行政院所屬各機關因公出國人員出國報告書
（出國類別： 實 習 ）

『實習 IDC 備援服務新技術/NOC 網管監控整合技術』

出國報告

服務機關： 中華電信股份有限公司
數據通信分公司
出 國 人： 職 稱 姓 名
副 處 長 尤能明
助理工程師 楊坤華

出國地點： 美 國
出國期間： 92.11.30 至 92.12.13
報告日期： 93. 2 .26

系統識別號:C09204908

公 務 出 國 報 告 提 要

頁數: 42　含附件: 否

報告名稱:

實習IDC備援服務新技術/NOC網管間監控整合技術

主辦機關:

中華電信數據通信分公司

聯絡人／電話:

／

出國人員:

尤能明　中華電信數據通信分公司　公眾數據處　科長
楊坤華　中華電信數據通信分公司　南區營運處　助理工程師

出國類別: 實習

出國地區: 美國

出國期間: 民國 92 年 11 月 30 日 -民國 92 年 12 月 13 日

報告日期: 民國 93 年 03 月 09 日

分類號/目: H6／電信　H6／電信

關鍵詞: SSL VPN ,Intrusion Detection & Prevention ,Direct Attached Storage ,Storage Area Network ,Disaster Recovery

內容摘要: 近年來天災人禍頻繁,大大提高各產業持續經營之危機意識,政府機構亦在中央所訂定相關分級異地備援之要求下,陸續執行各類之備援措施。中華電信提供IDC服務已有相當時日與基礎,有鑒於異地備援服務不應僅止於傳統的資料備份與系統備份，尚需要考量當資安事件類型的災害發生時，如何做好相關的備援處理，以達到快速復原的目標，故此行不僅是對傳統資料備援的新技術進行瞭解，且針對資安事件類型的災害的備援技術進行實習，期望能夠將兩個領域的技術整合並導入爲IDC之服務，期能推出新一代的備援服務及其衍生相關的加值服務。另針對日益增多的IDC客戶與日漸複雜的IDC機房環境，如何建置並整合一套有效的機房/網路管理系統，亦爲此行之重點，另外對運用新技術以增強維運效率及對未來IDC之經營，亦提出一些看法與建議。

本文電子檔已上傳至出國報告資訊網

題要表

近年來天災人禍頻繁，大大提高各產業持續經營之危機意識，政府機構亦在中央所訂定相關分級異地備援之要求下，陸續執行各類之備援措施。中華電信提供 IDC 服務已有相當時日與基礎，有鑒於異地備援服務不應僅止於傳統的資料備份與系統備份，尚需要考量當資安事件類型的災害發生時，如何做好相關的備援處理，以達到快速復原的目標，故此行不僅是對傳統資料備援的新技術進行瞭解，且針對資安事件類型的災害的備援技術進行實習，期望能夠將兩個領域的技術整合並導入為 IDC 之服務，期能推出新一代的備援服務及其衍生相關的加值服務。另針對日益增多的 IDC 客戶與日漸複雜的 IDC 機房環境，如何建置並整合一套有效的機房/網路管理系統，亦為此行之重點，另外對運用新技術以增強維運效率及對未來 IDC 之經營，亦提出一些看法與建議。

目錄

第一章　前 言

IT 委外處理之趨勢造就 IDC 產業蓬勃發展,而備援作業乃 BCP 計畫其中之一環,為了避免天災(火災、水災、雷擊、地震等）、人禍(暴動、戰爭、駭客攻擊、病毒侵略、錯誤的處理程序等）、軟硬體失靈、斷電等各種災害影響企業之正常運作,確保組織中之重要作業過程得以連續的計劃與方法, 以期當資料或資訊系統損害時能有效的應變及復原,使作業能順利執行並使損失降至最低。所以備援是確保高可用度的一種方法，而資訊安全的目標是確保資訊系統的可用度、保密性與一致性，因此備援也是一種資訊安全的保護措施。

網路管理的功能在 ITU-T 的 TMN(Telecommunication Management Network) 中包括障礙(Fault) 管理、組態(Configuration)管理、統計與計費事(Accounting)管理、效能(Performance)管理以及資訊安全(Security)管理。其資訊安全管理涉及預防與偵測任何在網路資源或服務上的不當使用，也包括資訊安全管遭破壞後的復原。

從以上兩點來看,備援服務及網路管理均與資訊安全密切相關，所以此次出國實習,除了研習備援服務、網路管理之外，也針對資訊安全技術--SSL VPN 進行瞭解。

第二章 行程概要

一、11 月 30 日（星期日）： 行程。

二、12 月 1 日 - 12 月 5 日：至 NetScreen 公司研習，NetScreen 公司為一家資訊安全設備製造商，瞭解該公司在資訊安全的產品佈局，從 Firewall/VPN 到 IDP(Intrusion Detection & Prevention)以及 SSL VPN 設備，以及 Security Management 管理軟體的開發。FalconStor 公司研習，包括新儲存技術與異地備援技術研習討論，以及其客戶美商藝電 EA(Electronic Arts)之異地備援實際案例探討。 Extreme Networks 公司研習，實習在 Router 或 Switch 上如何進行 Intrusion 的偵測與阻隔(Access Control List)，用以偵測可能的入侵行為與防止可能的駭客入侵，降低資安事件發生的機率。

