實習在 Internet 上建置企業專用網路(VPN)技術及規劃

出國報告

數據通信分公司 網際網路處 張立銘

到達國家： 美國

出國期間： 89 年 12 月 3 日至 12 月 16 日

提　要　表

根據 Gartner Group 公司的研究，到2003年前為止，幾乎百分之95企業將在既有的WAN (Wide Area Network)網路服務中使用 VPN (Virtual Private Network)的功能。從網路架構觀點而言，這樣的趨勢的動機是明顯的：VPN能夠支援今天絕大多數企業更多樣化連通性需求。

目　　次

前言

根據 Gartner Group 公司的研究，到2003年前為止，幾乎百分之95企業將在既有的WAN (Wide Area Network)網路服務中使用 VPN (Virtual Private Network)的功能。從網路架構觀點而言，這樣的趨勢的動機是明顯的：VPN能夠支援今天絕大多數企業更多樣化連通性需求。

VPN 是什麼

整體而言，VPN 是在使用相同的安全、管理和支援VPN功能的分享基礎網路(如IP backbone)上佈署的企業網路。VPN可建構於網際網路服務供應者(ISP)所提供之先進網路通信技術，如Frame Relay，ATM(Asynchronous Transfer Mode)， MPLS(Multi-protocol Label Switching)等。

然而，就實際的網路建置言之，VPN的功能是取決於企業與ISP之間介接的設備(如IPSec router，MPLS CE-PE router等)，網路骨幹本身僅就資料的傳遞扮演傳送的功能(packet transport，如MPLS P router或Label Switching Router)。

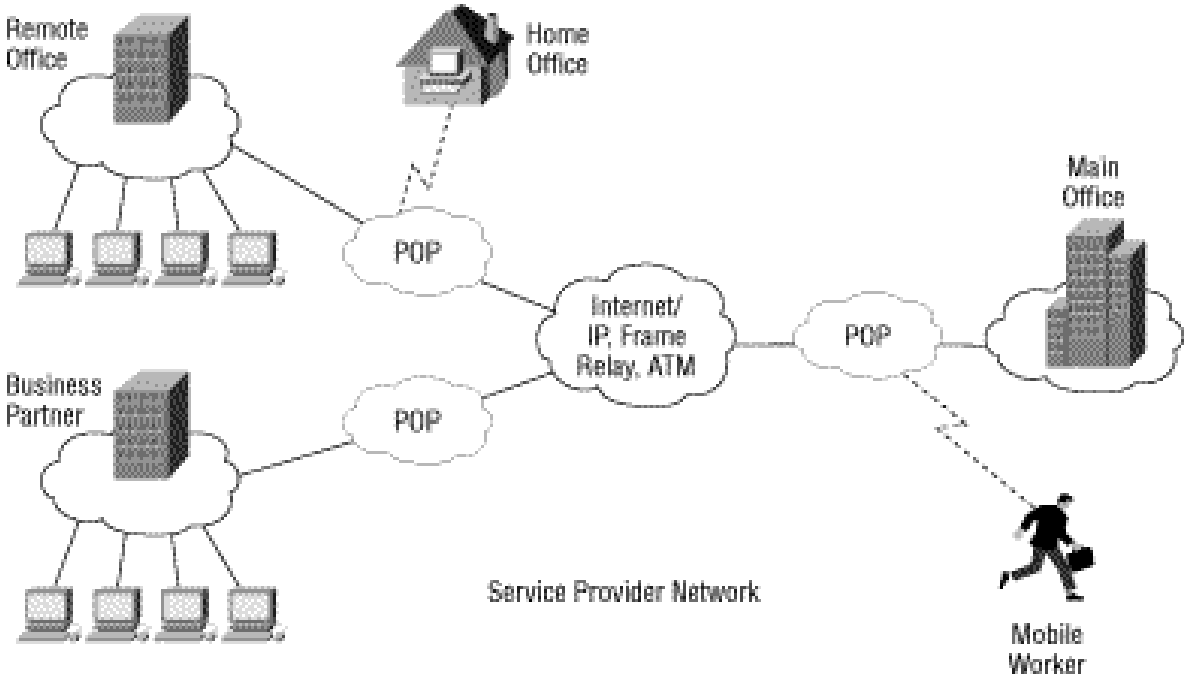


圖 1： Applicatoin of VPN

VPNs 的服務可略分為：遠端接取服務(remote access)、企業內網路(intranet)與企業間網路(extranet)。

遠端接取服務 VPN 提供 telecommuters 、機動用戶或者更小的遠端辦公室與企業總部的連接與資源分享。.

企業內網路提供公司總部與其它企業所屬之辦公室或相關從屬機構的骨幹網路。

企業間網路係擴展對商業夥伴之運作資源的提供, 供給者或顧客允許分享資訊的通路，在此架構內不同的 Intranet 皆有各自不同安全和頻寬的管理策略。

建構 VPN 所需的元件(Components)

建構 VPN 所需的元件如圖 2 所示。

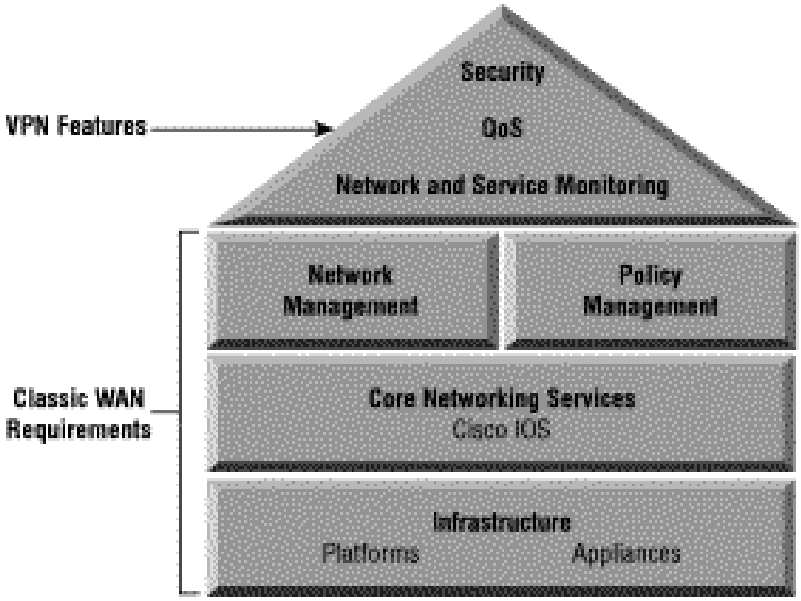


圖 2： VPN Building Blocks

網路平台的可擴展性(Platform Scalability)—網路的設計與技術的標準化是維持可擴展性的重要指標，標準化的作業與維運可確保網路架構的延續性與穩定。

安全性(Security)—Tunneling， 資料加密(encryption)與資料確認(packet authentication)是必要的，另外，針對不同的使用者提供授權則可確保資料的正確性與安全。

VPN 性能管理—針對頻寬、QoS 與特定服務之 SLA(Service Level Agreement)提供控管機能(如 queuing，network congestion avoidance，traffic shaping，packet classification 等)

VPN 安全控管—使用 Firewalls，IDS(intrusion detection system)，安全查核(security auditing)等。

圖 3 所示為一 VPN 應用示意圖，在圖中示範不同 VPN 服務的互動。

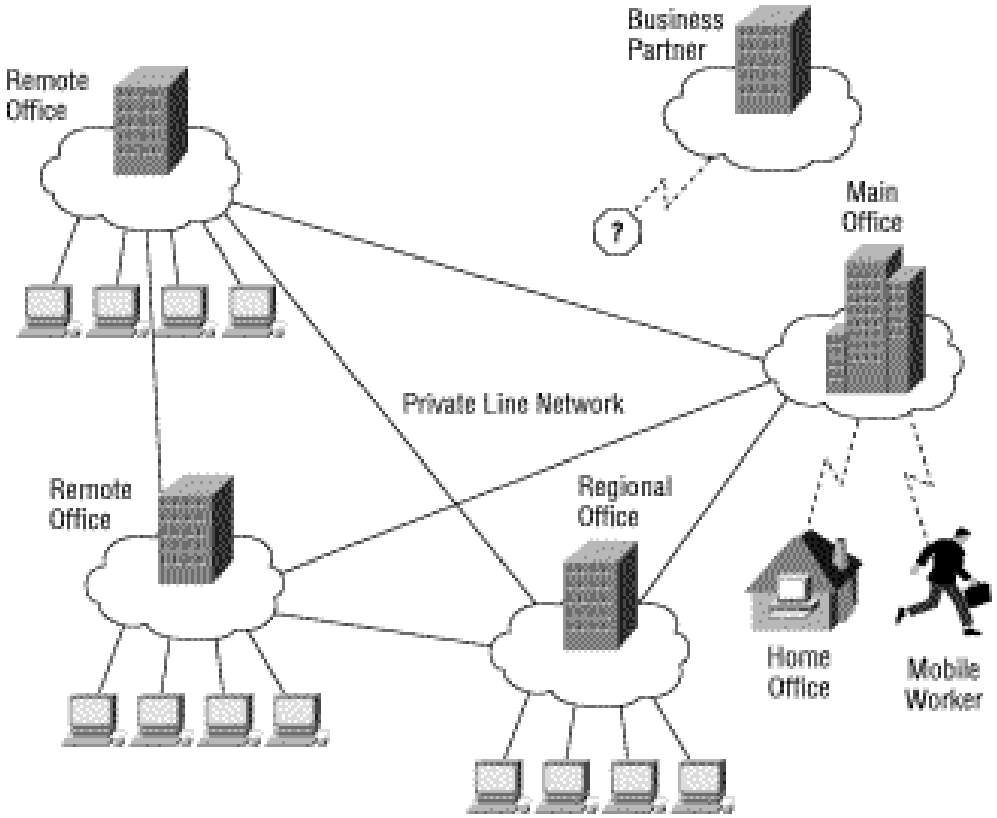


圖 3： Today's Corporate Network

遠端接取服務 VPN(Remote Access VPN)

遠端接取服務 VPN 可提供機動用戶或 telecommuters 藉由 ISP 提供之 VPDN 功能，使用者可經由 ISP 網路之 LAC(Layer-2 tunnel Access Client) 與企業的 LNS(Laye-2 tunnel Network Server) 連結，以 L2TP(Layer-2 Tunneling Protocol)，PPTP(Point-to-point Tunneling Protocol)或 IPSec tunnel 連接至企業內網路或透過授權連至企業間網路，如圖四所示。

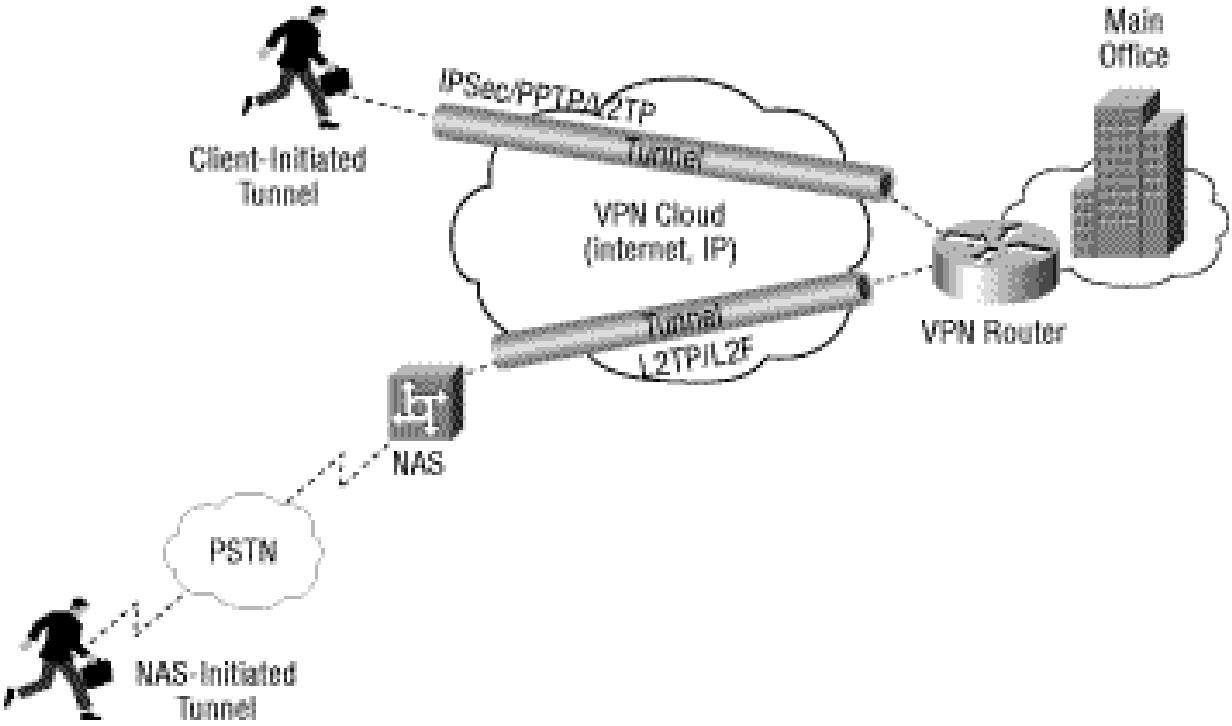


圖 4： 遠端接取服務(Remote Access)VPN

企業內網路(Intranet)

企業內網路提供企業總部與各分公司間的基礎網路服務，總部與各分公司間藉由 ISP 提供之 VPN 技術：Layer-2 switching (如 Frame Relay，ATM 等)，Layer-2 tunnel (如 GRE tunnel，IP-over-IP tunnel)，IPSec tunnel 或 MPLS VPN (RFC-2547bis)等彼此形成一虛擬的私有專

用網路，如圖五所示。.

