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）

赴加拿大「實習 IP-VPN 網管與客戶網管技術」

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：專　員

姓　名：陳潔俐

出國地點：加拿大

出國期間：92.9.14～92.9.21.

報告日期：92.12.12

行政院研考會／省（市）研考會
編號欄

H6/C09203880

系統識別號:C09203880

公 務 出 國 報 告 提 要

頁數: 38　含附件: 否

報告名稱:

實習IP-VPN網管與客戶網管技術

主辦機關:

中華電信國際電信分公司

聯絡人／電話:

／23445280

出國人員:

陳潔俐　中華電信國際電信分公司　網路處　專員

出國類別: 實習

出國地區: 加拿大

出國期間: 民國 92 年 09 月 07 日 -民國 92 年 09 月 21 日

報告日期: 民國 92 年 09 月 17 日

分類號/目: H6／電信　／

關鍵詞:　IP-VPN網管與客戶網管技術

內容摘要: 從1996年起VPN始終是一個不曾退燒的熱門話題，從標準的制定以及應用環境的建置與整體架構，有許多熱烈的討論、研究與進展。迄今，VPN市場所面臨的挑戰已從「如何連接分支單位與遠端的使用者？」演變爲「如何選擇市場中最好的IPVPN方案？」，也就是對VPN之服務的要求，已從：在可管理的IP網際網路上，或者是網路系統服務業者的骨幹網路上，結合穿隧技術(Tunneling)、加解密(Encryption)、認證(Authentication)，以及存取控制(Access Control)的技術，提供用戶點對點的私人資料、影像及聲音的傳輸服務，提高到：要符合安全性、商務等級的效能、投資保障、延展性、商務案例、加值服務及供應商信譽等七大特性才能滿足用戶對IPVPN充分應用的需求。其中又以提供『商務等級之效能』與我們建立IPVPN網管及客戶網路管理機制方向有密不可分的關係。因網際網路本身並無提供服務品質 (Quality of Service; QoS) 或99.999% 的高可用度之保證。因此，爲因應依客戶不同的VPN可用度及功能性需求，提供相對之QoS及確保商務等級之效能的趨勢下，IP QoS機制更顯得迫切與重要。故IP QoS之機制應具備進行流量管理(traffic Shaping)、管制(policing)、記帳(accounting)、過濾(filtering)、封包轉送策略(policy forwarding)以及封包差異性服務 (DiffServ)等功能。

本文電子檔已上傳至出國報告資訊網

目　　錄

摘要 2

行程及實習內容紀要 3

前言 4

1 Introduction IP Quality of Service 5

1.1 IP QOS 的益處 5

1.2 QOS 的等級 5

1.3 成效量測 6

2 Differentiated Services Architecture 8

2.1 Diffserv 架構 8

2.2 DSCP 9

3 Network Boundary Traffic Conditioners: Packet Classifier, Marker, and Traffic Rate Management 10

3.1 Classifier 11

3.2 Policing & Marking 11

3.3 Queuing & Dropping 12

3.4 Shaping 13

4 Per-Hop Behavior: Resource Allocation 14

5 Per-Hop Behavior: Congestion Avoidance and Packet Drop Policy 16

TCP Slow Start 16

Congestion Avoidance 16

6 Integrated Services: RSVP 18

RSVP 的訊息 18

7 QOS in MPLS-Based Networks 20

8 Committed Access Rate 21

9 Modular QoS CLI (MQC) 24

10 SAA(Service Assurance Agent) 25

Case Study 28

摘要

從 1996 年起 VPN 始終是一個不曾退燒的熱門話題，從標準的制定以及應用環境的建置與整體架構，有許多熱烈的討論、研究與進展。迄今，VPN 市場所面臨的挑戰已從「如何連接分支單位與遠端的使用者？」演變爲「如何選擇市場中最好的 IPVPN 方案？」，也就是對 VPN 之服務的要求，已從：在可管理的 IP 網際網路上，或者是網路系統服務業者的骨幹網路上，結合穿隧技術(Tunneling)、加解密(Encryption)、認證(Authentication)，以及存取控制(Access Control)的技術，提供用戶點對點的私人資料、影像及聲音的傳輸服務，提高到：要符合安全性、商務等級的效能、投資保障、延展性、商務案例、加值服務及供應商信譽等七大特性才能滿足用戶對 IPVPN 充分應用的需求。其中又以提供『商務等級之效能』與我們建立 IPVPN 網管及客戶網路管理機制方向有密不可分的關係。因網際網路本身並無提供服務品質 (Quality of Service; QoS) 或 99.999% 的高可用度之保證。因此，爲因應依客戶不同的 VPN 可用度及功能性需求，提供相對之 QoS 及確保商務等級之效能的趨勢下，IP QoS 機制更顯得迫切與重要。故 IP QoS 之機制應具備進行流量管理(traffic Shaping)、管制(policing)、記帳(accounting)、過濾(filtering)、封包轉送策略(policy forwarding)以及封包差異性服務 (DiffServ)等功能。

行程及實習內容紀要

奉總公司九十二年八月二十七日信人二字第92A3501452號函核准職等前往加拿大實習「IP-VPN網管與客戶網管技術」，實習期間(含行程)自民國九十二年九月十四日至九十二年九月二十一日爲期八天。本次實習課程計有：

VoIP Product Introduction	1天
IP Traffic Measure and Planning	1天
Technology Training	1天
Site Visit	2天

前言

從 1996 年起 VPN 始終是一個不曾退燒的熱門話題，從標準的制定以及應用環境的建置與整體架構，有許多熱烈的討論、研究與進展。迄今，VPN 市場所面臨的挑戰已從「如何連接分支單位與遠端的使用者？」演變爲「如何選擇市場中最好的 IPVPN 方案？」，也就是對 VPN 之服務的要求，已從：在可管理的 IP 網際網路上，或者是網路系統服務業者的骨幹網路上，結合穿隧技術(Tunneling)、加解密(Encryption)、認證(Authentication)，以及存取控制(Access Control)的技術，提供用戶點對點的私人資料、影像及聲音的傳輸服務，提高到：要符合安全性、商務等級的效能、投資保障、延展性、商務案例、加值服務及供應商信譽等七大特性才能滿足用戶對 IPVPN 充分應用的需求。其中又以提供『商務等級之效能』與我們建立 IPVPN 網管及客戶網路管理機制方向有密不可分的關係。因網際網路本身並無提供服務品質 (Quality of Service; QoS) 或 99.999% 的高可用度之保證。因此，爲因應依客戶不同的 VPN 可用度及功能性需求，提供相對之 QoS 及確保商務等級之效能的趨勢下，IP QoS 機制更顯得迫切與重要。故 IP QoS 之機制應具備進行流量管理(traffic Shaping)、管制(policing)、記帳(accounting)、過濾(filtering)、封包轉送策略(policy forwarding)以及封包差異性服務 (DiffServ)等功能。

