高可靠度新世代網路技術之探討

作者/陳國財、朱煜煌、徐浩然

提要

一、由於網路全面朝向 IP 化發展，因此所有的服務都希望能在這個網路平台上提供；然而早期的相關技術制定並無法完全滿足所有服務的需求，所以新世代網路的發展將扮演重要的角色。

二、新世代網路是一個能力更強的通訊網路，能夠在同一平台上提供使用者更高的速率，以及更具安全性和品質保證的傳輸環境，同時也提供更容易管理與維護的介面和功能。

三、利用目前 IP 網路中較成熟的技術，包含多重協定標籤交換技術與服務品質技術；以及新世代網路技術中所強調之服務階層和網路傳送階層分離的特性，這些都是達到網路高可靠度目的須參考的相關技術。

四、網路可靠度是網路在發展過程中的重要議題之一，因此備援保護機制成為電信業者或網路提供者確保服務不中斷的不可或缺要素。一般而言，備援保護機制設計會在網路架構上分成四個層次，分別為平台與鏈路層次的備援(Platform and Link Level Resiliency)、網路層次備援(Network Level Resiliency)、協定層次備援(Protocol Level Resiliency)和服務層次備援(Service Level Resiliency)，而這些機制都可以在既有網路與新世代網路中實現，所以當網路設備故障或設備之間鏈路中斷時，網路備援保護機制可以保證服務不受影響。本文也提出如何設計可達到高可靠度網路架構方式與流程，因此當網路節點鏈路發生故障中斷時，可以快速地從故障的路徑切換到備援路徑去，進而達到服務不中斷的目的。

關鍵字：網際網路協定(Internet Protocol, IP)、新世代網路(Next Generation Network, NGN)、多重協定標籤交換 (Multi-Protocol Label Switching, MPLS)、服務品質(Quality of Service, QoS)、備援(Resiliency)

前言

由於現有網際網路協定(Internet Protocol, IP)具備與生俱來的智能，在建置上又具備極大的彈性度並且支援各種應用服務與運作流程的調適性，因此大部分的電信業者確實朝向網路 IP 化的目標邁進。然而，電信業者很快的體認到同時管理多個因應不同服務而建置的網路並不是一個明智的作法，因此在單一網路

承載多重服務已逐漸成為電信業者未來網路的主流策略。也因為如此，新世代網路(Next Generation Network, NGN)的建設已成為許多電信業者的目標，其除了可提供全 IP 的網路環境之外，還可以在同一平台上提供使用者更高的速率，以及更具安全性和品質保證的傳輸環境，同時也提供更容易管理與維護的介面和功能。

網路可靠度是新世代網路在發展過程中的重要議題之一，然而在既有網路中也必須同時考慮提升此部分的相關功能。本文首先針對現有多重協定標籤交換 (Multi-Protocol Label Switching, MPLS)與服務品質(Quality of Services, QoS)議題進行探討，接著簡介 NGN 的概念；並詳細說明網路可靠度的相關技術，最後則提出具體可行之建議及結論。由內文可知本文主要介紹目前網路的一些進階技術，希望對電信業者在打造一個具備擴展性、安全性、可靠度、高效率及容易管理並且能承載既有與未來多元服務的網路有所幫助。

多重協定標籤交換技術介紹

傳統的IP網路利用各種鏈路狀態路由協定，如：開放式優先最短路徑(Open Shortest Path First, OSPF)和系統與系統間的協定(Intermediate System to Intermediate System, IS-IS)等，作為路由選擇的工具。這些協定利用最短路徑演算法(Shortest Path First Algorithm, SPF Algorithm)將各個網路連接路徑的頻寬化作簡單的公制(Metric)定義，並且利用這些公制的相加結果進行比較，計算出最佳化的訊務傳送路徑。這種資料傳送方式在所謂「盡力而為(Best Effort)」的網際網路應用環境中，尚可符合一般需求。然而，在數據影音三合一服務(Triple Play Services)的網路多媒體應用中，這種資料傳送技術將顯現出下列四項缺點：網路資源利用不佳、無法滿足網路頻寬保證的需求、QoS無法掌握、無法滿足網路可靠度的需求等。由於上述的種種缺失，IETF(Internet Engineering Task Force，網際網路工程專案小組)制定了MPLS[1]訊務工程(MPLS Traffic Engineering, MPLS-TE)技術來改善IP網路的缺點。MPLS使用標籤交換(Label Switching)方式來處理封包，MPLS網路內部的網路路由器只需要判別標籤來轉送封包；封包的交換及轉送動作只須在資料鏈結層以硬體來執行，使網路路由器處理每一個網路封包所需的時間縮短而且相對固定，網路封包傳送的延遲(Delay)和不穩定性(Jitter)機率也可以降低，因此可以有效的提昇網路的傳送效率和品質。

[1] IETF 標準組織，”Multiprotocol Label Switching Architecture”，RFC 3031，2001 年 01 月。

MPLS 技術除了縮短網路封包傳送的延遲時間外，其更重要的特點在一方面整合了第三層(Layer 3)IP 路由選擇作業與第二層(Layer 2)標籤交換作業於單一系統，同時在另一方面允許第三層 IP 路由選擇作業與第二層標籤交換作業獨立設定與運作，這使得新服務的提供更具彈性。

服務品質技術介紹

QoS 是一組服務需求，不同服務的 QoS 需求就不同。例如：資料類服務具有離散性特徵，對訊務傳遞的可靠度要求較高，雖然封包錯誤率是最重要的指標，但可以容忍一定的延遲；而語音和視訊這類服務具有流量大、延續性、即時性與相關性等特點，延遲會造成語音的變聲、變調和視訊的馬賽克等現象，因此對傳輸延遲和抖動要求非常嚴格。傳送網路必須提供適當的服務分級以及允許控制機制，方能滿足這些服務需求。

除了MPLS技術可以達到QoS的功能之外，IETF提出差異化服務模型的基本構想，是在網路的入口處為每個封包進行分類，並在封包中標記相應的差異化服務代碼點(DiffServ CodePoint, DSCP)[2]，用於代表封包在網路轉發路徑的中間節點上被處理的方式。在網路內部的核心路由器中只保存簡單的DSCP與PHB(Per Hop Behavior)的對應機制，根據封包標頭中的DSCP值，對封包進行相對應的優先級轉發，至於流量控制機制的實現則是在網路邊界節點來進行。

另外有關階層化服務品質(Hierarchical-QoS, H-QoS)技術是目前業界實現捆綁式頻寬總量控管與個別服務類型頻寬配置的先進技術。H-QoS 技術可以動態配置控制佇列的調度器，換句話說電信業者可以根據實際營運需要，設定調度器之間的上下層次的相依關係。H-QoS 藉由多級邏輯調度器的設定，由上級調度器控制一組下級調度器的總量頻寬，同時上級調度器能夠根據下級調度器的級別和權重合理分配下級調度器的個別頻寬。