各 VPN 所用技術之比較如表一所示。

Table 1: Comparison of Network Transport Infrastructures

Characteristic	Frame Relay	Internet	IP-VPN
Ubiquity	Low	High	Moderate
Cost	Moderate	Low	Moderate
Inherent Security	High	Low	High
Performance	High	Low-moderate	High
Guaranteed Service Levels	Yes	No	Yes

不同的 VPN 可根據不同的需求與提供不同的 QoS(如頻寬， packet loss rate)或 SLA(如 Mean-time-between-repair, Throughput， Round-trip delay 等)。

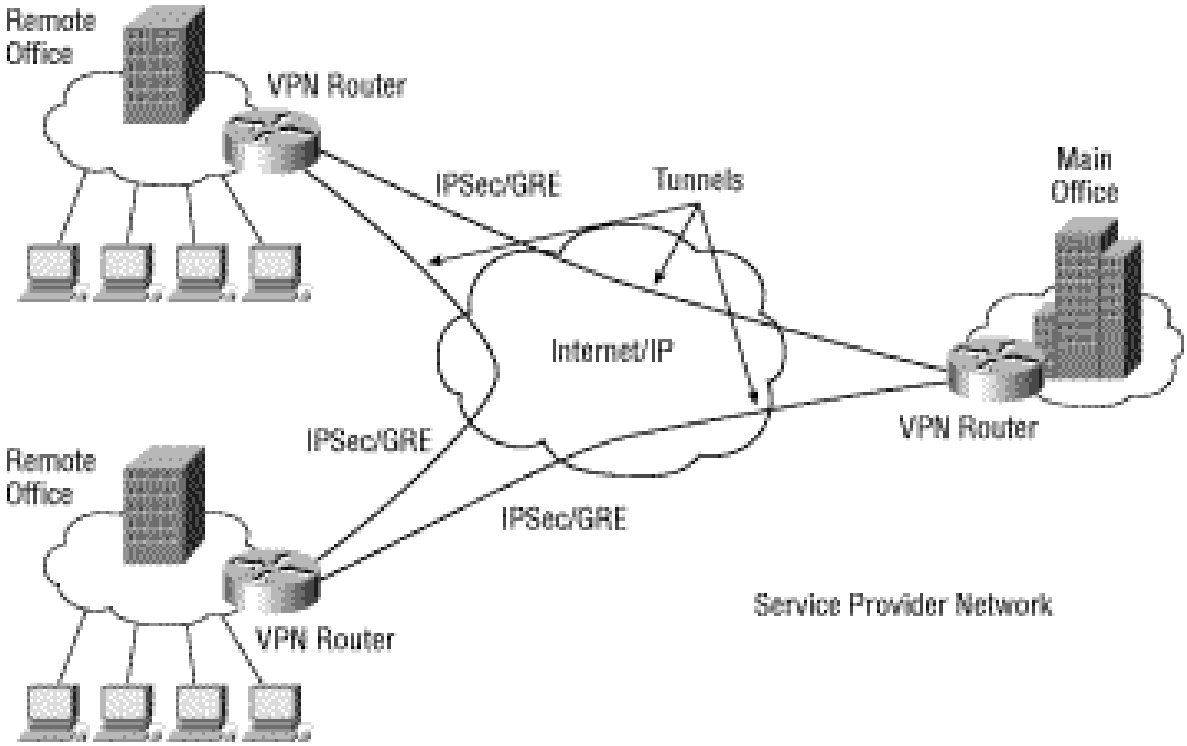


圖 5： 企業內網路應用架構

企業間網路(Extranet)

企業間網路的設計與應用架構與企業內網路與遠端接取服務 VPN 大致相同，主要的不同在於企業間網路係提供不同企業的互連，在位址(IP addressing)與安全管理(AAA，Authentication Authorization Accounting)不同於企業間網路的建置，應用架構如圖六所示。

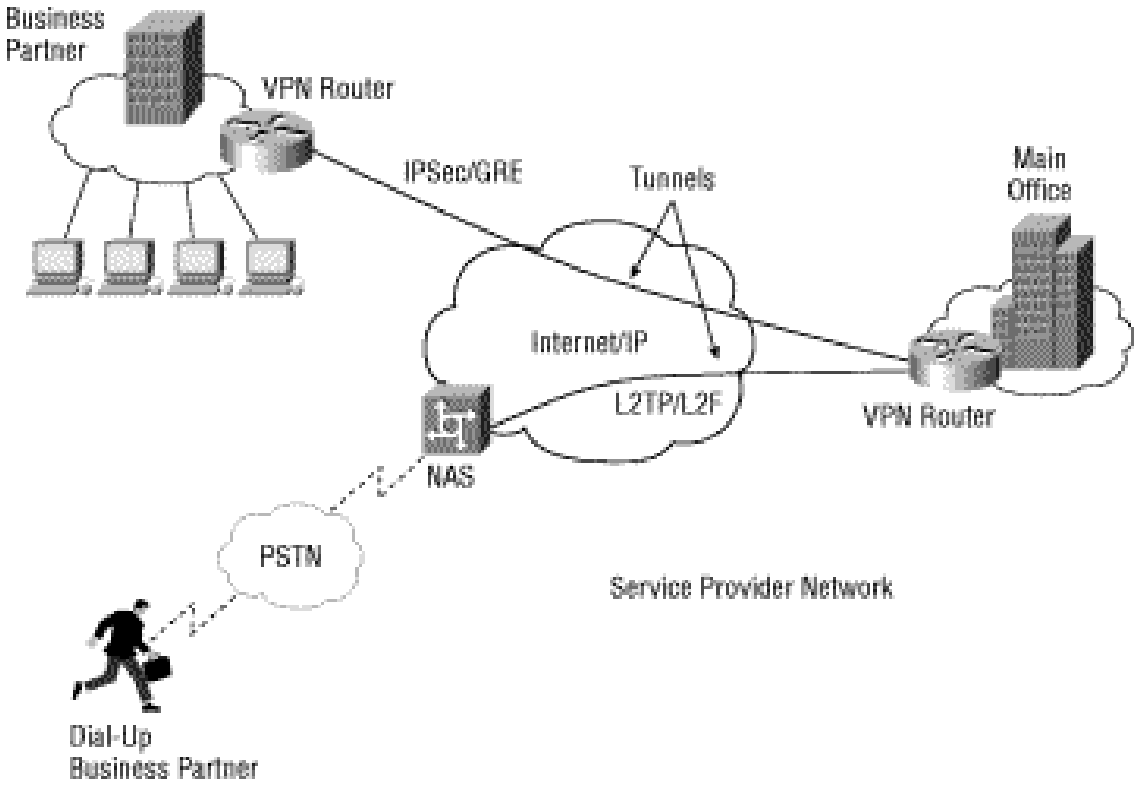


圖 6： 企業間網路 VPN

VPN 網路安全

VPN 網路安全是決定 VPN 建置成效的重要指標之一，本節就目前所事使用的安全機制作一簡述.

1. Layer-2 Tunnels

Tunnel 係在 connectionless 的 IP 網路中提供一點對點的邏輯通路(logical， point-to-point connections).在 tunnel 中可額外使用加密的方式(tunnel password)將 tunnel 的目地點予以確認。

2. IPSec (IP Security)

IPSec 一般用於 layer-2 tunnel(如 L2TP， PPTP， L2F 等)的資料加密，所使用的演算法有：Data Encryption Standard (DES)， triple-DES (3-DES)， 另針對 client 端使用 Microsoft 的 Point-to-Point Encryption

(MPPE)可選擇 40/128-bit RC4 加密。

3. 資料內容確認(Packet Authentication)

資料內容確認係用以防制內容遭篡改的封包進入系統造成損失，在 IPSec 的技術中，確認表頭(Authentication Header，AH)可用以避免遭修改的封包被傳遞，另外， 選則不同的表頭加密演算法(Encapsulation Security Protocol，ESP)，如 Message Digest 5 (MD5)、secure hash algorithm (SHA) 等皆可進一步保護在 Internet 上資料傳遞的正確性。.

4. 使用 Firewalls， IDS 與安全查核(security auditing)

正確使用 Firewalls 可避免 packet spoofing，smurf attack 與 DDoS 等現今頻發的系統攻擊，而 IDS 藉由訊務行為(signature)的分析可進一步擴展安全的防護，最後，經常性的安全查核可即早發現潛伏的入侵威脅。

5. 使用者身份確認

目前常用的使用者身份確認的機制為 AAA(authentication，authorization and accounting)系統，透過 RADIUS (Remote Access Dial-In User Service.)協定，使用者的 username 與 password 將被確認與授權執行特定功能，所有的行為將會被系統記錄，作為收費或安全查核的依據，針對提供遠端接取服務的企業而言，本項安全機制是不可或缺的。

下表所示為 Cisco System 針對 VPN 提供的技術與解決方案。

Feature	Function	Benefit
Cisco IOS	VPN devices run on Cisco IOS software.	• Ensures interoperability with all Cisco products • Leverages existing hardware infrastructure in deploying VPN solutions
Integrated Solution	This feature unites every aspect of the enterprise data network: intranet, extranet, and dial access.	• Reduces network complexity by creating a common platform for enterprise networking
Open Architecture	Cisco VPNs utilize Layer 2 and Layer 3 WAN facilities.	• Enables enterprises to choose a WAN transport that best fits their needs
Robust Security Features: Tunneling, Encryption, Packet/User Authentication, Firewall	This function enables enterprises to securely utilize service provider Layer 2 and Layer 3 back bones or the public internet for WAN bandwidth and dial access.	• Reduces bandwidth, management, and capital costs • Enables enterprises to focus on core business instead of managing a data network
Flexible, All-Encompassing Bandwidth Management/Qos	This feature manages network traffic based on priority and traffic patterns.	• Better manages expensive WAN bandwidth • Provides reliable throughput on Layer 2 and Layer 3 shared backbones
Integrates Single-Purpose Applications	This feature integrates firewall and bandwidth management on router	• Reduces network complexity • Lowers TCO
Enterprise Network Management	Integrated set of network management tools for configuring and monitoring the VPN.	• Ensures manageability across the enterprise VPN
Standards-Based Solution	This solution offers support for the following: IPSec, L2TP, GRE, DES, 3DES.	• Integrates with existing network infrastructure • Ensures logical technology migration path
Open Implementation Architecture	Cisco VPNs can be implemented in software or hardware.	• No forklift upgrades required • Preserves investment in networking gear
Strong Relationships with Service Providers	Cisco provides 80% of the networking equipment used on the Internet	• High degree of feature integration across service provider WAN infrastructures

建置新一代 VPN 的技術-MPLS(Multi-Protocol Label Switching)

市場綜述

根據 Yankee Group 預測：至 2004 年為止，百分之 90 的企業將依企業與資料通信需要使用 VPN。這對於服務供應者而言，代表一個潛在的營收利基，服務供應者認識到他們自己必須以服務水準(SLA)的區隔性以獲取這個市場。新一代的 VPN 技術也提供一個解決方案，允許服務供應者對顧客提供更全方位的網路服務。

下一代的 VPN 網路的核心技術

MPLS(Multi-protocol Label Switching)技術的出現係作為下一代的VPN網路的核心技術，特別是在高速的光傳輸網路中，以MPLS為主的VPN允許服務供應者減少顧客連網複雜性並降低通信費用以供應企業更多樣化的通信基礎網路。 MPLS為主的VPN解決了在VC為主或IP-tunnel式VPN在peer adjacency與scalability的瓶頸。

MPLS 為主的 VPN 使用"同儕(peer)"模型，這最終將代替"覆蓋(overlay)"模型(參見下面的圖 7)。雖然以覆蓋模型建構的 VPN 今天較為普遍，但是這類型的技術係基於點對點的連線建立，而非基於同質網路的建構，這將限制大規模的 VPN 網路服務的部署。

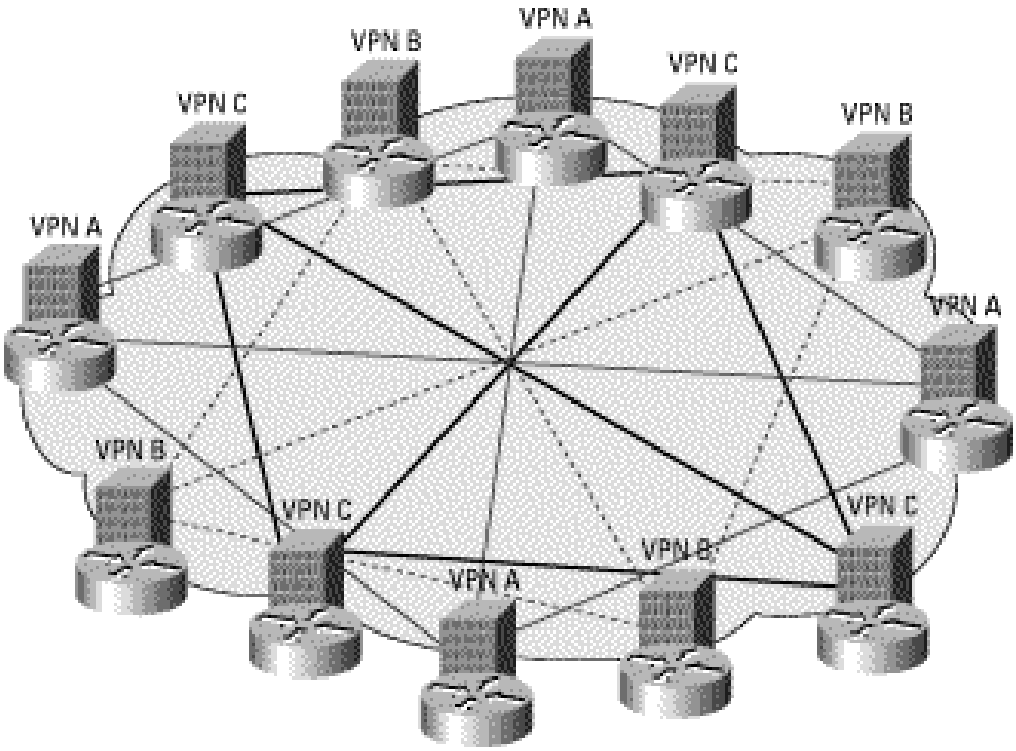


圖 7： VPN Overlay Network

MPLS為主的VPN使用同儕模型和layer-3 connectionless的架構特點(如圖8所示)，特別適合應用於具高度擴展性的VPN架構。

在同儕模型中，客戶端設備(Customer-edge router， CE router)僅須與服務供應者的接取設備(Provider-edge router， PE router)建立連接，而不用與所有其它點的客戶端設備建立連接。layer-3 connectionless的特點則可以讓VPN的建立如同Internet的架構一般，而不需建立layer-2的VC(Virtual Circuit)或tunnel。

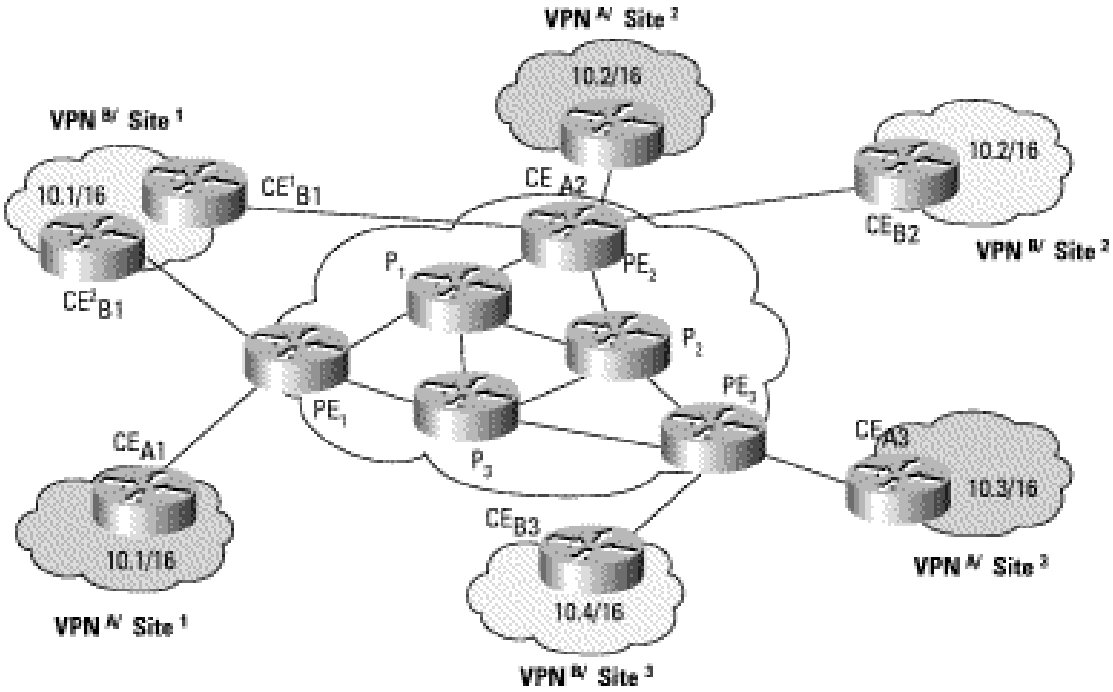


圖 8： BGP/MPLS VPN Peer Model

MPLS VPN 架構

MPLS VPN 網路架構如圖 9 所示，在網路的邊緣是 CE Router， CE Router 是客戶網路的一部分，且沒有任何的 VPN 介面與協定功能。PE Router 是專門處理 MPLS VPN 的設定與相關功能，PE Router 從 CE Router 那裡獲得到路由的資訊，並透過服務供應者的 MPLS 骨幹網路傳遞至所允許的 PE Router。在骨幹網路的 P Router(Provider Router)，或者 LSR(Label Switching Router)則專門執行 layer-3 MPLS 封包的傳遞。