本次出國實習內容涉及 IPVPN 網路及客戶網路管理、SLA 及 QoS 技術及應用服務層管理技術的探討，特別是針對 IP QoS 的技術趨勢進行了解。茲謹就 IP QoS 之相關技術問題及案例報告如下：

1 Introduction IP Quality of Service

隨著科技的進步，一般家庭與企業對 Internet 網路的需求日益殷切。除了傳統的網頁瀏覽、收發電子郵件及傳送檔案外，另外 VOIP 與視訊會議的使用也越來越多。然而目前 Internet 網路只能提供量力而爲(Best-Effort)的技術，品質好壞只能聽天由命了。爲了提供用戶更好及區隔性的服務，遂發展了 IP QOS 的技術。

1.1 IP QOS 的益處

- 滿足現有及發展中的多媒體服務之需求
- 使網路技術員可控制網路資源及其使用量
- 提供服務保證及訊務區隔。尤其在網路上傳送複合之語音、視訊及資料時特別明顯。
- 提供白金、金、銀、銅等各種服務等級以滿足不同客戶之需求

1.2 QOS 的等級

- Best-effort service

  是種量力而爲的服務，並不保證用戶資料是不是會遺失、延遲時間會在甚麼範圍內。這也是目前 Internet 上使用的方式。
- Differential Service

  訊務被分類爲多種服務等級(Class of service)，各種服務等級配合對等的服務。這種服務通常又稱爲 soft QOS。
- Guaranteed Service

  在訊務傳送前須先以信號方式配置所需的品質需求，如所需頻寬及最大延遲時間等，以保證訊務之需求。這種服務通常又稱爲 hard QOS。

1.3 成效量測

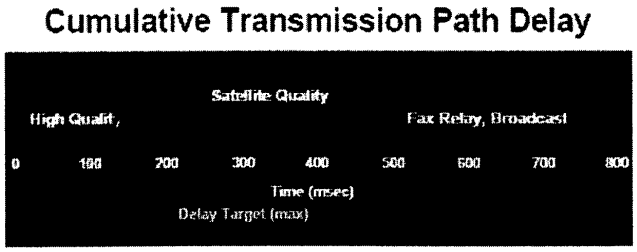
QOS 的主要目的爲提供更好的網路，但怎麼樣才是好的網路? 一般可以頻寬(Bandwidth)、封包延遲(Packet Delay)、延遲差異(Jitter)及封包遺失(Packet Loss)等方向來作考量。

- Bandwidth

  以用戶需求頻寬及可使用頻寬做比較，是否能滿足用戶需求。

- Packet Delay

  有些訊務可容許較長的延遲時間，但類似語音之服務就必須提供 150ms 以下的延遲時間。否則語音品質就無法接受。



圖一. 語音延遲的底限

- Jitter

  又稱爲延遲時間的變異性，此參數亦是應用於語音方面。

- Packet Loss

  檔案傳送較不能容許封包遺失，錯誤的資料會造巨大的損失。

表 1. 典型應用的 QOS 需求

	Voice	FTP	ERP and Mission-Critical
Bandwidth	Low to Moderate	Moderate to High	Low
Random Drop Sensitive	Low	High	Moderate To High
Delay Sensitive	High	Low	Low to Moderate
Jitter Sensitive	High	Low	Moderate

2 Differentiated Services Architecture

QOS 主要目的爲提供保證(Guaranteed)及區隔(Differentiated)的服務。保證服務及區隔服務爲兩種不同等級的 QOS。Diffserv 將訊務分類爲不同等級，並配置不同之優先順序。下列介紹區隔服務之架構及特性。

2.1 Diffserv 架構

DiffServ 架構可依下圖來解釋，與客戶或其他 Diffserv 區域界接之路由器爲 Edge 路由器，其餘位於區域內之路由器爲 Core 路由器。 QOS 機制在 Edge 端訂立訊務調節器(Traffic Conditioners)將來話作分類或建立各種政策性的拋棄原則，另在 Core 路由器內設定 PHB(Per HOP Behavior)機制以分配網路資源。

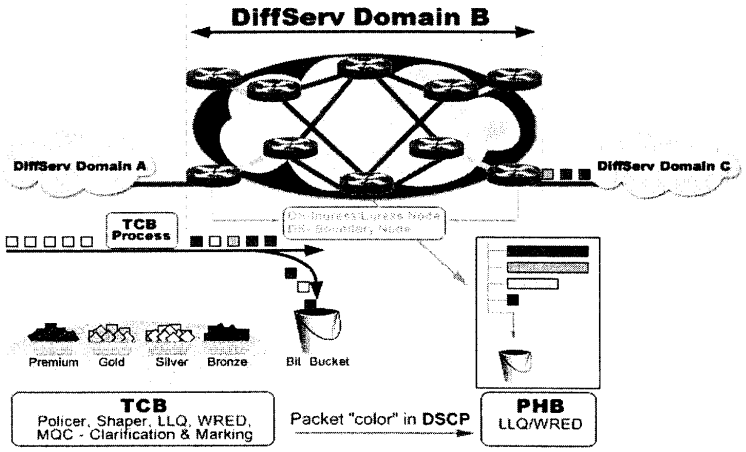


圖 2. DiffServ 架構圖

功能區塊	位置	起用功能	動作
Traffic Conditioner	通常應用於 Edge 路由器的輸入介面	Classfication、Shapping、Policing	根據輸入之資料設定 DSCP
PHB	適用於 DiffServ 內所有路由器	Resource Allocation、Drop Policy	依據 DSCP 處理經過的訊務

2.2 DSCP

在傳統的 IP 設計上即列入了 TOS(Type of Service)的觀念，但初期使用之場所爲美國軍方及校園。使用人數有限，網路並不會阻塞，故未引用此一參數。但隨著 Internet 的發展，使用人數越來越多，遂訂立了各種等級參數。其中 DSCP(Differential Service Code Point)係應用於 DiffServ 的環境。

