公務出國報告

（出國類別：實習 ）

實習Edge Router Switch系統規劃設計裝機及維運技術

服務機關：中華電信股份有限公司
雲林營運處 北台中營運處
出 國 人 職　　稱：課長　　助理工程師
姓　　名：王啟文　　李少華

出國地點： 澳大利亞

出國日期： 92 年 12 月 07 日至 20 日

報告日期： 93 年 3 月 3 日

系統識別號:C09205481

公 務 出 國 報 告 提 要

頁數: 30　含附件: 否

報告名稱:

實習Edge Router Switch系統規劃設計裝機及維運技術

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:

王啓文　中華電信台灣中區電信分公司　雲林營運處　課長
李少華　中華電信台灣中區電信分公司　北台中營運處　助理工程師

出國類別: 實習

出國地區: 澳大利亞

出國期間: 民國 92 年 12 月 07 日 -民國 92 年 12 月 20 日

報告日期: 民國 93 年 03 月 03 日

分類號/目: H6／電信　／

關鍵詞: Edge Router,Cisco 7600系列,Supervisor Engine 720,MPLS/VPN,IP Multicast,802.1q,802.1q Tunnel

內容摘要: 近年來網際網路與無線通信的快速成長、互動式多媒體應用的蓬勃發展，全世界資訊流量因而呈現爆炸性的增長，各種新型之服務甚至語音服務將建構於封包技術，電信公司爲追求降低網路維運成本，增裕營收，皆致力於將傳統電信網路、無線網路與網際網路整合成新一代網路。新一代網路需具備彈性、模組化及更開放型之網路架構。各種不同服務之網路經由POP之Edge Router Switch銜接至大容量之核心網路(CORE)交換。爲瞭解Edge Router Switch在下一代網路之發展趨勢與影響，職等二人奉派赴澳洲Cisco公司實習「Edge Router Switch系統規劃設計裝機及維運技術」（本公司92年12月4日信人二字第92A3502132號函核准）。藉以吸取先進國家之技術及經驗，提供本公司日後系統規劃設計裝機及維運之參考。

本文電子檔已上傳至出國報告資訊網

目錄

1.前言

近年來網際網路與無線通信快速成長、影音多媒體應用蓬勃發展，全世界資訊流量因而呈現爆炸性的增長，各種新型之服務甚至語音服務將建構於封包技術，電信公司為追求降低網路維運成本，增裕營收，皆致力於將傳統電信網路、無線網路與網際網路整合成新一代網路。新一代網路需具備彈性、模組化及更開放型之網路架構，各種不同服務之網路經由POP之Edge Router Switch銜接至大容量之核心網路(CORE)交換。

Edge Router Switch 須具備各種接取網路介面，以匯集各種客戶接取線路例如：ATM、Frame Relay、Ethernet、xDSL、Cable 等，對於 QoS、可靠度的要求也相對提高，並可支援各種應用服務例如：網際網路、VoIP、IP-VPN、影音多媒體等。本次區分公司引進 Cisco 76xx 系列產品主要是接取 IP DSLAM 及 Ethernet-based FTTB，作為網際網路上網及互動式多媒體應用的訊務分流點。

寬頻網路中 Edge Router 擔任重要的一環，提昇接取網路使用效益是未來相當重要的業務，急需掌握及引進寬頻邊緣網路新服務應用及規劃設計能力，以提供新穎服務增裕營收。奉總公司九十二年十二月四日信人二字第 92A3502132 號函核准前往澳洲 Cisco 公司實習「Edge Router Switch 系統規劃設計裝機及維運技術」，藉以吸取先進國家之技術及經驗，提供本公司日後系統規劃設計裝機及維運之參考。實習期間(含行程)自民國九十二年十二月七日至九十二年十二月二十日為期十四天。本次實習課程計有：

Edge Router Switch overview

Cisco 76xx Series HW&SW introduction

Cisco 76xx Series operation and maintenance

Application and service in broadband IP network

2. Edge Router簡介

2.1 簡介

近年來網際網路與無線通信的快速成長、互動式多媒體應用的蓬勃發展，全世界資訊流量因而呈現爆炸性的增長，各種新型之服務甚至語音服務將建構於封包技術，電信公司為追求降低網路維運成本，增裕營收，皆致力於將傳統電信網路、無線網路與網際網路整合成新一代網路。

新一代網路需具備彈性、模組化及更開放型之網路架構，如圖2.1，各種不同服務之網路經由POP之Edge Router Switch銜接至大容量之核心網路(CORE)交換。

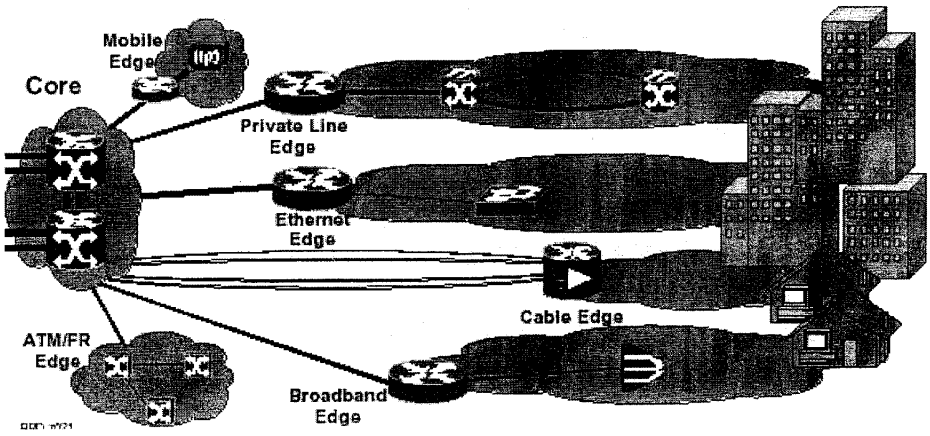


圖 2.1 新一代網路

2.2 Edge Router特性

為傳送大量之訊務並需維持高服務品質(QoS)及安全之需求，Edge Router須具備以下特性：

1.備援支援(Redundancy Support)--須有快速回復網路運作之備援措施以維持網路核心之穩固性。

2.多數目之佇列(Queues)--每一埠須支援多數目之佇列(至少四個)透過智慧形運算排列以管理流量。

3.智慧形網路之服務(Intelligent Network Services)--如服務品質(QoS)，安全(Security)及負載平衡(Load Balancing)。

4.第二層至第四層之服務品質(Layer 2 to Layer 4 QoS)—以支援大量的應用程式。

5.支援主要的路由通訊協定(Important Routing Protocols)—包括路徑選擇訊息協定【Routed Information Protocol (RIP)】、開放系統最短路徑優先協定【Open Shortest Path First (OSPF)】、進階內部閘道路由協定(Enhanced Interior Gateway Routing Protocol)及多點廣播協定(Multicast Protocols)，例如協定無關多點通訊協定【Protocol Independent Multicast (PIM) Protocol】。