在骨幹網路的 P Router 沒有任何的 VPN 介面與協定功能，也全然不知特定用戶的 VPN 資訊，因此可提供更好的擴展性，在 PE Router 僅需針對直接連接(directly connected)的 VPN 向其它所屬的 PE Router 發送路由資訊即可。

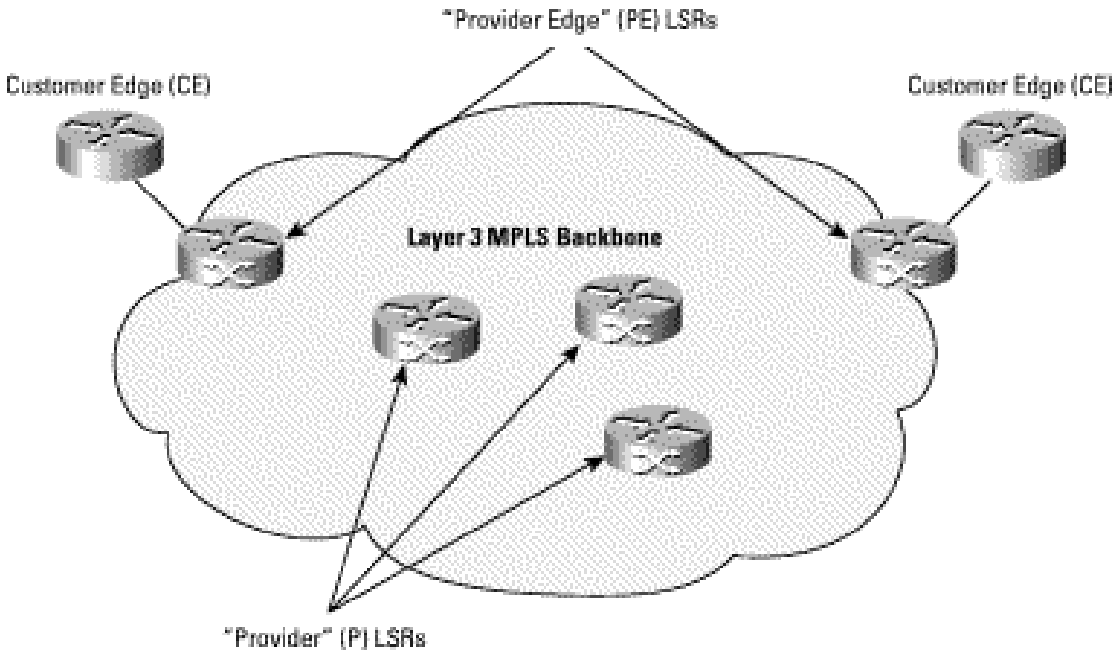


圖 9： MPLS VPN Network

建構 MPLS VPN

MPLS VPN 網路有三個主要部分：

1． VPN route target communities屬性—同一VPN的所有成員皆具有同一組屬性。

2 .提供多協定的BGP延伸功能(Multi-Protocol BGP Extension)—MP-BGP對同一VPN群組的所有成員傳送VRF(Virtual Routing and Forwarding)資訊。

3 .MPLS Forwarding-透過服務供應者的骨幹網路在讓 VPN 的成員彼此互通.

MPLS CoS

服務等級品質(Class-of-Service，CoS)在網際網路通訊協定網路中賦予裝置優先處理網路中策略性優先訊務的功能。CoS機制提供網路

管理人員控制頻寬、延遲、jitter和網路中的包遺失率的能力。

以Cisco System的IOS(Internetworking Operating System)為例，其CoS功能可提供端對端的QoS的建立：

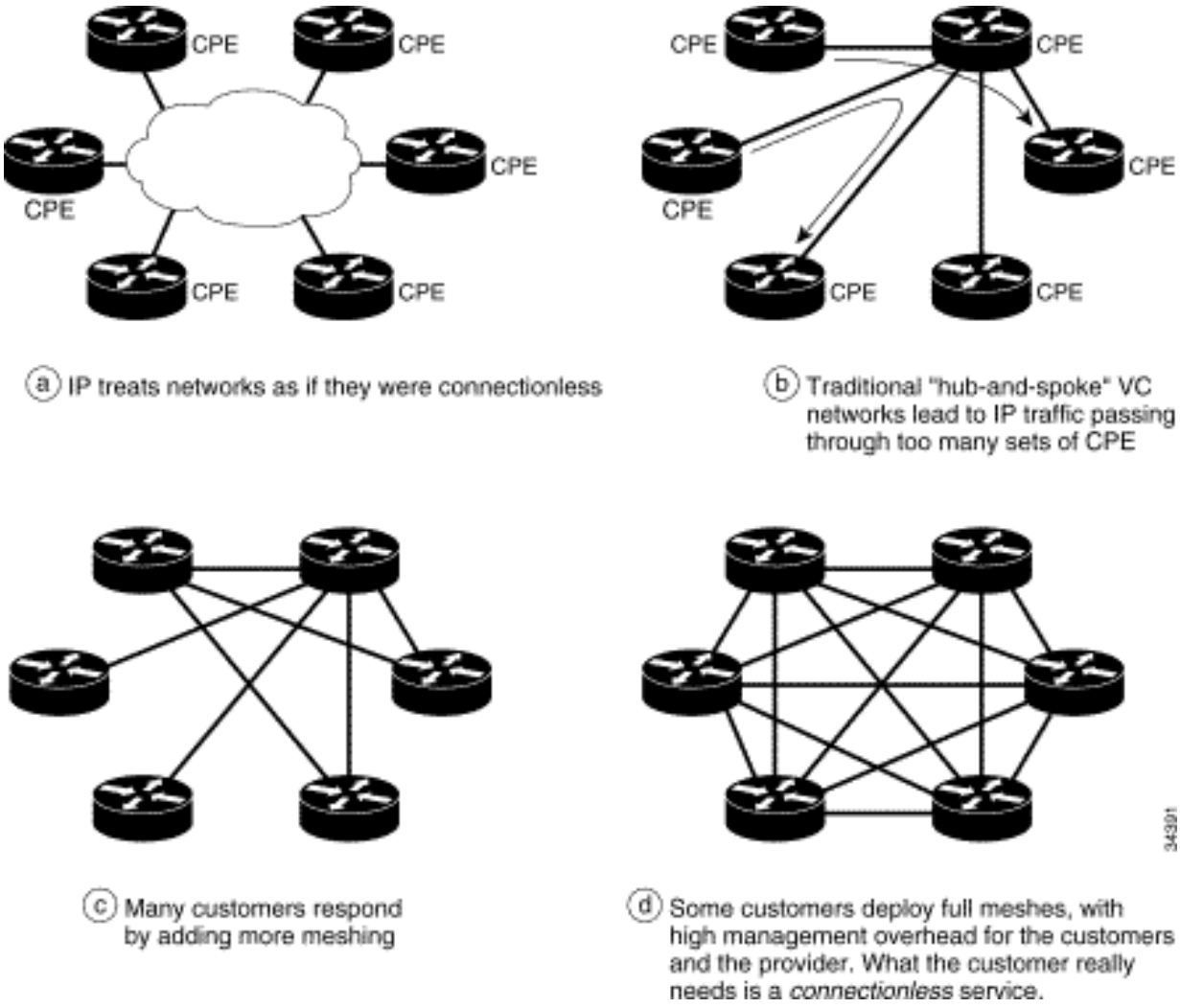
1. IP Precedence： 利用 IP header 中的三個位元提供八種不同的服務等級。
2. Committed Access Rate (CAR)： CAR 可用於管理特定訊務的頻寬使用量。
3. Weighted Random Early Detection (WRED)： WRED 利用先期的偵測以避免網路造成擁塞。
4. Class-Based Weighted Fair Queuing (CBWFQ)：CBWFQ 提供在 edge 端與骨幹中控制延遲的功能與 packet re-ordering 的能力。

與Overlay架構的網路管理比較，在MPLS VPN網路中，CoS的執行將使得其複雜性降低¸同時更有效的達成所需的服務品質。

Connectionless Traffic 的特性

圖10說明在一個hut-and-spoke架構中，中間的CPE將被用來轉送非本地的訊務，從而必須讓訊務越過虛擬電路兩次，這顯然不是很經濟的方法，這也意味著在中心點(hub)必須浪費頻寬作路由的轉接。

當VC-mesh的建立日漸複雜時，代表者routing table的維護與所需轉接非本地資訊的頻寬也跟著增加，此時，MPLS layer-3 connectionless的特點可有效的提升有效頻寬的使用，並簡化VPN routing的架構。



ⓐ IP treats networks as if they were connectionless

ⓑ Traditional "hub-and-spoke" VC networks lead to IP traffic passing through too many sets of CPE

ⓒ Many customers respond by adding more meshing

ⓓ Some customers deploy full meshes, with high management overhead for the customers and the provider. What the customer really needs is a *connectionless* service.

圖 10： How Connectionless Traffic Drives Meshing

Connectionless Traffic 在 QoS 的管理

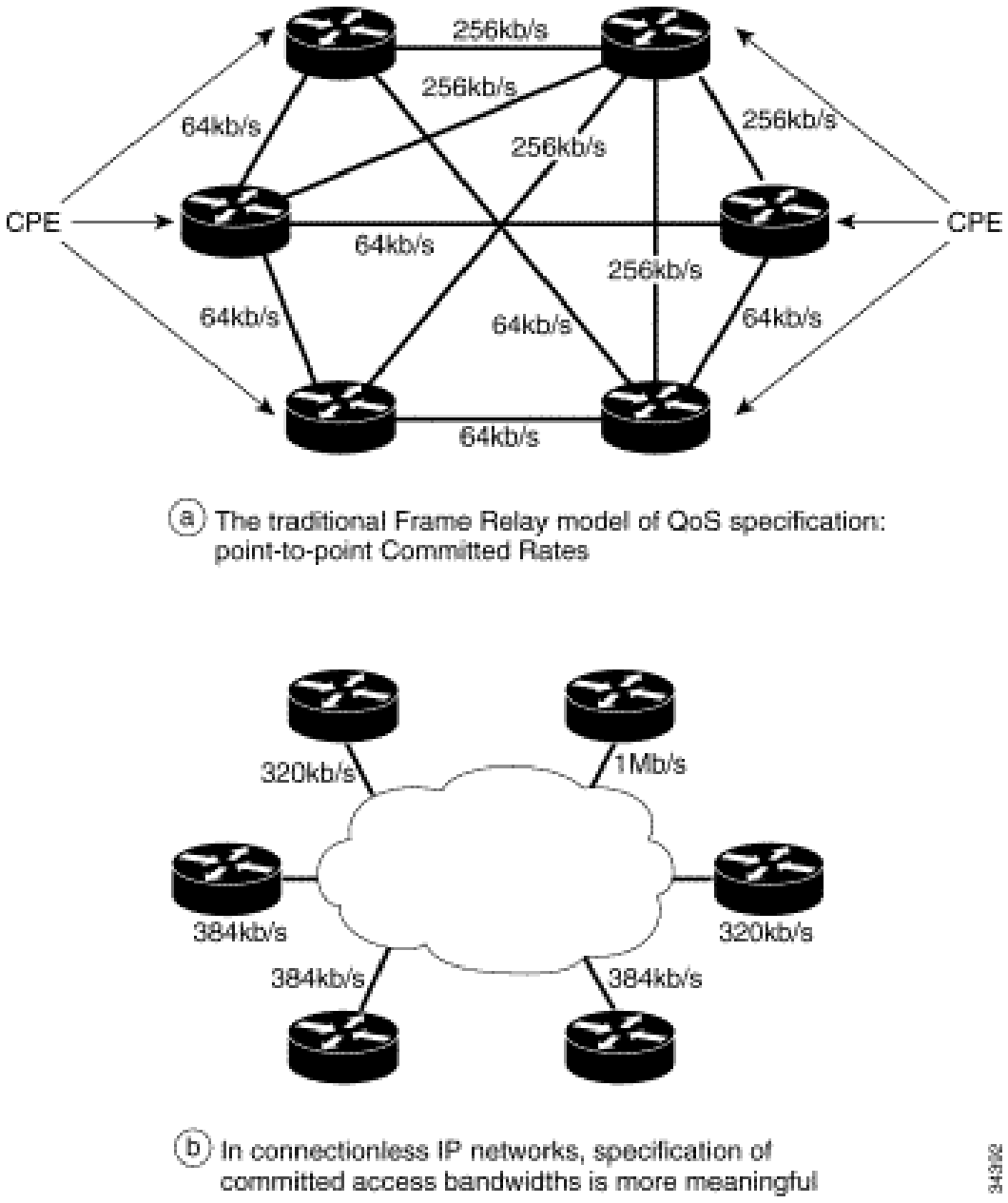


圖 11： Specifying Bandwidths for An IP Service

如圖 11 所示， 對於 connectionless 的網際網路通訊協定服務架構而言，QoS 需求可藉由加總的方式(aggregation)根據頻寬需要、主機或者 client 的數目估計而得， 這是使用新一代 VPN 的 QoS 管理機制的優勢之一。

