公務出國報告

（出國類別：實習）

『Intranet、VPN及新服務應用』
實習報告

服務機關：中華電信台灣中區電信分公司

出國人　職　稱：副工程師

姓　名：魏文科

出國地區：美國

出國期間：92年9月21日至92年9月30日

報告日期：92年12月24日

系統識別號:C09204019

公 務 出 國 報 告 提 要

頁數: 31　含附件: 否

報告名稱:

INTRANET 、 VPN 及新服務應用

主辦機關:

中華電信台灣中區電信分公司

聯絡人／電話:

呂鳳嬌／04-23442108

出國人員:

魏文科　中華電信台灣中區電信分公司　資訊處　副工程師

出國類別: 實習

出國地區: 美國

出國期間: 民國 92 年 09 月 21 日 -民國 92 年 09 月 30 日

報告日期: 民國 92 年 12 月 24 日

分類號/目: H6／電信　／

關鍵詞: Intranet,VPN

內容摘要: 隨著網際網路(Internet)的蓬勃發展，企業建置Intranet網路及導入多元化的應用需求快速成長，電信業者勢必爲滿足此一成長，積極建設新一代寬頻網路以有效擴充網路使用頻寬。爲順應此一趨勢及潮流，實習有關下一代寬頻網路—交換式全光網路之相關技術，以提供建置Intranet之參考。企業面對市場的激烈競爭，電子化與全球化是必然的趨勢，爲確保Intranet、Extranet資訊流通安全性，IP-based VPN成爲最熱門的解決方案，探討有關VPN的技術發展及差異比較。網際網路技術整合了數據、語音及影像服務，企業客戶建置Intranet的同時，會導入各式各樣整合性服務，以分享網路資源節省營運成本，提高公司的利潤。VoIP屬於企業最先考慮的服務應用，而該項服務的發展趨勢與成長速度將深切影響到本公司的營收結構。本次實習案有機會了解先進國家IP寬頻技術與應用服務的發展現況與未來趨勢，吸取國外經驗，獲益良多，期許在未來本公司企業資訊網路及配合企業客戶Intranet整合服務之規劃上能發揮助益。

本文電子檔已上傳至出國報告資訊網

摘要

隨著網際網路(Internet)的蓬勃發展，企業建置 Intranet 網路及導入多元化的應用需求快速成長，電信業者勢必為滿足此一成長，積極建設新一代寬頻網路以有效擴充網路使用頻寬。為順應此一趨勢及潮流，實習有關下一代寬頻網路—交換式全光網路之相關技術，以提供建置 Intranet 之參考。

企業面對市場的激烈競爭，電子化與全球化是必然的趨勢，為確保 Intranet、Extranet 資訊流通安全性，IP-based VPN 成為最熱門的解決方案，探討有關 VPN 的技術發展及差異比較。

網際網路技術整合了數據、語音及影像服務，企業客戶建置 Intranet 的同時，會導入各式各樣整合性服務，以分享網路資源節省營運成本，提高公司的利潤。VoIP 屬於企業最先考慮的服務應用，而該項服務的發展趨勢與成長速度將深切影響到本公司的營收結構。

本次實習案有機會了解先進國家 IP 寬頻技術與應用服務的發展現況與未來趨勢，吸取國外經驗，獲益良多，期許在未來本公司企業資訊網路及配合企業客戶 Intranet 整合服務之規劃上能發揮助益。

目　　錄

第一章 前言

1.1 目的

由於現代企業建置 Intranet 網路及導入多元化應用的需求快速成長，本案目的在實習有關下一代寬頻網路—交換式全光網路之相關技術與應用、VPN 技術的發展趨勢，以及企業 Intranet 之應用服務，吸收其寶貴之經驗，掌握最新的技術發展，作為規劃本公司與企業客戶 Intranet 之參考。

1.2 行程

本案係奉中華電信股份有限公司 92.9.17 信人二字第 92A3501611 號函，奉派赴美國亞特蘭大實習『Intranet、VPN 及新服務應用』，於民國九十二年九月二十一日啟程，九月三十日返國，共十天。

行程如下表：

日　　期	接受培訓項目	地點
9 月 21 日	啟　　程	
9 月 22~29 日	1. 全光網路技術。 2. Intranet、VPN 及新服務應用。 3. on site training。	美國亞特蘭大 Movaz 公司
7 月 29~30 日	返　　程	

第二章　Intranet、VPN 技術及新服務應用

2.1 Intranet 寬頻骨幹網路之趨勢

Intranet 本質上是將 Internet 的技術應用在企業內部，隨著語音、數據及影音應用之快速擴散及多元服務，網路頻寬的需求亦快速成長，隨著科技進步、網路技術不斷地創新，乙太網路由 10M、100M、1000M 提昇至 10G 的高速率，WAN 的選擇也由專線、FR、FDDI、ATM 不斷提昇速率，目前電信業者已可提供全光的 DWDM 寬頻網路；無論本公司企業資訊網路或企業客戶(尤其是區域化、全國化、全球化之規模企業)之 Intranet 規劃建置均必須考慮這項發展趨勢，因為它們都建構在相同的基礎架構(Infrastructure)上。網路實習部份以 Movaz 公司的 RAY™ 系統為主。

2.1.1 都會型全光網路架構(All-Optical Metro Networking)

DWDM 技術改變了數據與電信網路 long-haul 的傳送能力，第一代 DWDM 由於成本效益因素，阻礙了其商品化及大規模部署的可行性；不過，由於許多技術的聚合，包括波長(Wavelength)之傳輸技術、交換技術及系統管理技術等方面的進步，使得 DWDM-based 的都會型(Metro)及區域型(Regional)網路成為事實，而 long-haul 也將是可實現的。

都會型網路的拓樸架構、訊務型態及服務種類依服務供應商(如 ILECs、CLECs、Cable、ISPs、ASPs 及 SSPs 等)的不同而存在差異性，主要的網路基礎架構便不會相同，茲以一般 ILEC 業者(Incumbent Local Exchange Carriers)所提供的都會型網路架構為例說明(如下圖)。

都會型網路為階層式(Hierarchical)架構：分成接取節點(Access node)、彙集節點(Aggregation node)及核心局(Core office)等三個階層。在某些環境下，可能由數個核心局彼此互連形成一個區域性或骨幹的 hub，這種發展格局已顯現出 long-haul 的走向。

(一)、Access fiber network 階層：

支援多重服務(multiple service)介面、所佔空間小及成本低；不過

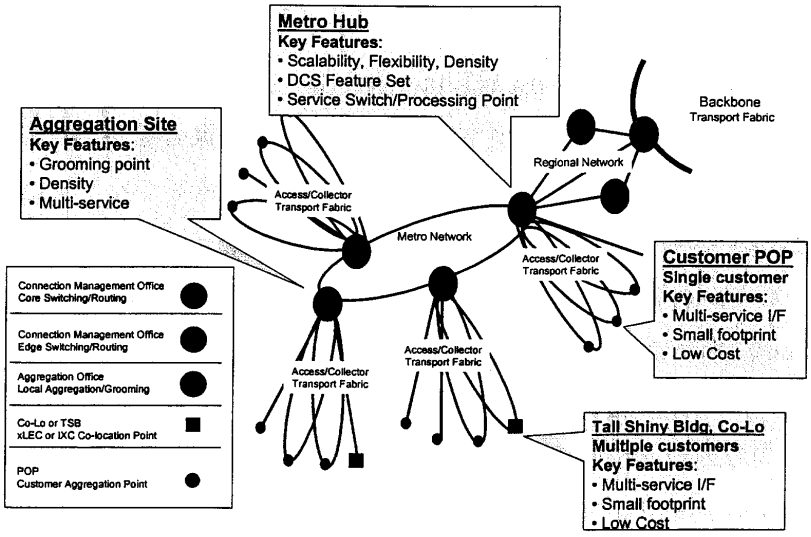
是業者營收的主要來源，通常以 Ring 方式建置，範圍侷限在有限的地理區域內，波長數目從 1(2)到 20；在某些需求較大的地區，接取節點與彙集節點間會採用 P2P 連接。