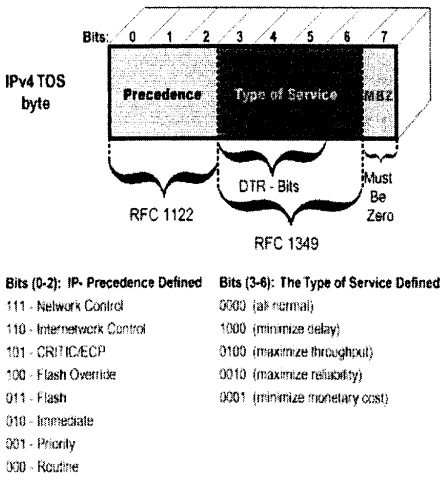
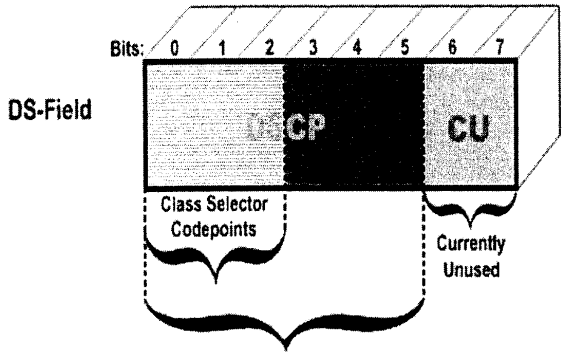


圖. IPV4 之 TOS



Differentiated Services Codepoint (DSCP)
RFC 2474

圖. DSCP

3 Network Boundary Traffic Conditioners: Packet Classifier, Marker, and Traffic Rate Management

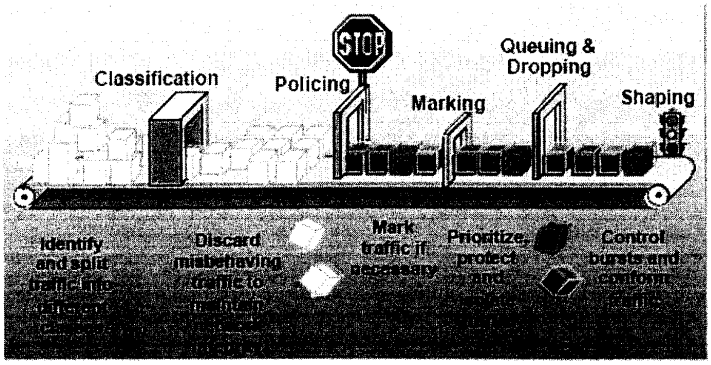


圖. Classifier, Marker, Policing, Queue and Shaping

3.1 Classifier

可依下列方式將訊務區分爲不同的等級

- **Incoming/outgoing interface**
- **All/any IP traffic**
- Standard or extended access control list
- **IP RTP ports (real-time traffic)**
- **Source/destination MAC address**
- **DSCP or IP precedence value**
- **(If trusted and marked appropriately)**
- **MPLS EXP (experimental bits)**
- **(If trusted and marked appropriately)**
- **Network-Based Application Recognition (NBAR)**

3.2 Policing & Marking

縮寫定義：

CIR—Committed rate

PIR—Peak rate

CBS—Committed burst size (max)

EBS—Excess burst size (max)

PBS—Peak burst size (max)

Tp—Current size of PBS bucket

3.2.1 A single Rate two color Marker

限制訊務在一定速率範圍內，將符合規定的訊務標示爲低拋棄等級，超過的訊務定爲高拋棄等級，拋棄違反規定的訊務

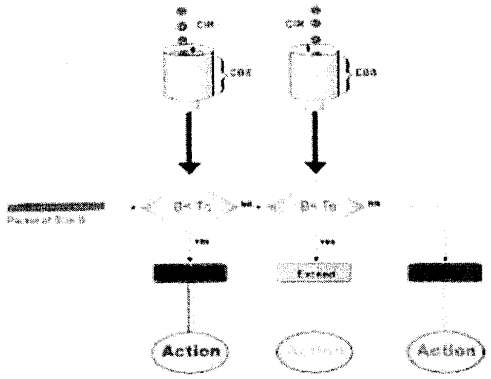


圖.A single Rate two color Marker

3.2.2 A Two Rate Three Color Marker

與上述方式類似，但方向相反。

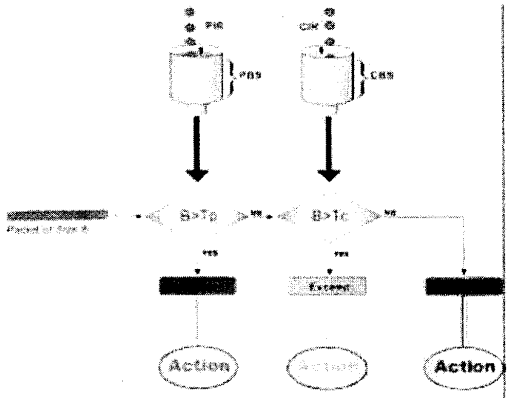


圖.A Two Rate Three Color Marker

3.3 Queuing & Dropping

3.3.1 Queuing

每個輸出的 queue 都會配置有固定的頻寬及緩衝容量，可用以保護及隔離訊務，其中之一可保留給低延遲的訊務(例如:VOIP)。

3.3.2 Dropping

一般而言，在緩衝區滿了之後, 隨後的封包會被拋棄。此一方式稱爲 Tail Drop。但爲考量防止阻塞，可能以預測的方式拋棄封包。後

續將會陸續介紹阻塞管理及防制之方式。

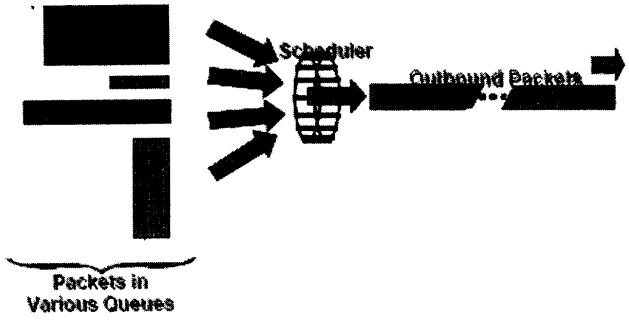


圖 Queue & Dropping

3.4 Shaping

Shaping 採取比 Policy 溫和的方式處理違反規定的封包，它將這些封包置入 Queue 內以撫平這些封包，防止封包遺失。

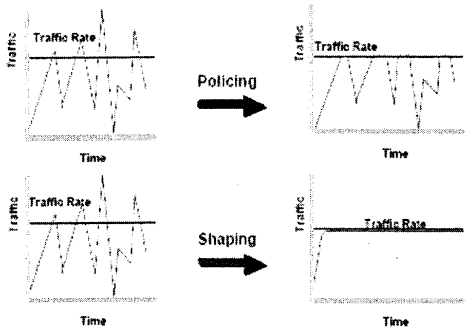


圖. Policing 與 Shaping 的比較

4 Per-Hop Behavior: Resource Allocation

路由器使用多種 Queue 來滿足客戶的需求, 並藉以判別優先及拋棄等級.下列將分別介紹常用的 Queue。

- FIFO(First In First Out)