具區隔性(differentiated)的 Quality of Service 管理

1. 提供約定的接取頻寬

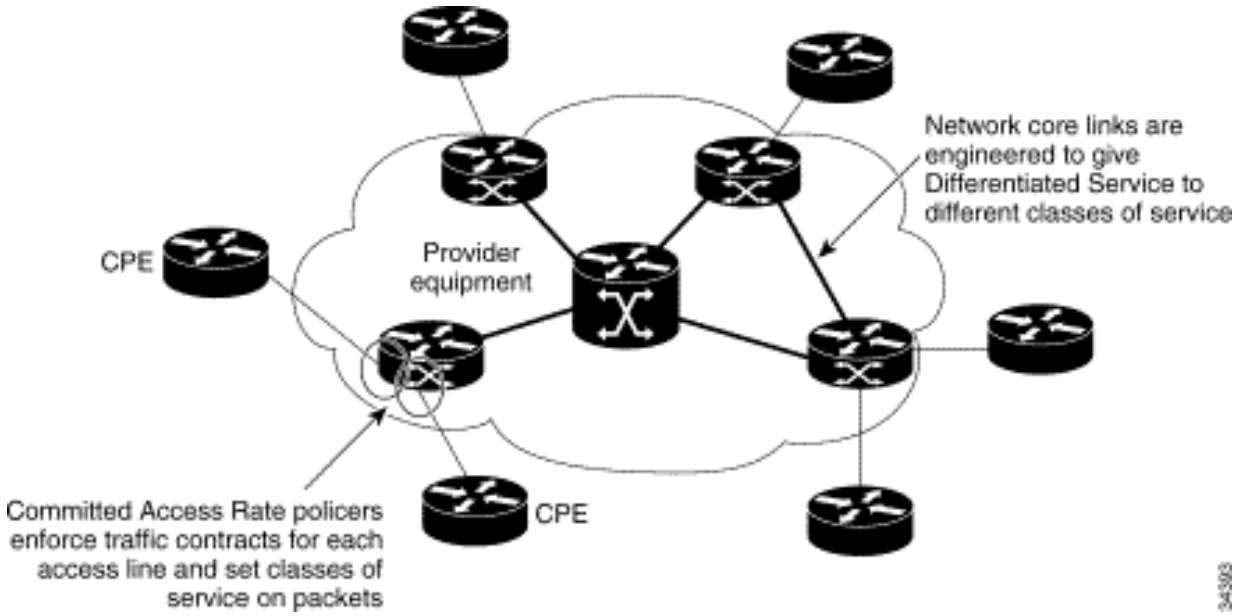


圖 12： Committed Access Rate Policers

利用圖 12 的 CAR policer 可有效控制客戶訊務的通信量, 並掌握網路的擁塞程度。

另外，服務供應者可利用 IP header 中的 Precedence 或 DS bits 提供 CoS. 將 CAR 的功能至於用戶端設背也可有效的落實 CoS 的服務品質，如圖 13 所示。

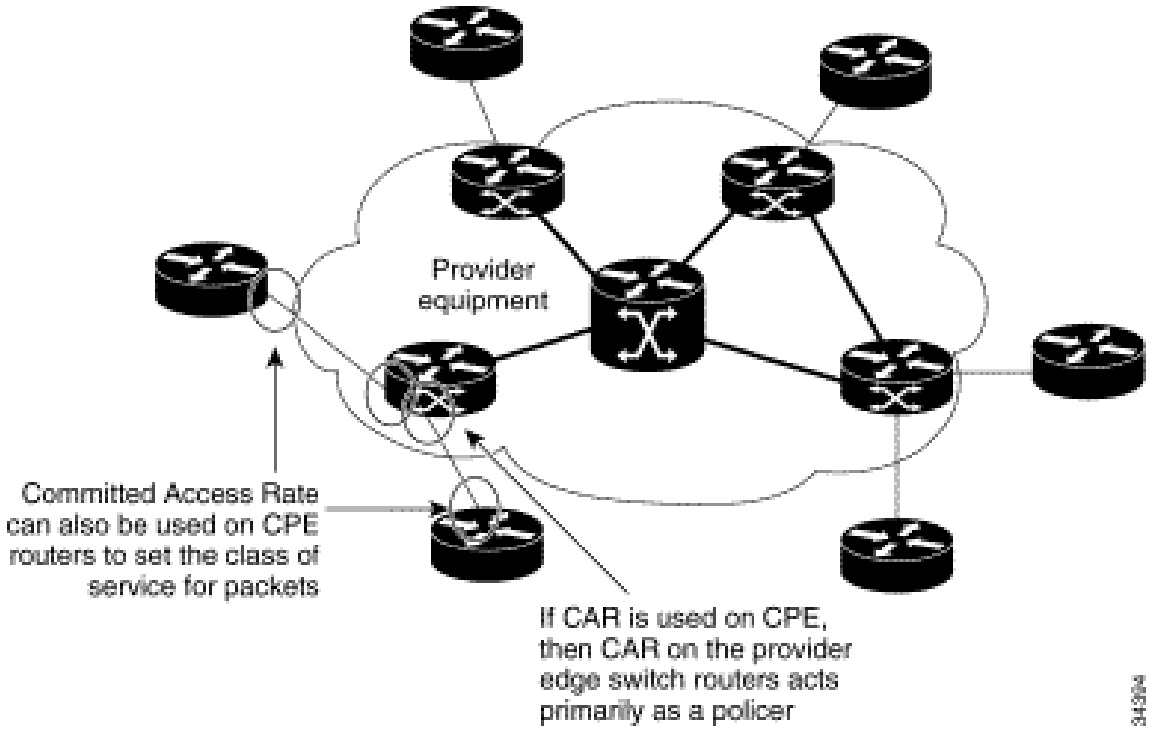


圖 13： Using CAR on Customer Premises

2. 使用 Best-Effort Traffic 提供約定頻寬

圖 14 所示為利用 Differentiated Services 針對重點訊務(premium traffics)提供 CoS，所示的範例為在一特定的鏈路中提供兩種 CoS 的訊務傳遞。

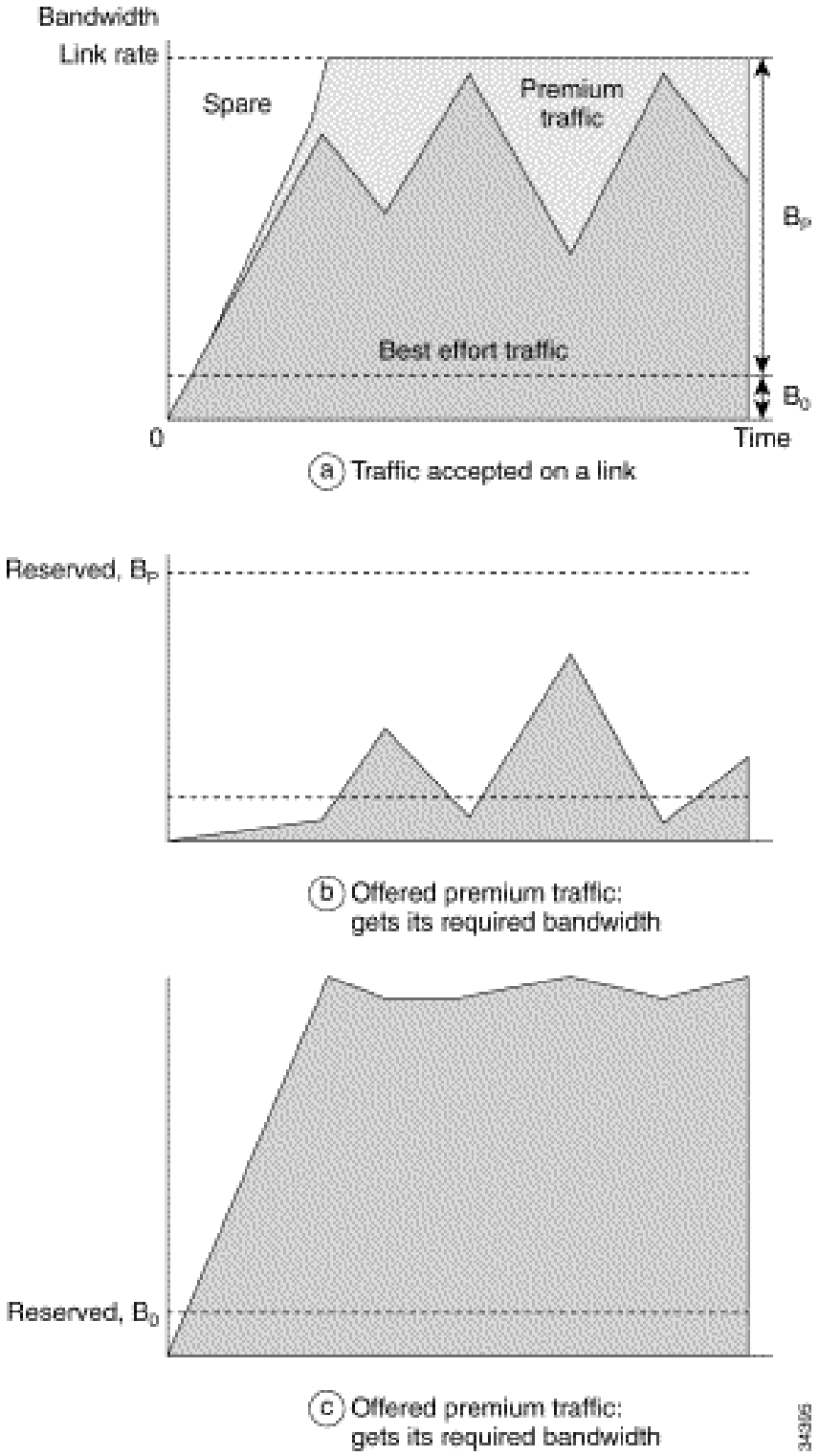


圖 14： Ensuring Access to Bandwidth Using Differentiated Services

3.DiffServ Per-Hop Behaviors 的探討

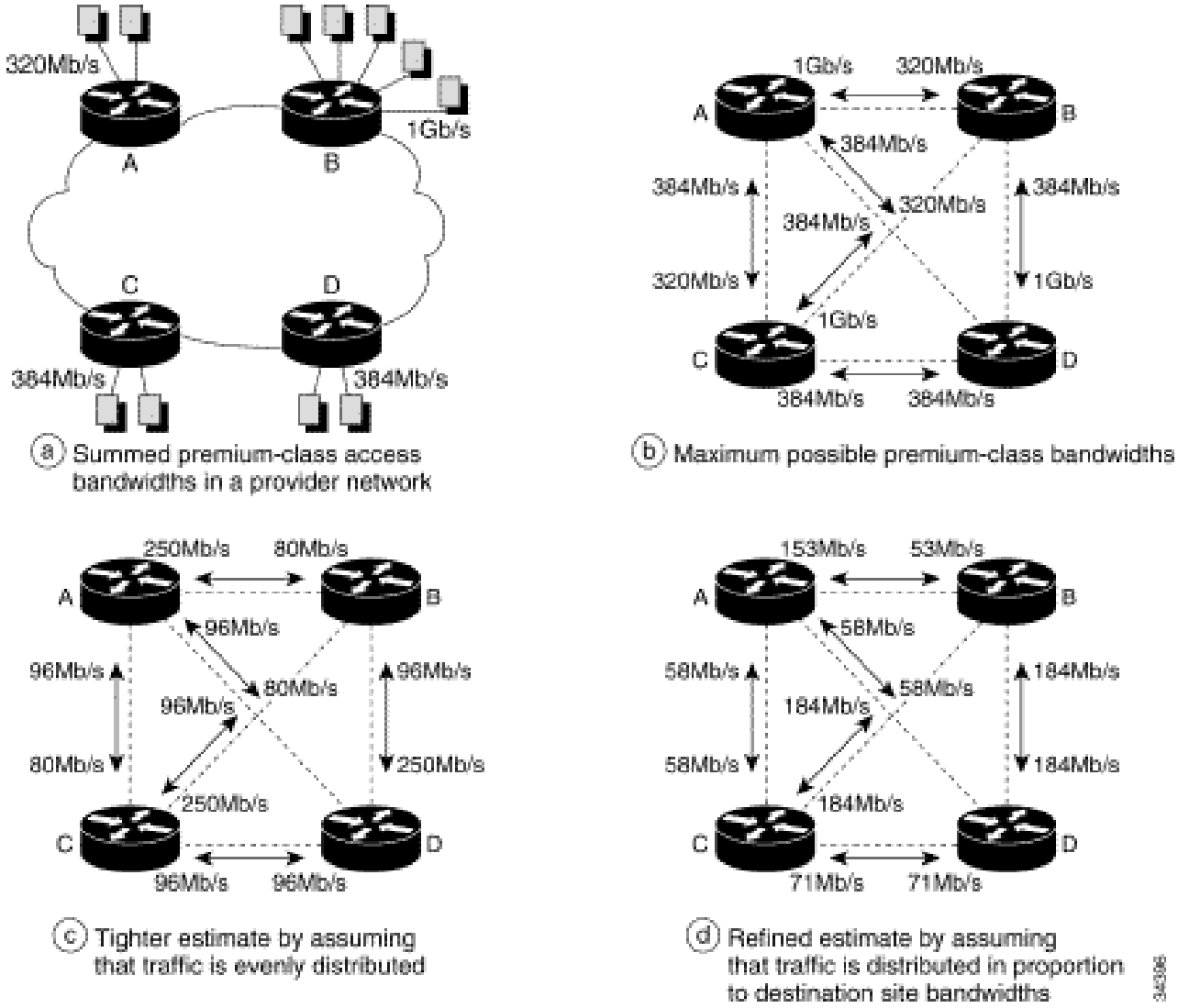


圖 15： Refining Estimates of Network Loads

DiffServ 係利用 queueing 的技術，如 Weighted Fair Queueing (WFQ)，對不同的 CoS 需求於封包傳遞路徑的設備中提供服務。圖 15(a)所示為同時載送重點訊務與一般訊務(best-effort traffics)的架構，在圖 15 (b) 說明實體網路與 LSR 中頻寬的配置，圖 15 (c)與(d)則把 routing 與 CoS 路徑的選擇一併納入成為最後的分析拓撲。