(二)、Aggregation site 階層：

一般擔任 grooming point 的角色；但在較大的網路規模中，可發展成為純 transit point 角色連接上 Metro hub；須能支援多重服務。

(三)、Core network 階層：

與 hubs 互連，涵蓋一個較廣闊的地理區域，具有同時交換數千個波長的能力，依光纜部署的環境及服務的訊務型態，可以建置成 ring 或 mesh 的網路拓樸架構。

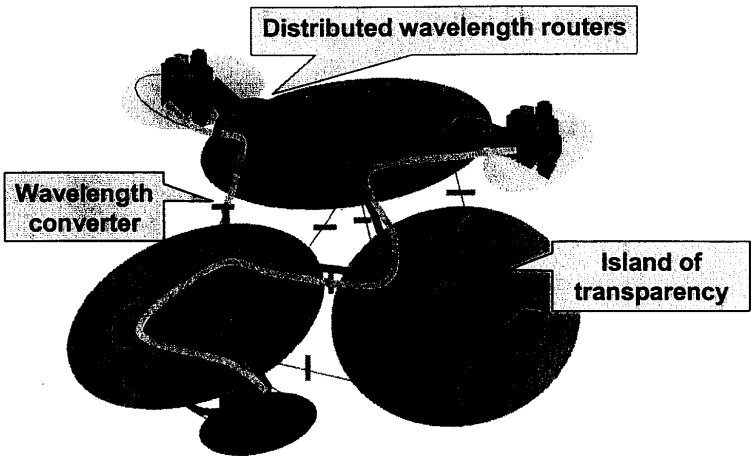


2.1.2 自動交換式全光網路(Automatically Switched All-Optical Network)的關鍵技術

以下說明全光網路的幾項關鍵技術發展：

(一) OEO 轉換元件(Optical-Electronic-Optical conversion)的成本相當昂貴，是第一代 DWDM 無法商品化的主要因素，但全光網路的技術提供了免除或減少 OEO 的方法，只有在全光網路 Domain 的邊緣才需要 OEO 轉

換元件(如下圖)，大幅地降低了建置成本。



要建構這種網路，網路之節點(node)必須滿足以下四點要件：

(1) 節點須能支援 4 或 5 個 access ring 或連接 4 或 5 個鄰接節點；每一 fiber connection 必須至少能處理 80 波長，這表示高密度的 Hub site 必須有能力提供數千個波長的交換。

(2) 任一芯輸入光纜的任一波長可以交換到任一芯輸出光纜上，其間不須經過電子式交接(electrical cross-connect)。

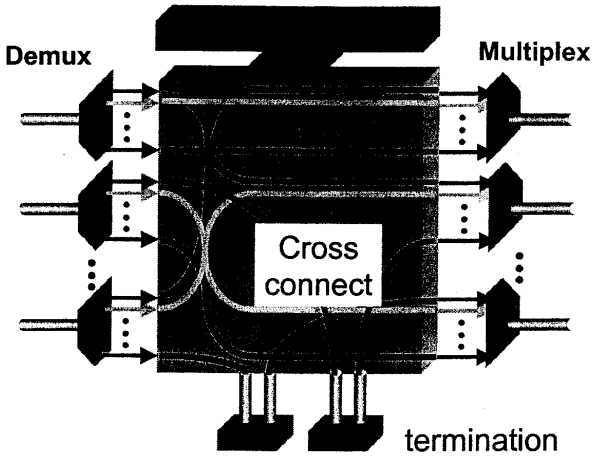
(3) 必須是可程式化，亦即可以接收來自作業系統或控制面(control plane)下達的交換指令。

(4) 必須具備障礙處理、效能監視與通報、電源穩定等特性，以保證可達到路徑完整性(Path Integrity)。

(二) DWDM Cross-Connect (WXC)

這是影響全光網路 Scalability 的關鍵技術之一，如下圖所示，分成解多工(Demux)、交接(Cross-connect)及多工(Multiplex)三個階段；第一階段，每芯進來的光纜在 Demux 終接(terminated)，Demux 將輸入的光解多工成個別的數據通道 (data channel，亦即個別不同的波長)後，導入第二階段的光交接器 (OXC)進行光信號的交換(no-blocking)，第三階段的 Multiplex 再將個別的數據通道多工成一芯光纜傳送出去，但並非所

有的波長都須繞徑到輸出光纜，某些通道可能在 OXC 被終接，轉換成電子信號或終接到服務介面。



有很多技術可以應用在建構 OXC 元件上，目前領先的技術是 MEMS(free space Micro-Electro-Mechanical System)，由排列整齊的一組光鏡片(optical mirror)所構成，其運作過程大致如下：

輸入的每一光束(optical beam)都聚射到輸入鏡片上，透過控制鏡片的偏斜角度(tilt angle)，讓光束繞經 free space 到輸出鏡片上，再反射到輸出埠上。

早期將 OXC 技術應用在 DWDM 交接上的方式是將三個 stage 分開，各 stage 間使用光纜連接，若考量一般 OXC 的規模約 1000*1000，即意味著必須管理這 2000 條連接光纜，此外，每一 stage 的佔用空間及電源需求，都是造成擴充性(Scalability)受限及成本昂貴的原因。目前發展出的波長交接器 (WXC ，wavelength cross-connect)元件，是將上述三個 stage 整合成一個 highly compact, free-space geometry，各 stage 間的數據通道之傳送是透過空氣而非光纜，使用單一 ASIC，與 MENS 光鏡片組整合在一起，以集中控制鏡片偏斜角度，此外，WXC 的管理也不似 OXC 那般複雜，因此 WXC 可以形成高擴充性、高密度、低成本及可程式化的光交換元

件。

(三) 控制面(Control Plane)

另一項影響全光 DWDM 都會型網路得以實現的關鍵技術是控制面的技術演進，控制面是掌握網路狀況及建立 end-to-end connection 的軟體，若要使全光網路的 Domain 極大，控制面必須能夠有效管理與光通道有關的各種 Constraints，包括：

(1) Routing-based constraints (如 diversity)。

(2) resources-based constraints (如 wavelength contention)。

(3) transmission impairments (如 loss and dispersion)。

此外，全光網路的控制面若要在 mesh 拓樸架構上任意地建立 end-to-end connection，它必須具備執行 TE (traffic engineering)的功能，包括：

(1) resource discovery。

(2) state information dissemination。

(3) path selection。

(4) path management。

而要符合以上需求的智慧型控制面，必須能支援 GMPLS 協定。

(四) 其他關鍵之 DWDM 傳輸元件，如 Amplifiers 及 Transceivers 等技術亦持續發展。

2.1.3 GMPLS (Generalized MPLS) Protocol

全光網路的產業標準正在發展中，特別是在繞徑(routing)與傳訊(signaling)方面，必須深入考慮 TDM 及 optical layer 的特性，從 1999 年 MPλS(Multi-protocol lambda switching) draft proposal 發表到進展為 GMPLS notion，終使 IETF 必須更改組織結構，設立新的 Sub-IP area 和建立許多新的 working group (如 CCAMP、GSMP、IPO、IPORPR、TEWG、

MPLS 及 PPVPN 等)，積極進行這方面的標準化制定，IETF 採取的策略是 reuse 現有的 IP 控制面技術(如 MPLS)以發展出適合全光網路的標準協定，其他如 OIF 與 ITU 等組織也在進行類似領域(OTN、ASON、ASTN)的努力。目前，GMPLS 在繞徑與傳訊方面的強化(extensions)功能摘述如下：

(一)、傳訊(signaling)

(1) 延伸 RSVP-TE 及 CR-LDP 規格，以支援各種傳輸網路(尤其是光網路)之 connection management。

(2) 可支援 bi-directional LSPs(MPLS 只支援單方向 LSP)。

(3) capability for upstream nodes to suggest a label。

(4) 「generalized label request」訊息內容增加與建立 LSP 有關的編碼參數(encoding parameters)，LSP 的編碼可以指出 LSP 是 packet-based、Sonet-based 或 Lambda-based。

(5) 「generalized label request」訊息內容也包含 LSP 所載送 payload 的相關資訊如 ATM、POS、Sonet 及 Lambda。