6.模組化架構

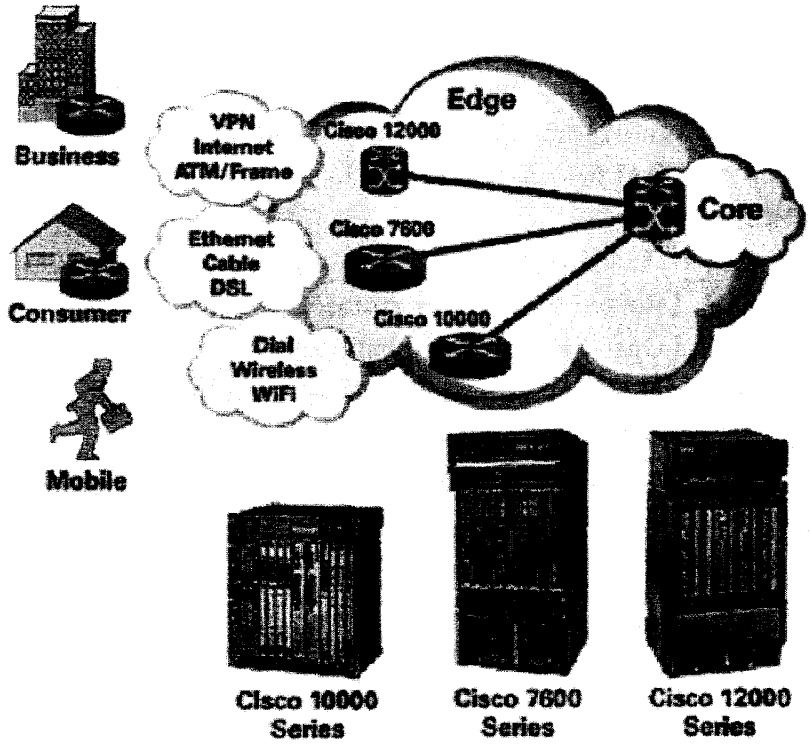
可依需要逐漸擴充。

7.支援多速率之介面

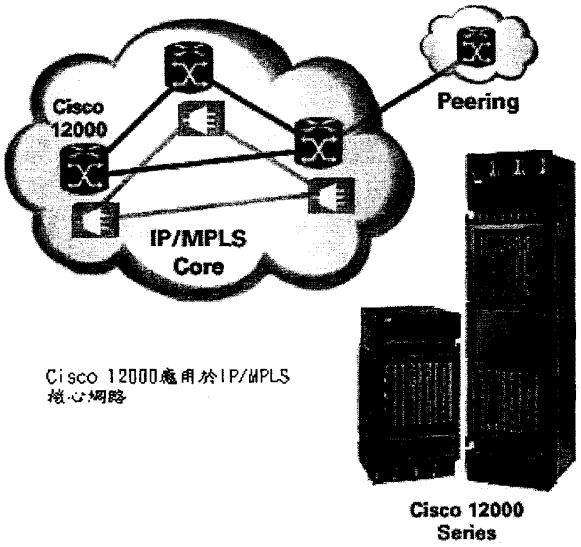
T1/E1、DS3/E3/OC-3c ATM、OC-3c POS(Packet Over SDH)、Gigabit。

2.3 適合之產品

Cisco 公司 Router 產品中有三種 Cisco 12000, 7600 and 10000 series routers 可供 Edge Router 使用。



思科新一代12800/12000/7600網路設備更是做到了性能更快、服務更智慧，從而讓企業和網路供應商可以真正地在整個網路中部署創新的、高性能的網路服務，以支援更高的用戶移動性、內容聯網和存儲聯網解決方案以及語音、視頻和資料一體化的結構體系。網路供應商需要不斷的拓展網路以滿足客戶不斷增長的服務需求。爲了提供高品質的Internet服務，網路供應商需要不斷提高每個用戶的接入頻寬。思科核心和邊緣產品Cisco 7600和Cisco 12000的平滑升級在提高產品性能的同時，最大限度地利用現有的網路設備，保護了以往的投資。Cisco 12000系列新品：將全球最大的核心網路的容量提升一倍。



Cisco 12000應用於IP/MPLS
核心網路

不論在網路核心和邊緣，思科12000系列產品都是業界性能價格比最好的產品，思科12800構建于12000系列路由器分散式結構，但該設備性能比12000有了數倍的增長，達到了質的提升，在開發Cisco 12800的過程中，思科特別注重保護現有的投資，因此客戶當前的所有Cisco 12000系列線路卡均可在Cisco 12800上使用。每塊線路板卡擁有高密度的OC-192和 OC-48埠，並提供40Gbps的交換容量，可以支援集中式和分散式分組轉發，大大提升資料轉發速度，思科12800提供一組業界領先的業務創建特性，特別是支援並拓展了業界領先的多協定標籤交換(MPLS)，可實現業務量管理、虛擬專用網(VPN)、ATM收容中繼業務，思科新一代核心路由器將滿足網路發展過程中企業和運營商不斷增長的網路可用性、網路可擴展性、網路安全性以及網路可控性。

思科新一代12010和12006產品配合ISE（IP Services Engine）板卡後，可以提供高效、高性能的網路邊緣服務，思科ISE板卡支援標準的IPV4和IPV6協定，可完美的實現QOS、內容組播和即時語音、視訊服務。全新的背板支援所有的2.5G線路板卡，高擴展性則爲用戶提供了一條經濟有效的、可移植的升級方案，只需軟體升級，就可以平滑升級到10Gbps，從而可以增強應用功能，最大限度地利用現有的網路投資。爲了滿足核心和邊緣的網路服務，思科還對12000系列產品進行了系統優化，其借助新引擎 (PRE2)在性能上取得了重大突破，通過增強CPU的性能和增加記憶體容量，新一代12000產品支援四百萬條路由表。

因本公司LAYER 3 SWITCH採購案，CISCO公司得標提供7600系列之ROUTER，此次前往CISCO公司實習，偏重於研習7600系列之ROUTER。

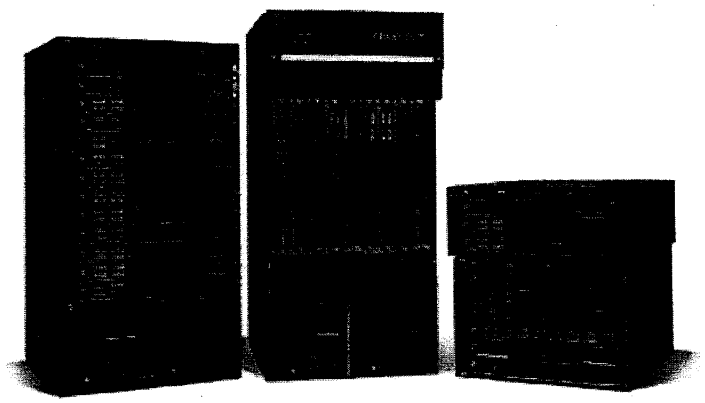
3. Cisco 7600 Series Router

3.1 產品定位

Cisco 7600 系列為企業、校園和 ISP 電信網路提出了新的 IP 資料傳輸和應用的支援標準，它不但能提高用戶的生產率，提升操作控制能力，還能提供優越的投資保護。作為 Cisco 重要的路由器，7600 系列路由器能夠提供安全的 End-to-End 整合式網路服務，提供使用的範圍從連接大量用戶端到核心骨幹，延伸到 ISP Data Center 和 WAN 連線。