4. VC merging

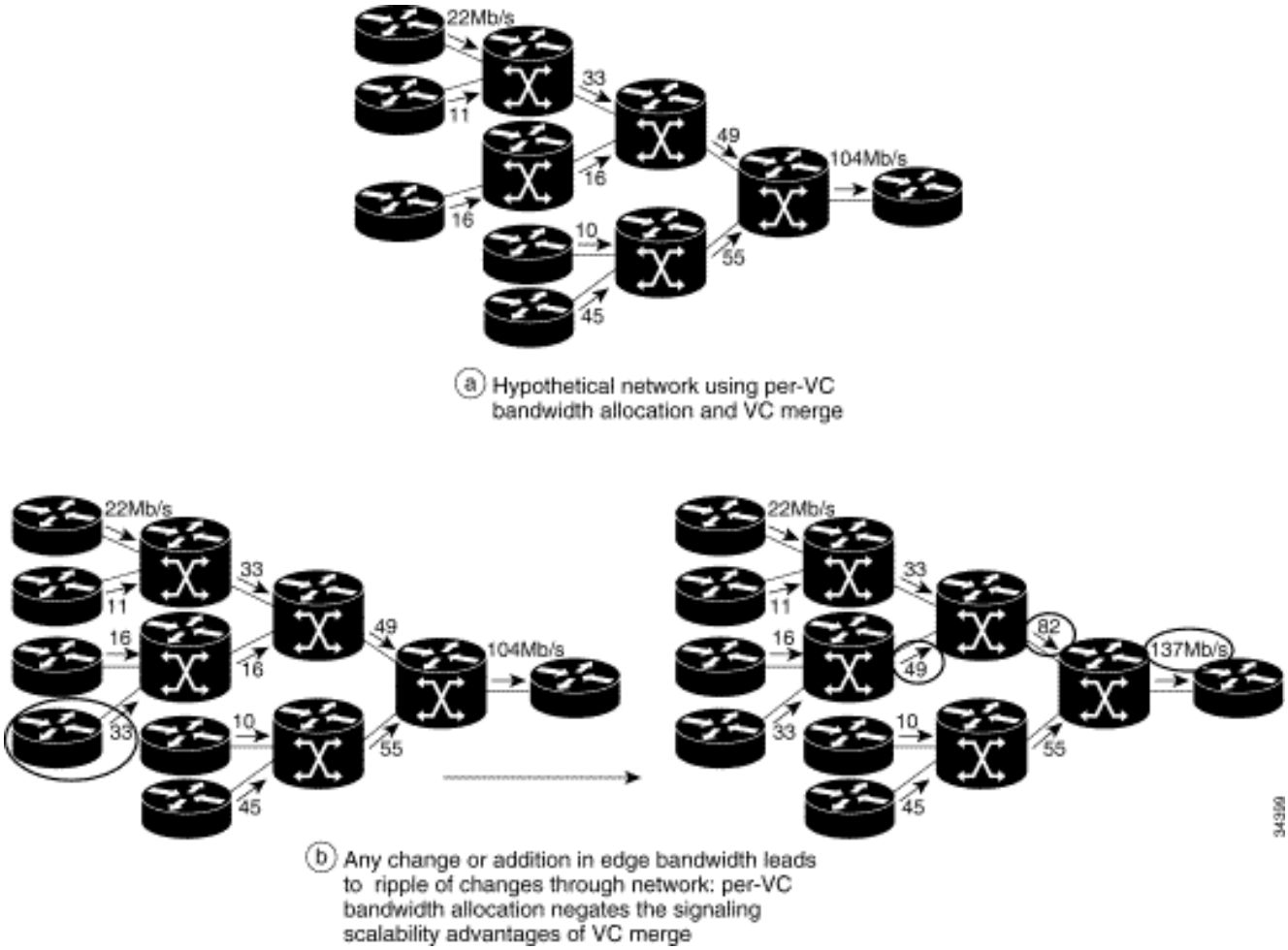


圖 16： Per-VC Service with VC Merge

利用 VC 合併功能(VC merge)，在 CoS-based 的 queueing 處理上要優於 per-VC queueing。就實務而言，相較於 per-VC queueing 在網路擴展性而言，VC merge 要擁有較好的能力(如圖 16 所示)。

MPLS Traffic Engineering

以MPLS Traffic Engineering優化訊務的範例如圖17所示。在圖17(a)中節點E和F間的平均負載是是百分之91，這代表即將有封包遺損失發生的情形，若利用MPLS Traffic Engineering，則可即早發現備用的

LSP鏈路以遠離可能擁塞的路徑。

例如， LSR A與LSR B 之間的 LSP 也許正在載送訊務。 MPLS Traffic Engineering試圖找到一或多路的備用LSP以疏解節點E和F間的平均負載，而不讓其它的鏈路因此而造成擁塞。

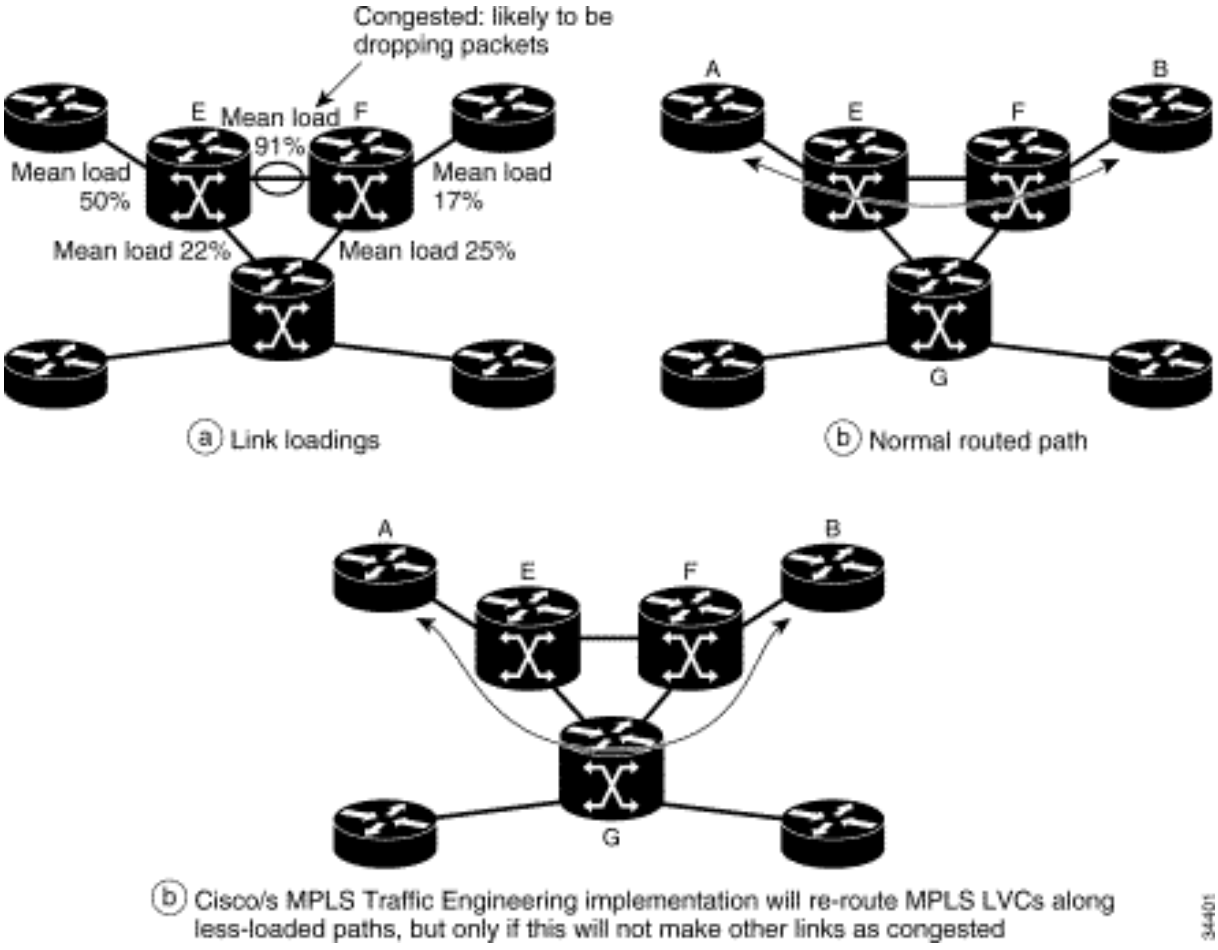


圖 17： Reoptimization of Traffic Using MPLS Traffic Engineering

MPLS VPN 的 Quality of Service

MPLS VPN與任何其他 MPLS 網路有相同的 QoS 選擇。各VPN的所在地點皆可預訂不同服務等級的服務規定，且服務供應者能夠提供對於這些等級提供服務水準協議(SLA)。如同圖18(b)所示，如果有

二個相同的起點與終點的點對點 LSP，則可如圖18(c)所示聚集至同一路LSP。

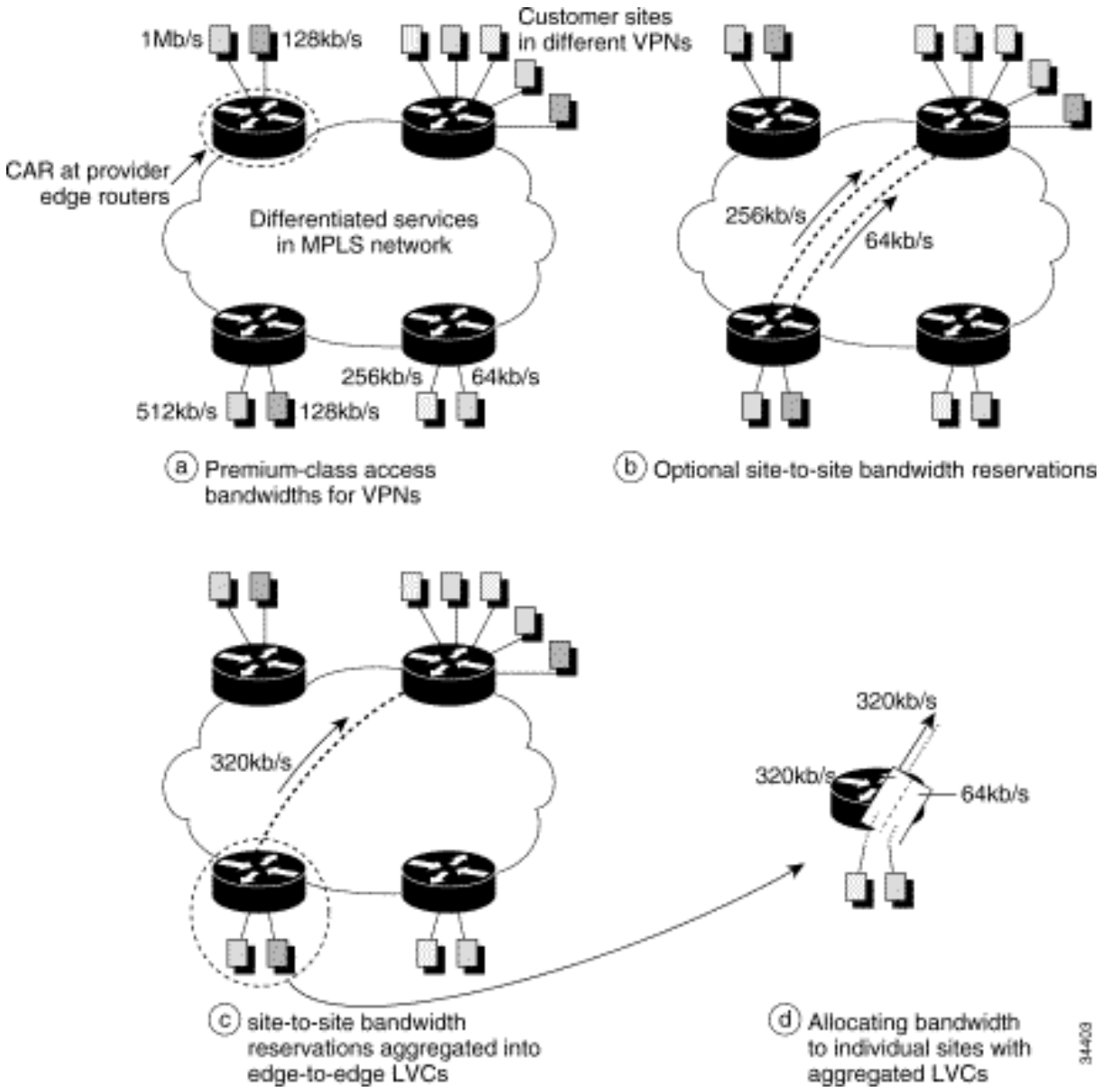


圖 18： Quality of Service in Virtual Private Networks

應用 CAR(Committed Access Rate)的功能可針對客戶所需要特定的訊務給予優先處理或保證頻寬，如圖 19 所示。

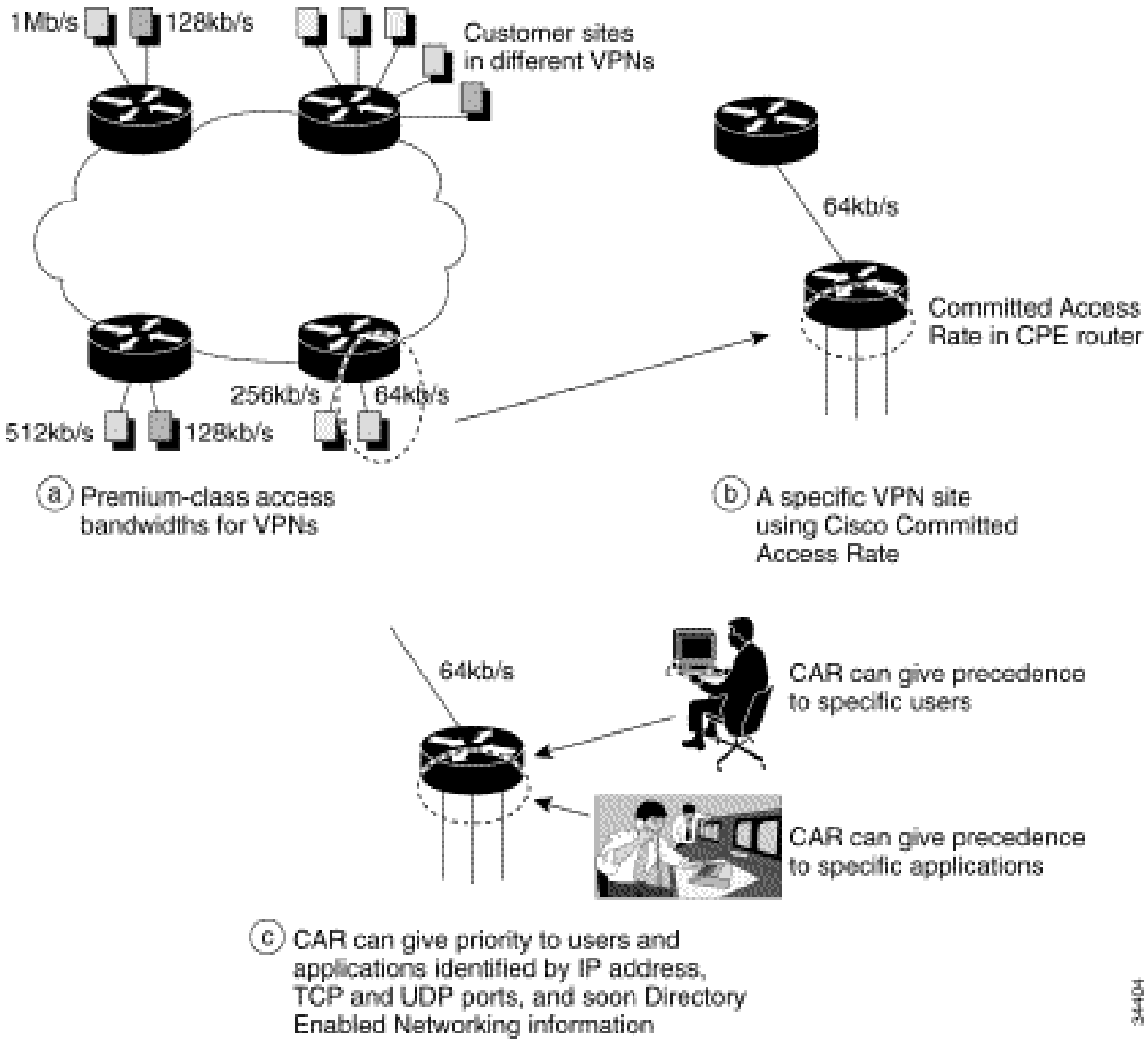


圖 19： Providing Bandwidth to Specific Users and Applications in Virtual Private Networks Discard Policies