新世代網路技術介紹

新世代的網路主要聚焦在兩部分，也就是區域匯集網以及IP/MPLS多重服務骨幹網。區域匯集網路主要功能可以分成兩部分：第一部分，針對高速上網服務而言，區域匯集網路扮演的是第二層電路提供者的角色，單純地將高速上網服務訊務以第二層傳輸方式傳送至遠端網路服務供應商的寬頻遠端存取伺服器(Broadband Remote Access Server, BRAS)設備，再由BRAS提供IP層的終結

[2] Microsoft 公司技術部門，〈Differentiated Services Code Point (DSCP) 概觀〉，台灣微軟， http://technet.microsoft.com/zh-tw/library/cc787218(WS.10).aspx。

(Termination)。區域匯集網路必須提供一種大量電路收容集縮的匯集機制，然而第二層(Layer 2)電路匯集機制的做法相當多樣化，因此當我們在選擇匯集機制時，必須考量該項做法是否具備易於供裝、未來具備擴展性及彈性、擁有豐富速率限制及H-QoS[3]能力，以及具備維運及障礙查測等功能。第二部分，針對所謂Managed IP 寬頻網路，其是一個能被有效控管，並提供各式各樣寬頻IP服務之寬頻網路，然而就Managed IP服務而言，區域匯集網路的重點工作之一就是提供基於動態用戶組態協定(Dynamic Host Configuration Protocol ,DHCP)及遠端用戶撥入驗證服務(Remote Authentication Dial In User Service ,RADIUS)等的用戶管理機制，而其具體的內涵至少須包括自動化及動態的QoS Policy指配、單一用戶統計資訊計數、用戶運作狀態的偵測及防止假冒位址封包入侵(Anti-Spoofing)的安全防弊機制等。

IP/MPLS 骨幹傳送網路主要功能在於連接各個區域匯集網路，提供跨區通訊傳輸及跨區媒體派送功能。其主要構成之網路元件包括骨幹核心路由器(Core Router, CR)及邊界路由器(Border Router, BR)。

新世代網路技術的另一個概念，是將服務階層(Service Stratum)與網路傳送階層(Transport Stratum)分離。位處上層的服務階層由「應用與服務支援功能」(Application & Service Support Functions)及「服務與控制功能」(Service and Control Functions)所構成，其中的「應用與服務支援功能」提供的是內容及應用服務。至於位處底層的網路傳送階層可進一步細分為「傳送控制功能」(Transport Control Functions)及「傳送功能」(Transport Functions)，其中的「傳送功能」又可再進一步細分為直接面對用戶(或客戶)並提供第二層(Layer 2)接取傳送功能的接入傳送網路，以及提供IP層匯集及服務傳送功能的傳送網路。[4]

高可靠度技術之探討

備援保護機制是電信業者或網路提供者確保服務不中斷的不可或缺要素，當網路設備故障或設備之間鏈路中斷而導致網路服務停擺時，如何在很短的時間內能恢復正常運作，是電信業者或網路提供者必須要考量的重要議題。為了要達到網路高可靠度之目的，在網路架構上分成四個層次的備援保護機制，分別為平台與鏈路層次的備援(Platform and Link Level Resiliency)、網路層次備援

[3] 杭州華三通信技術有限公司，〈H-QoS 技術介紹〉，H3C-IToIP 解決方案專家，2008 年 05 月，http://www.h3c.com.cn/Products___Technology/Technology/QoS/Other_technology/Technology_recommend/200805/605880_30003_0.htm。

[4] ETSI 標準組織，"TR 180 001 V1.1.1, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), NGN Release 1"，2005 年 12 月。

(Network Level Resiliency)、協定層次備援(Protocol Level Resiliency)和服務層次備援(Service Level Resiliency)。電信業者依據多年來網路設計與維運的經驗，將相關的備援機制技術運作在該四個層次中，此用意除了讓網路規劃或設計者能方便規劃網路備援機制外，亦可讓網路維運者於網路運作過程中，達到服務不中斷的目的。以下列出各個層次的備援機制相關之技術，並介紹每個技術的運作情形。

一、平台與鏈路層次的備援

(一)硬體模組架構(Modular Hardware Architecture)

硬體模組架構備援包括路由引擎備援、電源供應備援、散熱風扇備援等，其中電源供應備援模式為每個電源都能提供整個路由器或交換機所需的總電力負荷，如果一個電源出現故障，另一個電源將立刻承擔整個路由器或交換器機架的全部電力負荷，如此可避免因電源出現故障，而造成整台路由器或交換機無法運作的情況。

(二)鏈路匯集(Link Aggregation, LAG)

LAG[5]備援方式是透過多條捆綁的實體鏈路來提供的，如果其中的一條鏈路出現故障，通過該鏈路的資料流將會轉移到鄰接的鏈路上，故障切換在幾毫秒內就完成了，對於終端使用者來說是完全感覺不出來；若鏈路陸陸續續地出現故障，將有更多的資料流移到鄰接的鏈路上，當鏈路從故障中恢復過來時，負載將自動地在現有的鏈路之間重新分配。

(三)服務中軟體更新(In-service Software Upgrades, ISSU)

欲提供新服務、新功能和修補舊有缺失時，通常會在運行網路設備中進行軟體的更新，其作法為先在備援設備中進行軟體更新，更新完成後，將原本在主要設備中傳送的訊務引導到備援設備去進行轉送，接著對主要的設備進行軟體更新，更新完成後，再將訊務引導回主要設備去傳送，完成在不中斷服務的前提下進行設備軟體更新動作。

(四)不中斷路由(Non-stop Routing, NSR)

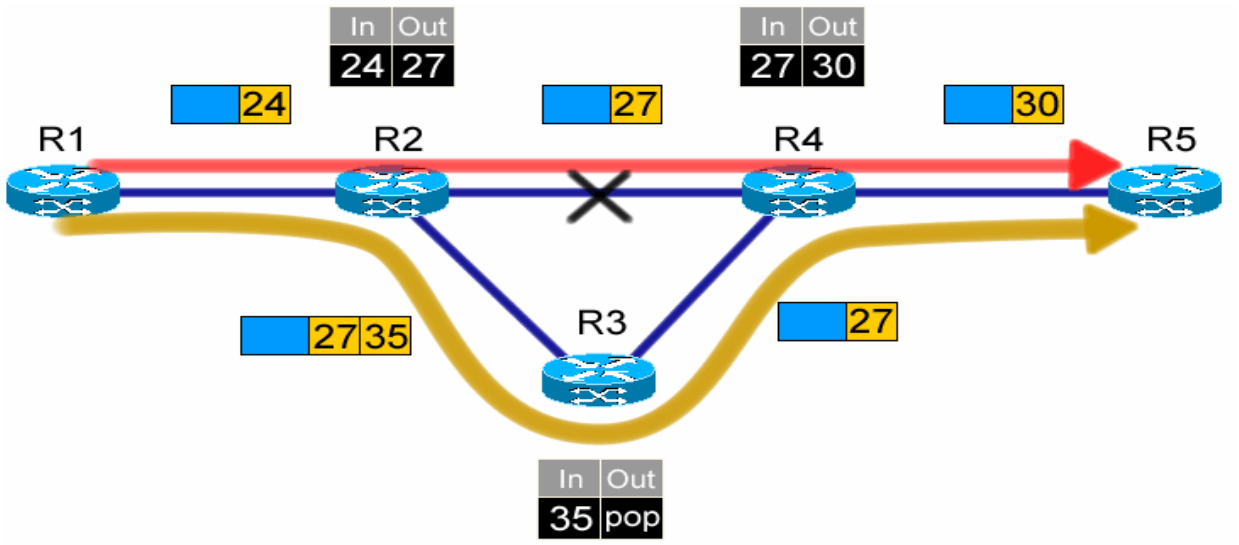
新版NSR使用內部處理模式來保證備援路由引擎知道路由協定的狀態，並維持與鄰接關係間的活動狀態。因此轉換之後，備援路由引擎負責維護現有的對等會話，而不是被迫重新建立新的對話。因此轉換對於鄰接節點來說是透明的，並且因為NSR流程是內部的程序，因此鄰接節點無需支援任何基於協定的擴展。