  在路由器未訂立任何 Queuing 方式時, FIFO 則爲預設方式. 封包將依到達的先後順序決定輸出順序. 當 Queue 被填滿時,則後續之封包將被拋棄。

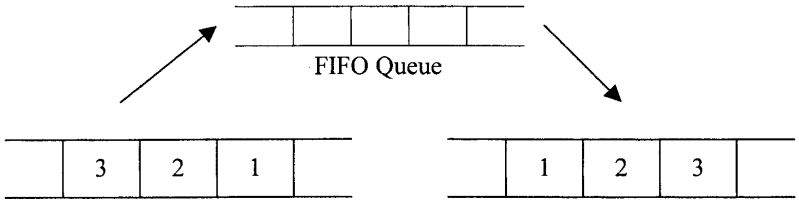


圖: FIFO Queue

- PQ (Priority Queue)

  PQ 保證重要之訊務得到最快速之服務. 此話務全部處理完之後才會考慮其他訊務。

- WFQ (Weighted Fair Queue)

  將訊務分成多種等級(Voice, Video, Data). 依不同權重決定 Queue 之分配比例。

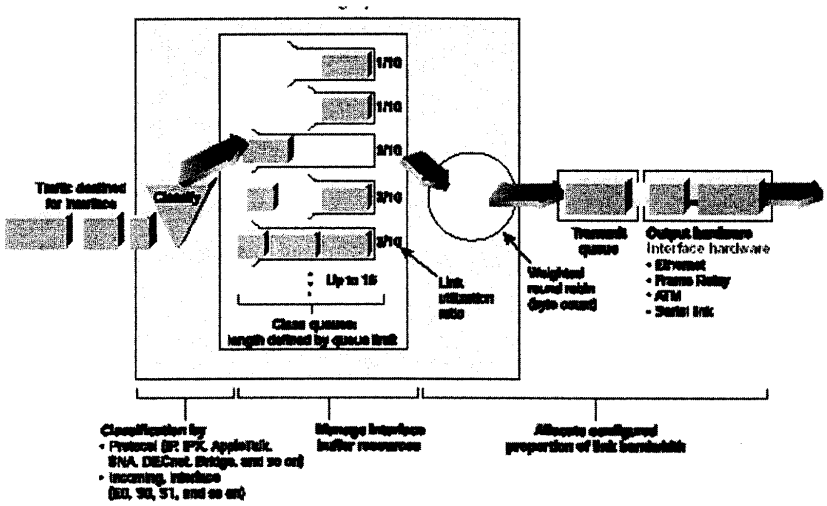


圖. WFQ(Weighted Fair Queue)

- LLQ (Low Latency Queue)

  結合 PQ 及 WFQ 之特性以滿足即時及可靠性等各種需求.

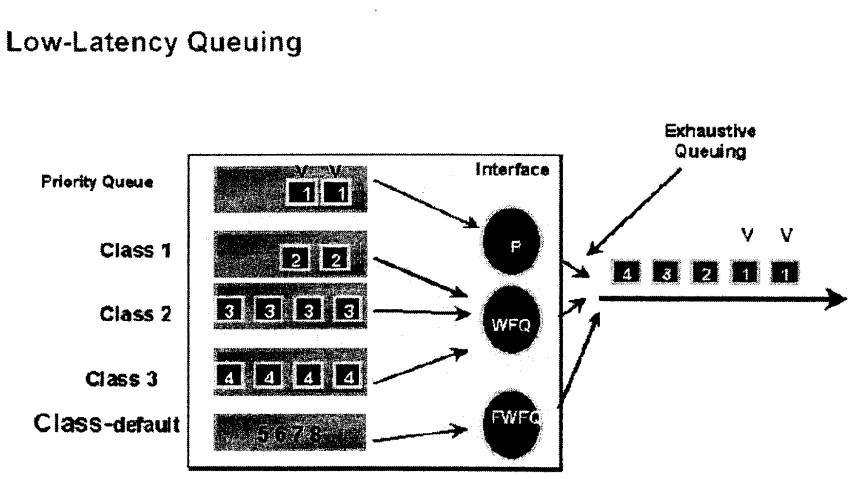


圖 Low-Latency Queuing

5 Per-Hop Behavior: Congestion Avoidance and Packet Drop Policy

封包拋棄法則也就是 Queue 的管理規則,可用以管理封包及 Queue 的長度. 傳統上的 FIFO 的 Queue 管理使用簡單的尾端拋棄方式(Tail Drop), 當 Queue 滿時, 拋棄後續到達的封包. 並將討論目前使用範圍最廣的 TCP(Transmission Control Protocol)的壅塞控制方式及其造成效應.

TCP Slow Start

TCP 的發送者使用壅塞視窗(Congestion Window)來執行壅塞防制. 當一個新的 TCP 對話開始時, 壅塞視窗就被啓動並設定爲 1 個片段(segment- 通常爲 512bytes 或 536bytes). 這視窗之意義爲當發送者未收到確認時可發送的最大容量. 一旦第一個封包被確認時, 視窗大小則更改爲 2. 也就是說發送端可於得到確認前, 連續發送 2 個封包. 依此類推, 視窗大小以指數成長(1,2,4,8....). 封包也可順利傳送, 資料量由小到大變化. 但是, 萬一遇到了壅塞而資料漏失時, 視窗大小就被重置爲 1. 資料量銳減. 壅塞時, 所有網路上的 TCP 封包都可能同時遺失. 也就是所稱之 Global Synchronization 現象.

Congestion Avoidance

爲防止 Global Synchronization 的現象, 造成訊務量的集體成長, 而產生定時壅塞之行爲. 遂有了 RED(Random Early Detection)的想法. 在還沒壅塞前, 先以隨機方式拋棄某些訊務, 改變部分視窗大小. 以平均訊務量, 並防止壅塞產生.