(6) 導入 bandwidth encoding 的觀念，可以指定 LSP 的頻寬。

(7) Link protection flags and capabilities (for particular LSP)。

(8) Hierarchical Connection setup：由低階 LSP 去 trigger 高階 LSP 的形成，LSPs 的高低階定義是基於節點的 link 多工能力；如下圖所示，兩個 Domain 的邊界節點，負責彙集低階 LSP 並形成高階 LSP 的例子。

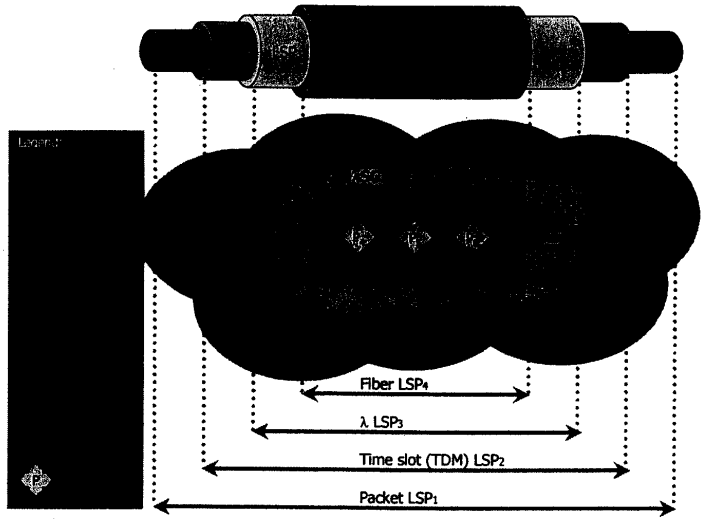


Figure 1: LSP_1 is setup from R_0 to R_{10} for 500Mbps of bandwidth. LSP_1 is nested in the subordinate LSPs 2, 3 and 4 respectively as depicted at the top of the figure. If an existing LSP has capacity the subordinate LSP is added to it, otherwise the setup of a new LSP of the appropriate type is triggered. The endpoints of LSP_1 classify packet data and source it into LSP_1. R_1 & R_9 are packet LSRs; S_2 & S_8 are SONET path level switches. The devices O_3 & O_7 are optical or lambda switches providing SONET/SDH section level signals (e.g. OC-192 including all overheads); they also have WDM capabilities between the photonic switches P_4 to P_6. The link between R_0 and R_1 is Gigabit Ethernet, between R_1 and S_2 is an OC-48, between S_2 and O_3 is an OC-192, between O_3 and P_4 is a WDM multiplex of 16 OC-192 signals which remains intact through to O_7 (P_4 through P_6 are pure photonic switches). The link between O_7 and S_8 is an OC-192, between S_8 and R_9 is an OC-48 and between R_9 and R_{10} is Gigabit Ethernet.

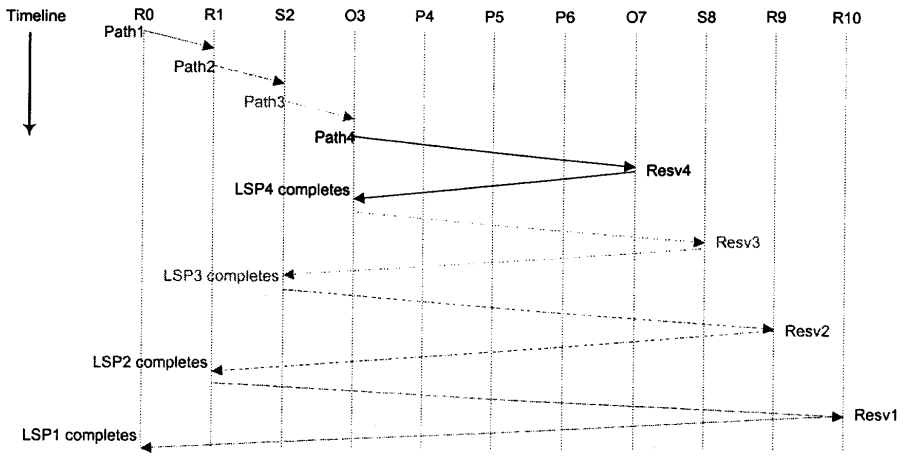


Figure 2: A Path request (PATH1) is generated at R0 that is sent to R1. At node R1 (a boundary node) this arrival triggers a requirement for a new LSP (LSP2) from R1 to R9. This dynamic LSP creation requests are triggered until Path4 is generated at 03. On the successful completion of LSP4, the Path3 message is tunneled through the LSP4 so formed. This process of LSP formation and a lower level LSP creation requests being tunneled through the higher-level LSP so formed, continues until the initial LSP (LSP1) is created thus forming a hierarchy.

(二)、繞徑(Routing)

(1) 延伸 OSPF 及 IS-IS 協定之功能，增加一些鏈路狀態資訊(link state information)以支援與鏈路有關之額外屬性的傳播(dissemination)。

(2) 導入 traffic engineering link 的觀念。兩個節點之間存在 TE 鏈路並不一定是 routing adjacency。

(3) 支援 dynamic wavelength management。

(4) 導入 constraint-based routing 的觀念，亦即應用 traffic engineering 和 fast re-route 技術，以及將來的 diversity routing 應用。

2.1.4 保護(Protection)與復原(Restoration)

透過繞徑、傳訊及鏈路管理協定(LMP，link management protocol)以支援智慧型障礙管理。在 connection level 的障礙管理包括四階段：

(1) fault detection：必須在最接近失能障礙(failure)的 layer 能夠處理。以光網路而言，就是實體(光)層，其障礙偵測之指標有 LOL(loss of light)、OSNR、BER、dispersion、crosstalk、以及仍在發展中的 attenuation。

(2) fault localization：當障礙發生後，節點間需要彼此溝通以確定發生障礙的地點，如 SONET AIS 係用來確認 span 間的障礙。LMP 協定內含障礙 localization 的處理流程，可用來確認全光(transparent)網路和光-電(opaque)網路的障礙點。

(3) fault notification。

(4) fault mitigation(即保護和復原功能)。

一旦障礙被偵測出來並確定了障礙點，便會啟動保護或復原機制以恢復網路正常運作，「保護機制」和「復原機制」的差別在於從障礙發生到恢復正常運作之時間的長短，保護機制通常設計成 100%之

備援，以期偵測到障礙時，可以快速(rapidly，<200ms)的切換因應，如 SONET 的 APS 可以在<50ms 時間內將訊務從主要的(primary)路徑切換到次要的(secondary)路徑，因此在正常運作時，訊務會同時經兩條路徑傳送(即 1+1 保護機制)，再由接收端節點選擇其一的訊務；「復原機制」的反映時間較「保護機制」慢(但仍然屬於 quickly)，因為復原機制是採用共用資源分享(pools of shared resources)的方式，也需使用較費時間的連接再繞徑(connection rerouting)技術。

路徑和復原機制有兩種處理問題的方式：

(1) 路徑切換(path switching)：障礙由端節點(路徑的兩端節點)負責處理，分為路徑保護(預先配置保護路徑)和路徑復原(須採用動態或預先計算方式進行再繞徑連接，而非預先配置方式)。

(2) 鏈路切換(link switching)：障礙由中間節點(或轉送節點)負責處理，分為 span 保護(訊務切換到替代之平行通道或鏈路以連接相同兩個節點)和路徑復原(訊務切換到相同兩個節點之替代路由，可能經過另外的中間節點)方式。

2.1.5 保護(Protection)機制

透過 GMPLS 的 RSVP-TE 傳訊可以指出 LSP 是主要的或次要的路徑，也可以指定 LSP 不同的保護等級(dedicated、shared 及 unprotected)。

(一) Span 保護

在兩個相鄰節點間，當障礙發生時會切換到備援通道或鏈路的機制。在 span level，鏈路可以是 protected(包括專屬 1+1，專屬 1:1，及分享式 M:N)、unprotected 或作為備援鏈路。GMPLS 的繞徑機制係根據 LPT(link protection type)選擇路由(route)，一旦路由選定，連接時使用 RSVP-TE 傳訊，內含 protection bit vector 可以指出 LPT 種類。