[5] IEEE 標準組織，”Link Aggregation”，IEEE 802.3ad，2001 年 11 月。

二、網路層次備援

(一)MPLS機制快速切換(Fast Reroute, FRR)[6]

圖一為 Fast Reroute 運作情形。首先在 R1 到 R5 間建立了一條主要的(Primary)標籤交換路徑(Label Switched Path, LSP) (R1->R2->R4->R5)用來傳送訊務。接著再於 R2 和 R4 間建立一條備用的(Backup) LSP (R2->R3-> R4)。正常情況下，R1 到 R5 的訊務會經由主要的 LSP 來傳送，當 R2 偵測到與 R4 間的鏈路出現故障時，除了執行原本的 Label Swapping (24->27)外，更會加入另一個 Label (35)於 Label (27)之上然後往 R3 傳送。R3 收到 Label 為 35 的封包後，便會將上層 Label (35)移走再往 R4 送，如此訊務便可以被正確且快速的傳送到目的地 R5。



圖一 MPLS Fast Reroute 運作情形示意圖

(資料來源：徐浩然等，〈NGN IP 網路整合技術探討〉《電信研究雙月刊》，中華電信股份有限公司，第 39 卷第 6 期，民國 98 年 12 月，頁 991-1010。)

(二)次要的(Secondary) LSP與待命的(Standby) LSP

首先簡述 Secondary LSP 運作情形。在封包進入(Ingress)和封包出去(Egress)的邊緣路由器(Provide Edge, PE)間，根據限制性優先最短路徑(Constraint-based Shortest Path First, CSPF)演算法選出一條主要的路徑。當主要的路徑發生故障時，才會由 Ingress PE 路由器根據 CSPF 演算法重新挑選出一條路徑來進行傳送，圖二為 Secondary LSP 運作情形示意圖。

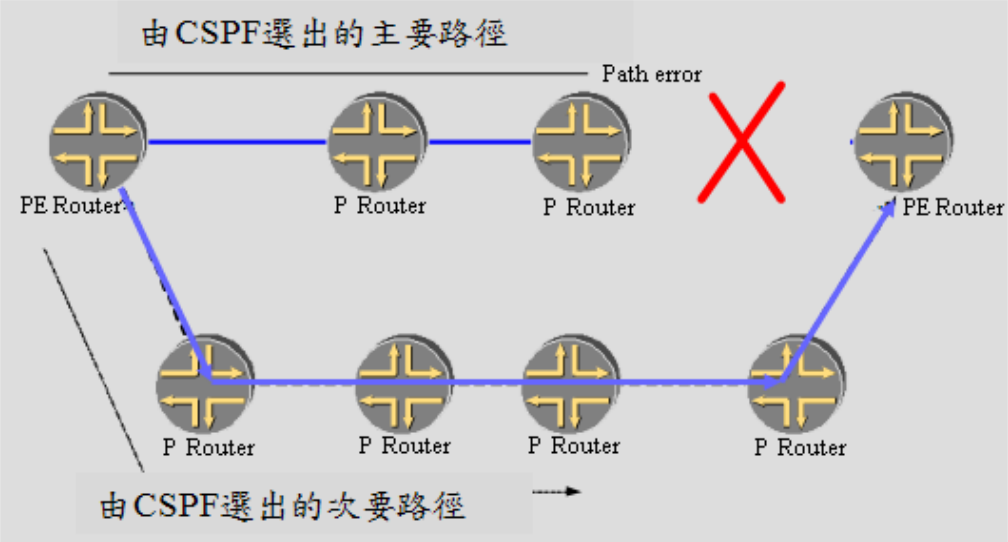
以下簡述Standby LSP運作情形。在Ingress和Egress PE路由器間，根據CSPF原則同時選出一條主要路徑和一條備援路徑。在正常情況下訊務都會往主要路徑來傳送，然而當主要路徑發生故障時，Ingress PE路由器會快速切換到備援路

[6] IETF 標準組織，"Fast Reroute Extensions to RSVP-TE for LSP Tunnels"，RFC 4090，2005 年 05 月。

徑，以繼續進行封包轉送的工作。[7]

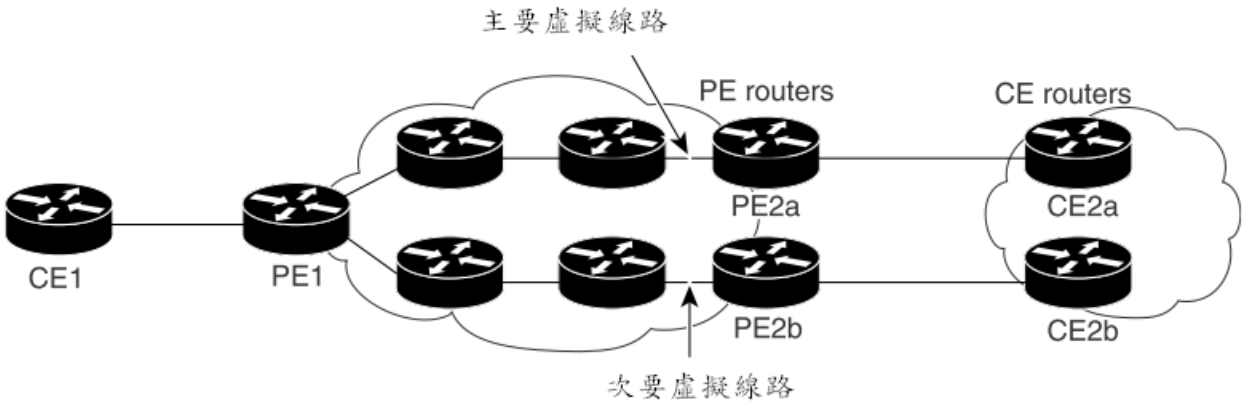
(三)虛擬線路(Pseudowire)備援

當遠端 PE 路由器 (Egress PE 路由器)或 Egress PE 路由器到客戶邊緣(Customer Edge, CE)路由器之間的鏈路發生故障時，虛擬線路備援所提供的恢復機制可動態地應對網路中的故障。