Cisco 7600 系列能夠提供多樣化的機型和 LAN/WAN/MAN 介面，提供可擴展的性能和連接埠數量，因而能幫助企業和 ISP 電信業者降低總體擁有成本。

Cisco 7600 系列交換器提供 3 插槽(7603)、6 插槽(7606)、9 插槽(7609)和 13 插槽(7613)的機型詳如圖 3.1，以及多種整合式服務模組，包括 Gigabit 等級的網路安全、內容交換、語音和網路分析模組。7600 系列中的所有機型都使用了相同的模組和作業系統軟體，形成了能夠針對未來擴充的硬體架構，由於能提供操作介面的一致性，因而能提高 IT 基礎設施的使用率，並增加投資效益。從 48 埠到 576 埠的 10/100/1000 Ethernet 埠或者 192 個 1Gbps 或 32 個 10Gbps 骨幹埠，提供高達 400Mpps 封包處理能力的網路核心，Cisco 7600 系列路由器能夠借助備援路由與轉送引擎之間的故障自動切換功能提高網路正常運作率。



7613(左)　7609(中)　7603(右上)　7606(右下)

圖 3.1 Cisco 7600 系列機型

Cisco 7600 系列具有許多領先的功能，它同時支援三代模組，這些模組不但能不斷提升 7600 的整體價值，也同時表現出思科對於技術創新的重視。思科的新一代 7600 系列模組和交換引擎 Supervisor Engine 720 包含思科新開發的 11 種 ASIC 晶片組，它不但提升了思科在網路界的領先地位，還能提供優越的投資保護。

3.2 Cisco 7600系列的優點及未來發展擴充策略

Cisco 7600 系列不但能為企業和 ISP 電信業者提供市場領先的服務、性能、埠密度和可用性，還能提供優越的投資保護能力，包括：

- 最長的網路正常運行時間--利用平臺、電源、管理模組、交換背板和網路協定服務的備援功能，可提供 1～3 秒的故障切換，提供應用和服務連續性整合在一起的完整網路環境，減少關鍵業務資料和服務的中斷。
- 全面的網路安全性--將 Gigabit 速率等級的思科安全解決方案整合到現有網路中，包括入侵偵測、防火牆、VPN 和 SSL。

- 可擴展性能--利用分散式封包傳輸硬體架構，提供高達400Mpps 的封包傳輸效能。
- 能夠針對未來發展並保護投資的硬體架構--在同一種機型中支援新舊可互換、可熱插拔的模組，以提高 IT 基礎設施利用率，增大投資回報，並降低總體擁有成本。
- 操作一致性--3 插槽 、6 插槽、9 插槽和 13 插槽機型可使用相同的模組、Cisco IOS Software、Cisco Catalyst Operating System Software 以及可以安裝在網路任意地方的網路管理工具。
- 卓越的服務整合和靈活性--將安全和內容等高級服務與傳輸網路整合在一起，提供從 10/100 和 10/100/1000 到 10GbE 網路，從 DS0 到 OC-48 的各種介面和密度，並能夠在任何專案中提供 End-to-End 的服務。

3.2.1 在End-to-End 安置Cisco 7600系列達成操作上的一致性

- 3 插槽、6 插槽、9 插槽和 13 插槽機型使用相同的模組、軟體和網路管理工具。
- 可安裝在網路的任意地方--從佈線室到核心、資料中心和廣域網路邊緣。
- 為降低備品和教育訓練成本，與 Cisco 6xxx 交換器系統使用相同的廣域網路埠子卡。
- 用戶可以自行選擇所有管理模組上支援的 Cisco IOS Software。

3.2.2 提高網路正常運行時間，提高網路彈性

- 提供封包丟失保護，能夠從網路故障中快速恢復。
- 能夠在備援管理模組間達到快速的 1～3 秒故障切換。
- 提供可選的高性能 Cisco 7600 系列 Supervisor Engine 720、Passive Backplane、多管理模組的備援能力；並可利

用 Cisco EtherChannel 技術、IEEE 802.3ad Link Aggregation、IEEE 802.1s/w 和 HSRP/VRRP 達到高可用性。

3.2.3.整合式高性能的網路安全性和網路管理

- 不需要部署外部設備，直接在 7600 機型內部署整合式的 10Gbps 的網路服務模組，以簡化網路管理，降低網路的總體成本。這些網路服務模組包括：
- 數個 Gigabit 速率等級的防火牆模組--提供接入保護。
- 高性能入侵檢測系統（IDS）模組--提供入侵檢測保護。
- Gigabit 速率等級的網路分析模組--提供可管理性更高的基礎設施和全面的 RMON 支援。
- 高性能 SSL 模組--提供高性能的安全電子商務流量傳送。
- Gigabit 速率等級的 VPN 和基於標準的 IP Security（IPSec）模組--降低 Internet 和 Intranet 的連接成本。

3.2.4 提供網路內容和網路應用的第 2～7 層交換服務

- 整合式內容交換模組（CSM）能夠為 Cisco7600 系列提供功能豐富高性能的伺服器和防火牆網路負載平衡連接，以提高網路基礎設施的安全性、可管理性和強大控制。
- 整合式 Gigabit 速率等級的 SSL 加速模組與 CSM 結合在一起，能提供高性能的電子商務解決方案。
- 整合數個 Gigabit 速率等級的防火牆和 CSM 能提供安全的高性能資料中心解決方案。
- 基於網路的應用識別（NBAR）等軟體特性可提供加強網路管理和 QoS 控制機制。

3.2.5 可擴展的性能

- 利用分散式 Cisco Express Forwarding dCEF720 平臺提供業界最高的交換器性能--400Mpps。
- 支援多種 Cisco Express Forwarding（CEF）高速交換方式和交換速率。在用戶端、核心骨幹、資料中心、廣域網路連線部署以及 ISP 電信業者網路均可提供最佳的網路設計。

3.2.6 豐富的第 3 層網路服務

- 豐富的第 3 層路由協定支援滿足了傳統的網路要求，並能夠為企業網路提供順暢的轉換機制。
- 硬體設計所支援的效能，提供從企業到 ISP 電信業者的大量路由表。
- 硬體支援 IPv6，提供高性能的 IPv6 服務。
- 在硬體中提供 MPLS 及 MPLS/VPN 的支援，可應用在高速 ISP 電信業者的網路核心和都會 Ethernet 網路，提供豐富的 MPLS 服務。