當網路發生擁塞時，網路設備必須決定丟棄某些封包以保護其它部份不被波及，網路設備利用同一佇列中不同 CoS 封包的訊務流量，可使用不同的先期封包丟棄策略(Random Early Discard，RED)，此即所謂的 Weighted RED (WRED)。Weighted RED 運作原理說明詳圖 20(d)。

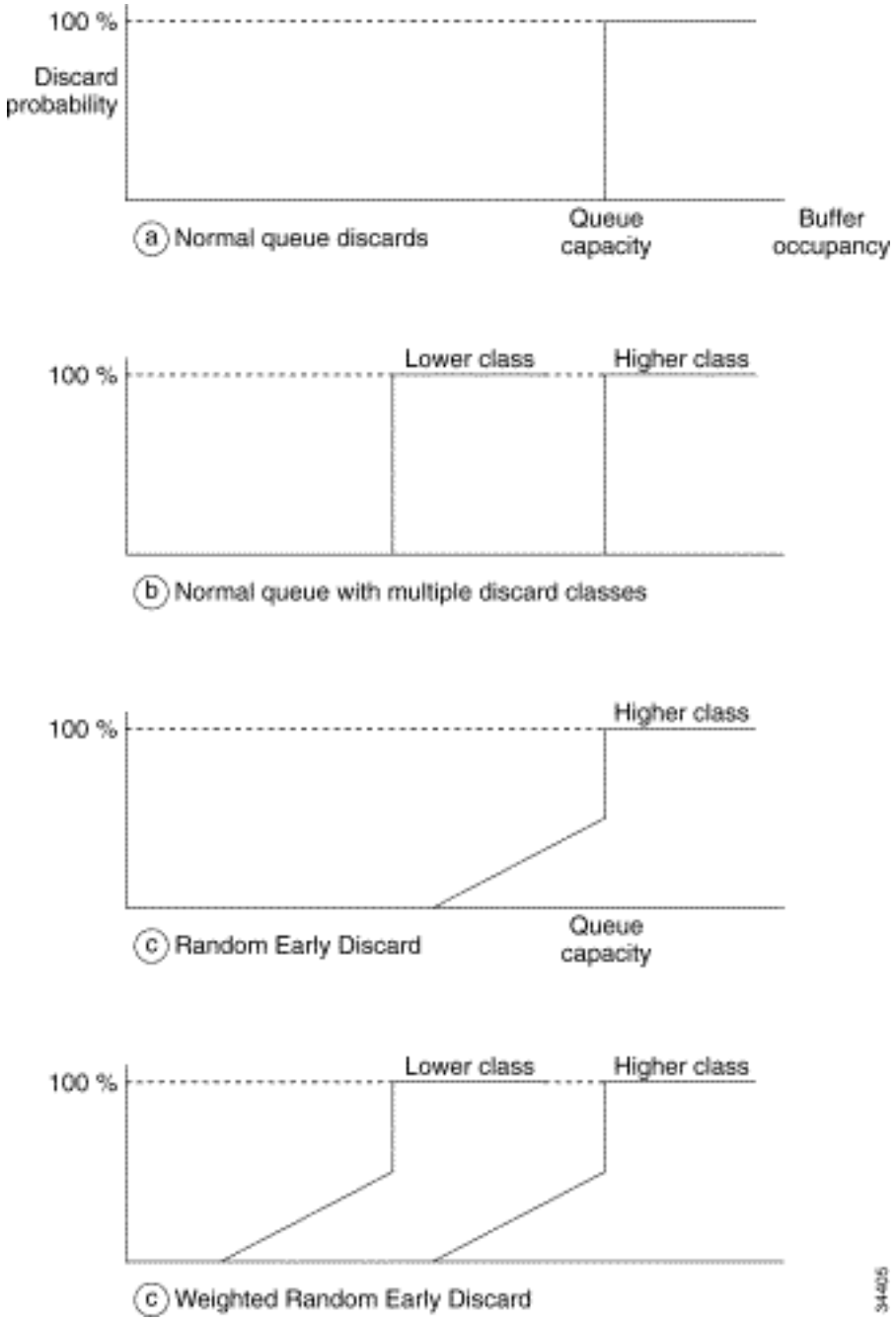


圖 20： Discard Policies

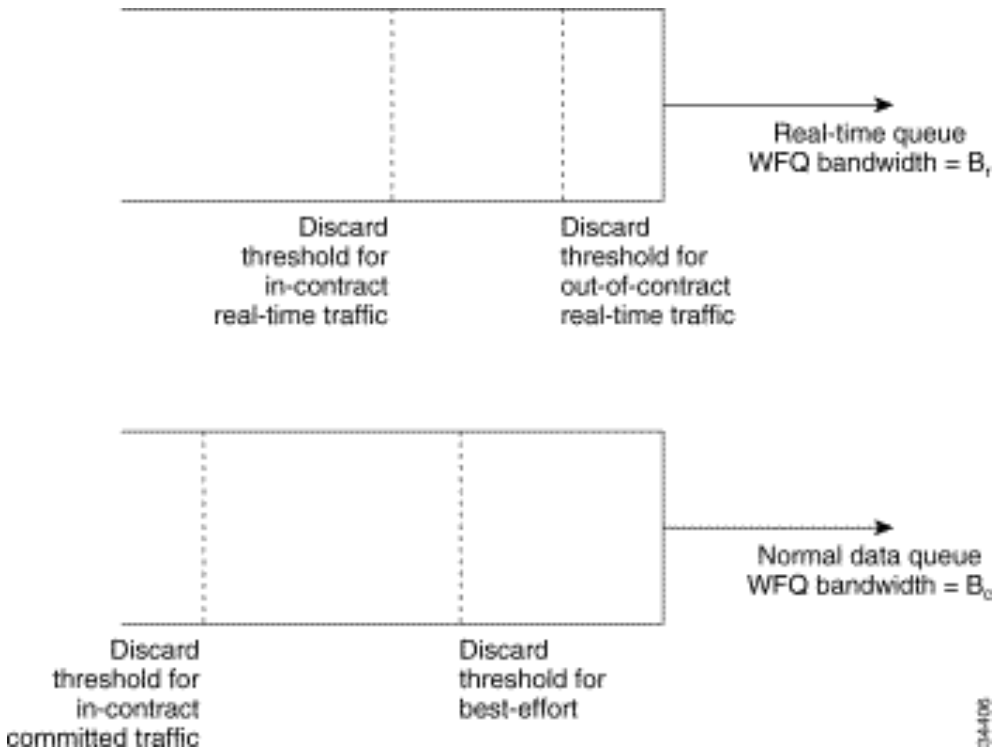


圖 21：Example of Combining Weighted Fair Queueing and Differential Discards

圖 21 的範例顯示當使用不同的 queue 與封包丟棄策略，頻寬的互動與資源的配置情形(如圖 22 所示)。.在圖 22 中，real-time 的訊務，若有需要，可使用 Br 的頻寬，一般訊務最多只能使用到 Bc 的頻寬。

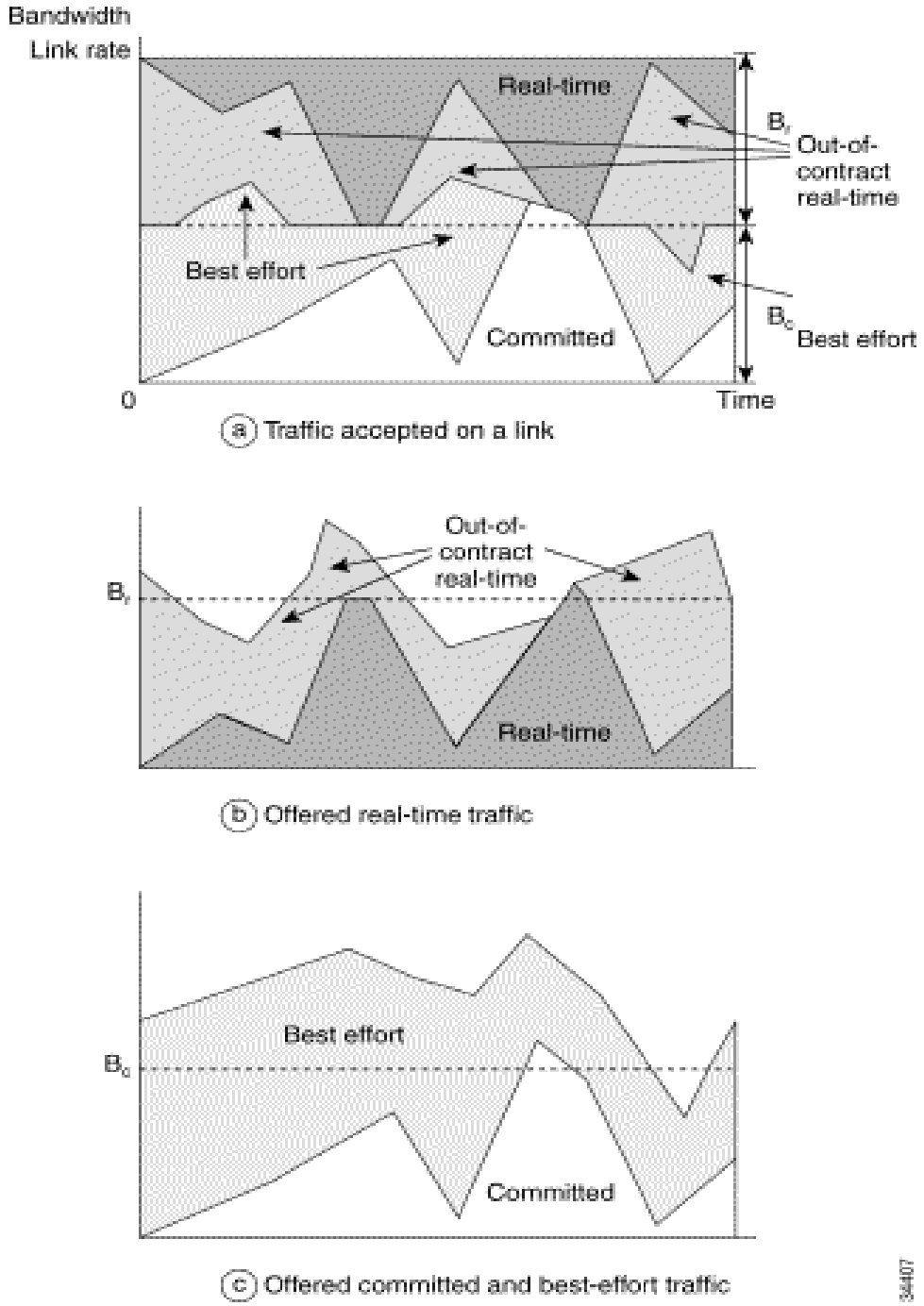


圖 22： Effects of Combining Weighted Fair Queueing and Differential Discards

服務水準管理(Service-Level Management)

服務水準協定(Service Level Agreement，SLA)的定義

服務水準協定是一個服務水準合約(Service Level Contract， SLC)的一個關鍵部分，服務水準合約係由服務供應者指定對終端用戶服務的連通性和效能的協議。 服務水準合約通常包含若干SLA，任何特定服務水準協定的缺失皆可能違反全部的服務水準合約，服務水準的管理即用以管理構成一個服務供應者簽訂合約的規範工具。

根據 Forrester Research 的研究顯示：百分之 70 的網路管理人員打算於 2001 前執行 SLA。而根據 Infonetics：有百分之 46 的網路管理人員則計畫以 per-tunnel 的基礎執行 SLA(參考圖 25).

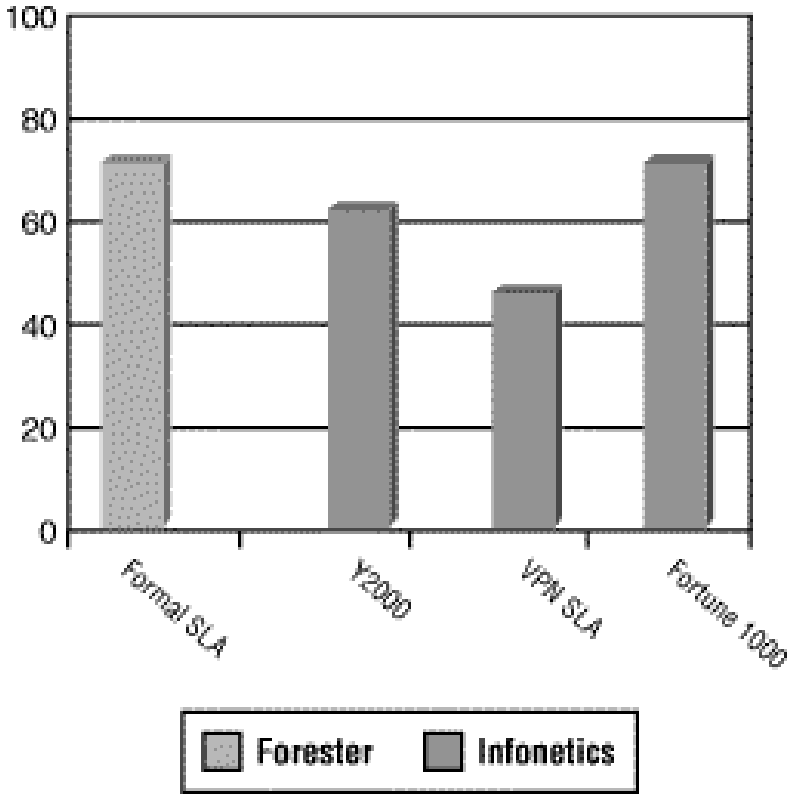


圖 25： Enterprise Customer Plans to Implement

在給定的幾個服務部分裡， 服務水準的管理定義了提供送服現務水準協定所需要的服務水準管理(SLM)。不同供應商針對管理服務水準皆有不同定義和執行能力，唯一對顧客有效的的定義是：只有在端對端應用層的連通性、效能和有效度的管理，對客戶而言，才是務實的訴求。

