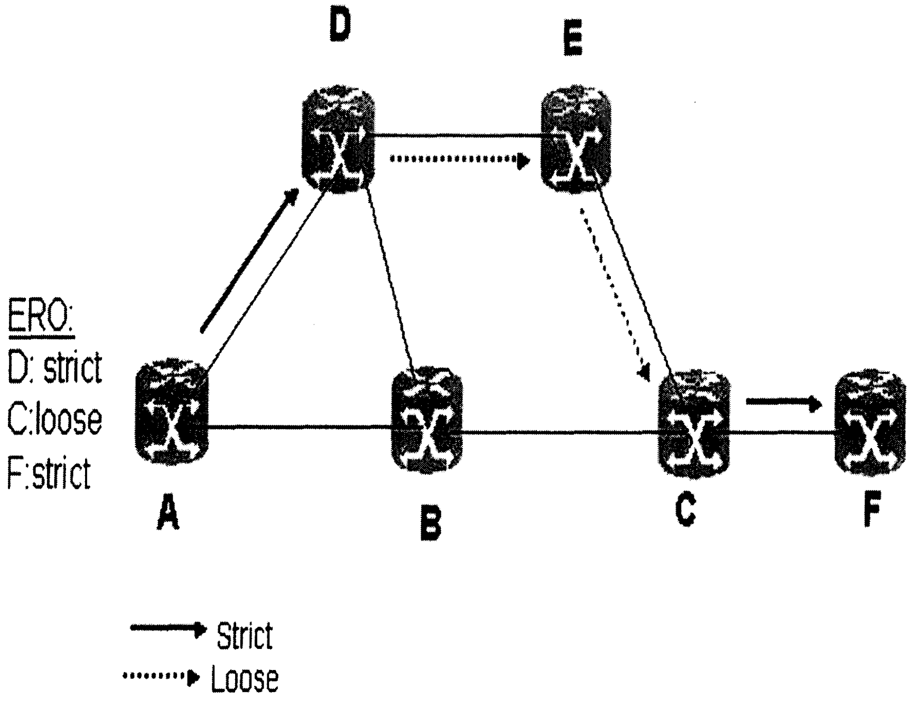
- **MPLS Extensions to RSVP**
  - Path and Resv message objects
    - Explicit Route Object (ERO)
    - Label Request Object
    - Label Object
    - Record Route Object(RRO)
    - Session Attribute Object
    - Tspec Object
  - For more detail on contents of objects:
    daft-ietf-mpls-rsvp-lsp-tunnel-04.txt
    Extensions to RSVP for LSP Tunnels

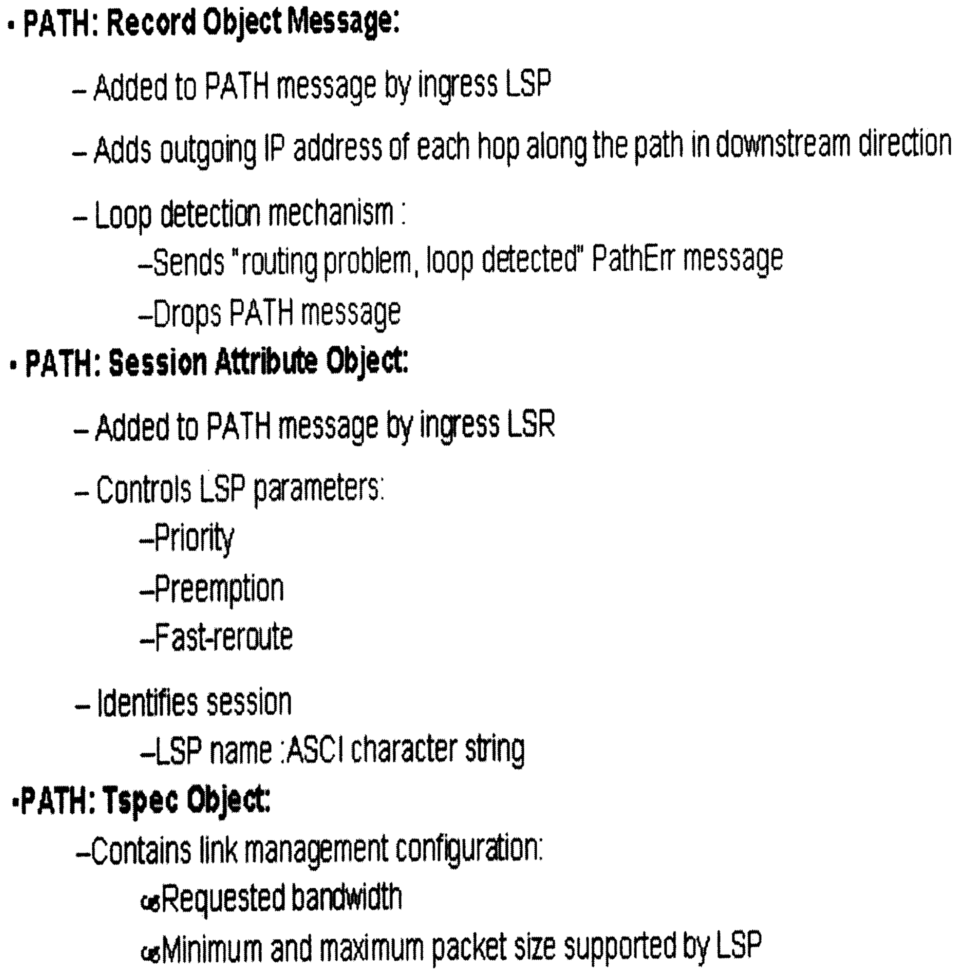
- **PATH/RESV: Label Objects:**
  –Label Request Object
    –Added to Path message at ingress LSR
    –Request that each LSR provide label to upstream LSR
  –Label Object
    –Carried in RESV message along retum path upstream
    –Provides label to upstream LSR

5.3.1 RSVP-TE PATH Message Objects

- **PATH: Explicit Route Object (ERO)**
  - Used to specify the route RSVP Path message to take
  - Can specify 'loose' or 'strict' route
    - – Loose – relies on routing table to find route to next specified LSR
    - – Strict – next LSR hop is directly connected
  - A route can have both loose and strict components

