

企業虛擬私有網路服務規劃與實作

-以 MPLS VPN 為實作平台

研究生：陳遠鴻

指導教授：羅濟群 博士

國立交通大學資訊管理研究所

摘要

企業將其虛擬私人網路的規劃、建置與管理工作，委外由ISP來處理已經是一個趨勢，本論文將探討ISP在提供企業虛擬私有網路服務這項產品時，如何設計一個商業自動化流程，能滿足企業客戶複雜的網路需求，增加企業資訊應用的彈性與創造其商業價值，並進一步降低企業管理的風險與成本。在ISP提供這項服務的同時，必需將企業網路的規劃、建置、維護、管理等流程做更專業有系統的設計與自動化，才能降低風險與成本，創造此項服務的商業收益是本論文重要的課題。

本論文建置一個企業客戶的虛擬私有網路服務，是以 MPLS VPN 網路技術為核心，並以政策為基礎的網路管理 (PBNM) 技術，應用於企業虛擬私有網路服務之組態設定管理、障礙與品質監控管理，論文最後規劃實作此網管系統的 prototype，並對此系統進行評估。

此網管系統是以 Web 為使用介面，讓管理者方便操作，自動執行組態設定，藉以改善目前 ISP 在 MPLS VPN 網路上，以手動設定方式所帶來的不便及人力的付出，並且此系統在建置企業 VPN 網路單一節點時，自動是手動組態設定所需時間的 1/10，隨企業網路的複雜度及總節點數越多所需時間的差異越大。在障礙與品質監控管理方面可以透過圖像化的方式顯示客戶端專屬的整體網路拓樸架構與網路品質狀況，並且讓網管人員可以快速的掌握骨幹端及客戶端障礙的即時資訊，降低處理網路問題所需時間，同時透過告警系統以簡訊及 E-mail 即時通知相關人員，降低網管監控人力的付出。

關鍵詞：政策為基礎的網路管理，多重協定標籤交換技術，企業虛擬私有網路

Enterprise Virtual Private Network Services' Planning and Implementation-Using an MPLS VPN as the Development Platform

Student : Yuan-Hung Chen

Advisor : Dr. Chi-Chun Lo

Institute of Information Management
Nation Chiao Tung University

ABSTRACT

It has been a trend that enterprises outsource the planning, implementation, and management of their virtual private networks to ISPs. In this thesis we will discuss how to design a business model to satisfy customers' complicated network needs, to increase the elasticity of enterprise information applications, to create its business value, and to decrease the risks and cost of business management when ISPs provide enterprise VPN service. When ISPs provide this service, it has to be more professional and more systematical in the process of planning, implementation, maintenance, and management of enterprise network, then it could decrease the risk and cost. It is the important topic to create value of the business by providing VPN service.

This thesis implements VPN services to enterprise. It is based on MPLS VPN technology combined with Policy-Based Network Management (PBNM) technology, and applied to the configuration management, fault and performance management of enterprise VPN services. At the end, we implement the prototype of this network management system, and make evaluation of this system.

The user interface of network management system is web based. It is convenient for users to operate, combined with auto-configuration that improves the efficiency of manual configuration. The time spent on manual configuration is 10 times to auto-configuration when ISPs implement single node for enterprise VPN. In fault and performance management, we can use graphic to show customers' network topology and performance status. It also informs relative persons by short message and E-mail.

Keyword : Policy-Based Network Management (PBNM), MPLS, VPN

誌謝

本論文得以順利完成，首先我要感謝我的指導教授羅濟群老師。從論文題目的定義到研究結果的產生，我由衷的感謝老師在旁的細心指導與不斷叮嚀，除此之外，在整個論文的研究過程中，從老師身上學習到如何做好研究，這樣的訓練讓我覺得獲益非淺，這也是我從工作職場上再回到學校學習的主要原因。同時在資管所修課的這兩年，不斷擴充了我的專業，學習到這個領域更完整的東西，因此對所上的每位老師都表示內心的感激！

另外，在修課期間感謝所上學長及同學們的支援與指導，才能讓我在這兩年內順利的把課程修完，同時我也要感謝我的家人及女朋友，讓我能再進入學校進修，使我能專心一致的投入研究工作。



目 錄

中文摘要.....	i
英文摘要.....	ii
誌謝.....	iii
目錄.....	iv
表目錄.....	vi
圖目錄.....	vii
第一章 諸論.....	1
1.1 研究動機.....	1
1.2 研究目的.....	4
1.3 論文架構.....	5
第二章 文獻探討.....	7
2.1 多重協定標籤交換技術.....	7
2.1.1 MPLS 技術背景簡介.....	7
2.1.2 Label 的格式與屬性.....	8
2.1.3 MPLS 網路的架構與組成.....	9
2.1.4 LSR 內部功能模組分析.....	10
2.1.5 Label 的指定與分配過程.....	11
2.1.6 MPLS 網路中封包運作原理.....	15
2.1.7 MPLS 技術之應用.....	18
2.2 VPN 的新趨勢--MPLS VPN.....	21
2.2.1 VPN 技術簡介.....	21
2.2.2 MPLS VPN 技術介紹.....	25
2.2.3 MP-BGP 的特殊屬性運作原理.....	29
2.2.4 MPLS VPN 封包實際運作狀況分析.....	30
2.3 網路管理技術.....	34
2.3.1 網路管理簡介.....	34
2.3.2 網路管理協定 SNMP.....	36
2.3.3 網管工具簡介.....	37
2.3.4 以政策為基礎的網路管理.....	38
第三章 企業網路服務需求分析.....	41
3.1 企業網路服務的商業市場分析.....	41
3.2 企業網路服務訂購選單分析.....	43
3.3 全球化企業私有網路服務案例分析.....	45
3.4 VPN Centre Platform 架構規劃.....	47
3.5 企業網路服務流程管理規劃.....	48
第四章 MPLS VPN 系統規劃與功能設計.....	50