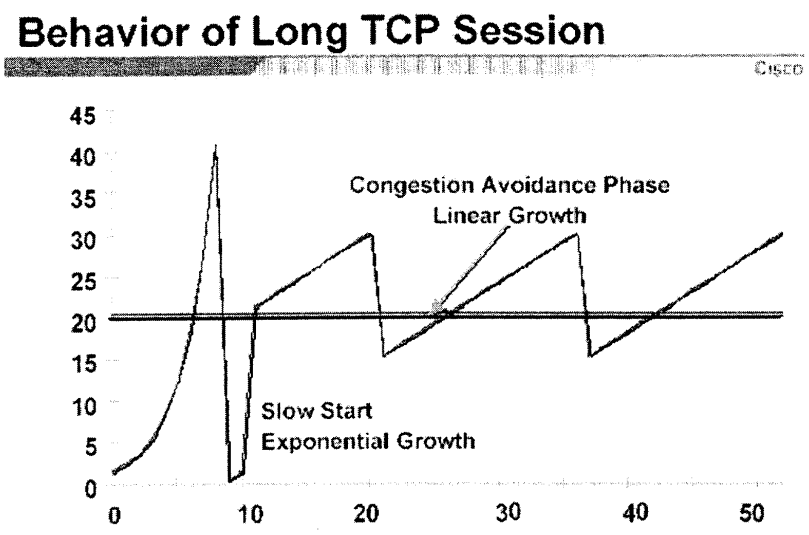


圖: Behavior of Long TCP Session

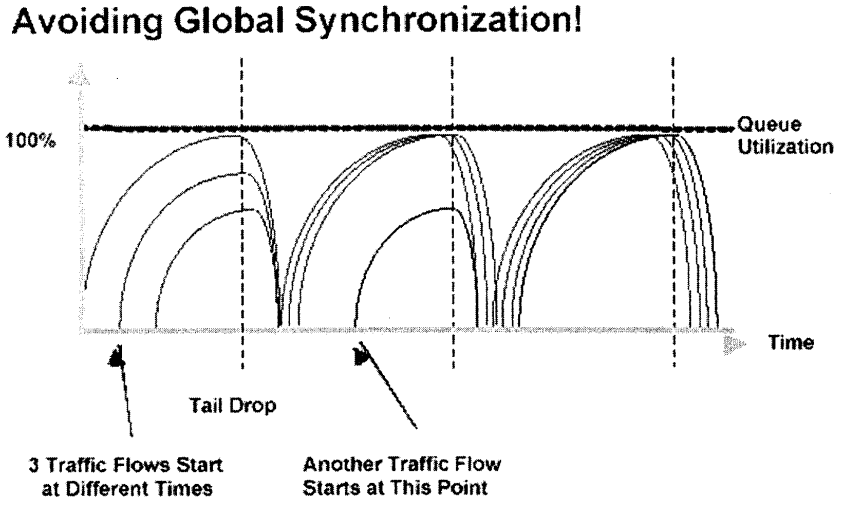


圖 Avoiding Global Synchronization

6 Integrated Services: RSVP

Intserv (Integrated Service) 可管控到每一個別封包的行爲. 其中 RSVP (Resource Revervation Protocol) 則是他的執行方式. 故名思義, RSVP 是以事先告知保留通道的方式達到其目的. 在所需通路建立前必先以訊號告知所經通道的路由器提供所需的頻寬及處理方式等需求.

RSVP 的訊息

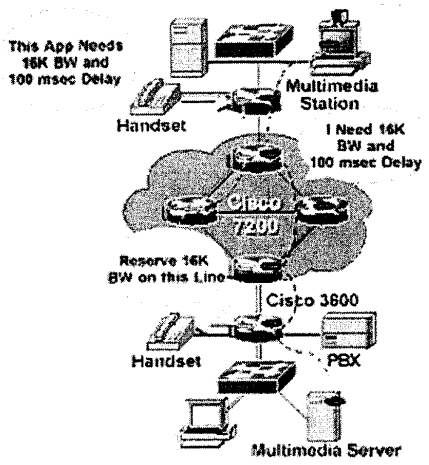
RSVP 的信息包括 PATH 及 RESV 二個必要訊息與 PATH ERROR, PATH TEARDOWN, RESV ERROR, RESV CONFIRM 及 RESV TEARDOWN 等五個選項訊息.

A. PATH

發送者發送PATH訊息, 內容包括主被叫的IP, Port和所需的頻寬及最低延遲時間等需求. 並以定期發送的方式, 保持所需路徑的必要性. 一但發送者不需保留路徑時, 則以 PATH TEARDOWN 訊息告知所經路徑之路由器解除,以保留資源給其餘使用者.

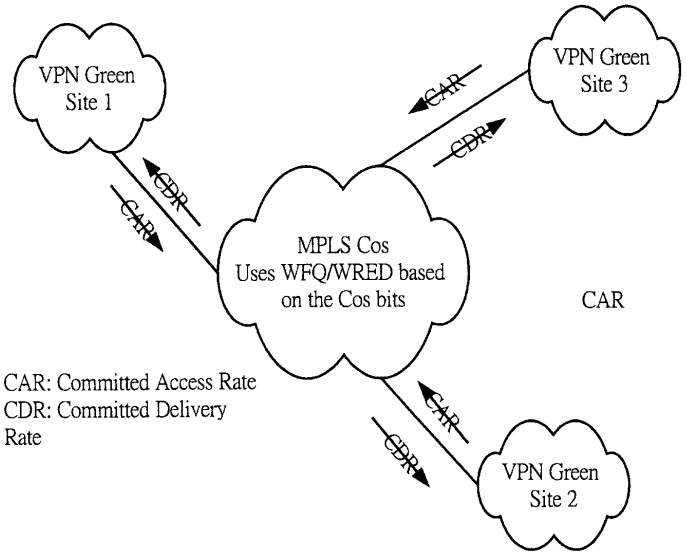
B. RESV

接收者收到 PATH 的需求後, 會先檢查資源是否足夠. 若足以配置資源給需求者, 則回應 RESV CONFIRM 訊息給發送者告知同意需求. 並定時傳送RESV訊息, 告知協約仍然成立. 一旦, 資源必須回收時, 則發出RESV TEARDOWN 訊息告知.


This App Needs
16K BW and
100 msec Delay
Handset
Multimedia
Station
I Need 16K
BW and
100 msec Delay
Cisco
7200
Reserve 16K
BW on this Line
Cisco 3600
Handset
PBX
Multimedia Server

7 QOS in MPLS-Based Networks

QOS 是 VPN 的一個主要的部分. 和 IP QOS 部分相同的是都可提供 DiffServ 及 Guarantee Service 兩種方式. VPN 在客戶及邊界路由器上設立 CAR 及 CDR 兩種應用以限制頻寬及設定分類等級. CAR 主要針對流向邊界路由器之訊務, 而 CDR 爲針對從邊界路由器流出去之訊務. 在骨幹路由器則利用 WFQ 及 WRED 等方式控制訊務.