圖二 Secondary LSP 運作情形示意圖

(資料來源：徐浩然等，〈NGN IP 網路整合技術探討〉《電信研究雙月刊》，中華電信股份有限公司，第 39 卷第 6 期，民國 98 年 12 月，頁 991-1010。)



圖三 虛擬線路(Pseudowire)備援運作情形示意圖

(資料來源：徐浩然等，〈NGN IP 網路整合技術探討〉《電信研究雙月刊》，中華電信股份有限公司，第 39 卷第 6 期，民國 98 年 12 月，頁 991-1010。)

圖三為虛擬線路備援運作情形，當主要虛擬線路上的節點設備(PE2a、CE2a)或鏈路(PE2a到CE2a之間鏈路)發生故障時，次要虛擬線路會接管主要虛擬線路

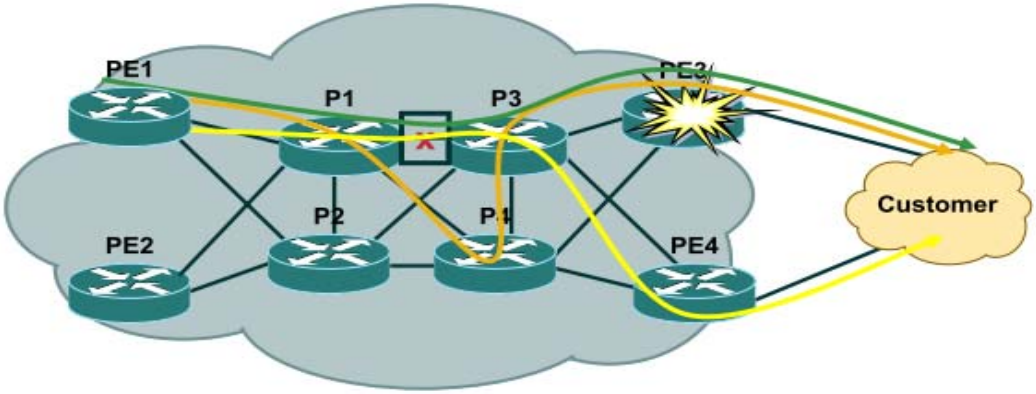
[7] IETF 標準組織，”Traffic Engineering (TE) Extensions to OSPF Version 2”，RFC 3630，2003 年 09 月。

的工作以便繼續提供服務。[8]

(四)多重機架鏈路匯集(Multi-Chassis LAG, MC-LAG)

Multi-Chassis LAG[9]主要用於跨PE路由器間的鏈路與節點保護。主要路由器和備援路由器間有Multi-Chassis LAG Control Protocol的聯絡機制，當主要路由器發生故障時，備援路由器會立即接管主要路由器的工作。一般而言Multi- Chassis LAG會搭配虛擬線路備援技術對第二層虛擬私有網路(Layer 2 Virtual Private Network, L2VPN)服務進行備援保護。

(五)網路閘道器協定快速收斂(Internet Gateway Protocol Fast Convergence)



圖四 網路閘道器協定快速收斂備援運作情形示意圖

(資料來源：徐浩然等，〈NGN IP 網路整合技術探討〉《電信研究雙月刊》，中華電信股份有限公司，第 39 卷第 6 期，民國 98 年 12 月，頁 991-1010。)

圖四為網路閘道器協定(Internet Gateway Protocol, IGP) 快速收斂運作情形示意圖。當節點或鏈路發生故障時，路由器會快速重新計算出一條到達目的地的最短路徑，例如當節點 PE3 發生故障時，訊務會被快速導入至 PE4；又假如 P1 到 P3 的鏈路發生故障時，訊務則會改從 P1 經由 P4 至 P3；如此訊務將會從原先的路徑被導到新的路徑，網路穩定度因而可以獲得大幅度的提升。

(六)IEEE 802.1ag CFM 與 ITU-T Y.1731

美國電氣和電子工程師協會（IEEE）制訂 802.1ag 連結錯誤管理(Connectivity Fault Management, CFM)標準與國際電信聯盟(ITU-T)制訂 Y.1731 乙太網路 OAM 標準，其包括以下相關功能：故障偵測(Fault Detection)、故障確認(Fault Verification)、故障隔離(Fault Isolation)和故障通知(Fault Notification)等。IEEE 802.1ag CFM 標準主要是針對乙太網路傳輸層，用於障礙管理的部分，

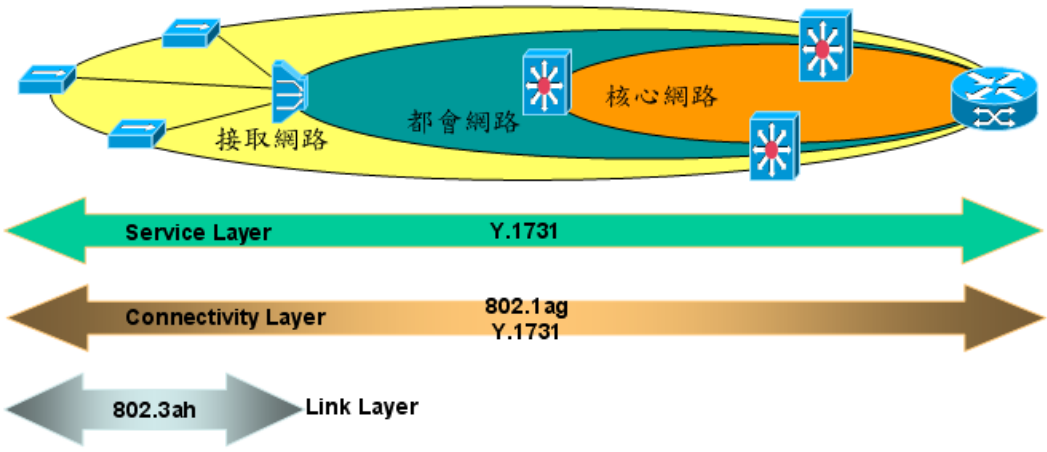
[8] IETF 標準組織，"Framework for Layer 2 Virtual Private Networks (L2VPNs)"，RFC 4664，2006 年 09 月。

[9] Alcatel-Lucent 公司技術部門，"VPLS Insights"，Alcatel-Lucent 公司，http://www1.alcatel-lucent.com/bnd/vpls/insights/MB_oct07.jhtml .