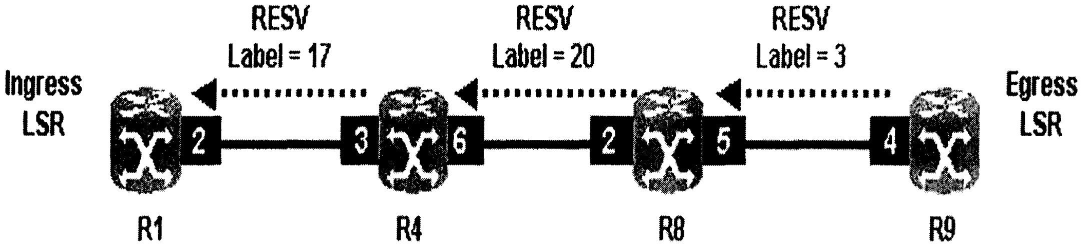
•ERO: Strict/Loose Path Mixed:





- **PATH: Record Object Message:**
  - –Added to PATH message by ingress LSP
  - –Adds outgoing IP address of each hop along the path in downstream direction
  - –Loop detection mechanism :
    - –Sends "routing problem, loop detected" PathErr message
    - –Drops PATH message
- **PATH: Session Attribute Object:**
  - –Added to PATH message by ingress LSR
  - –Controls LSP parameters:
    - –Priority
    - –Preemption
    - –Fast-reroute
  - –Identifies session
    - –LSP name :ASCI character string
- **PATH: Tspec Object:**
  - –Contains link management configuration:
    - ❧Requested bandwidth
    - ❧Minimum and maximum packet size supported by LSP

5.3.2 RSVP-TE RESV Message Objects



Ingress Routing Table

In	Out
IP Route	(2, 17)

MPLS Table

In	Out
(3, 17)	(6, 20)

MPLS Table

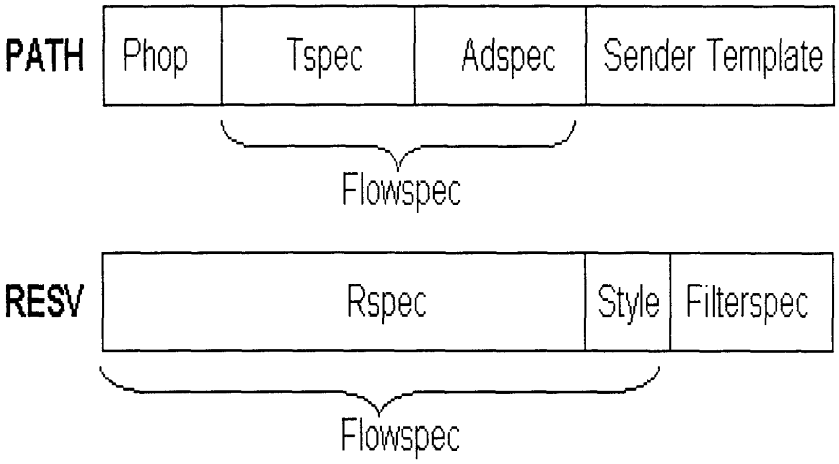
In	Out
(2, 20)	(5, 3)

- Distribute labels & reserve resource
- R9 transmits a RESV message to R8
  - Label = 3
  - Session object to uniquely identify the LSP
- R8 and R4
  - Stores "outbound" label, allocate an "inbound" label
  - Transmits RESV with inbound label to upstream LSR
  - R1 binds label to FEC

- **RESV:Record Object Message**

- Added to RESV message by egress LSR
- Adds outgoing IP address of each hop in path in upstream direction
- Loop detection mechanism
  - Sends 'routing problem, loop detected' ResvErr message
  - Drops RESV message