4.1 MPLS VPN 骨幹網路規劃	50
4.1.1 MPLS VPN 骨幹網路擴充性架構設計	50
4.1.2 MPLS VPN 骨幹網路國際延伸規劃	52
4.2 MPLS VPN 網管系統架構規劃	53
4.3 MPLS VPN 組態管理系統規劃	55
4.3.1 MPLS VPN 組態參數規劃	55
4.3.2 MPLS VPN 組態政策規則設計	56
4.3.3 MPLS VPN 組態自動設定	58
4.4 障礙與品質監控系統規劃.....	59
4.4.1 障礙與品質監控項目規劃.....	60
4.4.2 網路管理監控政策規劃.....	61
第五章 系統實作與評估分析.....	63
5.1 MPLS VPN 網管系統實作	63
5.1.1 組態政策資料表建置.....	66
5.1.2 網路組態設定實作.....	67
5.2 MPLS VPN 網管系統導入後效益	68
5.2.1 導入後定性的效益分析.....	68
5.2.2 導入後定量的效益分析.....	73
第六章 結論與未來研究方向.....	78
6.1 結論.....	78
6.2 未來研究方向.....	79
參考文獻.....	80

表 目 錄

【表 2-1】各種應用程式對 QoS的需求	19
【表 3-1】企業網路服務需求訂購表	45
【表 5-1】MPLS VPN 客戶(基本資料)表單欄位	67
【表 5-2】MPLS VPN 客戶(VPN組態資料)表單欄位	67
【表 5-3】客戶線路品質監控效能分析	75
【表 5-4】MPLS VPN 骨幹網路品質監控效能分析	76
【表 5-5】MPLS VPN 路由資訊監控效能分析	76
【表 5-6】MPLS VPN骨幹網路設備監控效能分析	77



圖 目 錄

【圖 1-1】策略網路管理需求分析	2
【圖 1-2】研究流程架構	6
【圖 2-1】Label Stack架構圖	9
【圖 2-2】MPLS 網路的架構及組成圖	10
【圖 2-3】封包在LSR中的處理架構	11
【圖 2-4】LSR路由表建立的過程	12
【圖 2-5】LSR Allocating Label過程	13
【圖 2-6】LSR初步建立自己的LIB及LFIB	13
【圖 2-7】LSR Label Distribution過程	14
【圖 2-8】相鄰LSR送來的Label資訊做彙整的過程	15
【圖 2-9】封包在MPLS網路中傳送的過程	16
【圖 2-10】MPLS網路中Egress LSR double lookup問題	16
【圖 2-11】Penultimate Hop Popping運作原理	17
【圖 2-12】MPLS防止Loops及TTL運作機制	18
【圖 2-13】IP precedence 與MPLS Label EXP bit	20
【圖 2-14】封包在IP網路與MPLS網路中被標示QoS等級	20
【圖 2-15】IPsec Transport Mode (AH and ESP)	23
【圖 2-16】IPsec Tunnel Mode (AH and ESP)	23
【圖 2-17】MPLS VPN Connection Model	26
【圖 2-18】PE Router有兩種互相獨立的Routing Table	27
【圖 2-19】每個客戶獨立執行一個IGP的路由協定	27
【圖 2-20】專有路由協定經骨幹各節點攜帶客戶的路由資訊	28
【圖 2-21】PE Router間透過專有路由協定攜帶客戶路由資訊	28
【圖 2-22】加入RD值的運作原理	29
【圖 2-23】去除RD值的運作原理	30
【圖 2-24】MPLS VPN客戶路由資訊透過MP-BGP的交換過程	31
【圖 2-25】PE1 將進入MPLS網路的封包加上VPN及IGP label	32
【圖 2-26】MPLS網路中P Router負責做IGP Label Swap	32
【圖 2-27】Penultimate Hop Popping運作原理	33
【圖 2-28】PE2 負責去除VPN label並轉送封包到所屬的界面	33
【圖 2-29】網路管理五大功能模組	35
【圖 2-30】網路管理系統運作方式	37
【圖 2-31】MRTG網路管理技術運作方式	38
【圖 2-32】Policy-based網路管理系統架構	40
【圖 3-1】企業網路服務市場成員供需關係	43
【圖 3-2】全球化企業私有網路服務的案例圖	47

【圖 3-3】 VPN Centre Platform架構.....	48
【圖 3-4】 企業虛擬私有網路服務流程圖	49
【圖 4-1】 ISP網際網路BGP擴充性網路架構.....	51
【圖 4-2】 MPLS VPN 擴充性網路架構圖設計	52
【圖 4-3】 MPLS VPN骨幹網路國際延伸架構.....	53
【圖 4-4】 MPLS VPN網路管理系統架構.....	55
【圖 4-5】 Policy Rule範例簡圖	57
【圖 4-6】 VPN type1 Profile範例	57
【圖 4-7】 組態自動設定架構圖	59
【圖 4-8】 障礙與品質監控架構圖	60
【圖 5-1】 網管系統實作環境.....	66
【圖 5-2】 MPLS VPN客戶服務申請表基本資料輸入圖	69
【圖 5-3】 MPLS VPN客戶連線資料圖	69
【圖 5-4】 MPLS VPN骨幹網路即時監控系統.....	70
【圖 5-5】 MPLS VPN 客戶端網路即時狀況查詢系統.....	71
【圖 5-6】 客戶端網路拓樸即時監控系統	72
【圖 5-7】 全省PE Router設備即時監控系統.....	72
【圖 5-8】 網路流量統計圖	73
【圖 5-9】 自動與手動組態設定時間需求比較.....	74