進行分段障礙查測，確保網路發生障礙時可以回報給營運業者，以進行適當的處置。IEEE 802.3ah 標準屬於接取網路鏈路層(Link Layer)的保護機制，其規定了連線監控(Link Monitoring)、錯誤警示(Fault Signaling)、遠端迴路(Remote Loopback)等功能的相關條件標準，因此有了這些功能，電信業者能更有效管理乙太網路服務用戶連線。相關標準與對應之區段與查測層次如圖五所示。

(七)PIM-Dual Join

群播獨立協定(Protocol Independent Multicast, PIM)之多重加入(Dual Join)模式的運作前提是路由設備一定要具備兩條 Equal Cost 的鏈路與上游(靠近骨幹端)設備界接，以便在群播路由表中依群組目的 IP 位址分別建立兩筆 Incoming RPF(Reverse Path Forwarding)介面，包括 Primary Interface 與 Secondary Interface。Secondary Interface 作為 Primary Interface 備援介面。換言之，串流媒體會透過此兩條鏈路並以耗用雙倍頻寬的主動式 Active-Active 注入至路由設備內，路由設備再依串流媒體目的 IP 位址，分別歸類為奇數類與偶數類，且以奇偶數交替方式決定 Incoming Primary RPF 介面，並將串流媒體下放至出口端。



圖五 相關標準與對應之區段與查測層次示意圖

(資料來源：李明鴻等，〈乙太網路 OAM 測試技術研究〉《電信研究雙月刊》，中華電信股份有限公司，第 39 卷第 1 期，民國 98 年 2 月，頁 147-163。)

一旦因突發狀況導致Primary介面出現障礙並且威脅到一半的串流媒體群組(奇數群或偶數群)之傳送時，Secondary介面可以在短短數十毫秒之內接手，將媒體傳送中斷的風險降低。因此PIM-Dual Join 模式大大提升了群播服務的可靠度。[10]

三、協定層次備援

[10] Redback，”SmartEdge 1200 Multi-Service Edge Router”，Ericsson公司，http://www.ericsson.com/ru/market/redback/docs/SmartEdge%201200.pdf .

(一)雙向送收偵測機制(Bidirectional Forwarding Detection, BFD)

BFD 是一個 UDP-based Layer 3 協定，提供路由協定(例如 BFD 針對指定路由(Static))與 BFD 針對公開優先最短路徑(Open Shortest Path First, OSPF)等去偵測網路下一個節點是否發生故障。系統之間會週期性發送檢測信號，當系統在一段時間內未收到對方的檢測信號時，則會判定系統之間連線發生故障。BFD 在檢測前，需要在通道兩端建立區段連線，在區段連線建立之後才能以雙方協商的速率各自向對方發送 BFD 的檢測封包來進行鏈路檢測。在過程中雙方同時協商好相關參數(如發送週期等)，之後 BFD 的狀態變化就是根據檢測結果來進行，並做相關程序處理。

(二)得體的重開機機制(Graceful Restart, GR)

對於路由器的控制層(Control Plane)發生故障時，GR[11]協定是最優先被啟用的備援機制，雖然每一個路由協定都有自己專門的GR擴展，但他們的工作基本原理相同。當一台路由器的Control Plane出現故障時，它的鄰接路由器不是立刻向自己的鄰接節點通告這台路由器不可用，而是等待一段時間，這段時間稱之為得體週期(Grace Period)。如果路由器在Grace Period過期之前重新建立起對等會話，對等會話的臨時中斷不會影響鄰接節點後面的網路。

四、服務層次備援

(一)虛擬路由器備援協定(Virtual Router Redundancy Protocol, VRRP)

VRRP[12]設計的主要目的是用來增進子網段閘道的可靠度。可靠度增進的作法是通知同一子網段的所有主機，將「虛擬路由器」視為「子網段閘道」，而非是將某一特定實體路由器視為其閘道。通常一群實體路由器共同組成VRRP群組。在VRRP群組中，正在使用中的實體路由器被稱為主路由器(Master Router)，其優先權最高，並且代表虛擬路由器處理訊務的轉送工作；至於其他所有的路由器都處於備用狀態(Backup state)，因此被稱為備援路由器。一旦主路由器發生障礙，備用路由器將接管主路由器的工作提供服務。

(二)閘道器負載平衡協定(Gateway Load Balancing Protocol, GLBP)

GLBP[13]不僅提供備援閘道器位址，還在各閘道器之間提供負載平衡，其和VRRP不同的是GLBP可以綁定多個配接卡位址(Media Access Control, MAC)到虛擬IP位址，允許用戶端選擇不同的路由器作為其閘道器，而閘道器位址仍使用相同的虛擬IP，以利實現備援保護。

---

[11] IETF 標準組織，"Graceful OSPF Restart"，RFC 3623，2003 年 11 月。

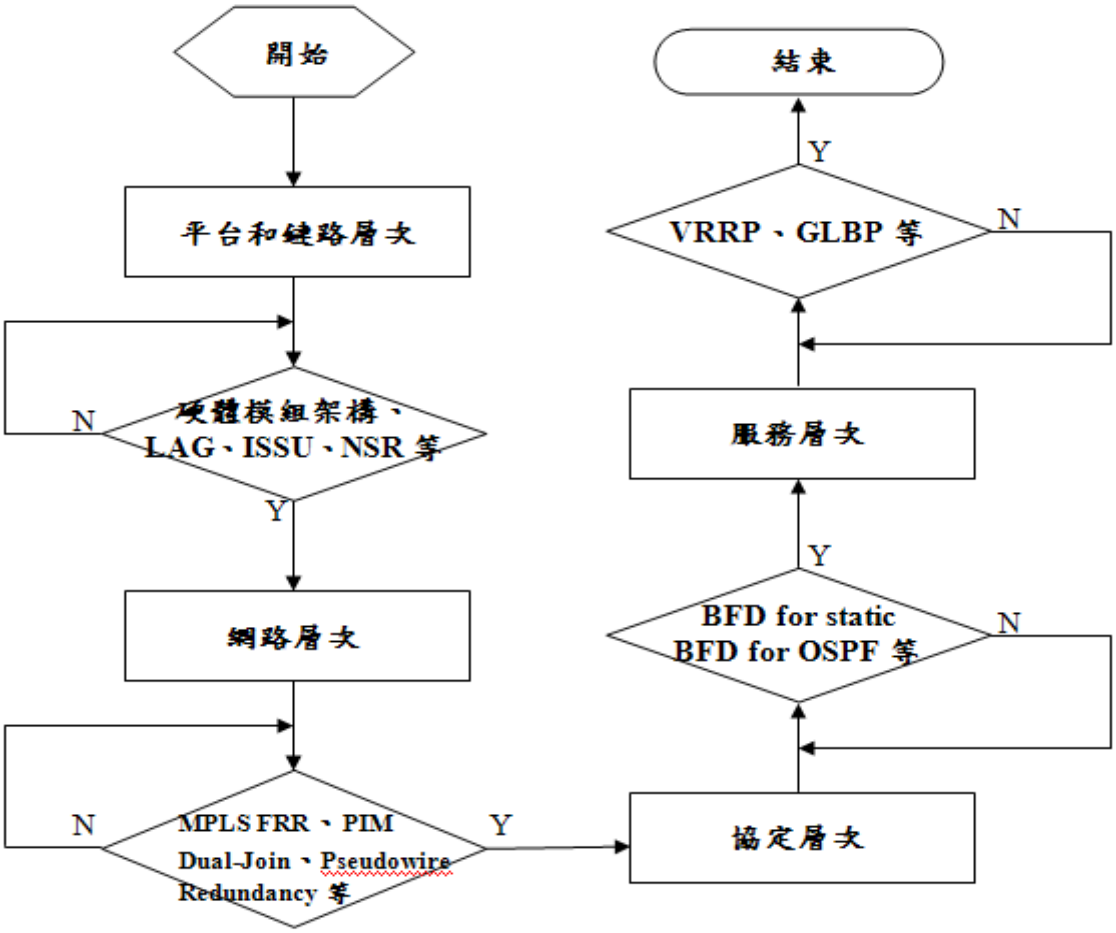
[12] IETF 標準組織，"Virtual Router Redundancy Protocol (VRRP)"，RFC 3768，2004 年 04 月。