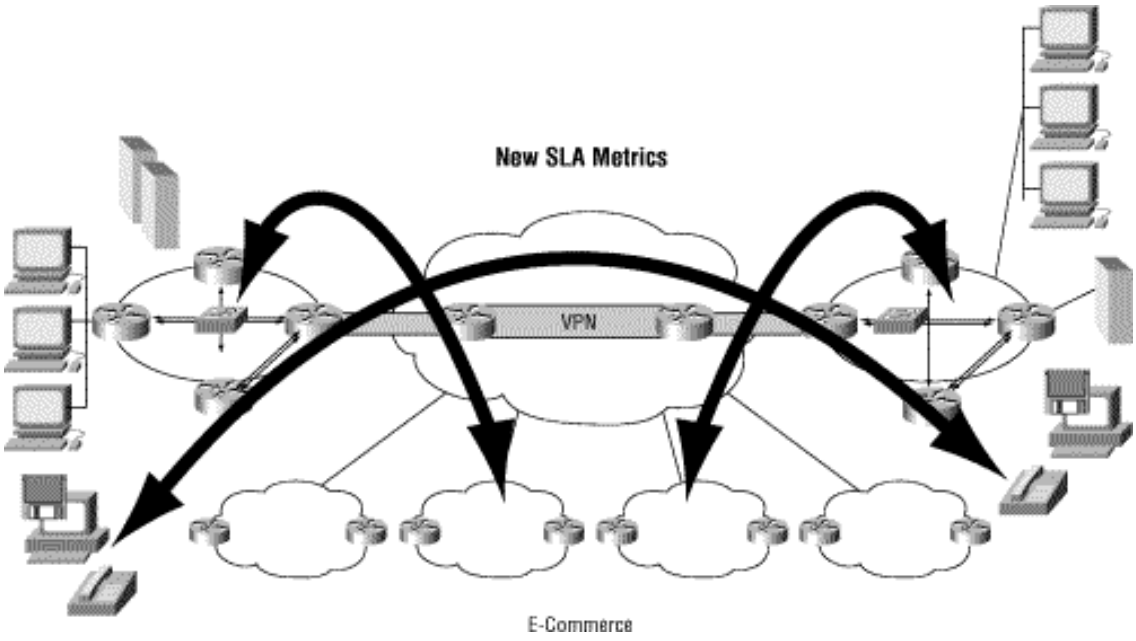


圖 26： Effective SLM Requires Monitoring and Management of all Aspects of the Infrastructure for Service Delivery. Collecting Data through the Stacks

回 應 式 的 服 務 水 準 管 理 (Reactive Service Level Management)

一般而言，企業網路的服務水準的管理可藉助諮詢中心(Help-desk)的資料庫統計報表和週期性的記錄稽而建立。以下的例子藉由不同事件所代表的嚴重性(Severity)開始說明，如何以層層管理的方式對事件做出適當的回應。

Severity 1	Severity 2	Severity 3	Severity 4
Severe business impact • LAN user or server segment down • Critical WAN site down	High business impact through loss or degradation, possible workaround in place • Campus LAN down; 5-99 users affected • Domestic WAN site down • International WAN site down • Critical performance impact	Some specific network functionality is lost or degraded, such as loss of redundancy • Campus LAN performance impacted • LAN redundancy lost	A functional query or fault that has no business impact for the organization

Support Tier	Responsibility	Goals
Tier 1 Support	• Full-time help desk support • Answer support calls, place trouble tickets, work on problem up to 15 minutes, document ticket and escalate to appropriate tier 2 support	Resolution of 40% of incoming calls
Tier 2 Support	• Queue monitoring, network management, station monitoring • Place trouble tickets for software identified problems • Implement • Take calls from tier 1, vendor, and tier 3 escalation • Assume ownership of call until resolution	Resolution of 100% of calls at tier 2 level
Tier 3 Support	• Must provide immediate support to tier 2 for all priority 1 problems • Agree to help with all problems unsolved by tier 2 within SLA resolution period	No direct problem ownership

Problem Severity	Help Desk Response	Tier 2 Response	Onsite Tier 2	Hardware Replacement	Problem Resolution
1	Immediate escalation to tier 2, network operations manager	5 minutes	2 hours	2 hours	4 hours
2	Immediate escalation to tier 2, network operations manager	5 minutes	4 hours	4 hours	8 hours
3	15 minutes	2 hours	12 hours	24 hours	36 hours
4	15 minutes	4 hours	3 days	3 days	6 days

Elapsed Time	Severity 1	Severity 2	Severity 3	Severity 4
5 minutes	Network operations manager, tier 3 support, director of networking			
1 hour	Update to network operations manager, tier 3 support, director of networking	Update to network operations manager, tier 3 support, director of networking		
2 hours	Escalate to VP, update to director, operations manager			
4 hours	Root cause analysis to VP, director, operations manager, tier-3 support, unresolved requires CEO notification	Escalate to VP, update to director, operations manager		
24 hours			Network operations manager	
5 days				Network operations manager

Network Device or Link Down	Detection Method	5 x 8 Notification	7 x 24 Notification	5 x 8 Resolution	7 x 24 Resolution
Core LAN	SNMP device and link polling, traps	NOC creates trouble ticket, page LAN-duty pager	Auto page LAN duty pager, LAN duty person creates trouble ticket for core LAN queue	LAN analyst assigned within 15 minutes by NOC, repair as per service response definition	• Priorities 1 and 2 immediate investigation and resolution • Priorities 3 and 4 queue for morning resolution
Domestic WAN	SNMP device and link polling, traps	NOC creates trouble ticket, page WAN duty pager	Auto page WAN duty pager, WAN duty person creates trouble ticket for WAN queue	WAN analyst assigned within 15 minutes by NOC, repair as per service response definition	• Priorities 1 and 2 immediate investigation and resolution • Priorities 3 and 4 queue for morning resolution
Extranet	SNMP device and link polling, traps	NOC creates trouble ticket, page partner duty pager	Auto page partner duty pager, partner duty person creates trouble ticket for partner queue	Partner analyst assigned within 15 minutes by NOC, repair as per service response definition	• Priorities 1 and 2 immediate investigation and resolution; • Priorities 3 and 4 queue for morning resolution

Network Area/Media	Detection Method	Threshold	Action Taken
Campus LAN Backbone and Distribution Links	• SNMP polling at 5-minute intervals • RMON exception traps on core and distribution links	• 50% utilization in 5-minute intervals • 90% utilization via exception trap	• E-mail notification to performance and capacity e-mail alias • Group to resolve issue or plan upgrade
Domestic WAN Links	SNMP polling at 5-minute intervals	75% utilization in 5-minute intervals	• E-mail notification to performance e-mail alias • Group to evaluate QoS requirement or plan upgrade for recurring issues
Extranet WAN Links	SNMP polling at 5-minute intervals	60% utilization in 5-minute intervals	• E-mail notification to performance e-mail alias • Group to evaluate QoS requirement or plan upgrade for recurring issues

Network Area/Media	Measurement Method	Threshold	Action Taken
Campus LAN	• None • No problem expected • Difficult to measure entire LAN infrastructure	10-millisecond round-trip response time or less at all times	E-mail notification to performance and capacity e-mail alias group to resolve issue or plan upgrade
Domestic WAN Links	Current measurement from SF to NY and SF to Chicago only using Internet Performance Monitor (IPM) ICMP echo	75-millisecond round-trip response time averaged over 5-minute period	E-mail notification to performance e-mail alias group to evaluate QoS requirement or plan upgrade for recurring issues
San Francisco to Tokyo	Current measurement from San Francisco to Brussels using IPM and ICMP echo	250-millisecond round-trip response time averaged over 5-minute period	E-mail notification to performance e-mail alias group to evaluate QoS requirement or plan upgrade for recurring issues
San Francisco to Brussels	Current measurement from San Francisco to Brussels using IPM and ICMP echo	175-millisecond round-trip response time averaged over 5-minute period	E-mail notification to performance e-mail alias group to evaluate QoS requirement or plan upgrade for recurring issues

網路實作範例

A. 遠端接取服務 VPN 的設定範例

圖23顯示如何提供遠端用戶，透過安全隧道(secure tunnel)連接至企業內網路示意圖。

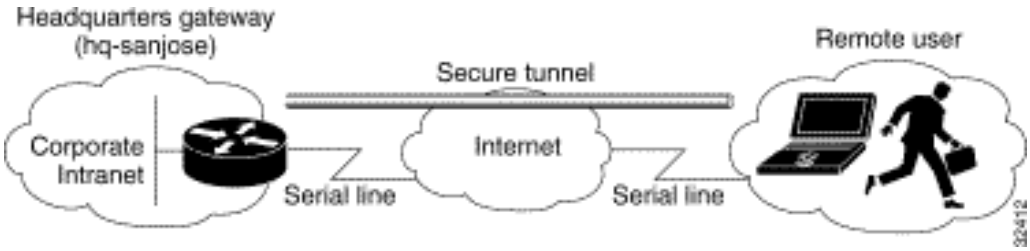


圖 23： Remote Access VPN Business Scenario

圖 24 顯示所需的設備元件，以下就本架構所需使用到的技術(MPPE，PPTP 等)以 Cisco System 的 IOS 為平台作一實作的說明。

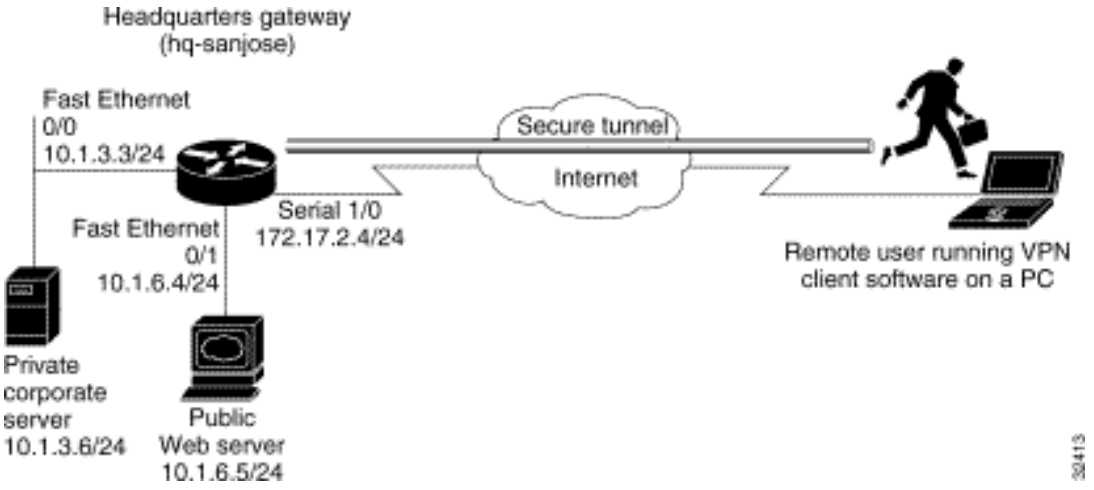


圖 24： Remote Access VPN Scenario Physical Elements

PPTP/MPPE 的設定範例

1. Configuring a Virtual Template for Dial-In Sessions

	Command	Purpose
Step 1	hq-sanjose(config)# interface virtual-template number	Creates the virtual template that is used to clone virtual-access interfaces.
Step 2	hq-sanjose(config-if)# ip unnumbered interface-type number	Specifies the IP address of the interface the virtual-access interfaces uses.
Step 3	hq-sanjose(config-if)# ppp authentication ms-chap	Enables MS-CHAP authentication using the local username database. All windows clients using MPPE need to use MS-CHAP.
Step 4	hq-sanjose(config-if)# ip local pool default first-ip-address last-ip-address	Configures the default local pool of IP addresses that will be used by clients.
Step 5	hq-sanjose(config-if)# peer default ip address pool (defaultname)	Returns an IP address from the default pool to the client.
Step 6	hq-sanjose(config-if)# ip mroute-cache	Disables fast switching of IP multicast.
Step 7	hq-sanjose(config-if)# ppp encrypt mppe {auto | 40 | 128} [passive | required] [stateful]	(Optional) Enables MPPE encryption on the virtual template[1] if you are not using an ISM with your Cisco 7100 series router. If you are using an ISM with your Cisco 7100 series router, see the "Configuring MPPE" section.

[1]Stateful MPPE encryption changes the key every 255 packets. Stateless (historyless) MPPE encryption generates a new key for every packet. Stateless MPPE is only supported in recent versions of Dial-Up Networking (DUN1.3).

2. Configuring PPTP

	Command	Purpose
Step 1	hq-sanjose(config)# vpdn-enable	Enables virtual private dialup networking on the router.
Step 2	hq-sanjose(config)# vpdn-group 1	Creates VPDN group 1.
Step 3	hq-sanjose(config-vpdn)# accept dialin	Enables the tunnel server to accept dial-in requests.
Step 4	hq-sanjose(config-vpdn-acc-in)# protocol pptp	Specifies that the tunneling protocol will be PPTP.
Step 5	hq-sanjose(config-vpdn-acc-in)# virtual-template template-number	Specifies the number of the virtual template that will be used to clone the virtual-access interface.
Step 6	hq-sanjose(config-vpdn-acc-in)# exit hq-sanjose(config-vpdn)# local name localname	(Optional) Specifies that the tunnel server will identify itself with this local name. If no local name is specified, the tunnel server will identify itself with its host name.

3. Configuring MPPE

	Command	Purpose
Step 1	hq-sanjose(config)# controller isa slot/port	Enter controller configuration mode on the ISM card.
Step 2	hq-sanjose(config-controller)# encryption mppe	Enables MPPE encryption.

4. Verifying PPTP/MPPE

```
hq-sanjose#show VPDN tunnel | show VPDN session
PPTP Tunnel Information (Total tunnels=1 sessions=1)

LocID RemID Remote Name    State   Remote Address  Port  Sessions
22    22    172.16.230.29  estabd   172.16.230.29   1374  1
```

5. Configuring L2TP/IPSec

	Command	Purpose
Step 1	hq-sanjose(config)# vpdn-enable	Enables virtual private dialup networking on the router.
Step 2	hq-sanjose(config)# vpdn-group 1	Creates VPDN group 1.
Step 3	hq-sanjose(config-vpdn)# accept dialin	Enables the tunnel server to accept dial-in requests.
Step 4	hq-sanjose(config-vpdn-acc-in)# protocol l2tp	Specifies that the tunneling protocol will be L2TP.
Step 5	hq-sanjose(config-vpdn-acc-in)# virtual-template template-number	Specifies the number of the virtual template that will be used to clone the virtual-access interface.
Step 6	hq-sanjose(config-vpdn-acc-in)# exit hq-sanjose(config-vpdn)# local name localname	(Optional) Specifies that the tunnel server will identify itself with this local name. If no local name is specified, the tunnel server will identify itself with its host name.

6. Verifying L2TP

```
hq-sanjose#show VPDN tunnel
L2TP Tunnel and Session Information (Total tunnels=5 sessions=5)

LocID RemID Remote Name   State  Remote Address  Port  Sessions
  10   8     7206b       est    10.0.0.1     1701     1

LocID RemID TunID Intf   Username    State  Last Chg Fastswitch
   4    6    10   Vi1     las         est   01：44：39   enabled
```

7. Configuring Authentication， Authorization， and Accounting

	Command	Purpose
Step 1	hq-sanjose(config)# aaa new-model	Enables the AAA functionality on the router.
Step 2	hq-sanjose(config)# aaa authentication login default TACACS+ RADIUS	Defines the list of authentication methods at login.
Step 3	hq-sanjose(config)# aaa authorization auth-proxy default [method1 [method2....]]	Enables authentication proxy for AAA methods.
Step 4	hq-sanjose(config)# tacacs-server host hostname	Specifies an AAA server. For RADIUS servers, use the **radius server host** command.
Step 5	hq-sanjose(config)# tacacs-server key sting	Sets the authentication and encryption key for communications between therouter and the AAA server. For RADIUS servers use the **radiusserverkey** command.
Step 6	hq-sanjose(config)# access-list access-list-number permit tcp host source eq tacacs host destination	Creates an ACL entry to allow the AAA server return traffic to the firewall. The source address is the IP address of the AAA server, and the destination address is the IP address of the router interface where the AAA server resides.