RSVP: TE Flow Descriptors



PATH | Phop | Tspec | Adspec | Sender Template

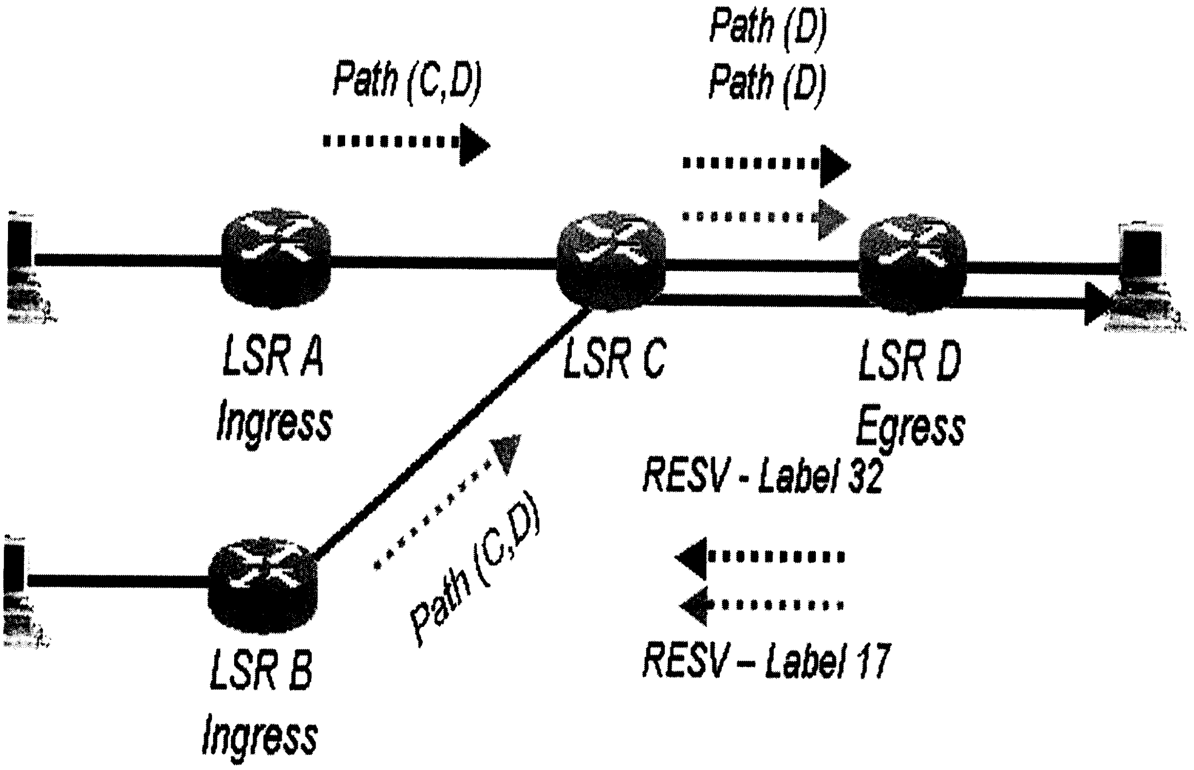
Flowspec

RESV | Rspec | Style | Filterspec

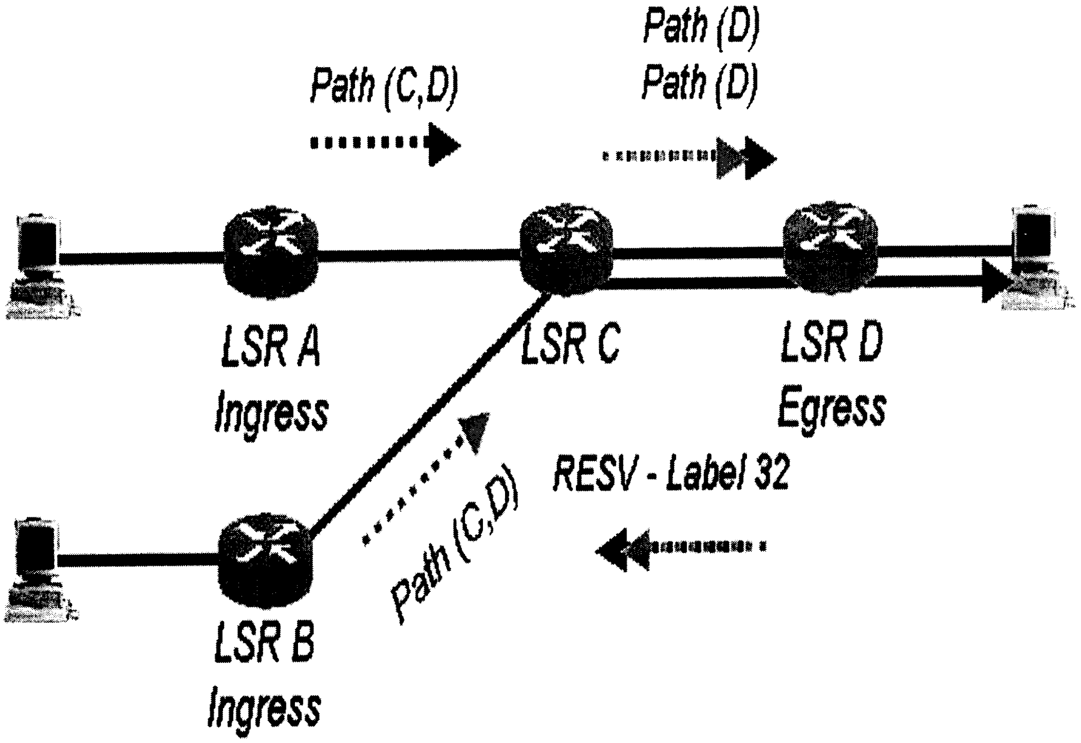
Flowspec

- Part of RESV that defines the merging capabilities of the flow
- *Wildcard-Filter (WF) style* creates a single reservation for all flows from upstream senders
- *Fixed-Filter (FF) style* – creates a distinct reservation for selected senders
- *Shared Explicit (SE) style* – creates a shared reservation for selected senders

- **Fixed Filter Style:**

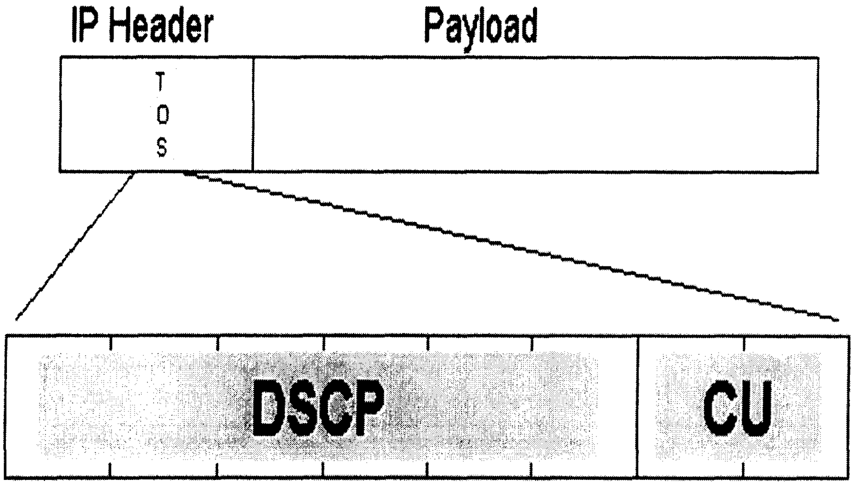


•Shared Explicit Style:



第五章 Differentiated Service

5.1 The IETF Differentiated Services

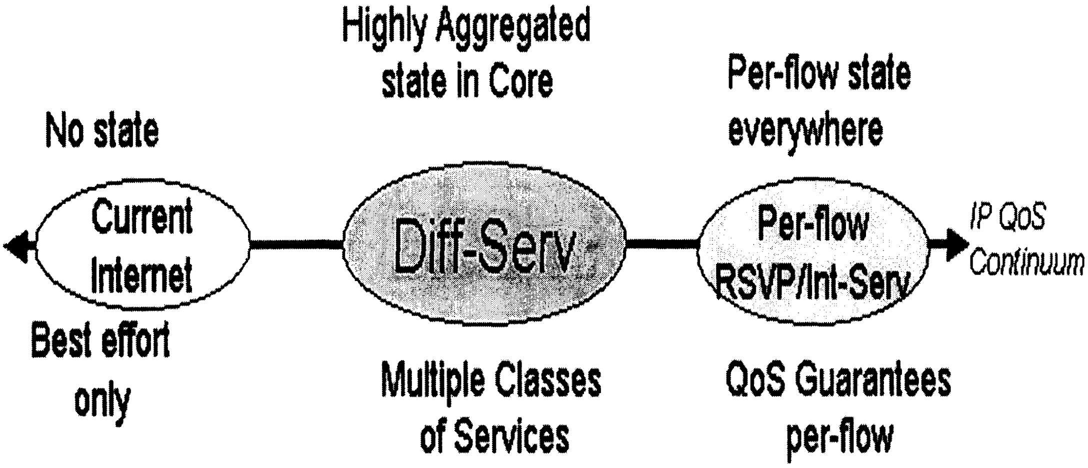


- DSCP : Differentiated Service Code Point = 6 bits
- DSCP encodes which treatment the packet should received
- in TOS Field for IPv4 (rfc 791) and Traffic Class octet for IPv6
  --> DS field in Header of every IPv4 and IPv6 packet
  --> supersedes TOS, DTR,..
- CU: Currently Unused = 2 bits (lined up for ECN)
- PHB= Per Hop Behavior
  The Diff-Serv treatment (scheduling/dropping) applied by a Router to all the packets which are to experience the same Diff-Serv service
- DSCP=Differentiated Services Code Point
  The value in the IP Header indicating which PHB is to be applied to the packet