(1)專屬 1+1 span 保護

每一節點必須將數據複製(data replicated)到兩個不同的通道上，相鄰節點在維持信號完整性的原則下選擇接收其中的一個通道。這是最快速的保護機制，但在每對節點間需要兩倍的連接頻寬，也必須有複製數據到兩個不同的通道的能力。

(2)分享式 M:N 保護

N 條主要路徑共同分享使用 M 條備援路徑，因為數據並沒有複製到主要及備援通道上，因此切換之前必須先由 LMP 進行障礙隔離，再由 upstream 節點(依 *RSVP Path message* 傳送方向定義)送出「*RSVP Path refresh message*」以啟動 span 保護。「*RSVP Path refresh message*」包括一個 *label set object* 內含 M 條備援路徑的 label、可能之新鏈路 ID、PHOP，和以分享式保護組態為基礎的 *modified ERO objects*；預先用 LMP 交換分享式保護組態的好處是，當進行保護切換時可以將潛在的 label 衝突極小化。當 downstream 節點收到帶有 new object 的 Path messages 時，它必須 verify 這些參數，update RSVP Path state，再回應一個 *RSVP Resv refresh message(with a new label)*或產生一個 *PathError message*。

(二)、路徑保護(Path protection)

路徑保護是由端節點(即來源和目的地節點)負責處理的，當失能障礙發生時必須切換到替代路徑。對 1+1 路徑保護而言，信號同時送經兩條不相關連之路徑(disjoint path)，再由接收節點選擇最好的信號；對 M:N 路徑保護而言，N 個不同的信號分由 N 條不相關連之路徑傳送，同時預先建立 M 條不相關連之路徑作為 N 條主要路徑之分享保護資源。

(1) 1+1 路徑保護有幾種方式，提供保護的層次也因此不同，最常用的是選擇兩個不相關連之路徑(主要的和次要的)的方式，沿這兩條路徑的每一鏈路都是 unprotected，這種保護方式可以解決單一鏈路或節點之失能障礙，其關鍵在於如何決定兩條不相關連之路徑。另一種方式是選擇單一路徑，但其中的每一鏈路都是 1+1 span 保護，這種

保護方式可以解決單一鏈路之失能障礙，但不能保護節點失能障礙的情況。

也可以結合上述兩種方式，其運作實例如下圖。

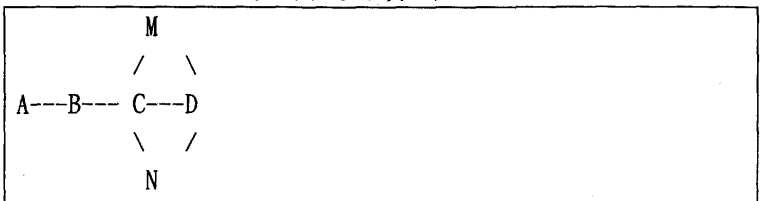


Figure 3: Path protection example. Only links A-B and C-D support 1+1 protection. Node A wants to establish a 1+1 protected path to D. In this case, A computes the primary path {A, B, M, C, D} where the segment {B, M, C} has links that do not support 1+1 protection. Therefore, A computes a link-disjoint segment {B, N, C} and uses it to construct a second path {A, B, N, C, D}. A initiates a setup of two connections indicating the desire for SE reservations; the first path is routed along {A, B, M, C, D} and the second path is routed along {A, B, N, C, D}. Since the two connections branch out at node B, B sends the data it receives from A to both M and N. At node C, the two connections merge and C selects the data received over one of these connections (based on the integrity of the signal), and forwards this data to D.

(2)M:N 路徑保護

提供N個繞徑不相關連之主要路徑及預先建立M個不相關連之備援路徑，作為N個主要路徑的分享式保護，GMPLS的特性是容許預先將備援路徑組態到主要路徑上，當主要路徑發生失能障礙時，迅速切換到次要的路徑上，雖然這些備援路徑的資源是預先配置好的，但正常運作時，一些較低優先等級的訊務仍可以使用它，而且當主要路徑發生失能障礙時，這些平時使用中的較低優先等級的訊務仍擁有繼續優先使用權。

2.1.6 復原(Restoration)機制

復原機制的設計同時考量反應障礙的速率及頻寬使用的效率，因此通常會涉及動態資源之建立與路由計算的動作，因此切換到替代路徑所花費的時間會比保護機制的方式稍長，一旦負責的節點(來源節點或中間節點)收到 notify message 時，便啟動復原功能，失能障礙的通報係使用 *Notify procedure* 或標準 *RSVP Path Error messages* 方式。

(1) 鏈路復原(Line restoration)

當失能障礙發生時，會在障礙點周遭將訊務切換到替代路由，在中間節點間選擇新的路徑，新路徑也可能經過新增加的中間節點，對於 span multiple hops 或大距離的連接而言，鏈路復原是比較有利的方式，因為失能障礙的通報所帶來的延遲可能相較程度的減少，而且只有部份連接會再繞徑(而不是整個路徑的再繞徑)。然而，若是 strict-hop route 下的連接，鏈路復原可能不符合 TE 的要件；此外，繞徑連接的 constraints 必須能夠傳送出去，使負責進行鏈路復原的中間節點能計算出適合的替代路由(這有點類似 span multi-areas 在建立/維護 TE requirement 的麻煩)。

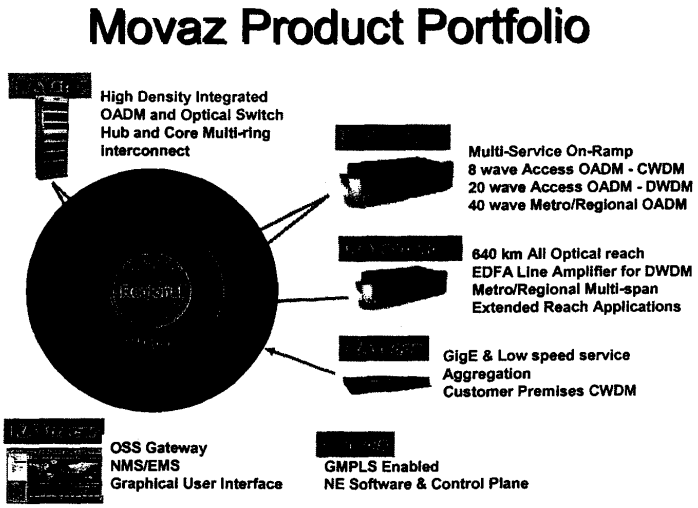
(2) 路徑復原(Path restoration)

當失能障礙發生時，會在障礙點周遭將訊務切換到替代路由，由來源節點選擇新的路徑，可能使用原來路徑的節點及(或)包含一些新增加的中間節點。對 strict-hop routing 來說，TE requirements 可直接應用到路由計算，因此可排除已經失能障礙的節點或鏈路；然而，假如失能障礙發生在 loose-route hop，來源節點將沒有足夠的資訊去進行再繞徑的連接。

GMPLS 是部署下一代數據與光網路不可缺少的關鍵部份，它提供了 IP 與 photonic layer 間必須具備的溝通橋樑，使 IP 與 photonic 技術各自發展的過程中，同時具有 interoperable 及 scalable 的特性。

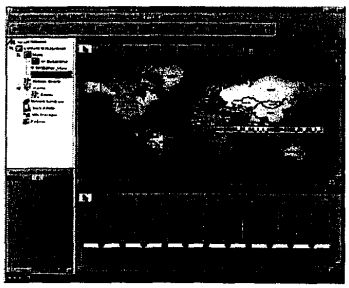
2.1.7 RAY™設備元件及其特性

Movaz 公司的全光網路系統具備了完整的產品組合，包括 RAY*star*、RAY*express*、RAY*extender*、RAY*edge*、RAY*o/s* 及 RAY*tracer* 等設備，其基本特性如下圖：



2.1.8 網路管理系統

RAY™全光網路的RAY*tracer*網管系統，採用集中管理方式，透過SNMP協定，可以Auto discovery全光網路上的所有節點並予以納管，進行效能監測與障礙管理等功能，如下圖所示：