8. Configuring the HTTP Server

	Command	Purpose
Step 1	hq-sanjose(config)# ip http server	Enables the HTTP server on the router. The authentication proxy uses the HTTP server to communicate with the client for user authentication.
Step 2	hq-sanjose(config)# ip http authentication aaa	Sets the HTTP server authentication method to AAA.
Step 3	hq-sanjose(config)# ip http access-class access-list-number	Specifies the access list for the HTTP server.

9. Configuring the Authentication Proxy

	Command	Purpose
Step 1	hq-sanjose(config)# ip auth-proxy auth-cache-time min	Sets the global authentication proxy idle timeout value in minutes. If the timeout expires, user authentication entries are removed, along with any associated dynamic access lists. The default value is 60 minutes.
Step 2	hq-sanjose(config)# ip auth-proxy auth-proxy-banner	(Optional) Displays the name of the firewall router in the authentication proxy login page. The banner is disabled by default.
Step 3	hq-sanjose(config)# ip auth-proxy name auth-proxy-name http [auth-cache-time min] [list std-access-list]	Creates authentication proxy rules. The rules define how you apply authentication proxy. This command associates connection initiating HTTP protocol traffic with an authentication proxy name. You can associate the named rule with an access control list, providing control over which hosts use the authentication proxy feature. If no standard access list is defined, the named authentication proxy rule intercepts HTTP traffic from all hosts whose connection initiating packets are received at the configured interface. (Optional) The auth-cache-time option overrides the global authentication proxy cache timer. This option provides more control over timeout values for a specific authentication proxy rule. If no value is specified, the proxy rule assumes the value set with the ip auth-proxy auth-cache-time command. (Optional) The list option allows you to apply a standard access list to a named authentication proxy rule. HTTP connections initiated from hosts in the access list are intercept by the authentication proxy.
Step 4	hq-sanjose(config)# interface type	Enters interface configuration mode by specifying the interface type on which to apply the authentication proxy.
Step 5	hq-sanjose(config-if)# ip auth-proxy auth-proxy-name	In interface configuration mode, applies the named authentication proxy rule at the interface. This command enables the authentication proxy rule with that name.

10.完整的設定範例

```
hq-sanjose# show running-config

Current configuration
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mp12
!
no logging console guaranteed
enable password lab
!
username tester41 password 0 lab41
!
ip subnet-zero
no ip domain-lookup
!
vpdn enable
!
vpdn-group 1
! Default PPTP VPDN group
accept-dialin
  protocol pptp
  virtual-template 1
local name cisco_pns
!
memory check-interval 1
!
controller ISA 5/0
encryption mppe
!
process-max-time 200
!
interface FastEthernet0/0
ip address 10.1.3.3 255.255.255.0
no ip directed-broadcast
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.1.6.4 255.255.255.0
no ip directed-broadcast
duplex auto
speed auto
!
interface Serial1/0
no ip address
no ip directed-broadcast
shutdown
framing c-bit
cablelength 10
dsu bandwidth 44210
!
interface Serial1/1
no ip address
no ip directed-broadcast
```

```
shutdown
framing c-bit
cablelength 10
dsu bandwidth 44210
!
interface FastEthernet4/0
no ip address
no ip directed-broadcast
shutdown
duplex half
!
interface Virtual-Template1
ip unnumbered FastEthernet0/0
no ip directed-broadcast
ip mroute-cache
no keepalive
ppp encrypt mppe 40
ppp authentication ms-chap
!
ip classless
ip route 172.29.1.129 255.255.255.255 1.1.1.1
ip route 172.29.63.9 255.255.255.255 1.1.1.1
no ip http server
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
!
aaa new-model
aaa authentication login default tacacs+ radius
!Set up the aaa new model to use the authentication proxy.
aaa authorization auth-proxy default tacacs+ radius
!Define the AAA servers used by the router
tacacs-server host 172.31.54.143
tacacs-server key cisco
radius-server host 172.31.54.143
radius-server key cisco
!
! Enable the HTTP server on the router：
ip http server
! Set the HTTP server authentication method to AAA：
ip http authentication aaa
!Define standard access list 61 to deny any host.
access-list 61 deny any
! Use ACL 61 to deny connections from any host to the HTTP server.
ip http access-class 61
!
!set the global authentication proxy timeout value.
ip auth-proxy auth-cache-time 60
!Apply a name to the authentication proxy configuration rule.
ip auth-proxy name HQ_users http
!
! Apply the authentication proxy rule at an interface.
interface e0
        ip address 10.1.1.210 255.255.255.0
        ip auth-proxy HQ_users
```

```
!
end
```

L2TP/IPSec Congfiguration

```
hq-sanjose# show running-config

Current configuration：
 !
 version 12.0
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname LNS
 !
 enable password ww
 !
 username LNS password 0 tunnelpass
 username test@cisco.com password 0 cisco
 ip subnet-zero
 !
 vpdn enable
 !
 vpdn-group 1
  accept dialin l2tp virtual-template 1 remote LAC
  local name LNS
 !
 crypto isakmp policy 1
  authentication pre-share
  group 2
  lifetime 3600
 crypto isakmp key cisco address 172.1.1.1
 !
 crypto ipsec transform-set testtrans esp-des
 !
  !
  crypto map l2tpmap 10 ipsec-isakmp
  set peer 172.1.1.1
  set transform-set testtrans
  match address 101
 !
 interface Ethernet 0/0
  ip address 10.1.3.3 255.255.255.0
  no ip directed-broadcast
  no keepalive
 !
 interface Ethernet 0/1
  no ip address
  no ip directed-broadcast
  shutdown
 !
 interface Virtual-Template1
  ip unnumbered Ethernet0
  no ip directed-broadcast
  no ip route-cache
  peer default ip address pool mypool
  ppp authentication chap
 !
 interface Serial 1/0
  ip address 172.17.2.4 255.255.255.0
```

```
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 no fair-queue
 clockrate 1300000
 crypto map l2tpmap
!
interface Serial 0/0
 no ip address
 no ip directed-broadcast
 shutdown
!
ip local pool mypool 172.16.3.1 172.20.10.10
no ip classless
!
access-list 101 permit udp host 172.17.2.4 eq 1701 host 172.1.1.1 eq
1701
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
aaa new-model
aaa authentication login default tacacs+ radius
!Set up the aaa new model to use the authentication proxy.
aaa authorization auth-proxy default tacacs+ radius
!Define the AAA servers used by the router
tcacs-server host 172.31.54.143
tacacs-server key cisco
radius-server host 172.31.54.143
radius-server key cisco
!
! Enable the HTTP server on the router：
ip http server
! Set the HTTP server authentication method to AAA：
ip http authentication aaa
!Define standard access list 61 to deny any host.
access-list 61 deny any
! Use ACL 61 to deny connections from any host to the HTTP server.
ip http access-class 61
!
!set the global authentication proxy timeout value.
ip auth-proxy auth-cache-time 60
!Apply a name to the authentication proxy configuration rule.
ip auth-proxy name HQ_users http
!
! Apply the authentication proxy rule at an interface.
interface e0
        ip address 10.1.1.210 255.255.255.0
        ip auth-proxy HQ_users


!
end
```

B. MPLS VPN 的設定範例

圖25顯示不同的VPN(VPN 1， 2， 3)如何ISP的MPLS骨幹建構VPN示意圖。

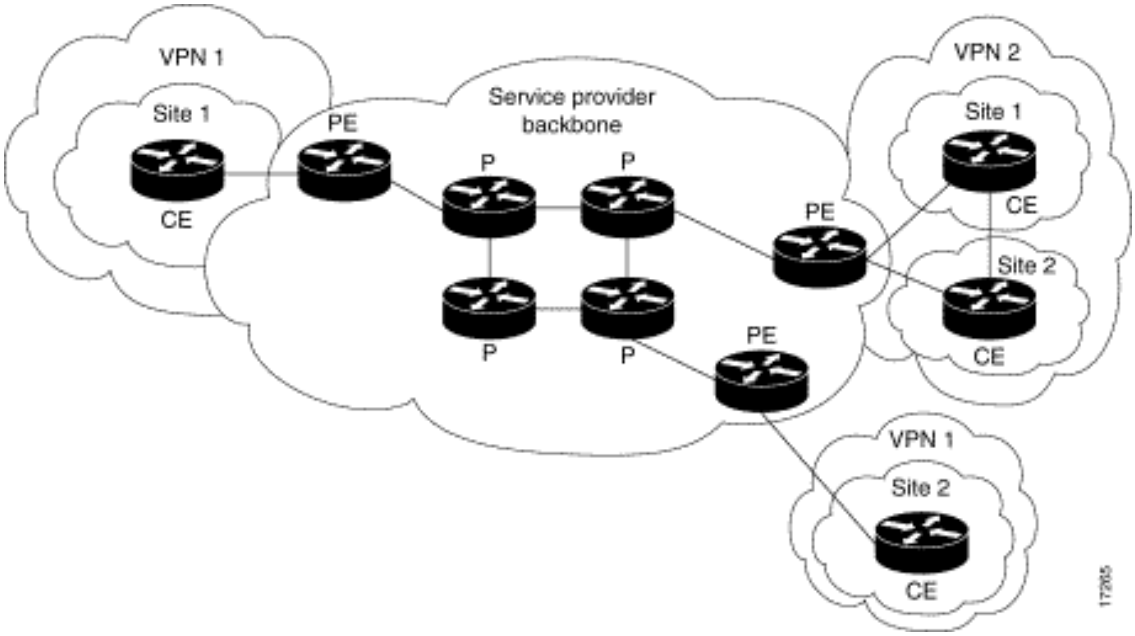


圖 25： BGP/MPLS VPN Scenario

1. Define VRF (Virtual Routing/Forwarding)

Step	Command	Purpose
1.	Router(config)#**ip vrf** *vrf-name*	Enter VRF configuration mode and define the VPN routing instance by assigning a VRF name.
2.	Router(config-vrf)#**rd** *route-distinguisher*	Create routing and forwarding tables.
3.	Router(config-vrf)#**route-target {import | export | both}** *route-target-ext-community*	Create a list of import and/or export route target communities for the specified VRF.
4.	Router(config-vrf)#**import map** *route-map*	(Optional) Associate the specified route map with the VRF.
5.	Router(config-if)#ip vrf forwarding vrf-name	Associate a VRF with an interface or subinterface.

2. Configure PE-to-PE BGP session

Step	Command	Purpose
1.	Router(config)#**router bgp** *autonomous-system*	Configures the IBGP routing process with the autonomous system number passed along to other IBGP routers.
2.	Router(config-router)#**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *number*	Specifies a neighbor's IP address or IBGP peer group identifying it to the local autonomous system.
3.	Router(config-router)#**neighbor** *ip-address* **activate**	Activates the advertisement of the IPv4 address family.

3. 若客戶使用在其 VPN 內使用 RIP，則參考以下設定。

Step	Command	Purpose
1.	Router(config)#**router rip**	Enables RIP.
2.	Router(config-router)#**address-family ipv4** [**unicast**] **vrf** *vrf-name*	Defines RIP parameters for PE to CE routing sessions. **Note** The default is Off for auto-summary and synchronization in the VRF address-family submode.
3.	Router(config-router)#**network** *prefix*	Enables RIP on the PE to CE link.

4.在 PE 端的設定範例

```
ip cef distributed     ! CEF switching is pre-requisite for label
Switching
frame-relay switching
!
ip vrf vrf1    ! Define VPN Routing instance vrf1
 rd 100：1
 route-target both 100：1      ! Configure import and export route-
targets for vrf1
!
ip vrf vrf2    ! Define VPN Routing instance vrf2
 rd 100：2
 route-target both 100：2      ! Configure import and export route-
targets for vrf2
 route-target import 100：1    ! Configure an additional import
route-target for vrf2
 import map vrf2_import! Configure import route-map for vrf2
!
interface lo0
 ip address 10.13.0.13 255.255.255.255
!
interface atm9/0/0     ! Backbone link to another Provider router
!
interface atm9/0/0.1 tag-switching
```

```
 ip unnumbered loopback0
        no ip directed-broadcast
        tag-switching atm vpi 2-5
 tag-switching ip

interface atm5/0
        no ip address
        no ip directed-broadcast
        atm clock INTERNAL
        no atm ilmi-keepalive

interface Ethernet1/0
        ip address 3.3.3.5 255.255.0.0
        no ip directed-broadcast
        no ip mroute-cache
        no keepalive

interface Ethernet5/0/1        ! Set up Ethernet interface as VRF link
to a CE router
 ip vrf forwarding vrf1
 ip address 10.20.0.13 255.255.255.0
 !
interface hssi 10/1/0

 hssi internal-clock
 encaps fr
 frame-relay intf-type dce
 frame-relay lmi-type ansi
!
interface hssi 10/1/0.16 point-to-point
 ip vrf forwarding vrf2
 ip address 10.20.1.13 255.255.255.0
 frame-relay interface-dlci 16 ! Set up Frame Relay PVC subinterface as
link to another
!       ! CE router

router bgp 1    ! Configure BGP sessions
 no synchronization
 no bgp default ipv4-activate          ! Deactivate default IPv4
advertisements
 neighbor 10.15.0.15 remote-as 1              ! Define IBGP session
with another PE
 neighbor 10.15.0.15 update-source lo0
!
 address-family vpnv4 unicast          ! Activate PE exchange of VPNv4
NLRI
  neighbor 10.15.0.15 activate
  exit-address-family
!
 address-family ipv4 unicast vrf vrf1         ! Define BGP PE-CE
session for vrf1
  redistribute static
         redistribute connected
  neighbor 10.20.0.60 remote-as 65535
  neighbor 10.20.0.60 activate
  no auto-summary
  exit-address-family
!
```

```
 address-family ipv4 unicast vrf vrf2         ! Define BGP PE-CE
session for vrf2
  redistribute static
         redistribute connected
  neighbor 10.20.1.11 remote-as 65535
  neighbor 10.20.1.11 update-source h10/1/0.16
  neighbor 10.20.1.11 activate
  no auto-summary
  exit-address-family
!
! Define a VRF static route
ip route vrf vrf1 12.0.0.0 255.0.0.0 e5/0/1 10.20.0.60
!
```

結論

本次在美國的實習內容雖以 Cisco System 的產品為主，仍可看出:雖然目前的企業 VPN 多數仍以 CPE-based 搭配 layer-2 VPN(Frame Relay, ATM 等)，但下一代在 Internet 上建置 VPN 的技術仍是以 IETF 的標準為主(RFC 2547bis: BGP/MPLS VPN, RFC 2858: Multiprotocol Extension BGP, RFC 2401: Security Architecture for the Internet Protocol (IPSec), extended ISIS for dual-stack)，架構上則以 peer model 為主，即透過 MP-BGP 交換 extended community，同時 ISP 在 VPN 網路的設計也具有較好的擴展性。

在 Remote Access VPN 的服務方面，目前除了 layer-2 tunneling 外, 還有 IP Mobility 與 IPv6 的相關標準即將面市，這代表未來的 remote access 客戶使用上更有彈性，對 ISP 在維運能力的挑戰也更上一層。

其次在行程中也參觀了 tier-1 ISP 的 NOC 維護流程, 對於日後在 VPN 的客戶服務上有相當的助益。