•BA= Behavior Aggregate
The set of all the packets which have the same DSCP (and thus that will receive the same PHB)

•OA= Ordered Aggregate
The set of BAs which have an ordering constraint ("must go into the same queue")

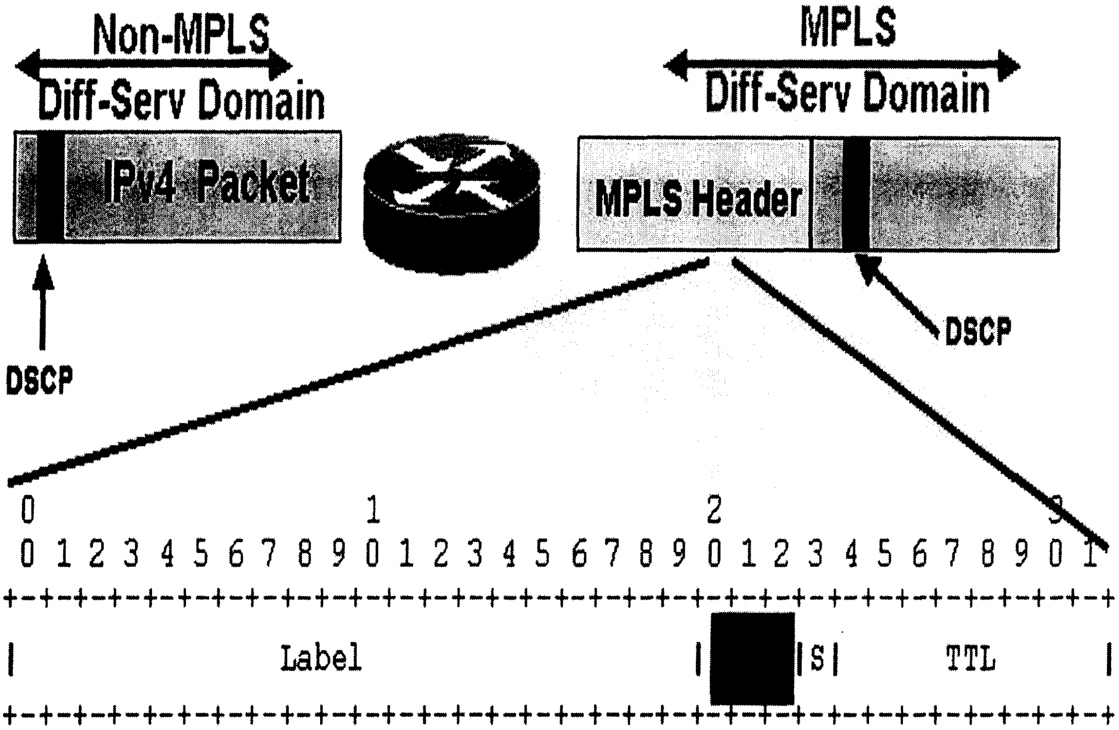
•PSC= PHB Scheduling Class
The set of PHBs applied to an OA (the set of PHBs using the same queue")



IP QoS Model which offers service differentiation and remains highly scalable. Diff-Serv scalability comes from aggregation of traffic on edge and processing of Aggregate only in Core. Aggregation on edge, then many flows associated with a Class (marked with DSCP). Aggregated Processing in Core,then Scheduling/Dropping (PHB) based on DSCP.