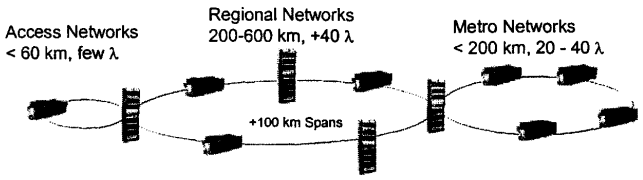


- Auto Discovery
- Commissioning
- Maps & Chassis Views
- Fault Management
- Service Provisioning
- Performance Management
- Inventory
- Software Download/Backup
- Security & Telnet
- Audits & Synchronization

2.1.9 全光網路系統規劃基本資料

RAY™全光網路應用於接取網路、區域性及都會型網路時的範疇及建

置之基本原則。如下圖：

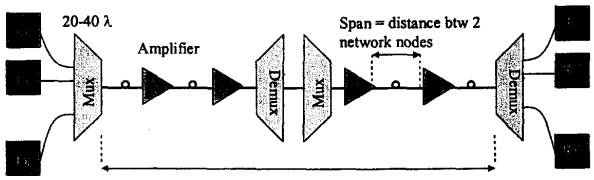


Optical System needs to transport data with low bit error rate (< E-12) across fiber distances

Network design requires precise estimation of impairments due to:
- Network Fiber (loss, dispersion, PMD, nonlinear effects, etc)
- DWDM Equipment (loss, noise, chirp, crosstalk, etc)
- Operation of System (adding services, nodes, aging, etc)

其中，全光網路的傳送損失(impairments)包括四大主要元件(Transmitter、Amplifier、OADM 及 Receiver)的各種損失(如下圖)：

Transmitter impairments	Amplifier impairments	OADM impairments	Receiver impairments
• Power	• Noise (ASE)	• Loss	• Sensitivity
• Noise	• Gain stability	• Crosstalk	• Noise
• Chirp	• Gain flatness (ripple)	• Loss flatness (ripple)	• bandwidth
• Extinction Ratio	• Transient suppression	• Passband width & shape	• Other (linearity, detection threshold, etc)
• Other (linewidth SMSR, etc)			



Optical Link = multiple spans

Link distance is limited by transmission impairments

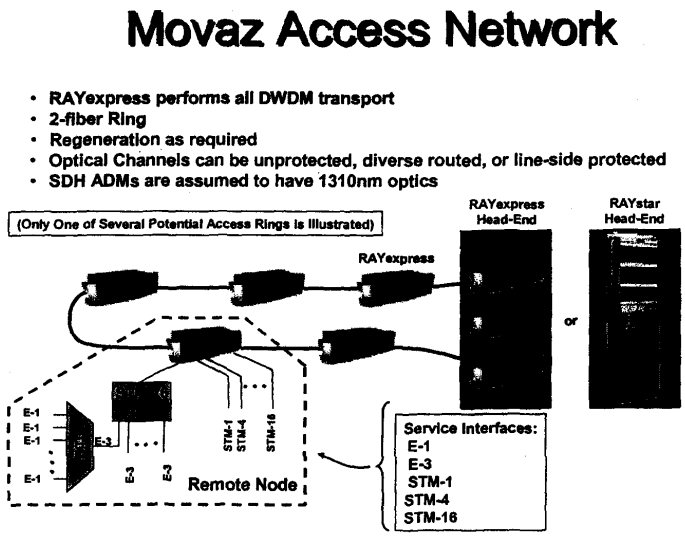
2.1.10 全光網路系統之應用

RAY™全光網路相較於現有設備(1990' s)可以節省 40%~60%的 CAPEX 及 60~70%的 OPEX 成本，而且在 GMPLS 協定下，未來新的服務將更有效率且成本較低，目前應用成功實例有

(1) Business Enterprise 應用來支援各種 data 服務，包括 GbE、ESCON、FICON 及光通道(如傳統的 SONET/SDH 介面)。

(2) Educational Institutions 應用來支援數位影像服務、remote learning 應用(如虛擬教室)服務，及各種分享式應用，可以在「無論何時」及「無論何地」發生需求時，更容易地建立服務。

(3)Enterprise Gateway 提供服務供應商的 flexible connectivity，如下圖。

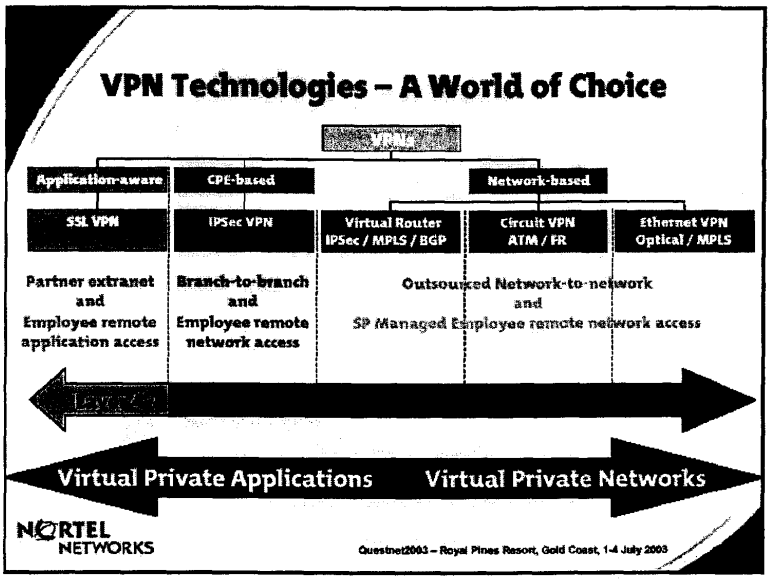


此外，RAY™全光網路可提供 Optical VPNs 服務，在 GMPLS 協定下客戶可以在專屬波長(dedicated wavelength)上，自行管理 optical bandwidth 及傳遞多重服務。

2.2 VPN 技術發展

2.2.1 VPN 技術發展

可區分為 Network-based、CPE-based 及 Application-aware 等三種 VPN 技術發展方向，如下圖所示。



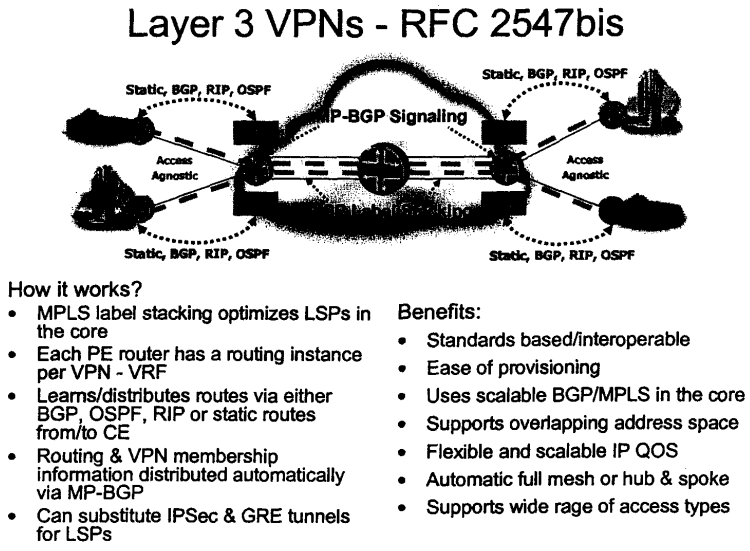
2.2.2 MPLS VPN 技術(Network-based)

由於網際網路的盛行，促成企業電子化、網路化、全球化的快速發展，傳統 circuit-based 之 FR/VPN 及 ATM/VPN 等服務，已逐漸被 IP-based 的 MPLS VPN 所取代，在全光網路上 IETF 也有工作群組(PPVPN)進行 GMPLS VPN 方面的探討，而目前 router-based 的 MPLS VPN 有 layer 2 及 layer 3 兩種服務。