步驟	QOS 設置點	QOS 功能
1	入口路由器	選項 1: 在客戶路由器(CE)上根據簽訂合約,設定訊務的 IP Precedence. 此值會被複製到 MPLS COS 值上. 選項2: 在服務提供者的邊界路由器(PE)上根據簽訂合約,設定訊務的 MPLS COS.
2	骨幹路由器	在服務提供者的骨幹路由器上以 WFQ 及 WRED 方式對待不同 MPLS COS 的訊務
3	出口路由器	MPLS COS 的值被複製到 IP Precedence.
4	出口路由器	以 CAR(Commit Access Rate) 所設原則處理輸出之訊務.

8 Committed Access Rate

功能:

- 依據彈性的準則條件, 限制輸出入的訊務量及設定動作.
- 利用設定 IP precedence 或 QOS group 的方式, 作封包的分類
- 準則條件可爲 incoming interface, IP Precedence, QOS group 或 IP access list
- 動作可爲 transmit, drop, set precedence, set QOS

語法

Task	**Command**
(Optional) Specify a rate-limit access list.	**access-list rate-limit** *acl-index* {*precedence* | *mac-address* |**mask** *prec-mask*}
(Optional) Specify a standard or extended access list..	**access-list** *acl-index* {**deny** | **permit**} *source* [*source-wildcard*] **access-list** *acl-index* {**deny** | **permit**} *protocol source* *source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log**]
Specify the interface or subinterface.	

This task puts the router in interface configuration mode.	**interface** *type number*
Specify the rate policy for each particular class of traffic.	**rate-limit {input | output} [access-group [rate-limit]** *acl-index* **| qos-group** *number*] *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action*
Verify the configuration.	**show interfaces rate-limit**

範例 1：將連接的 T3 限速設定爲 20M, 允許 burst 爲 24000bytes, 拋棄其餘的封包

```
interface Hssi0/0/0
description 45Mbps to R1
rate-limit input 20000000 24000 24000 conform-action
transmit exceed-action drop
ip address 200.200.14.250 255.255.255.252
rate-limit output 20000000 24000 24000 conform-action
transmit exceed-action drop
```

範例 2：

- 傳送所有的 web 訊務, 且設定於限速範圍內的封包之 IP Precedence=5,限速範圍外的封包之 IP Precedence=0.
- 傳送限速範圍內之 FTP 封包, 並設定 IP Precedence=5.拋棄範圍外的封包.
- 限制所有其餘之封包頻寬爲 8M, normal burst= 16000bytes, excess burst=24000bytes, 傳送符合限速的封包並設定 IP precedence=5, 拋棄不符合的封包.

```
interface Hssi0/0/0
description 45Mbps to R2
rate-limit input access-group 101 20000000 24000 32000
conform-action
set-prec-transmit 5 exceed-action set-prec-transmit 0
rate-limit input access-group 102 10000000 24000 32000
conform-action
```

```
set-prec-transmit 5 exceed-action drop
rate-limit input 8000000 16000 24000 conform-action
set-prec-transmit 5 exceed-action
drop
ip address 200.200.14.250 255.255.255.252
!
access-list 101 permit tcp any any eq www
access-list 102 permit tcp any any eq ftp

Router# show interfaces hssi 0/0/0 rate-limit
Hssi0/0/0 45Mbps to R2
Input
matches: access-group 101
params: 20000000 bps, 24000 limit, 32000 extended limit
conformed 3 packets, 189 bytes; action: set-prec-transmit 5
exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
last packet: 309100ms ago, current burst: 0 bytes
last cleared 00:08:00 ago, conformed 0 bps, exceeded 0 bps
matches: access-group 102
params: 10000000 bps, 24000 limit, 32000 extended limit
conformed 0 packets, 0 bytes; action: set-prec-transmit 5
exceeded 0 packets, 0 bytes; action: drop
last packet: 19522612ms ago, current burst: 0 bytes
last cleared 00:07:18 ago, conformed 0 bps, exceeded 0 bps
matches: all traffic
params: 8000000 bps, 16000 limit, 24000 extended limit
conformed 5 packets, 315 bytes; action: set-prec-transmit 5
exceeded 0 packets, 0 bytes; action: drop
last packet: 9632ms ago, current burst: 0 bytes
last cleared 00:05:43 ago, conformed 0 bps, exceeded 0 bps
```

9 Modular QoS CLI (MQC)

爲簡易應用QOS的設定, MQC 將QOS區分爲三個步驟: traffic class definition, policy definition 及 policy application

Step 1: Traffic class definition

----- 設定訊務的類別, 使用class-map指令

Step 2: Policy definition

----- 設定各種訊務類別的marking, policing, shaping, queuing等, 使用policy-map指令

Step 3: Policy application

----- 將policy 應用在設備介面上或ATM的VC(Virtual Circuits)的出入訊務, 使用service-policy指令

基本語法

```
class-map [match-any | match-all] class-name

policy-map policy-name

service-policy {input | output} policy-name
```

Policy的語法

```
Marking  ---
     set {ip | mpls | cos | atm-clp | … }

Policing ---
     police avg-rate Bc Be conform-action action
     exceedaction action violate-action action
```

```
Shaping ----
     shape {average | peak} cir [bc] [be]

Queueing ----
     priority {percent percentage | bandwidth-kbps}
or
     bandwidth {percent percentage | bandwidth-kbps}

Congestion Avoidance ----
     random-detect [dscp | dscp-based | … ]
```

10 SAA(Service Assurance Agent)

功能:

- SAA 是 RTR(Response Time Reporter)的新名稱, 且指令名稱仍沿用 RTR
- 用以量測網路的 SLA(Service Level Agreement)參數, 如 response time, network resources, availability, jitter, connect time, packet loss 及 application performance.
-

組態任務:

A. Configuring the Operation (Required)

Configure a Jitter Operation		
Step	**Command**	**Purpose**
1	**rtr** number	Specifies an SA Agent operation and enters RTR configuration mode.
2	**type jitter dest-ipaddr** { name | ipaddr} **dest-port** port number [**source-ipaddr** { name | ip addr}] [**source-port** port number][**control** { enable | disable}] [**num-packets** number of packets] [**interval** inter-packet interval]	Defines a UDP Jitter operation.

B. Configuring Optional Operation Characteristics (Optional)

C. Scheduling the Operation (Required)

Command	Purpose
rtr schedule number [life seconds] [start-time {pending | now | hh: mm [month day | day month]}] [ageout seconds]	Schedules the operation by configuring the time parameters.