5.2 Diff-Serv over MPLS

Because MPLS is there primarily to transport IP, MPLS's primary QoS goal is to support existing IP QoS Models.Because MPLS is there to support very large scale operations, MPLS's primary IP QoS Model to support is Diff-Serv. IETF Progress on Diff-Serv over MPLS <draft-ietf-mpls-diff-ext-03.txt>, MPLS Support of Differentiated Services, Feb 2000, Le Faucheur et al.



```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Label                  |     |S|       TTL     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

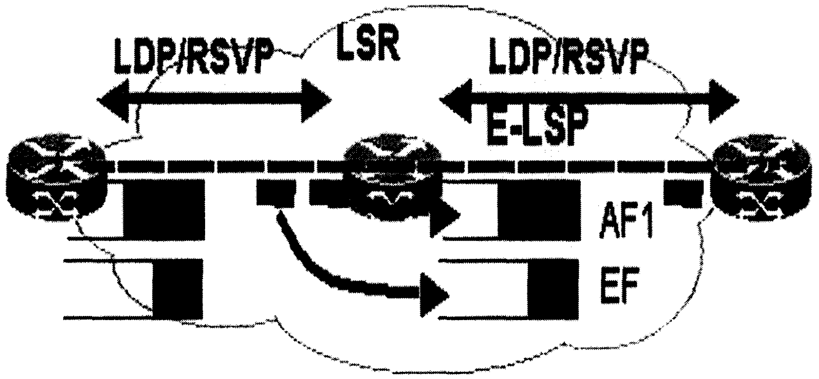
- DSCP field is not directly visible to MPLS Label Switch Routers (they forward based on MPLS Header) --> information on Diff-Serv must be made visible to LSR in MPLS Header (using EXP field and label)

- Diff-Serv IP Routers make their forwarding decision independently of packet's BA:
  - – Forwarding decision (next hop/egress interface selection) is based only on Destination IP Address
  - – Scheduling decision (on egress interface) is based only on DSCP
- Diff-Serv MPLS Routers make a forwarding decision which may be dependent on packet's BA:
  - – Forwarding decision (egress label selection) may depend on packet's BA
- This describes how "Diff-Serv" information is conveyed to LSRs in MPLS Header
- Two methods:

  -E-LSP: "Queue" inferred from Label and EXP field. "drop priority" inferred from label and EXP field.

  -L-LSP: "Queue" inferred exclusively from Label. "drop priority" inferred from EXP field.

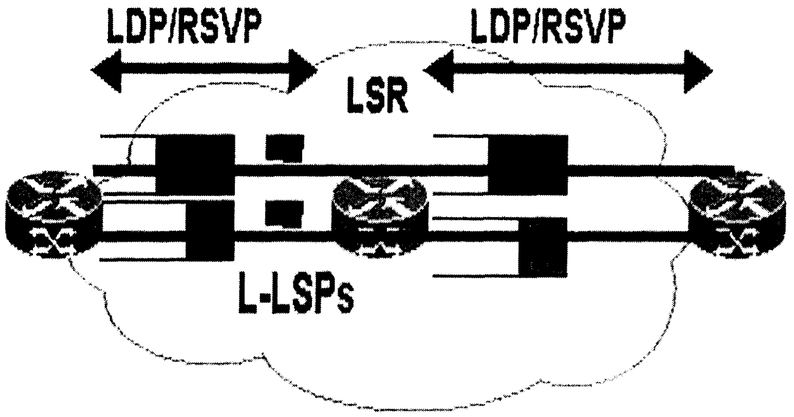
5.2.1 E-LSP Example



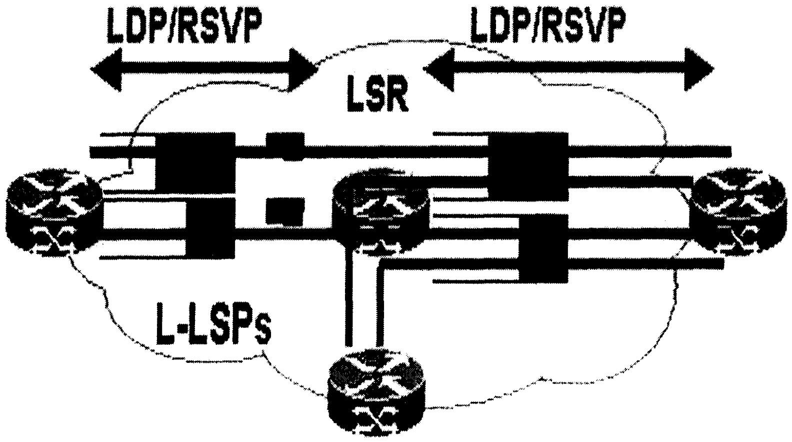
- E-LSPs can be established by various label binding protocols (LDP or RSVP)
- Example above illustrates support of EF and AF1 on single E-LSP

  -Note: EF and AF1 packets travel on single LSP (single label) but are enqueued in different queues (different EXP values)
- Queue is selected based on EXP (and possibly label)

5.2.2 L-LSP Example



- L-LSPs can be established by various label binding protocols (LDP or RSVP)
- Example above illustrates support of EF and AF1 on separate L-LSPs
  - EF and AF1 packets travel on separate LSPs and are enqueued in different queues (different label values)
- Queue is selected based on label



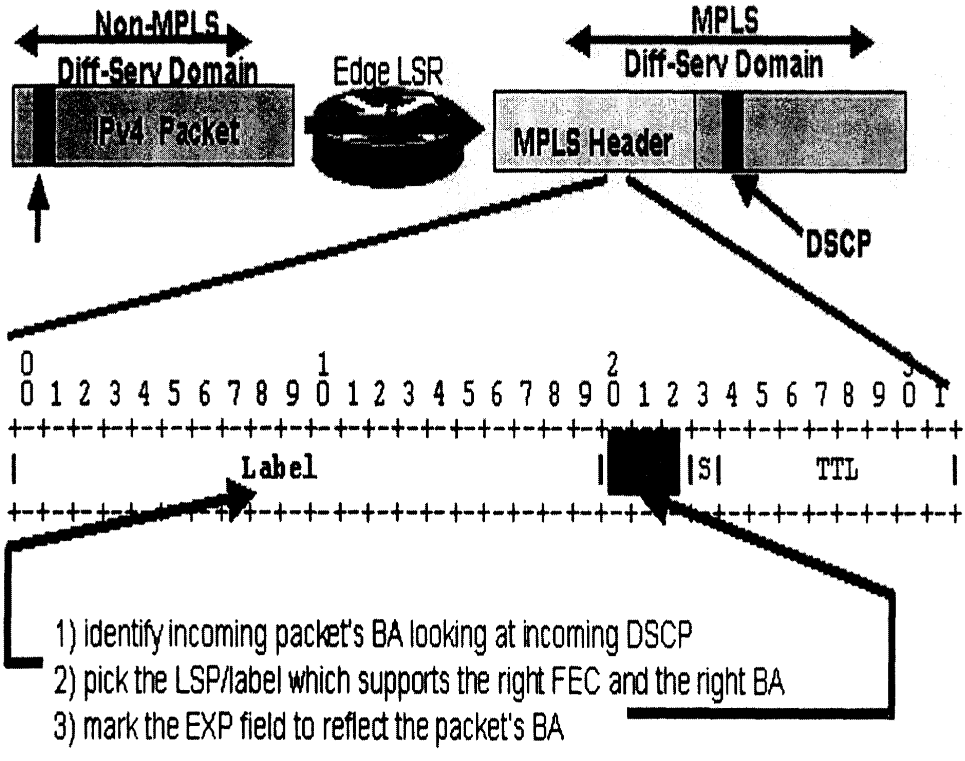
- E-LSPs and L-LSPs support IP Diff-Serv model:

--> the scheduling is as per Diff-Serv: at the granularity of the OA (ie all packets belonging to the same OA go into the same Diff-Serv queue

→ Diff-Serv over MPLS does not use per-label-queuing but rather retains Diff-Serv's scalable Aggregate queuing
(all packets of same OA go into single queue regardless of which LSP they use)

- Exact same PHB Mechanisms as IP Diff-Serv: Diff-Serv Queues with Diff-Serv drop profiles
- Only difference is packet classification
  - For IP Diff-Serv, packets classified by DSCP
  - For MPLS Diff-Serv, packets classified by label/EXP
- MPLS Diff-Serv is Un-distinguishable from IP DiffServ

•**Edge Diff-Serv LSR**



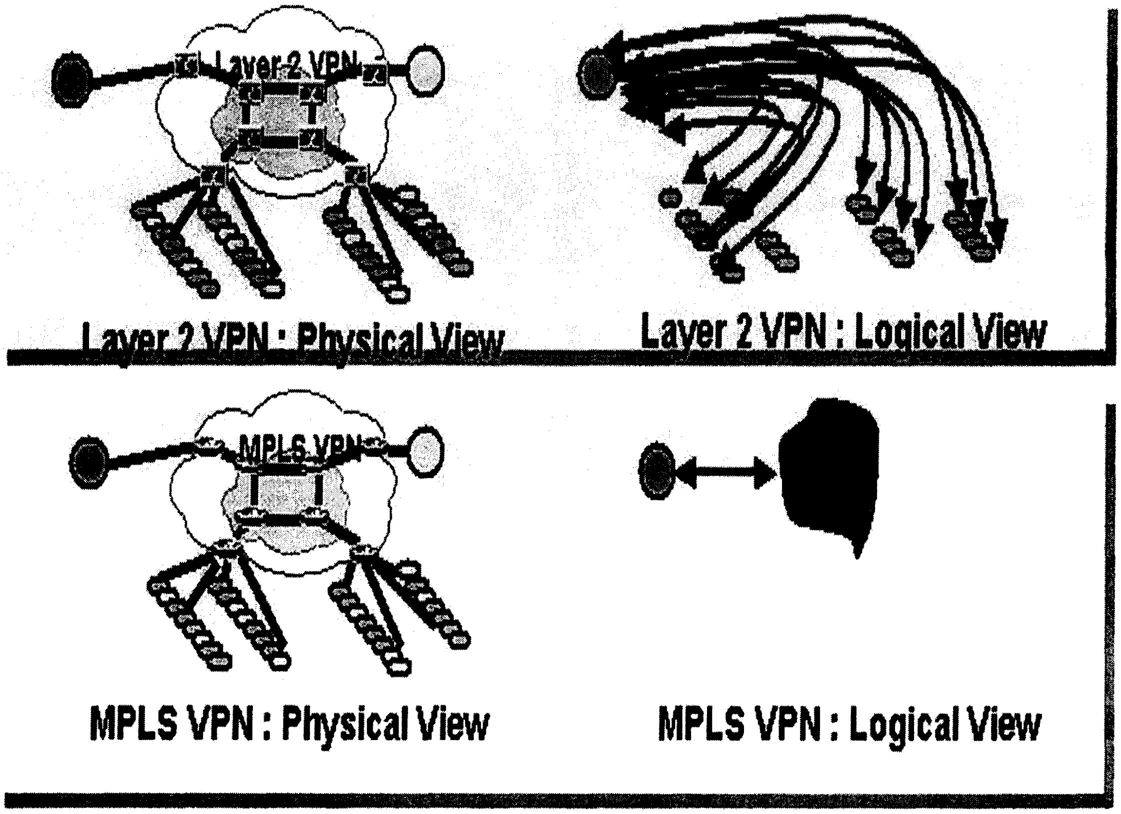
```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Label                  |     |S|      TTL      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