(1)Layer 3 MPLS VPN 服務

客戶端的 CE 路由器藉由 Static/RIP/OSPF 協定與電信業者或 ISP 業者的 PE 路由器介接，然後經過 MPLS Cloud 中建立的標籤交換路徑 (LSP，Label switch path)，將客戶路由資訊交換到 VPN 另一端的 PE 路由器，再傳送給客戶另一端的 CE 路由器。這種 MPLS VPN 的方式可以建構 IP-based P2P 或 P2MP 的企業 VPN 網路，若再加上 MPLS 之 TE (traffic

engineering)功能，則可達到與傳統 VPN 類似的服務品質。不過，這種 MPLS VPN 模式只能提供 IP-based 的服務，而且大部份企業沒有能力維護這種 VPN，通常需要電信業者代為調整設定及維護，因此這種服務存在著客戶與 ISP 的互信問題。



(2)Layer 2 VPN 服務

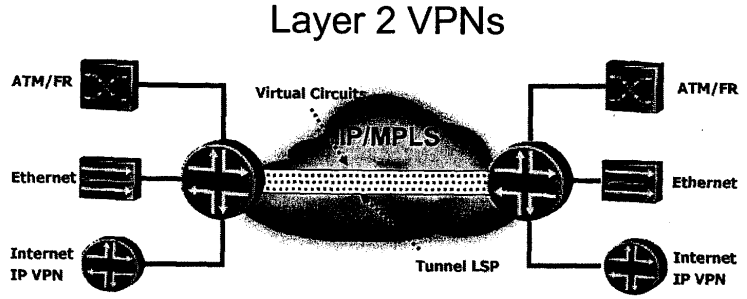
將 VPN 客戶分隔兩地的區域網路，透過公眾網路(FR、PPP、ATM 及 Ethernet)以類似 Tunnel 的方式建立一個虛擬連接，可讓兩地網路的第二層 Frame 直接互相進行交換，在這種架構下，客戶可以自己設定路由組態及傳送多種協定(包括非 IP 協定)，而且具有傳統專線的安全性。依連線的網路型態可區分為：

(I) 點對點 Layer 2 VPN 服務

要在 IP 網路上提供這項服務，必須將 FR/ATM 的 DLC/PVC 透過 MPLS 的封裝，經由 MPLS 建立的 LSP，對應到另端之 FR/ATM 的 DLC/PVC；然後封包從 Ingress PVC 透過 MPLS 網路的 LSP 傳送到 Engress PVC，而將兩端的網路連接起來。因此客戶可以利用這種

layer 2 VPN 來取代傳統的 FR/ATM 網路；目前有兩種 Draft 標準：Kompella 及 Martini。

其中 Martini 提供 Transparent LAN 服務，可以將企業 VPN 兩端的區域網路連接起來；不過市場較趨向 draft Kompella，因為它除了具備 Martini 功能外，還具備 Over provisioning 功能，可以解決建置大型 L2 MPLS VPN 網路的問題。



- Consolidate multiple service networks onto a single core network
- Focus of two IETF working groups
  - Provider Provisioned VPN (PPVPN)
    - Layer 2 VPNs over tunnels - Draft-kompella-ppvpn-l2vpn
    - Virtual Private LAN service - Draft-kompella-ppvpn-vpls
  - Pseudo Wire Emulation Edge to Edge (PWE3)
    - Various IETF drafts supporting encapsulation and service emulation of pseudo wires
    - Also known as Draft-Martini

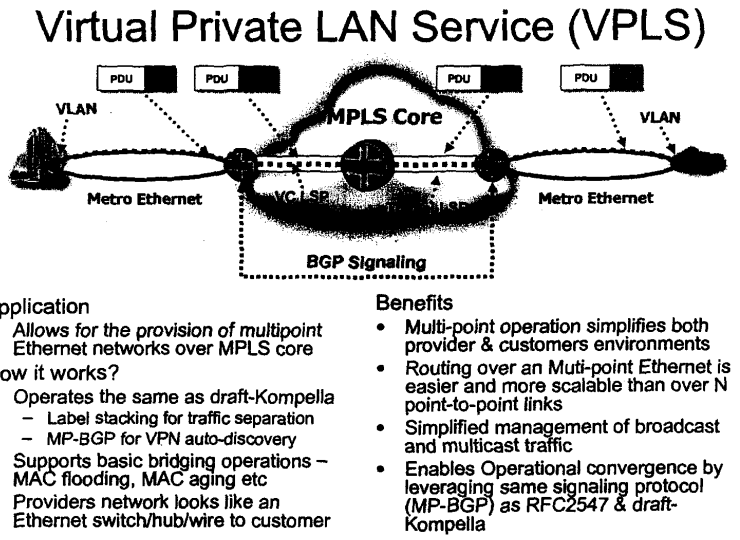
(II)多點互連 Layer 2 VPN 服務

這類服務比較符合大多數企業 Intranet 的需求，可提供客戶使用獨立的虛擬電路與路由交換協定，依據使用技術可分為 Layer 2 POS/ATM 與 Layer 2 MPLS 兩種。

(a) Layer 2 POS/ATM VPN：將 layer 2 的 VLAN Tag 對應在 POS 介面，使乙太網路的 VLAN Tag 可透過 POS 介面傳送，並具備 Spanning tree 等相關功能，以計算出最佳路徑。對 ATM 介面而言，VLAN ID 也可與 ATM PVC 號碼互相對應，透過 ATM 虛擬電路將相同 VLAN ID 的網路串接。不過，由於乙太網路需採用 Spanning tree 演算法計算最佳路徑，並將備用路徑暫時阻斷，因此每個

VLAN 的 Spanning tree 穩定度變成很大的問題，當故障發生時，重新選徑之收斂時間需要數十秒之久。

(b) Layer 2 MPLS VPN：即建立 VPLS(Virtual Private LAN Service)的方式，所謂 VPLS 方式是將電信業者所提供的 MPLS VPN 當成 Switch/Hub，連接不同的 CE，各點間可依據 MAC 位址互相交換封包。在建立 VPLS 服務時，每個 PE 路由器之間會建立 fully-meshed 的 LDP Sessions 作為 Signaling，用以建立正確的 LSP 資訊，因此 PE 路由器必須扮演 Transparent Bridge 的功能，只要學習每個 LSP 所含的目的地 MAC 位址，便可以知道封包要透過哪個 LSP 傳送到目的地，對於未知 MAC 位址的封包，則以 flooding 方式傳送給每個 VPLS 成員。目前有兩種 draft 標準：Laserre 及 Kompella。

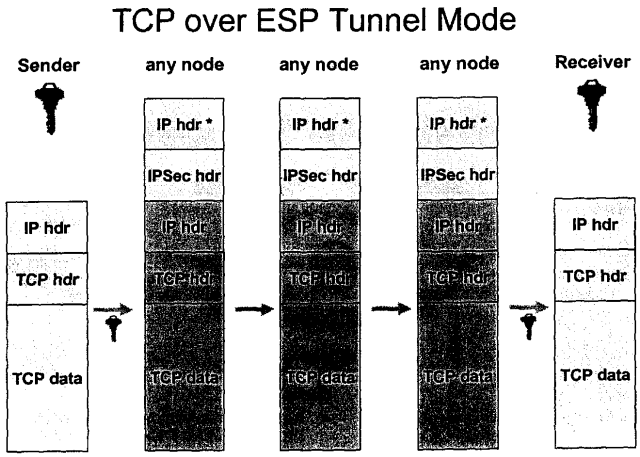


2.2.3 IPSec VPN 技術(CPE-based)

IPSec(Internet Security Protocol)是 IETF 提出的通用架構，為 IP 提供了許多安全措施的服務，保護 IP 協定方面有三個議題：加密演算法、

驗證演算法和 key management。在概念上，IPSec 是設計來保護網路本身，不會影響到所有應用程式的運作。

IPSec 支援兩種加密法：傳輸模式(transport mode)及通道模式(tunnel mode)。傳輸模式只針對封包中的 payload 加密，而通道模式則對 IP Header 及實際數據內容均予加密，因此理論上通道模式比較安全。IPsec 在 IP 的 datagram 使用 ESP(Encapsulating Security Payload)加密協定，ESP 支援大多數的對稱式加密系統，如 DES 和 Triple DES 等，也支援驗證功能；如下圖所示，ESP 能被用在另一個 IP 封包的內部，所以 ESP 可以在一般的 IP 網路上傳送。