[13] Cisco 公司技術部門，"GLBP - Gateway Load Balancing Protocol"，Cisco 公司，http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glbp.html。

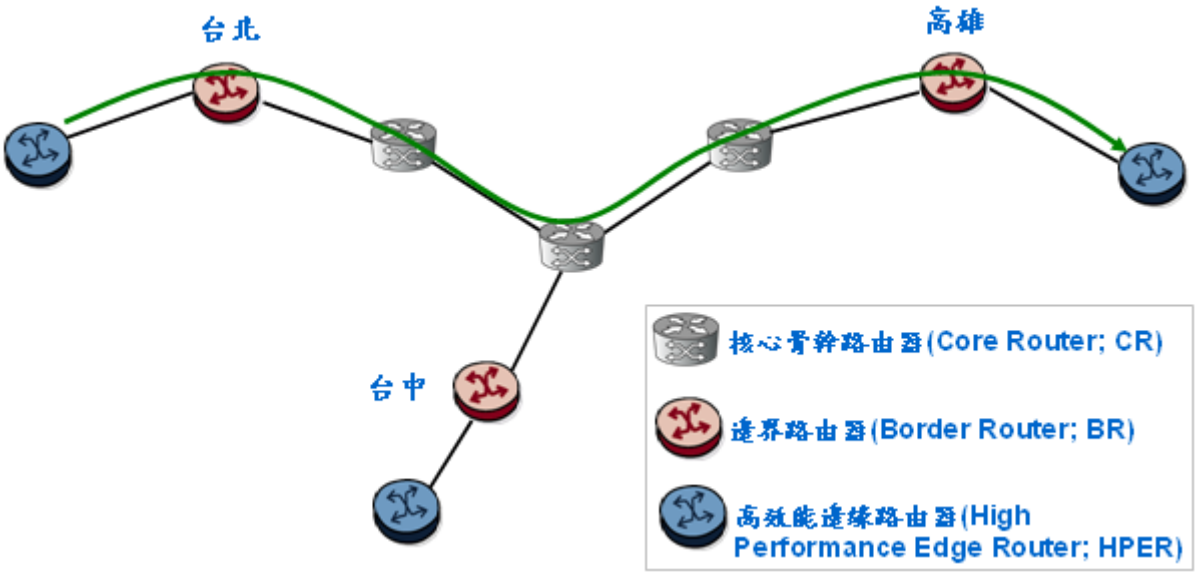
範例研析

圖六為設計一個高可靠度網路架構流程圖。首先先規劃設計平台和鏈路層次備援，決定硬體和鏈路備援功能，包括電源供應與 ISSU 等，若此層次考慮不周全時，則對此層次重新再檢視，檢視妥當後往下一層次去規劃設計，循序地規劃設計每個層次備援，包含網路層次與協定層次與服務層次。完成四個層次備援規劃設計，即可規劃出一個高可靠度的網路架構。

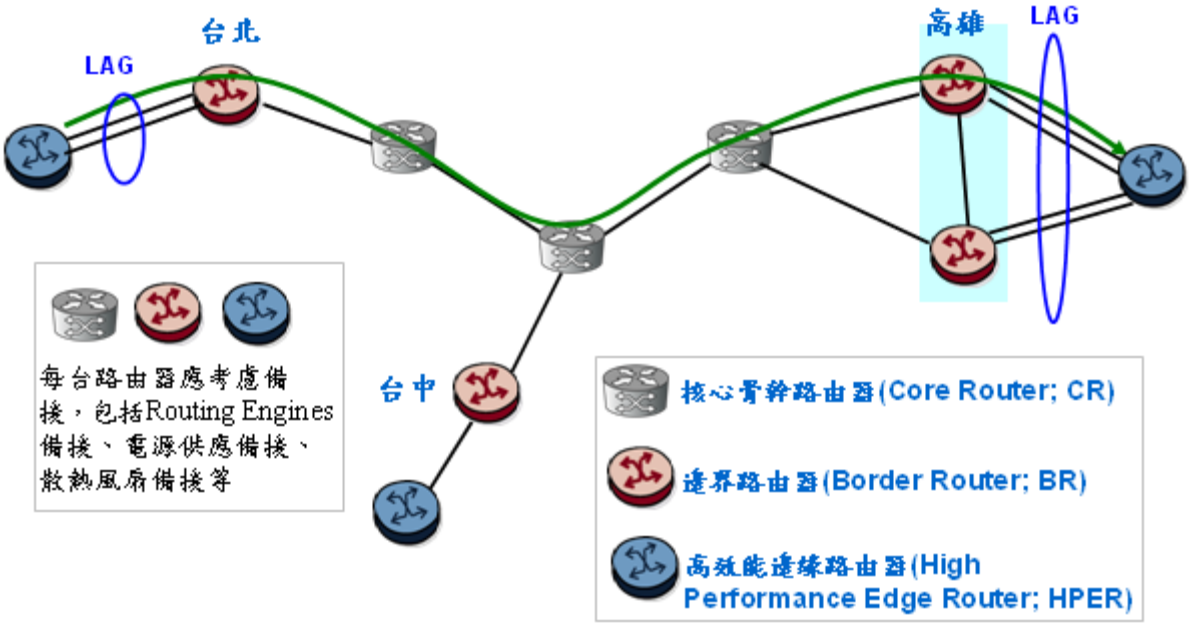
依據圖六的設計流程步驟，本範例在網路備援機制開始設計時，首先考慮無任何備援機制的網路架構著手，如圖七所示；接著考慮每個設備其硬體狀態，是否具備電源備援保護、路由處理模組備援等，相關設計的範例如圖八所示；其次依據網路拓樸圖，設計鏈路節點的保護機制，其範例如圖九所示；然後考慮是否有完善的偵測機制，當偵測到故障時，會立即發出通知並確認故障位置，圖十為設計的範例；最後考慮與區域網路(內網)界接設備備援保護、訊務流備份等，當網路節點鏈路發生故障中斷時，能在短時間內切換完成，使運行的訊務不中斷，相關設計的範例如圖十一所示。綜合完成上述四個步驟，即可規劃出一個完整且高可靠度的網路架構，其網路架構規劃設計如圖十二所示。