1) identify incoming packet's BA looking at incoming DSCP
2) pick the LSP/label which supports the right FEC and the right BA
3) mark the EXP field to reflect the packet's BA

- MPLS over PPP and LAN: both E-LSPs and L-LSPs are applicable
- MPLS over ATM/FR: only L-LSPs possible (EXP is not seen by ATM LSR or FR LSR)
- E-LSPs can be set up with existing (non-DS-aware) signalling: LDP, RSVP etc. EXP -> PHB mapping is configured on every router as per Diffserv
- L-LSPs require signalling extension to bind "queue" to a label: New DIFFSERV object added to RSVP/LDP to signal the "queue" in which to enqueue the label. Meaning of EXP bits is well-known

5.3 QoS Model for MPLS VPN

5.3.1 How it feels for a CPE:Routing Viewpoint



Layer 2 VPN : Physical View

Layer 2 VPN : Logical View

MPLS VPN : Physical View

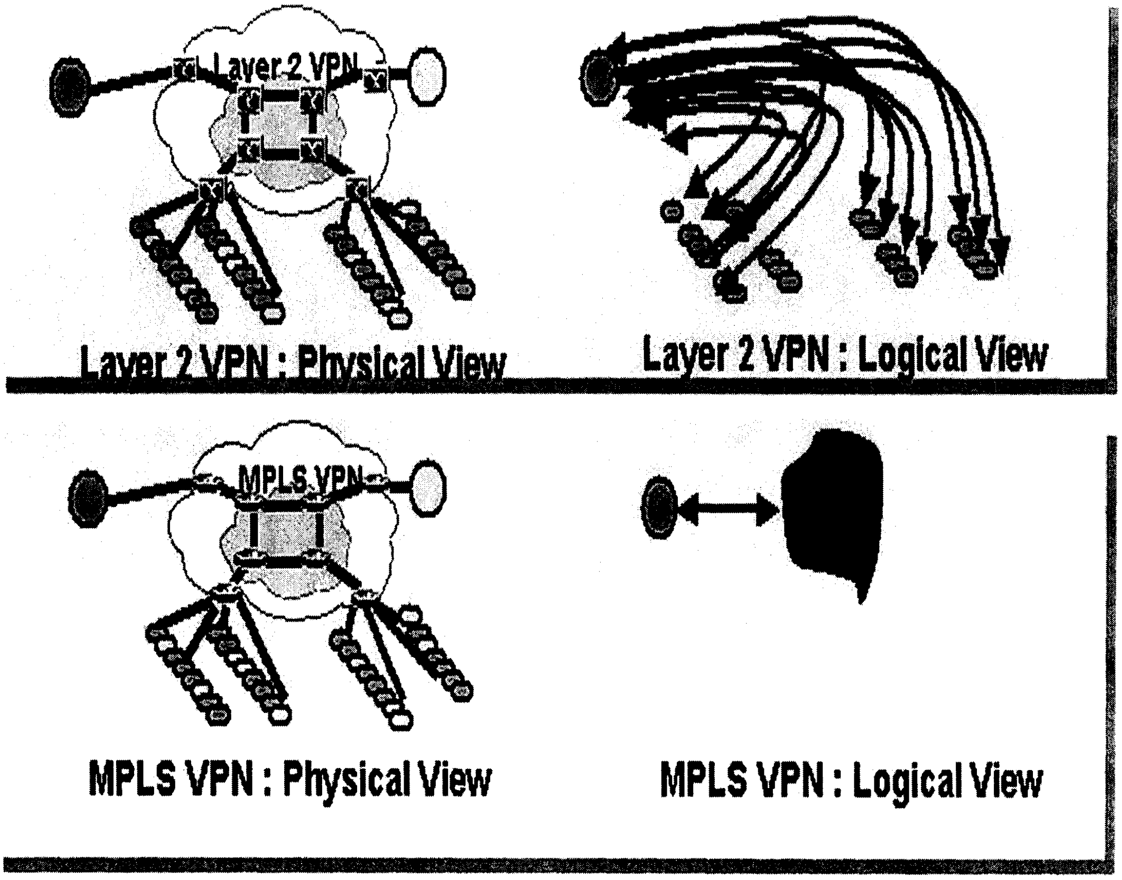
MPLS VPN : Logical View

Routing Adjacencies:

- Before MPLS VPN:
  Point-to-point to all remote sites
- With MPLS VPN:
  point-to-cloud