3.2.7 加強的資料、語音和視訊服務

- 在所有 Cisco 7600 系列平臺上提供整合式的 IP 資料傳輸 。
- 提供 10/100 和 10/100/1000 介面模組，借助在介面模組內增加電源子卡就可讓這些介面模組提供 In-Line Power，提供 IEEE 802.3af 的支援，保護今天的投資。
- 提供高密度的 T1/E1 和 FXS 的 VoIP 語音閘道介面，可與公共電話網（PSTN）、傳統的電話、傳真和 PBX 連接，提供 VoIP 服務。
- 支援高性能的 IP Multicast 語音和視訊應用。
- 提供一個統一管理的、經濟的、可靈活擴展的網路。

3.2.8 最高的介面靈活性、可擴展性和埠密度

- 滿足高密度用戶端、核心骨幹和分佈網路需要的埠密度和介面類型
- 每台設備可提供 576 個支援語音的，具有線上電源的 10/100/1000M Ethernet Copper 介面。
- 提供 192 個 GBIC Gigabit Ethernet 介面。
- 率先推出業界第一個 10Gigabit Ethernet 網路介面，和可提供高密度的 OC-3 POS 介面的 Channelized 的 OC-48 介面。
- 機型從 3 插槽（7603）、6 插槽（7606）、9 插槽（7609）到 13 插槽（7613）。

3.2.9 高速廣域網路介面

- 提供與其他核心路由器相容的高速廣域網路、ATM 和 SONET 介面。
- 單一平臺實現 WAN/LAN/MAN 網路整合管理和優越的投資保護。
- 高度靈活的模組化硬體架構，在同一機型內支援新舊模組搭配使用。
- 所有交換管理模組上都支援 Cisco IOS Software。
- 10/100Mbps 和 10/100/1000Mbps 乙太網路模組可現場升級為 InLinePower 的模組，可讓用戶在需要時升級支援 IP 電話技術和無線網路連接。
- 可在各種應用場合中增加的不斷推出的網路服務模組。
- 包括 Cisco 7600 系列網路安全、內容交換和語音功能等各種模組。
- 未來的模組將進一步提高性能、埠密度，並推出其他服務。

3.2.10 適用於都會 Ethernet 網路廣域網路服務

- 802.1Q 和 802.1Q Tunnel（Q in Q）提供點對點和點對多點的乙太網路服務。

- EoMPLS 的功能提供了 VLAN 的 Transparent 功能，大幅提升 MPLS 骨幹網中的乙太網路服務擴展能力。
- 通過在第 2 層和第 3 層 QoS 功能中提供 Rate Limit 和 Traffic Shaping，可在都會 Ethernet 網路服務中提供分級的寬頻服務。
- Enhanced Spanning Tree、IEEE 802.1s、IEEE 802.1w 和 Cisco EtherChannel IEEE 802.3ad Link Aggregation 功能大幅提升了網路的可用性。

3.3. Cisco 7600 系列交換器硬體轉送架構

Cisco 7600 系列路由器模組使用下列三種轉送技術 每一種都有不同的特性和架構以及效能：

- Cisco Express Forwarding (CEF)—高達 30 Mpps 效能，這種技術使用位於管理模組上的 PFC 子卡，作為集中式 CEF 的轉送引擎。配合 CEF 轉送表，轉送引擎集中地決定封包如何轉送。
- Accelerated Cisco Express Forwarding (aCEF)—適合用在高效能的企業環境，這種技術使用 aCEF 引擎和模組上的 aCEF 轉送表來轉送封包，模組上的 aCEF 轉送表是依據管理模組上 PFC 子卡的 CEF 轉送表而產生，可以協助模組作大量封包的區域封包交換。
- Distributed Cisco Express Forwarding (dCEF) —適合在最需要大量傳輸的環境，這種技術使用位於模組上 DFC 子卡的 dCEF 引擎，並配合由管理模組上集中 CEF 轉送表所複製而來的 dCEF 轉送表來自行轉送封包，提供最高的效能和延展性。

3.4. Cisco 7600 系列交換器之交換架構

Cisco 發展下列的交換架構使得交換器平台得以持續擴充：

- 32-Gbps 匯流排—可以存取集中分享式的匯流排。
- 256-Gbps 交換背板—位於交換背板模組。

- 720 Gbps 交換背板—位於 Cisco Catalyst 6500 Series Supervisor Engine 720。

3.5 管理模組 Supervisor Engine 720

Supervisor Engine 720 其整合更多強大的功能以及更優秀的效能，如下：

硬體支援 IPV6 (Hardware Based internet Protocol Verision 6)。

硬體支援 ACL (Hardware Based Access Control List)。

硬體支援 GRE 通道 (Hardware Based GRE tunneling)。

系統傳輸效能最高可達 400Mpps。

系統背板頻寬可達 720Gbps。

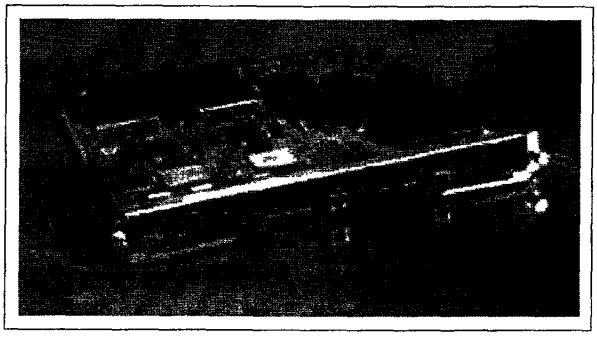


圖 3.2 Supervisor Engine 720

Supervisor Engine 720 支援 Catalyst 7600 系列的第三代管理模組，能夠能爲使用者提供先進的 IP 服務，並提高連接埠密度。Supervisor Engine 720 爲使用者在多層交換網路中的 IP 通信和應用設立了新標準，它不但能提高網路的效能，還能增強對所有 Catalyst 7600 系列介面的操作控制，包括新推出的高密度 10 Gigabit 模組。Supervisor Engine 720 支援所有現有的模組，以及各種新應用。新推出的 Catalyst 7600 Supervisor Engine 720 將高性能的 720Gbps 交換背板與新型的路由和傳輸引擎，包括第三代 Policy Feature Card（PFC3）以及 Multilayer Switch Feature Card 3(MSFC 3)，整合在同一片模組中。此外，Supervisor Engine 720 是建立在成熟的 Cisco Express Forwarding（CEF）體系結構上，支援集中轉發送（CEF）以及分散式轉發送（dCEF）、加速 CEF（aCEF），以提供適合高效能核心交換器的高度可擴充性且經濟有效的平臺，以滿足網路供應商部署的最高

要求，並建立具有彈性、安全可靠、可以擴充的模組化多層交換解決方案。藉由 720Gbps 的交換背板頻寬，Supervisor Engine 720 的交換能力可達到 400Mpps 相較於前一代的 210Mpps 有著長足的進步，因而非常適合部署在需要高效能的核心層。