ESP 利用對資料加密的方法來保障資料的安全，而 IPSec 中的另一個重要協定 AH(Authentication Header)則是專門用來進行驗證的工作，AH 可與 ESP 在通道模式搭配使用(或單獨使用)，AH 確保 IP Header 的安全，而 ESP 則著重於 payload 的保密。

最後，還必須在通訊雙方溝通時有一套 Security Association 的機制，也就是當通訊一開始時，雙方就必須協調出要用那一把 key，更必須

共同決定加密及驗證方法，而 IKE(Internet Key Exchange)協定提供了所有端點的驗證，掌握能夠使用的保全政策，並控制 key 的交換(使用 Diffie-Hellman)事宜。

目前企業 Intranet 或 Extranet 在穿過 Internet 時，多半搭配防火牆建置 Site to Site VPN(IPSec 加密)的架構；公司外動態作業員工與公司內部 Intranet 間則搭配防火牆建置 Client to VPN Gateway，再加上 Certificate management 機制(如 CA、LDAP、Radius)的方式，當使用者從家裡的網路環境連結上 VPN 時，IPSec VPN 可以提供以下安全通道:

(1) 每個使用者端必須安裝專屬的 VPN Client 軟體。

(2) 提供點對點的安全通道。

(3) 必須提供特定的網路位址。

(4) 必須做特定的網路設定。

(5) 必須提供使用者名稱及密碼做個人身份驗證。

但在無線網路的環境，IPSec VPN 的連線方式可能會遭受威脅。因為 IPSec VPN 主要是網路對網路的連結，具有長時間 Active 的特性。

2.2.4 SSL VPN 技術

SSL-VPN 機制係應用 SSL 通訊協定，由使用者端產生一個 SSL 加密通道，與後端的 SSL-VPN 主機建立連線。它可以針對 Web-based 或非 Web 的應用程式做保護，提供企業外部員工透過網路遠端登入公司內部所有應用程式的安全通道。而且在使用者端，不須安裝任何的專屬軟體或特別設定。在伺服器端，也不須更動原有的設定而致影響到應用程式的功能。SSL VPN 的運作模式，大幅降低了 IPSec VPN 的複雜設定，也擴大了更多應用程式的安全登入與存取，使用者只要使用一般瀏覽器，便能透過 SSL-VPN 安全通道查閱企業 Intranet 內的電子郵件及操作公司內部的所有應用程式。

SSL-VPN 的優勢，主要可以分為以下幾個層面來看:

(1) 不需要安裝 Client 軟體。

(2) 支援更多作業系統。

(3) 所有使用者的遠端連線都需要經過 SSL-VPN 伺服器，因此可以在 SSL-VPN 伺服器使用 ACL 管控機制，提供系統或網管人員更易於管理使用者權限，增加存取的安全控管。

2.2.5 IPSec 與 SSL VPN 的比較

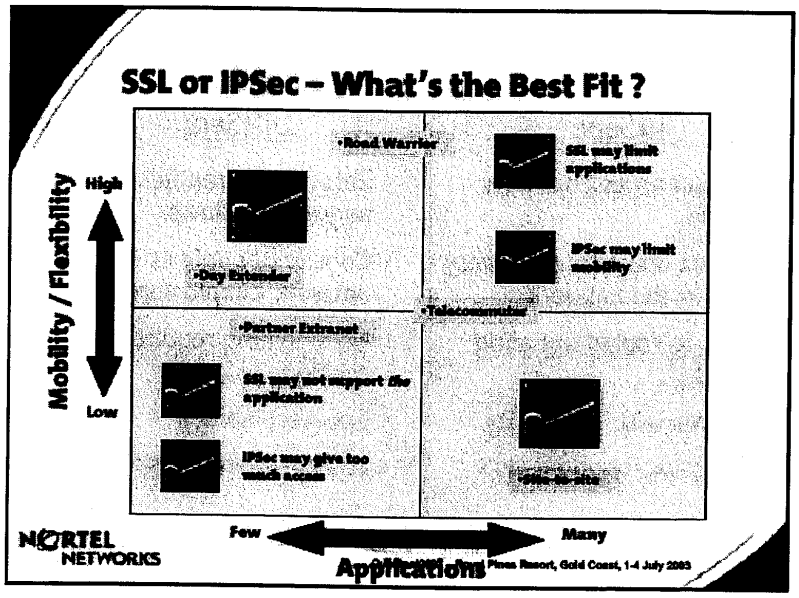
行動辦公室的發展趨勢相當明顯，企業對其重要資料安全存取之要求相形提高，尤其以遠端安全登入機制來看，IPSec 與 SSL VPN 均是目前企業考慮的解決方案。

使用 IPSec 的連線方式，每一個使用者端在網路上會被當成一個節點，而此連線會一直處於 Active 的狀態。因此，一但使用者端的電腦被駭客入侵，駭客就可以透過此 Active 的網路連結進入另一個端點，也就是公司內部。使用 SSL-VPN 的連線方式則可以避免類似的問題發生。因為 SSL 協定的運作模式就是 Client 端與 Server 端進行資料交換時，是採用 Stateless 機制處理(所謂 Stateless 機制是每一筆 Client/Server 的連線會在交易完成後，切斷連線，下一筆交易時將會重新啟動連線)，因此駭客入侵的機率大為降低。

當企業在外的動態員工需要從某客戶公司的網路環境登入企業內部 Intranet 存取資料時，如果使用 IPSec 的 VPN 架構，很可能他的連線要求會被客戶端的防火牆攔阻，因為這牽涉到該防火牆的安全政策、轉址與連線的問題。但是若使用 SSL VPN 方式，Application 在應用層交換時，都是透過 Port 80 和 443(一般 HTTP 連線都是經由這兩個 Port 溝通)，因此防火牆必須開通這兩個 Port；對系統管理者而言，使用 SSL VPN 可以提高管理的便利性，既然 SSL VPN 是應用層的協定，所有資料交換都會透過 Port 443 來處理，管理者只須管控 Port 443 及使用者 ACL 即可，不需要在防火牆上針對每一個應用程式開通所需的 Port，而造成防火牆打太多洞的風險。另外透過 Proxy Server 的幫助，可以增加了 SSL 連線速

度和穩定。

不過 IPSec VPN 已經為多數企業所使用，若全部改成 SSL VPN 機制，必須考慮到轉換成本，而且各種資訊應用的特性和安全要求不盡相同，可以由「Application」及「Mobility/Flexibility」兩個構面來分析 SSL 與 IPSec 的適用範疇，如下圖。



2.3 服務應用

Intranet 的服務應用相當廣泛，如視訊會議、網路教學、e 化、m 化、k 化及 p 化等多元應用，其中對本公司影響最大的是 VoIP 技術的導入企業 Intranet 網路，此趨勢將使得企業內之通訊網路發生變革，以往企業同時擁有電話網路及數據網路，選擇 VoIP 技術後企業內將不再需要電話網路，所有的通訊服務將整合在單一網路上。

要確保 VoIP 應用的通話品質(<200ms 的延遲)，IP 網路必須能夠提供 QoS 保證，以目前網際網路的運作模式及技術，要實現 Internet 上任何 end-to-end 的 QoS 有其困難，不過企業內部 Intranet 網路的 Domain 較

小、設備品牌單純，其 QoS 是可實現的，也因此 VoIP 在企業內部由最初的節費需求而逐漸全面採用，傳統 PSTN 反而成為備援或溢流話務之用。

2.3.1 QoS 技術

目前 IP community 制定了兩個 QoS 標準，分別為 IntServ (Integrated services) 和 DiffServ (Differentiated services)。其差異如下：

Comparison of IntServ and DiffServ

IntServ	DiffServ
• Hard guarantees per flow possible	• Relative guarantees for aggregated flows
• Complex operations at every router in the network	• Complexity only at edge of network, simple core routers
• Router to router signaling needed	• No signaling required (just configuration)
• Problems with scalability	• Good scalability
• Connection-oriented QoS	• Packet-oriented QoS

IntServ 使用 RSVP(resource reservation protocol)協定，針對各個 traffic session 建立一保留頻寬的 virtual circuit 來滿足 QoS 上的需求。此架構的好處是，首先，它對使用者提供了絕對保證的服務，再者，每個使用者的資料流都可以輕易地監控管理，並且可以運用現有的 routing protocols。相反地，IntServ 除了處理上有過多的 overhead 外，由於 IntServ 的特性使得網路在擴充性(scalability)上有相當限制是其最致命的缺點。