"Point-to-Cloud" is key to MPLS VPN benefits from Routing Viewpoint

5.3.2 How it feels for a CPE: Qos Viewpoint



Layer 2 VPN : Physical View

Layer 2 VPN : Logical View

MPLS VPN : Physical View

MPLS VPN : Logical View

QoS Commitment:

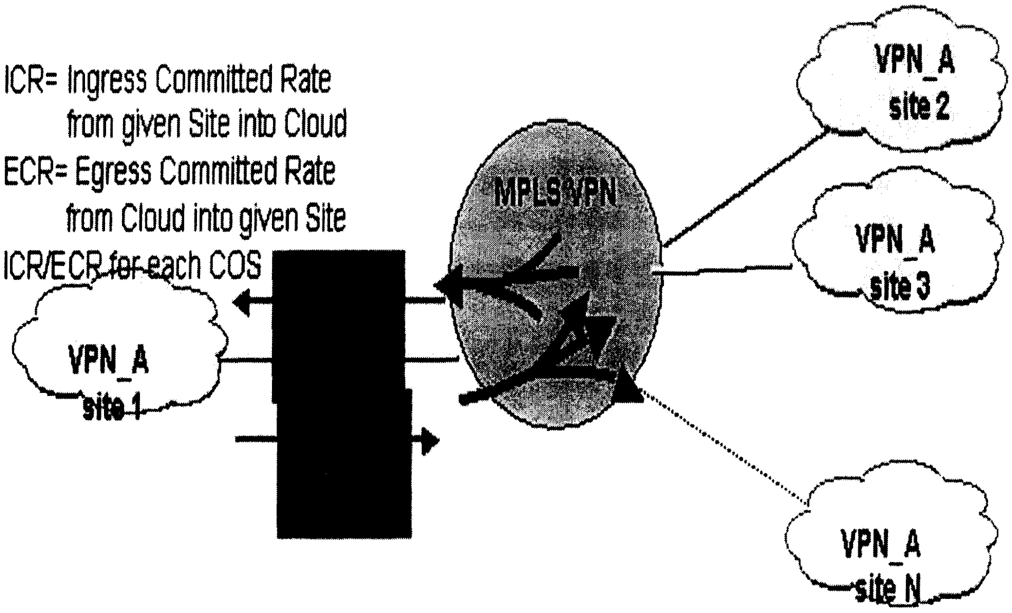
- Before MPLS VPN:
  point-to-point to all remote sites
- With MPLS VPN:
  point-to-cloud

"Point-to-Cloud" is in line with the Diff-Serv model

"Point-to-Cloud" is key to MPLS VPN benefits from QoS Viewpoint:

- scalability in SP Backbone
- simplicity for Customer

5.3.3 MPLS VPN QoS Service: *Point-to-Cloud" model*



ICR= Ingress Committed Rate from given Site into Cloud

ECR= Egress Committed Rate from Cloud into given Site

ICR/ECR for each COS

Proposed SLA for CoS C1

- As long as for each site S of VPN X:
  - S sends less than ICR
  - S receives less than ECR
- Then:
  - loss ratio is < 10^(-n1)
  - RTT is < m1 ms

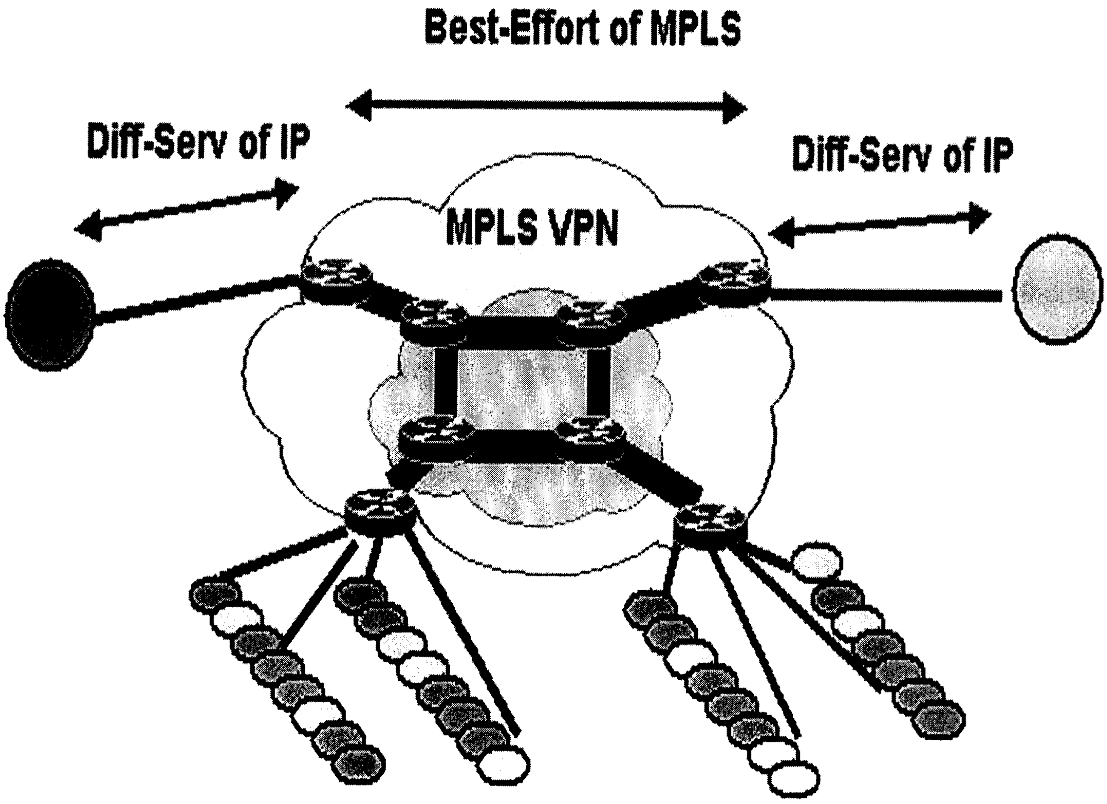
CoS X:	[nx, mx],	price Px
Gold:	[-10, 100ms],	$$$
Silver:	[-8, 200ms],	$$
BE:	[be, be],	$

Benefits:

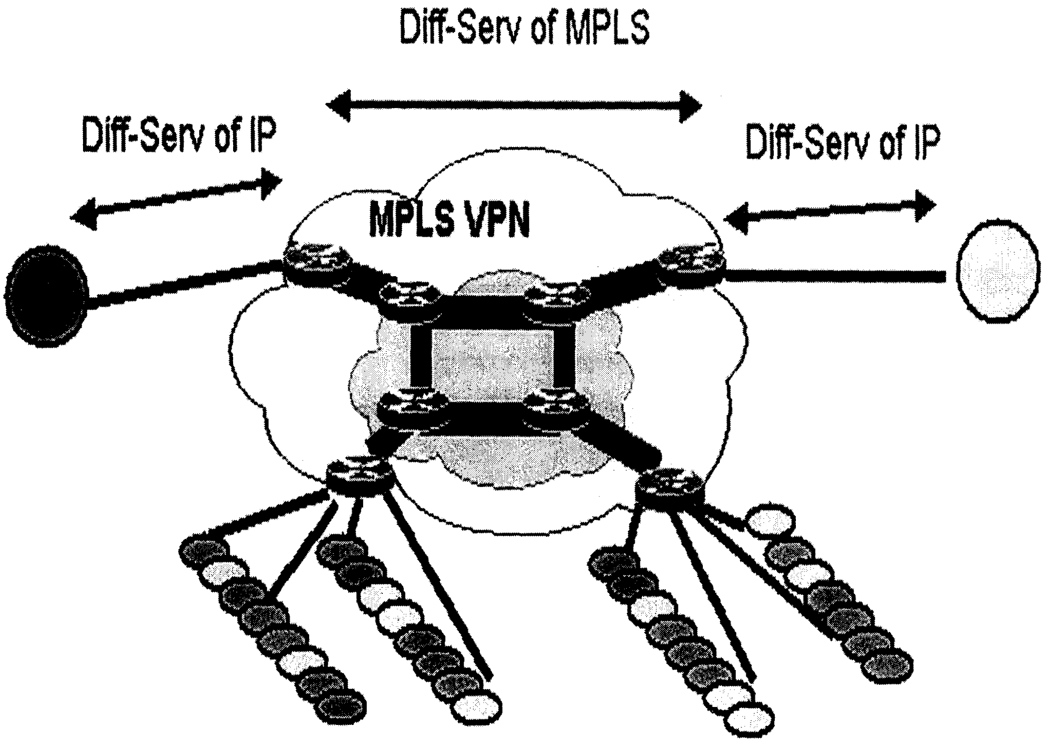
- Any to any connectivity ...
- ... without requiring the customer to know or specify its traffic matrix.
  Changes in traffic matrix accommodated by SP without change in the QoS contract
- Preserves MPLS VPN scalability
  (no "per- VPN-Site" awareness in SP backbone)
- Resource Allocation by SP is at very aggregate level (per COS):
  easier, higher statistical gain

5.3.3 How to Build "Point-to-Cloud" Service?

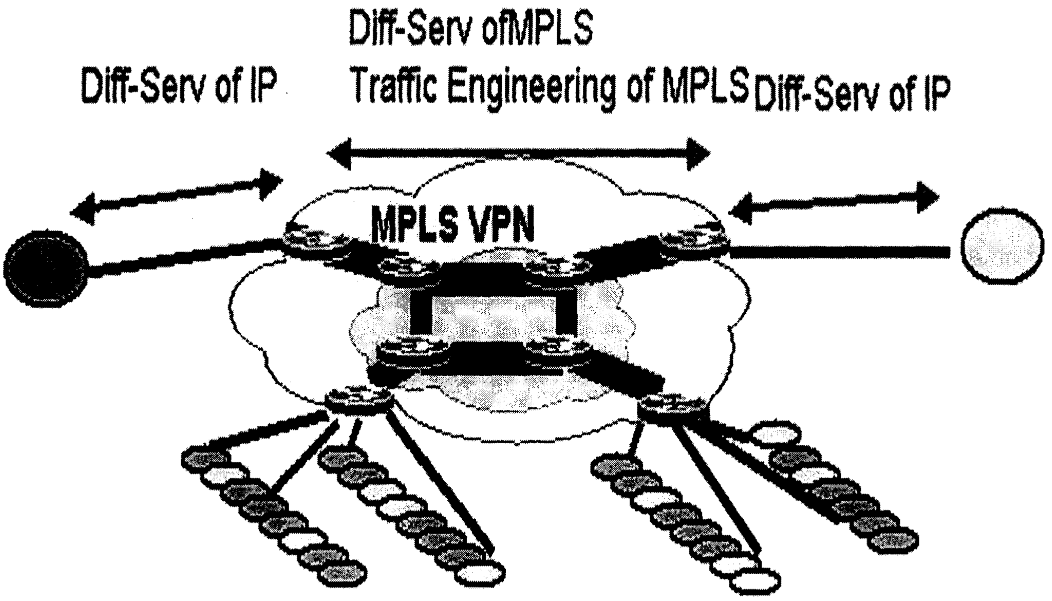
- Scenario 1:
  - Constrained access
  - Unconstrained Backbone



- Scenario 2:
  - Constrained access
  - Constrained Backbone (or requirement for tightest possible delay)



- Scenario 3:
  - Constrained access
  - Constrained Backbone (or requirement for tightest possible delay)
  - Requirement to maximise use of backbone resources



5.3.3 MPLS QoS - Conclusions

- MPLS QoS number one goal is to support Diff-Serv, the whole of Diff-Serv and nothing but Diff-Serv
- IETF is nearing standardisation of Diff-Serv over MPLS
- Diff-Serv over MPLS provides same service as
  Diff-Serv over IP
- Diff-Serv model easily applicable to MPLS VPN service to offer an attractive "point-to-cloud" QoS service

第六章 實習心得

由於網際網路的快速成長，IP網路之建置非常普遍。在IP公眾網路(Public Network)平台上,我們進一步思考是否也能提供專屬私有網路(Dedicated Private Network)之服務,提昇附加價值。而MPLS（多重協定標籤交換，Multiprotocol Label Switching）技術在VPN (虛擬私有網路)服務上提供了建置選擇之一, 其主要效益在於功能的提昇並提供商業IP VPN之服務 。

提供VPN服務的供應商常常必須為客戶提供某程度的QoS。MPLS VPN便利用Differentiated Service技術支援CoS，這些技術可以讓客戶的資料在進入服務供應商網路時，能夠根據各種管理政策--例如原始站址、應用型態等，來區分為不同的等級。在此網路中，資料流的等級是根據表頭位元與不同的標籤來辨別，而路由器便是據此來決定佇列處理方式及CoS等級--如Precedence。

本次出國實習內容係針對MPLS相關技術,包含有VPN服務的建置、Traffic Engineering-RSVP及QoS 之Differentiated Service等議題進行深入之研究,對於本公司現在之IP VPN服務建置將提供有利之參考價值。