Cisco Catalyst 7609/7613 搭配 Supervisor Engine 720 管理模組將可以提供極佳的效能以及更高更穩定的備援機制，不但管理模組本身可以支援備援功能，且由於將背板模組(Switch Fabric)整合進入管理模組內後，無須如同前一代之設計管理模組與背板模組需分開佔用不同模組插槽而減低 Catalyst 7609/7613 的可用性。以目前 Supervisor 720 之架構而言可以支援完全的負載備援的能力，不會因為單一背板模組(Switch Fabric Module)的失效而對於效能產生極為嚴重的影響，進而造成 本公司網路系統效能大幅的大幅下降。

新一代的 Cisco Supervisor Engine 720 不論在交換容量或是交換效能上相較於 Cisco Supervisor Engine II 均有長足的進步，多數的重要路由協定(Routing Protocol)均由硬體來做處理，有效解決交換器在面臨大量封包流量時所可能產生的系統延遲或是交換器效能大幅下降之困擾，成功解決設備在現在或是未來再擴充所產生網路流量大幅成長時所可能遭遇到的問題，為快速成長的網路系統提出一個有效的解決方案，並且能有效的抵抗電腦病毒對於網路所發出的攻擊封包譬如：拒絕服務攻擊(Denial of Service)等其他的攻擊，在相同攻擊模式下 Supervisor 720 均能承受更大幅度的網路封包攻擊，不至於產生效能的大幅下降。

4. 在Catalyst 7600/6500系列交換器上運用.1q來構成第二層虛擬私人網路

802.1q隧道化功能能經由使用CatalystR 7600/6500系列交換器上的IEEE 802.1q協定來建立安全的VPN，這個功能令服務供應商從它們基礎建設裡的不同客戶來分離流量，同時明顯地減少支援VPN所需的VLAN數量。多重客戶VLAN可以在Catalyst 7600/6500交換器上的單一VLAN裡運送，而不會失去自己專屬的VLAN ID。在服務供應商網路裡，支援.1q隧道所需的VLAN數量可以明顯地減少，在一個分享的基礎建設上部署VPN作企業級聯線就如同在私人網路裡一般，一樣能擁有安全性，優先排序，可靠性和易於管理等優點。這個應用方案提供了一個.1q隧道化的概要和在網路裡的應用性，尤其是服務供應商的網路。這份文件也包含了一個簡略的設定導覽以及.1q隧道化的範例。

4.1 無 .1q 隧道化的服務供應商網路設計

客戶可能會提出有關於所支援的VLAN總數或特定VLAN數量之任務的第二層連線需求，但客戶所需的VLAN範圍可能會重疊(請參閱圖4.1)，一個錯誤的安排可能導致不小心混合了不同客戶的流量通過該網路基礎建設，雖然利用分派一個獨特的VLAN範圍給服務供應商網路裡的每個客戶便可解決這個問題，但是這個解決方法將會很容易的便消耗掉802.1q裡所支援的4096 VLAN空間。

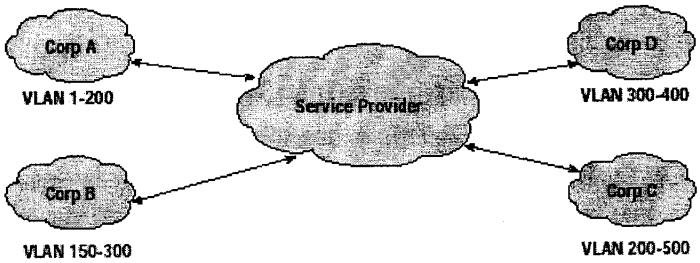


圖 4.1 Corp B 和 Corp C 的流量在重疊 VLAN 之上

.1q 隧道化能透過在隧道裡不遺失原有的客戶 VLAN ID 情況下，允許服務提供者去分配一個 VLAN 給每個客戶便能處理這個限制。

4.2 .1 q 隧道化的網路設計

一個在服務供應商環境裡去支援眾多客戶的理想方案，是讓客戶利用任何範圍的 VLAN 數字同時服務供應商轉送不受那些 VLAN ID 支配的流量。經由分配一個獨特的 VLAN 給每個客戶，從客戶方來的多重 VLAN ID 身分便不會遺失。如此能構成一個在服務供應商核心裡便隔離來自不同商業客戶流量以及.1q 標示過有適當 VLAN ID 的第二層 VPN。.1q 隧道化本質上是種透過重新標記已標記過的封包進入服務供應商之基礎建設來延伸 VLAN 空間的 1q-in-1q 技術，如圖 4.2 所示:

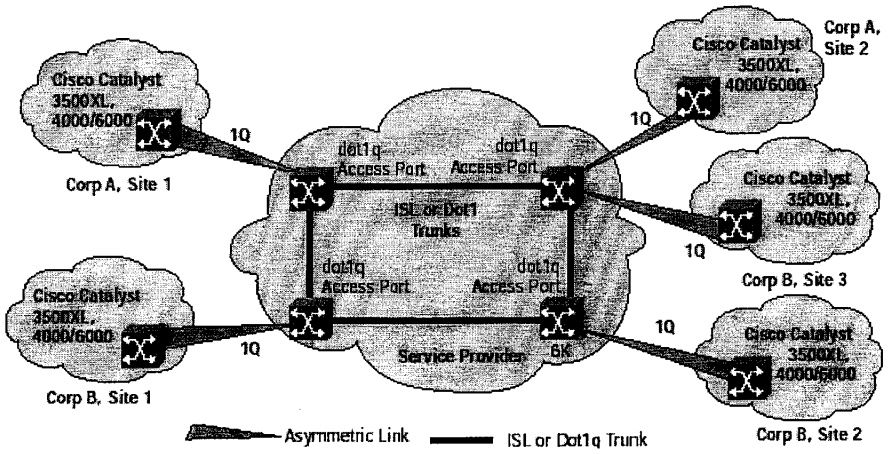


圖 4.2 服務供應商網路裏的單點對多點之.1q 隧道化設計

客戶方的介面被設定為 802.1q trunks(InterSwitch Link[ISL]並不被支援)，而服務供應商邊緣交換器的介面則被設定為特殊的.1q 隧道存取埠，這個特殊存取埠是被設定了一個服務供應商分配給每一個客戶的獨特 VLAN，當這個通訊埠接收到來自鄰近設備的隧道流量時，並不會依照平時從訊框標頭移除 802.1q 的程序，而是會保留原來的標記並放入所有接收到的 802.1q 流量至分配的 VLAN 到該隧道埠去，結果便是流量被雙重標記就像進入服務供應商的基礎建設一樣，用戶端設備(CPE)可以是任何能理解 802.1q 幹線協定的 Cisco 交換器。