DiffServ 則是將具有相似 QoS 需求的 traffic 合在一起，對同一類型的資料提供一致性的服務與相對性的保證，而不是針對個別的 traffic session。每一類型的資料會有一個固定的 DSCP (DiffServ codepoint) 來區分，傳遞資料時，每一個 DiffServ node 會根據此類型資料的 DSCP，依據相對應的 Per-Hop Behavior 在 DiffServ domain 上傳送。這樣的方

法雖然沒有辦法對 QoS 達到絕對的保證，但相對於 IntServ 的致命傷，DiffServ 的架構漸漸取得其主流地位，但如何在 DiffServ 的架構上，提供各個的 traffic session 的 end-to-end QoS 保證正是亟待解決的主要問題。

DiffServ 中定義了幾種基本的 behaviors 為標準：

(1) Best Effort - 儘可能支援，在網路壅塞時首先遭 drop 的服務類別。

(2) Expedited Forwarding - 不能因網路壅塞而降低服務品質，以支援低延遲需求的服務。

(3) Assured Forwarding - 在網路壅塞時可依 contract 降低定量的服務品質(依據 drop precedence 來決定當網路壅塞時，那一個封包是可以放棄)。

2.3.2 VoIP 的應用發展

根據 IDC 統計顯示，2003 年網路電話的話務量預估將佔全球通訊流量的 43%，到 2006 年時其用量更將高達 6,345 億分鐘，由此可見網路電話已經成為重要的技術服務。

一個簡單的 VoIP 架構包含四個組成要素：

(1) 媒體閘道器(Media Gateway) - 負責將語音訊號轉為 IP 封包。

(2) 媒體閘道控制器(Media Gateway Controller) - 用來管理訊號傳輸與轉換，一般稱為 Gate Keeper 或 Call Server。

(3) 語音伺服器 - 提供忙線或電話不通時語音回應。

(4) 傳訊閘道器(Signaling Gateway)，亦即 SS7 傳訊閘道器，其中傳訊如同交換過程的控制單元，決定通話建立與否，以及提供相關加值應用服務。

目前 VoIP 的實際建置方法有三種方式：

(1) Basic Trunk/Route Replacement

在這種架構下，總公司與各地分公司之間透過WAN傳送VoIP的話務。企業內的話機收容在傳統PBX上，而該PBX已預先設定好內部話務會優先選用VoIP的路由；同時，PBX還維持傳統中繼電路到PSTN網路，以提供一條備用路由，供WAN發生用戶過量(Over subscription)時使用。

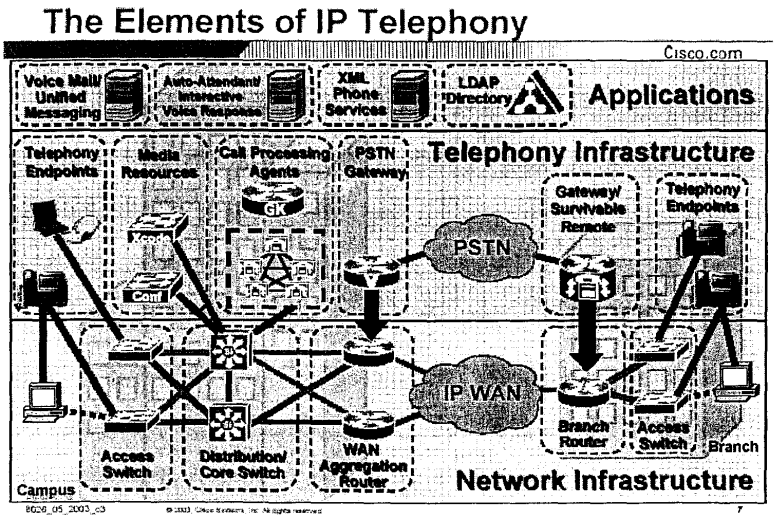
(2) Router-Based Key System

以路由器為基礎的Key System取代傳統的PBX，企業內的話機直接連接到一個多重服務的路由器平台，該平台包含了基本的Key System功能，透過WAN傳送總公司與各地分公司之間的通話，並利用PSTN傳送外線電話(Outbound Call)。

(3) Off-Premise Extension

在這種模式中，分公司的路由器使用WAN線路由總公司的PBX取得撥號音。該PBX讓分公司的分機號碼猶如在本地運作一般，且分公司的分機也同樣使用總公司的撥號對應表(Dial Plan)及語音信箱(Voice Mail)。所有從分公司撥打出去的外線電話，皆透過WAN傳送到總公司的PBX，然後再外傳至PSTN。

比較完整的VoIP商品如Cisco新一代IP電話系統為例，其語音、視訊及數據整合架構(Architecture for Voice Video & Intergraded Data; AVVID)解決方案，透過IP／PBX介面以及Voice Gateway，來取代原來交換機的架構，將整個企業環境整合在一起。全IP網路架構是直接採用IP PBX而不用傳統PBX，每位員工桌上配置的是乙太網路介面的IP Phone，撥出時以IP PBX中的Call Manager做轉接，一旦撥打到企業以外電話，只需再加一個VoIP Gateway即可連至PSTN轉送出去。相關元件參考架構如下：



隨著全球網路環境成熟及技術日新月異，網路電話解決方案也有革命性的突破，不僅使用界面更為容易，應用也更為多元。未來在相關技術及應用上的發展，將依個人及市場反應與需求，帶來更新、更經濟以及更人性化的多元化服務。

第三章 心得與建議

現代企業建置 Intranet 並導入多元應用服務已成為企業必備的商業基礎建設之一，藉由 IP 網路為基礎，更能提供企業整合語音、視訊及數據的網路架構，以提昇企業運作效率、節省時間、降低營運成本，進而增進生產力與企業競爭力。因此，適時導入新一代全光網路系統以滿足市場需求的頻寬，是確保本公司競爭優勢的必然趨勢。

企業為確保 IT 服務與功能的可用性、可靠性與安全性，VPN 會是企業建置 Intranet 與 Extranet 時的必要選項，商機無限。本公司是 IP 網路的最大供應者，在現有 IP 網路上已可提供 Network-based VPN 的產品；不過，企業營運模式存在多樣化，其建置 VPN 的方式也不盡相同，因此

CPE-based 及 Application-aware 模式的 VPN 仍存在很大的市場，而建置這兩種模式 VPN 之 IP 網路的選擇是個變數，並不是非本公司莫屬，因此，建議與優勢品牌的 VPN 設備廠商策略聯盟，以建立完整的 VPN 產品組合，增加市場縱深及滲透力，同時確保 IP 網路之市場佔有率。

由於實習時程很短，服務應用方面只能聚焦於 VoIP 的技術發展，VoIP 無論在 Dial Plan、Bearer Features、通訊品質各方面均逐漸接近傳統 PSTN 的水準，促成近年來 IP 網路電話之應用呈現爆炸性的成長，大多數的財星五百大企業，不是已開始建置這項技術，就是正在部署計畫中。根據 Phillips Group InfoTech 2000 的調查指出，四年內將會有超過 80% 的企業可能採用 VoIP，而擁有 500 名以上員工的企業將佔整個 IP 電話市場的最大部分。這樣的快速成長，勢必嚴重影響本公司的固網營收結構，有關整個固網服務產品的結構變革，本公司另有專業團隊積極進行評估與決策，本案實習重點旨在學習企業應用 VoIP 的經驗，以期在未來配合企業客戶 Intranet 整合服務之規劃上能發揮助益。

在電信自由化、全球化的趨勢下，市場競爭激烈，而 IP 科技進步的速度正符合摩爾定律，為使本公司能在快速變局下持續掌握市場優勢，透過了解歐美等先進國家 IP 寬頻技術與應用服務的發展現況與未來趨勢，吸取國外經驗，是技術深耕的有效策略之一，建議依技術屬性及其發展需要，適度延長研習時程，以充分發揮學習效果增廣見聞，累積資源建立競爭優勢。