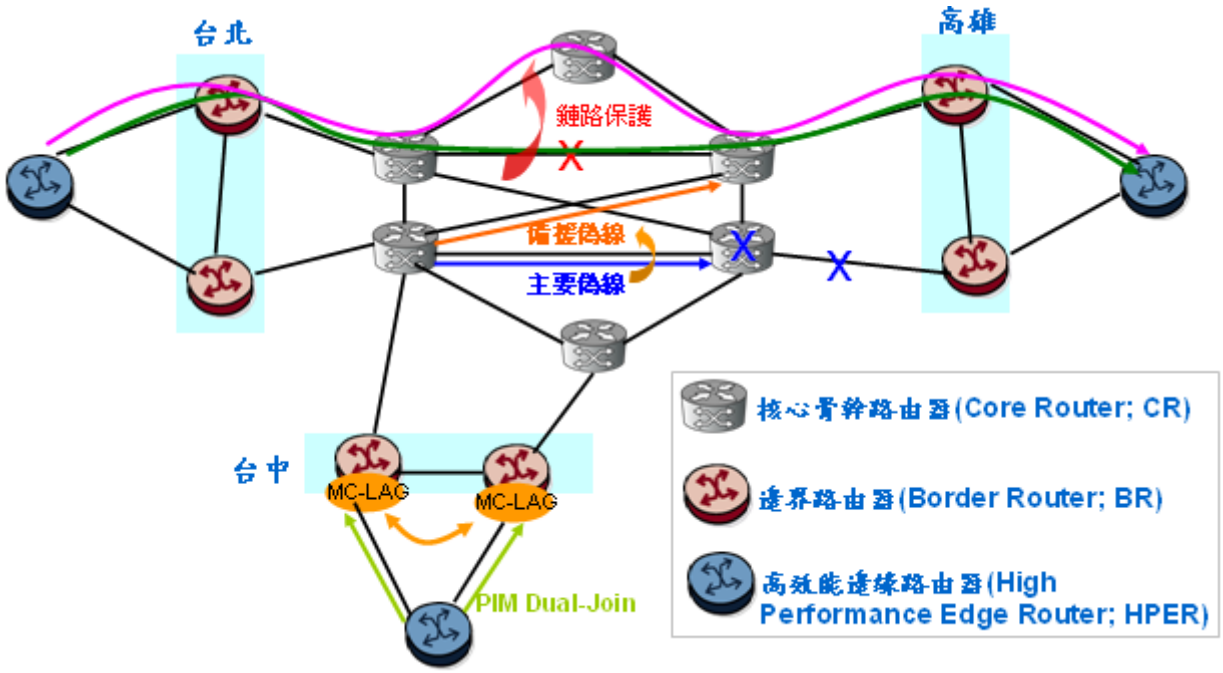
圖六 高可靠度網路架構設計流程圖（資料來源：作者繪製）



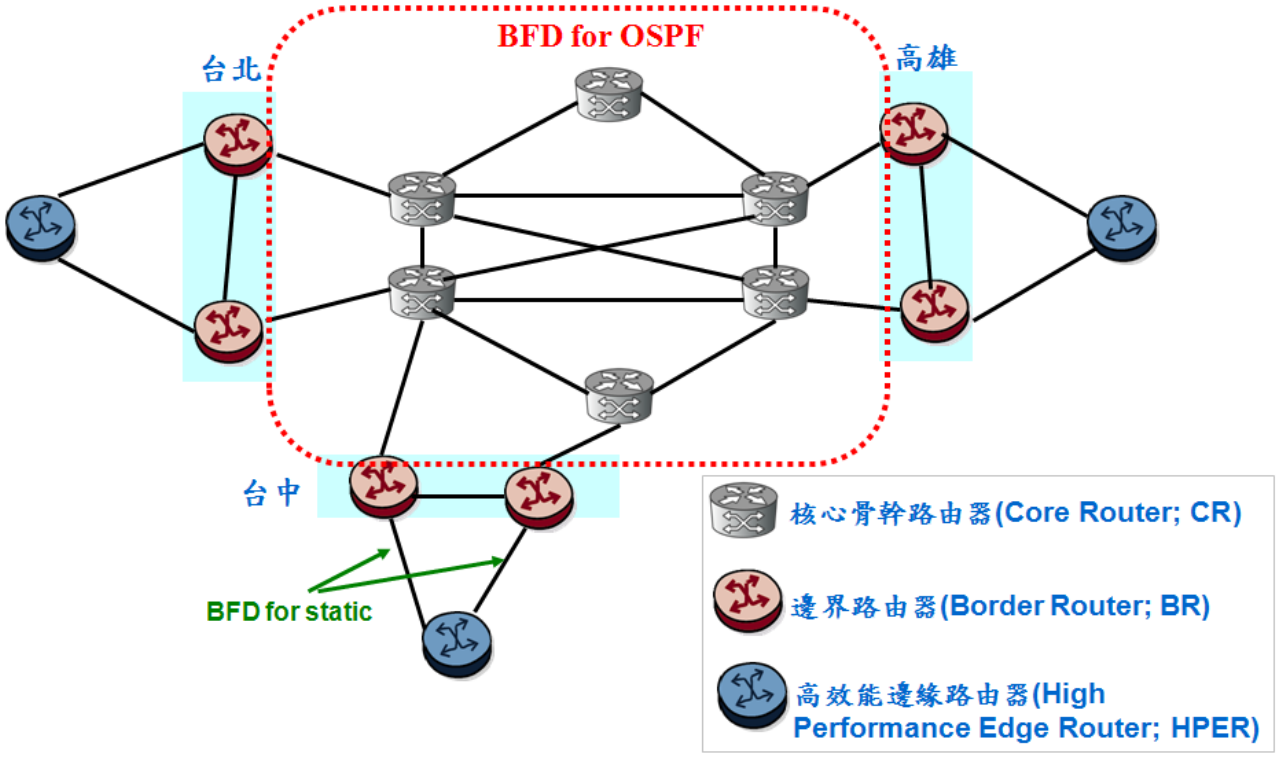
圖七 無任何備援機制的網路架構（資料來源：作者繪製）



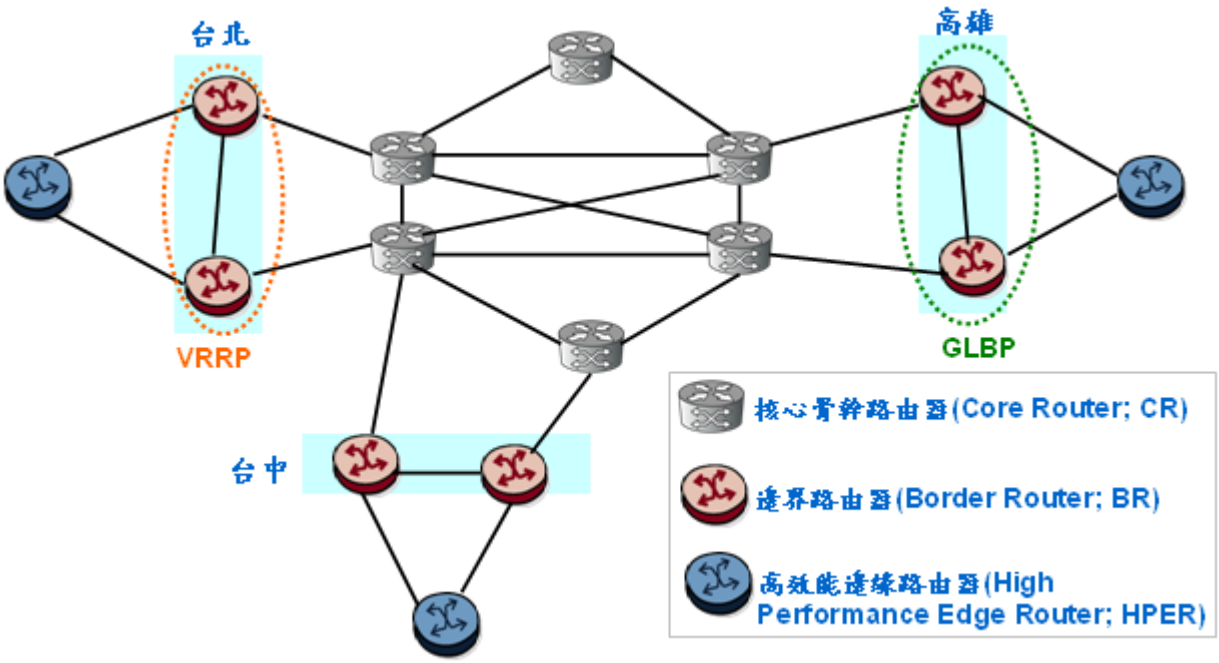
圖八 規劃設計平台和鏈路層次備援機制（資料來源：作者繪製）



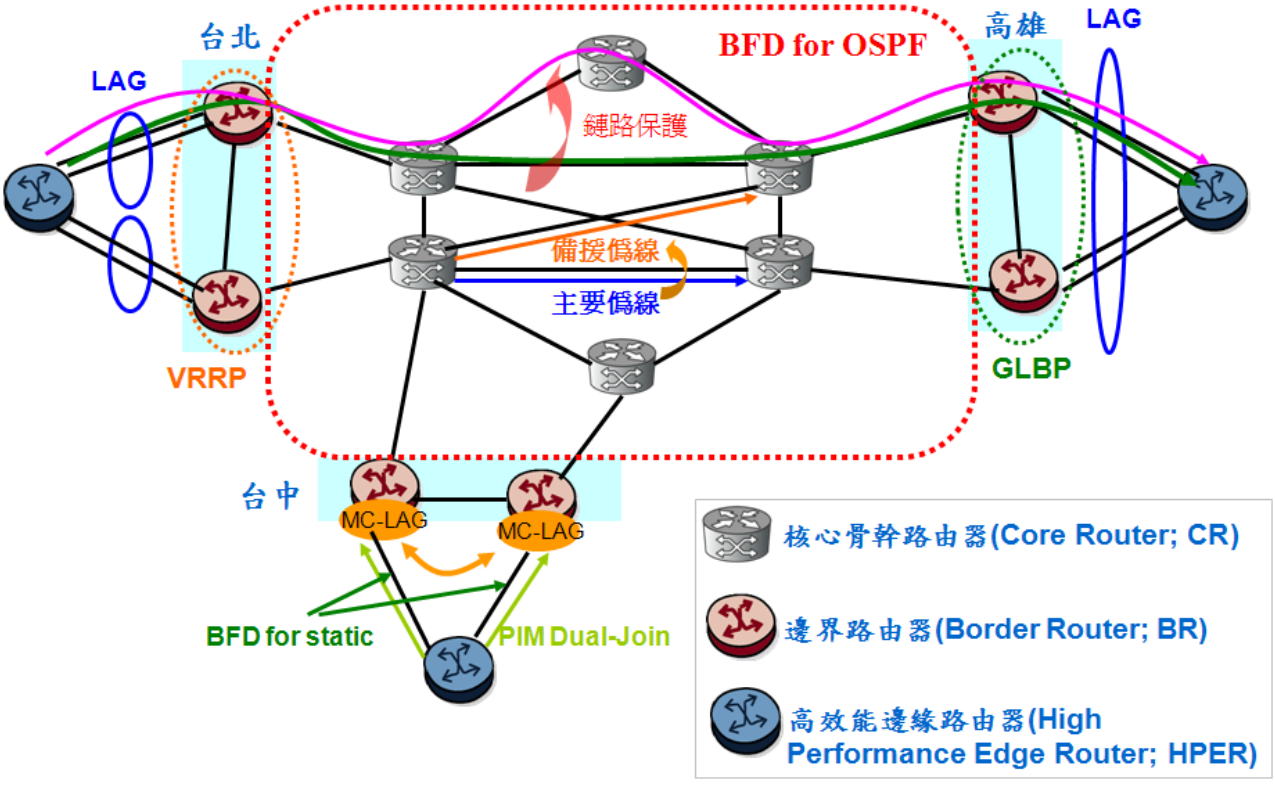
圖九 規劃設計網路層次備援機制（資料來源：作者繪製）



圖十 規劃設計協定層次備援機制（資料來源：作者繪製）



圖十一 規劃設計服務層次備援機制（資料來源：作者繪製）



圖十二 高可靠度新世代的網路架構設計範例（資料來源：作者繪製）

結論

本文介紹了各種進階的 IP 網路整合技術，以及新世代網路的基本概念，除

了讓電信業者或網路提供者可以同時提供多項服務與降低營運成本及資本支出之外，還可以讓網路的可靠度、擴展性與彈性獲得大幅提昇。同時配合日益進化的 QoS 機制，大規模建置提供優質多元的網路應用服務將更容易達成，加上強化的用戶管理及網路安全功能，使得服務的供裝、維運更加簡化。文中也提出 MPLS 技術除可以提供快速備援、訊務工程外，更重要的是可以增加網路可靠度。然而除了 MPLS 技術可以提供高可靠度的功能外，本文也提出如何設計出高可靠度的網路所需參考的流程與相關技術。相較於電信業者所提供的開放式網路架構與技術，用於軍事用途的網路則有其他更特殊的需求，例如高可靠性、隱密性、安全性與迅速性等特性，平時軍方可利用此網路進行相關軍事資訊的溝通與傳遞，戰時更顯得這些功能的重要性。當軍方朝向國家型計劃的方面來發展時，基本上是配合國家政策的執行，相關資源除了可以參考民間業者的寶貴經驗之外，更能結合國家網路工業運用於國防的好處，如此除了不須太依賴國外的解決方案，更能長期發展國內相關的產業，達成國防自主之目的。