4.3 操作與維護

4.3.1 操作細節

這章節描述訊框假設從 CPE 通過.1q 隧道到達服務供應商網路上的出入口之流動過程，圖 4.3 說明過程，而程序將會在下面以分段式敘述。

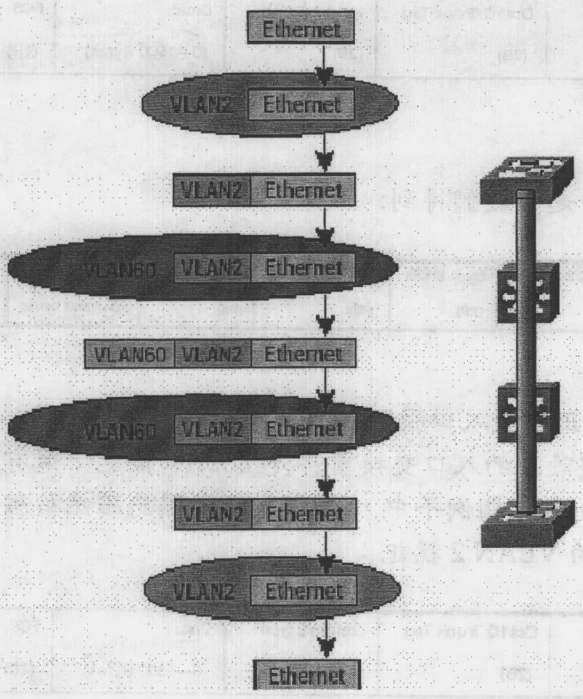


圖 4.3 訊框穿越一個.1q 隧道

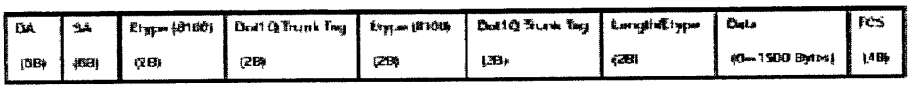
1. VLAN 2 上的乙太網路訊框從客戶那裡抵達服務供應商交換器，客戶交換器可以是任何能支援.1q trunks 的 Cisco 交換器。

   註：ISL trunks 並不被支援；來自 CPE 的對外訊框必須如描述般具有.1q 封裝。

2. 服務供應商網路上的入口 Catalyst 6500 交換器並不會從進來的訊框中剝除任何.1q 標頭，但會依據幹線協定加上額外的封裝，在這個例子中，在服務供應商交換器上的這個客戶除了使用 VLAN 60 外還加上了標記，建議最好是讓 ISL trunks 在服務供應商基礎建設內來搬運隧道流量，標準的 802.1q trunks 需要非常仔細的設定，因為錯誤可能引導隧道流量至錯誤的通訊埠進而流至錯誤的客戶，下面是訊框離開 Catalyst 6500 交換器的圖表。

DA	SA	Etype (8100)	Dot1Q Trunk Tag	Length/Etype	Data	FCS
(6B)	(6B)	(2B)	(2B)	(2B)	(0—1500 Bytes)	(4B)

與.1q trunk 封裝一起，我們得到:



註：兩個.1q 標記正離開入口服務供應商交換器。

3. 服務供應商基礎建設上的入口交換器移走 802.1q 標記，還有流量被從隧道中移走，在這個例子中，VLAN 60 的標記雖然被移走了但仍保留了原來的 VLAN 2 標記：

DA	SA	Etype (8100)	Dot1Q Trunk Tag	Length/Etype	Data	FCS
(6B)	(6B)	(2B)	(2B)	(2B)	(0—1500 Bytes)	(4B)

最後，客戶交換器移走了原來的 VLAN 2 標記然後轉移訊框到最後的主機：

DA	SA	Length/Etype	Data	FCS
(6B)	(6B)	(2B)	(0—1500 Bytes)	(4B)

由於隧道流量在 Catalyst 交換器裡保留了 802.1q 標記以及到背板的封包已被標記(意思是指在 MAC 位址域後面多了一個額外的四位元組)，訊框內的位元組進行重新組合，而且 IP 標頭資訊不再能夠被辨識，第二層訊框除了是無效長度標頭，將加強下列限制：

- 第二層訊框裡的第三層封包無法被辨識。
- 第三層(含以上)參數無法在隧道中被辨識(譬如，來源/目的地 IP 位址)也因此無法被路由或第三層監督。
- 交換器只用第二層參數(VLANs，來源/目的地 MAC 位址)來過濾隧道流量。
- 交換器只能提供實體層 QoS 給隧道流量，基礎建設裡的流量無法

享有如同在客戶層裡般的同等 QoS。

- 802.1q 隧道化功能無法在通訊埠上設定來支援私人 VLANs 或是 IP phones，VLAN 幹線協定(VTP)無法在非同步連接上的設備作用，還有在客戶網路與服務供應商網的 VTP domains 是不一樣的。
- 非同步連接不支援動態幹線協定(DTP)，因為只有一端的連接是 trunk，在客戶端上的 802.1q trunk 埠之設定，需要 nonnegotiate dot1q trunking keyword。

4.3.2 擴充樹協定指導方針

.1q 隧道化的主要作用是在於能在服務供應商團打開通道讓客戶的第二層數據封包以及橋接器通訊協定資料單元(BPDUs)通過，客戶必須在入口交換器上使用多重擴充樹(PVST+)，而服務供應商基礎建設則可能是使用多重服務擴充樹協定(MISTP)-PVST+擴充樹模式(Spanning-Tree Mode)或是 PVST+模式，MISTP-PVST+擴充樹模式是一種能在 Catalyst 6500 交換器/Cisco 7600 上使用 MISTP 功能，同時還能與其他像是 Catalyst 3500/4000/5000 系列/Cisco 7600 等使用 PVST+擴充樹模式的交換器繼續通訊的轉變擴充樹模式，MISTP 模式並無法在服務供應商基礎建設裡使用，因為使用 PVST+模式的交換器連結使用 MISTP 模式的交換器時並無法發現其它交換器的 BPDUs，這會在網路裡形成迴遞的狀態，MISTP-PVST+擴充樹模符合 PVST+的限定。

4.3.3 擴充樹互動

擴充樹協定(STP)主要是設計用來移除第二層交換網路裡的迴遞，現存區域網路環境也定義了 STP，在交換網路裡，802.1q trunking 定義了 VLAN 必須在交換器之間傳遞的方式。然而，每個 VLAN 的 STP 並非皆完全被 802.1q 所限定，起碼必須有使用一個標準的 STP(原有 VLAN 的 STP)，但是對已標記之 VLAN 的 STP 傳輸並無任何限定，加上了 802.1q 隧道化功能會讓擴充樹狀況更為複雜，比如說，一個客戶的 VLAN 2 之 STP 絕不能干擾另一個客戶的 VLAN 2 之 STP，要解決這個問題，802.1q 隧道功能就不能傳輸已通之 VLAN 的

STP，只有原有的 VLAN STP 被使用，由於 STP 互動的關係，當使用 802.1q 隧道化時並非所有的設計皆有效，802.1q 隧道化並不允許客戶方之間的互相聯繫有第二層迴遞，如圖 4.4 所示，唯一被允許有迴遞的設計是讓客戶方的 CPE 交換器連接上服務供應商核心裡一樣的 Catalyst 6500/Cisco 7600。