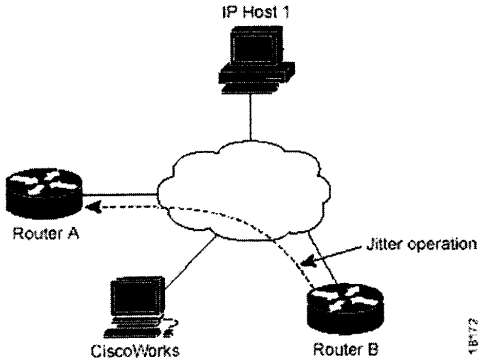
D. Verifying SA Agent (Optional)

```
o show rtr application
o show rtr collection-statistics
o show rtr operational-state
o show rtr configuration
```

範例:

- 量測 Router B 到 Router A 的 Jitter 值
- 設定 RTR=5
- destination ip=172.24.132.100 udp port=99
- send 20packets at 20 ms intervals
- enable RTR responder on Router A for the Jitter Operation to run

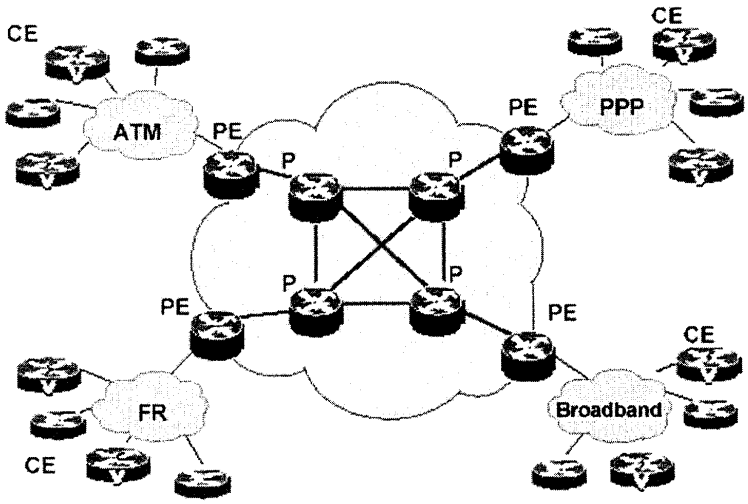
Figure 4 Jitter Operation




```
RouterB(config)# rtr 5
RouterB(config-rtr)# type jitter dest-ip 172.24.132.100
dest-port 99 num-packets 20 interval 20
!
RouterB(config)# rtr schedule 5 start-time now
```

Case Study

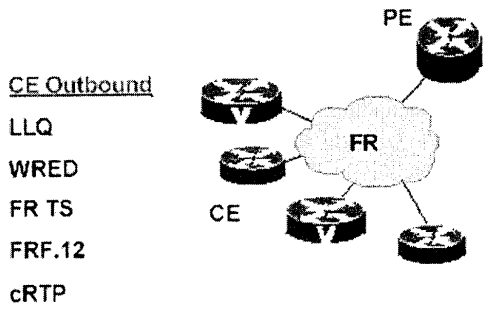
案例一:



服務定義: 網路提供者提供三種等級的類別Premium, Business, Best Effort

- Premium: Max BW, low latency, no loss
- Business: Min BW, low loss
- Best Effort: No guarantees

CE-to-PE QoS for Frame Relay Access CE Outbound



- 設定每條PVC 的LLQ, 以保證最低頻寬及應用壅塞管理機制
- 應用 WRED 執行 dropping policy 及增加電路使用率
- 限制超出CIR的封包 bursting above CIR
- 在低速電路上切割封包

!

使用指令

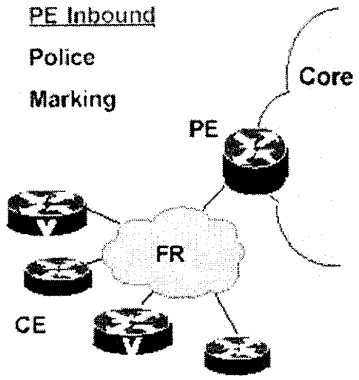
```
class-map match-all PREMIUM
  match ip access-group 101
class-map match-all BUSINESS
  match ip access-group 102
!
policy-map OUT-POLICY
  class PREMIUM
  priority 128
  set ip dscp ef
  class BUSINESS
  bandwidth 256
  set ip dscp af31
  random-detect dscp-based
  class class-default
  set ip dscp 0
  random-detect dscp-based

!
```

```
interface Serial0/0.1 point-to-point
  ip address 10.10.1.2 255.255.255.0
  frame-relay interface-dlci 16
  class FR-class
!
map-class frame-relay FR-class
  frame-relay cir 512000
  frame-relay bc 512
  frame-relay mincir 512000
  service-policy output OUT-POLICY
  frame-relay fragment 512
  frame-relay ip rtp header-compression
```

CE-to-PE QoS for Frame Relay Access

PE Inbound



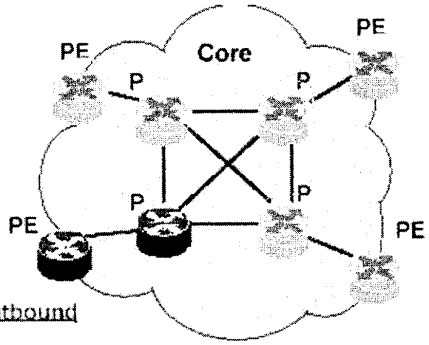
動作:

- 根據合約做 Mark 及 Policy
- P router 會根據 marking 的值, 對待訊務
- 如果使用 MPLS, 則做 DSCP/IP Prec 與 EXP 的轉換

使用指令

```
!
class-map match-all PREMIUM
   match ip dscp ef
class-map match-all BUSINESS
   match ip dscp af31 af32 af33
!
policy-map IN-POLICY
   class PREMIUM
      police 128000 4000 4000 conform-action transmit
         exceed-action drop
   class BUSINESS
      police 256000 8000 8000 conform-action transmit
         exceed-action set-dscp-transmit af32
         violate-action set-dscp-transmit af33
   class class-default
      set ip dscp 0
!
interface Serial0/0.1 point-to-point
  ip address 10.32.14.2 255.255.255.0
  frame-relay interface-dlci 16
  class FR-class
!
map-class frame-relay FR-class
  frame-relay cir 512000
  frame-relay bc 512
  frame-relay mincir 512000
  service-policy input IN-POLICY
  frame-relay fragment 512
!
```

PE-to-P QoS, PE Outbound



PE Outbound

LLQ

WRED

動作:

- 根據inbound的mark 分類訊務
- 用LLQ設定保證頻寬及做壅塞管理
- 應用 WRED 執行 dropping policy 及增加電路使用率

使用指令

PE Outbound (POS)

```
!
class-map match-all PREMIUM
  match ip dscp ef
!
class-map match-all BUSINESS
  match ip dscp af31 af32 af33
!
policy-map OUT-POLICY
  class PREMIUM
    priority 16384
  class BUSINESS
    bandwidth 65536
    random-detect dscp-based
  class class-default
    random-detect dscp-based
!
interface POS1/0
  ip address 10.150.1.1 255.255.255.0
  service-policy output OUT-POLICY
!
```

PE Outbound (Ethernet)

```
!
class-map match-all PREMIUM
 match ip dscp ef
!
class-map match-all BUSINESS
 match ip dscp af31 af32 af33
!
policy-map OUT-POLICY
 class PREMIUM
  priority 16384
  set cos 5
 class BUSINESS
  bandwidth 65536
  set cos 3
  random-detect dscp-based
 class class-default
  set cos 0
  random-detect dscp-based
!
interface FastEthernet1/0
 ip address 10.150.1.1 255.255.255.0
 service-policy output OUT-POLICY
```

PE Outbound (MPLS)

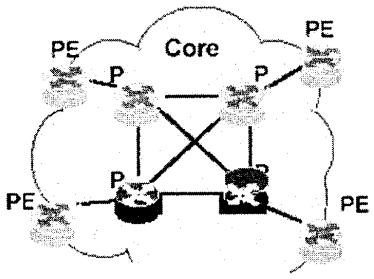
```
!
class-map match-all PREMIUM
 match mpls experimental 5
!
class-map match-all BUSINESS
 match mpls experimental 3 4
!
policy-map OUT-POLICY
 class PREMIUM
  priority 16384
```

```
  class BUSINESS
    bandwidth 65536
    random-detect
  class class-default
    random-detect
!
interface POS1/0
  ip address 10.150.1.1 255.255.255.0
  service-policy output OUT-POLICY
```

PE Outbound (ATM)

```
!
policy-map OUT-POLICY
  class class-default
  random-detect
!
interface ATM1/0/0
  no ip address
  bundle BOSTON
  protocol ip 10.23.45.2 broadcast
  encapsulation aal5snap
  pvc-bundle 0/35
    service-policy output OUT-POLICY
    vbr-nrt 5000 3000 500
    precedence 4-7
  pvc-bundle 0/34
    service-policy output OUT-POLICY
    vbr-nrt 4000 3000 500
    precedence 2-3
  pvc-bundle 0/33
    service-policy output OUT-POLICY
    precedence other
  !
```

P-to-P QoS, P Outbound



P Outbound

LLQ (MDRR)

WRED

動作:

- 用LLQ設定保證頻寬及做壅塞管理
- 應用 WRED 執行 dropping policy 及增加電路使用率
- 不需使用inbound的policy

使用指令

```
interface POS2/0
  ip add 10.64.12.1 255.255.255.252
  tx-cos OUT-POLICY
!
cos-queue-group OUT-POLICY
  precedence 0 queue 0
  precedence 3 queue 1
  precedence 5 queue low-latency
  precedence 0 random-detect-label 0
  precedence 3 random-detect-label 1
  random-detect-label 0 3000 5000 1
  random-detect-label 1 6000 8000 1
  queue 0 5
  queue 1 10
  queue low-latency strict-priority
!
```

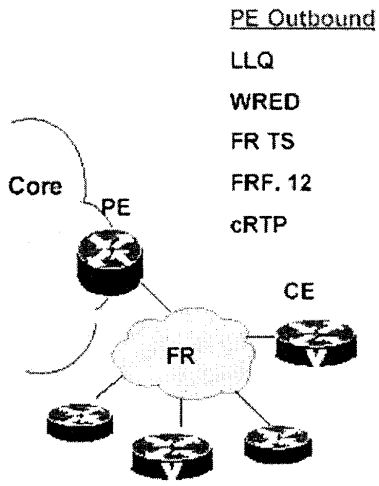
P-to-PE QoS, P Outbound

動作:

- 使用與P-to-P相同的QOS

PE-to-CE QoS for Frame Relay Access

PE Outbound



動作:

- 用LLQ設定保證頻寬及做壅塞管理
- 應用 WRED 執行 dropping policy 及增加電路使用率
- 由於PE到CE的速度不匹配，使用Shaping機制
- 做封包切割

使用指令

```
!
class-map match-all PREMIUM
  match ip dscp ef
!
class-map match-all BUSINESS
  match ip dscp af31 af32 af33
!
policy-map OUT-POLICY
  class PREMIUM
    priority 128
  class BUSINESS
    bandwidth 256
    random-detect dscp-based
  class class-default
    random-detect dscp-based
!
interface Serial0/0.1 point-to-point
  ip address 10.10.1.2 255.255.255.0
  frame-relay interface-dlci 16
  class FR-class
!
map-class frame-relay FR-class
  frame-relay cir 512000
  frame-relay bc 5120
  frame-relay mincir 512000
  service-policy output OUT-POLICY
  frame-relay fragment 512
  frame-relay ip rtp header-compresssion
```

心得與建議

近年來，因以 IP 爲基礎的數據通訊業務與網路發展迅速，傳統電信與 IP 網路各自發展，而電信業務將會跨網路互通，就未來而言，這將是一個長期漸進的過程，因此兩種網路共存的情形勢必會持續很長的一段的時間。基於利用 IP 網路具有：企業可以節省成本、針對市場需求與業務模式的改變可迅速調整企業網路架構、網路擴充性強、降低技術支援及設備需求等優勢，各行各業都會受到 IP 整合應用及服務品質提升的影響，勢將更樂於使用此項 IP 服務。

從本公司立場而言，爲使 IP 市場的企業客戶樂於尋求我們所提供的相關的 IPVPN 網路服務，除了滿足客戶對網路安全及服務品質等基本需求外，更應積極開發與 IPVPN 網路相關之增添服務，創造 IP 更多之新應用。目前 IPVPN 的增添服務依其服務項目分成多種類型，例如：1.就分支單位間之連線服務來看：可提供遠端接取 ERP、Vedio sever、Hosted Content 及 Extranet 網路連線。2.就安全服務來看，可加強其競爭籌碼的有：Stateful 防火牆、加密功能、anti-spoofing、NAT 及 DOS 防護等。3.就傳輸管理服務來看：利用差異化服務、頻寬管理、管制等功能，將用戶的某些封包分類，以進行優先處理或服務品質處理，以達到 QoS 的最佳化。當然，在掌握市場的方向的同時，內部人才的培養及設備的升級更是刻不容緩的，因優秀的技術人才加上優化進步的設備，才能讓我們在這個眾多電訊業者競爭的市場上勝出。