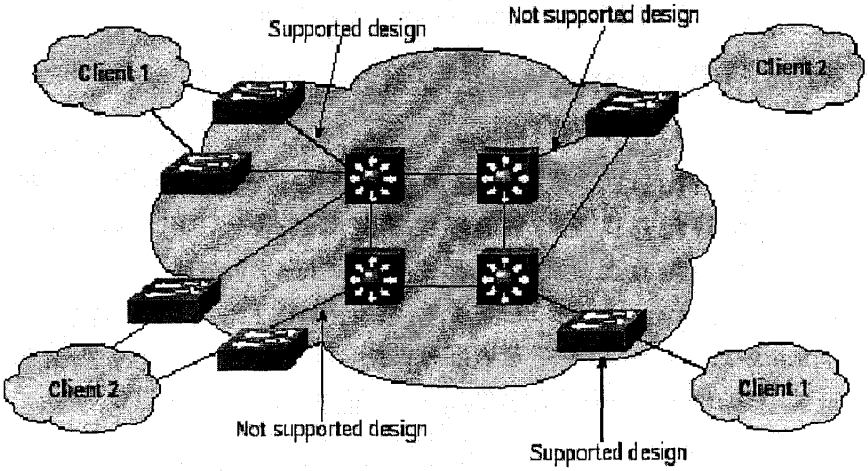


圖 4.4 .1q 隧道化客戶與服務供應商之擴充樹拓樸

4.3.4 在入口交換器的根守衛

在交換網路裡，擴充樹的根(root)是非常重要而且必須在服務供應商與客戶網路時連接時被防護，而這時候就需要根守衛(Root-Guard)的功能來達成這個目的。擴充樹的計算係利用橋接器 ID (BID)與路徑成本(path cost)，BID 是一個單一、由兩個次域所組合成的 8 位元組域，如下圖所示：

Bridge Priority	MAC Address
(2 bytes)	(6 bytes)

在網域中往往具有多台交換器，但是在擴充樹架構中只有一台交換器能夠擔任根(Root)的角色。因此 Catalyst 交換器將從眾多橋接

器中選擇具有最低BID值的來作為唯一的根橋接器。而在每一台交換器中，預設的橋接器優先序是32768。橋接器優先序越低，則愈可能成為根橋接器。如圖 4.5所示，假如在.1q隧道化方案裡的客戶交換器具有比服務供應商的交換器還低的實體位置以及橋接器優先序，則該交換器將成為擴充樹根並且能從許多客戶處取得資料。

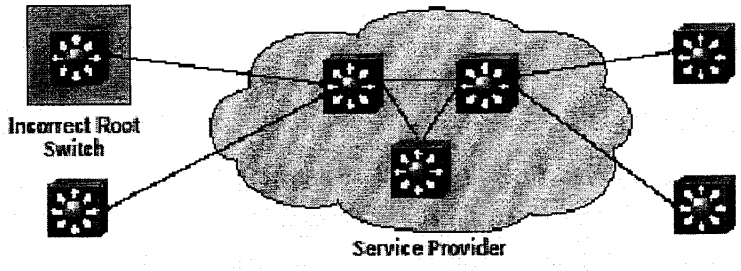


圖 4.5 服務供應商網路外的一個錯誤根交換器選擇

Root-Guard 的功能能從服務供應商處針對個別的通訊埠來啟用，進而限制客戶交換器成為根交換器。首先，先定義好所想要選定的根交換器範圍，然後在這個範圍內的每個通訊埠啟用 Root-Guard。這個功能能針對個別的通訊埠來啟用，而非個別VLAN，假如客戶方嘗試想成為根交換器，則.1q 隧道存取埠將進入根不一致(root-inconsistent)的狀態，如下所示：

cat6k-2> (enable) set spantree guard root 1/1
Rootguard on port 2/13 is enabled.
Warning!! Enabling rootguard may result in a topology change.
2001 Apr 20 12:31:20 pdt -07:00
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 (agPort 13/38) tried to become
non-designated in VLAN 2. Moved to root-inconsistent state
cat6k-2> (enable)

這個功能可核對該通訊埠是否在 STP 裡有其特定的作用，假如根守衛通訊埠從客戶交換器那裡收到了更高階的 BPDU 同時客戶的BPDU也丟棄掉了，則根守衛通訊埠也可以進入根不一致的狀態，引

起問題的交換器會被切斷連線，它不可在所定義的範圍裡插入高階BPDUs，而服務供應商的 STP 拓樸不受到引響，假如該通訊埠停止接收到高階 BPDUs，它將在所允許的最長時間後離開根不一致狀態。

```
cat6k-4 (enable) show spantree guard 1/1
Port VLAN Port-State Guard Type
---------------------- ---- ------------ ----------
4/13-14 20 forwarding root
cat6k-4 (enable)
```

服務供應商的交換器偶而會從客戶方得到高階 BPDU，然後馬上進入根不一致狀態，下列的步驟能解決這種狀態：

1. 將擴充樹優先序設定為較客戶的交換器來得高，該數值越低則客戶 VLAN 的優先序越高；(假設 20)：
   set spantree priority 200 20
2. 在該通訊埠上啟用根守衛：
3. set spantree guard root 1/1

BPDU 濾除機制並無法在啟動 802.1q 隧道化的存取埠發生作用。BPDU 濾除機制只能用在啟動 PortFast 功能的非 trunking 通訊埠。也因為如此，部分特殊協定如思科網路設備自動發現協定(CDP)、通訊埠聚合協定(PAgP)、VPT 以及 GARP VLAN 註冊協定(GVRP)等來自下層交換器的控制封包將會在邊緣交換器上被丟棄。因此，為減輕交換器上不必要的負擔，應將服務供應商交換器上的思科網路設備自動發現協定(CDP)關閉。

4.3.5 VLAN跳躍與 .1q全標記功能

另一個與.1q 隧道化類似的功能便是 Catalyst 6500/Cisco 7600 上的.1q 全標記(dot1q-all-tagged)功能，這個功能將.1q trunk 上的所有外出封包標記，包括原來 VLAN 上的封包，它還能確保所有進入的未標記封包會在.1q trunk 上被丟棄，這功能是由總指令(global command)來啟用，也就是說當開啟後便會適用在交換器上所有的.1q trunk 之上，它也可以是個獨立的功能，就算 Catalyst 交換器沒有任何隧道埠

也能夠啟動，Dot1-all-tagged 功能能防止 VLAN 跳躍(VLAN 安全)問題並且是 802.1q 順應標準，它還能防止某些客戶嘗試入侵他人的惡意攻擊。(請參閱圖 4.6)

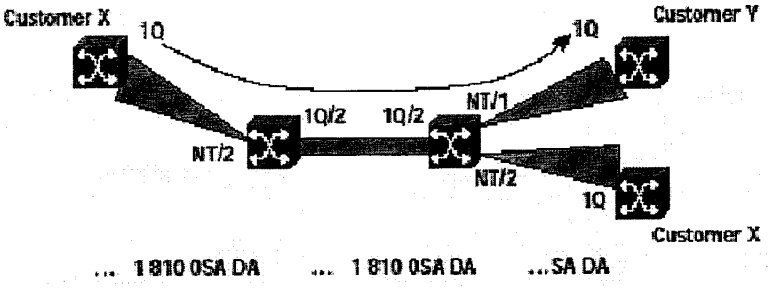


圖 4.6 VLAN 從跳 Customer X 躍到 Customer Y

舉例來說，客戶 X 可能嘗試去產生一個有.1q 標記的訊框來與客戶 Y 取得聯繫，假設客戶 X 在 VLAN 1 上傳送流量，該訊框將會有目的地位址，保全的相關訊息以及有 VLAN 1 資訊的.1q 標記，如果說服務供應商入口交換器是使用 VLAN 2 來搬運所有客戶 X 在.1q 隧道存取埠上的流量，該訊框現在便被分配到 VLAN 2 了，假如 VLAN 2 是.1q 上原有的 VLAN，則該訊框將會在不被加上任何額外的標記下離開，而出口交換器所收到的已標記之訊框將會移除其標記然後分配該訊框至 VLAN 1，此訊框將會以 VLAN 1 到客戶 Y 那裡，訊框從客戶 X 跳躍到客戶 Y，這種問題能藉由自服務供應商邊緣交換器上啟動 dot1q-all-tagged 功能來避免發生。dot1q-all-tagged 功能之所以能避免這種 VLAN 跳躍問題，以及確保來自某客戶的訊框將只會與另一端服務供應商之基礎建設相同的客戶取得聯繫，是因為在正常.1q trunk 上之所有訊框都必須經過標記，這種問題的另一種解決方式是去確定連接在服務供應商網路裡的邊緣交換器之間的.1q trunk 沒有和客戶 VLAN 一樣相同的原始 VLAN，並且建議最好是服務供應商核心交換器使用 ISL trunks 而非.1q trunk，因為這樣設定便能排除 VLAN 跳躍的問題。

4.3.6 包含.1q隧道化之冗餘部署

客戶無法擁有冗餘路徑至服務供應商之基礎建設裡的兩個不同的邊緣交換器，但是客戶可以在乙太通道(EtherChannel)裡有冗餘路徑至網際網路服務供應商(ISP)之網路裡的相同邊緣交換器，該客戶的擴充樹必須是 PVST+，而服務供應商則可以是用 PVST+或是 MISTP/PVST+。

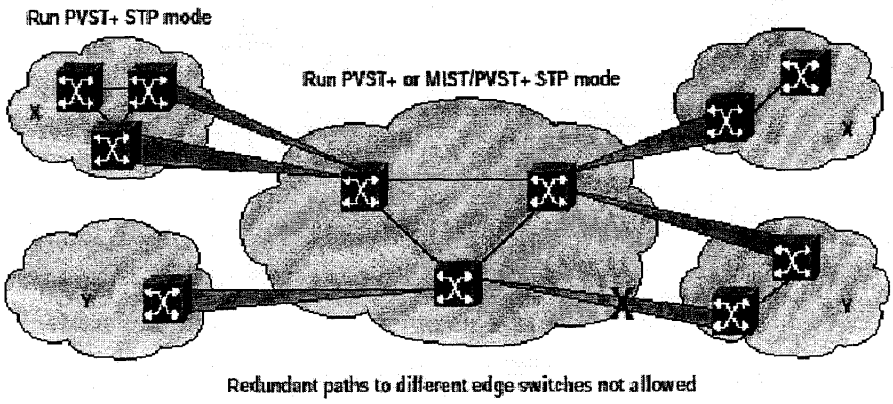


圖 4.7 含有.1q 隧道化之冗餘部署

圖 4.7 所展示的拓樸並不被支援，因為 BPDUs 在服務供應商之邊緣交換器裡被隧道化，進而可能導致客戶 Y 的網路裡發生迴遞，請注意，單點對多點拓樸是被支援的，並且不同客戶方可以接連不同的邊緣交換器。

5. 實習心得與建議

網際網路連接和支援網際網路的應用需求與日俱增，促使服務供應商網路發展的規模和範圍不斷擴大，隨著頻寬的可用性逐漸擴展，行業競爭不斷加劇，使傳統網路傳輸業務面臨著空前的價格壓力。因此，服務供應商需要尋找新的途徑來滿足頻寬快速增加的要求，同時降低成本並從競爭中脫穎而出。光網路設備具有無縫、高效的擴展功能，能夠爲高速資料傳輸提供 10Gbps 介面，從而很好地解決了擴展性的難題。Edge Router 可將客戶業務彙聚到靠近網路邊緣，簡化了部署在城域傳輸網路中的設備，減少重新生成中間信號的需求，從而可以降低成本和遠端傳輸的複雜性。在今後幾年決定服務供應商成功與否的關鍵因素將是他們能否充分利用光網路技術來加速業務的開發和提供，另一個同樣重要的因素是在競爭激烈的市場環境中，服務供應商能否提供層次化的價格結構。此外，成功的服務供應商還應該能夠在通用光纖基礎設施上提供多種獨一無二的加值業務，這些加值業務將使服務供應商在市場佔據領先地位，贏得持續的競爭優勢，如設備缺乏可擴展性，將限制他們快速採用和開發下一代 Internet 業務。

連接光纖到各大樓時，要考慮的部份可分為下列二項：一項是設備的穩定度，另一項是維護設備所需要花費的人力時間。設備的穩定度不夠時，設備時常會發生故障，不論是硬體或是軟體方面出問題時，在各大樓的客戶端將會耗費許多人力處理，且在維修處理期間，多少會對客戶的心理上產生某種程度的負面影響，這樣在客戶心理方面會對本公司的信譽降低很多。若採用設備的穩定度極高時，在維修方面可以減少掉許多的維護人力，在心理上也少了一個不確定性的負擔。

建議在客戶端使用的設備，盡量是選擇和核心端一樣的廠牌，此廠牌的一系列產品在穩定度上應有一定的口碑，且此廠牌的設備對於技術人員的安裝及維護方面已是駕輕就熟。另一方面此一系列的產品，有很多樣化的選擇，在第一次安裝時，可以依據各大樓之間的網點數目，來選擇所要之產品。此一產品支援堆疊的功能，可以支援到例如八臺以上設備連接在一起，不佔用到面板上的任何埠數，相互連

接背板頻寬的速度也可以達到 32Gbps 以上。當客戶端的設備，在第一次建置好了之後，由於大樓間的客戶端網點數目增加，在不損失任何頻寬且不會造成任何的瓶頸情形下，還能夠增加對客戶的網點服務數，除了增加的設備外，不用再多增加任何的成本，這對於成本上的考量，是一個非常有利的方式。