三、12 月 6 日 - 12 月 7 日：假日，資料整理。

四、12 月 8 日 - 12 月 11 日：Network Associated 實習，實習 McAfee 產品之防毒技術，以及 IntruShield 產品之入侵預防技術。HDS(Hitachi Data System)公司實習，包括儲存服務之規劃、儲存空間配置、服務架構與維護管理之技術實習。

五、12 月 12 日 - 12 月 13 日：搭機由舊金山返回台北。

第三章 備援服務與網管發展趨勢

一. 儲存架構

處理器與儲存設備(如磁帶、磁碟或 RAID)間的 I/O 方式(或 I/O 通信協定) 有兩種: SCSI (Small Computer Systemic Interface) I/O 與 file I/O

SCSI (Small Computer Systemic Interface) I/O:

SCSI I/O 指令可以告訴磁碟裝置由某一個磁碟的特定位置傳回資料，也可以要求某一個磁帶櫃 mount，SCSI 通常被稱為”block level”通信協定或 block I/O，因為 SCSI 指令明確指定某一個磁碟特定 block(磁碟區塊)位置，所以 block I/O 是由磁碟 block 編號來識別資料；並藉由 SCSI 通信協定來傳送原生(raw)資料

File I/O:

有時稱為檔案系統通信協定，用來存取和分享資料。一個檔案系統指令可以要求讀取某個檔案的前幾個字元，而不須知道資料在磁碟上的位置。File I/O 藉由檔案名稱和 byte offset 來識別資料，藉由 TCP/IP 通信協定傳送檔案資料和控制資料(METADATA):如檔案所

有者、存取權限等，常用的兩種檔案系統為 UNIX 的 NFS(Network File System)和 Microsoft 的 CIFS(Common Internet File System)。

儲存架構一般分為三種:

(一)直接附加儲存(DAS: Direct Attached Storage)

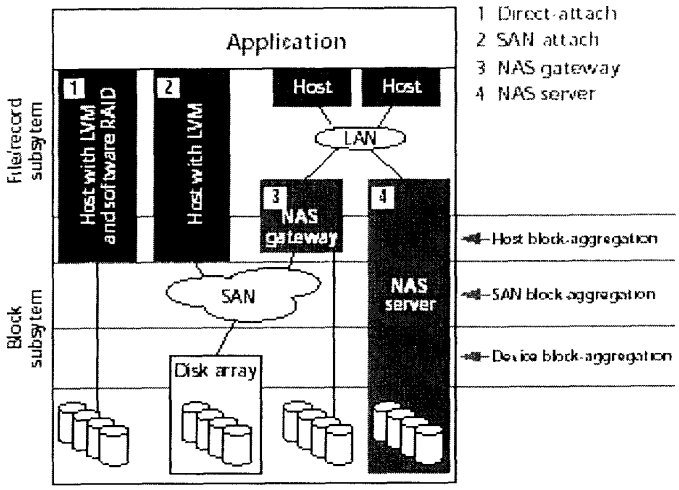
儲存裝置直接藉由一條纜線連接到主機處理系統，這條纜線可能跑 SCSI、fiber channel 等通信協定，其 I/O 方式是 block I/O。

(二)儲存區域網路(SAN: Storage Area Network)

各個儲存裝置與各個主機藉由特定的專用網路連接起來，提供主機與儲存裝置間 any-to-any 的連接性,該專用網路常用的通信協定為 Fibre Channel,而以 Ethernet 為基礎的 SAN 也在快速成長中。SAN 是由伺服器、儲存裝置、網路設備(HBA:Host Bus Adapter、交換機、集線器、路由器等)以及軟體所構成。SAN 的 I/O 方式是 block I/O，可以提供”block”應用程式最佳化處理,這些應用程式通常是高效能且直接從磁碟讀寫大 block 資料，例如 Oracle 或 Microsoft Exchange。

(三)網路附加儲存(NAS: Network Attached Storage)

NAS 伺服器是最佳化的檔案伺服器，附加在以 TCP/IP 為基礎的網路上, 其 I/O 方式為 file I/O，提供”檔案”應用程式最佳化處理,這些應用程式如 Power Point 或 Lotus Notes。NAS 伺服器是獨立單機型(stand-alone)設備，預先載入檔案系統(作業系統)以提供檔案分享，包括 Windows CIFS、Unix NFS、Web(HTTP)等。NAS 伺服器也內含磁碟陣列、資料保護計技術、管理軟體、診斷錯誤軟體及容錯功能(冗餘備用、熱插拔元件）。對於所有資料進出 NAS 伺服器則是以 file I/O 方式經由 IP 網路傳送接收,NAS 作業系統會把 file I/O 轉成 block I/O 格式，然後藉由 SCSI 指令把資料存放在整合式磁碟陣列。(註:所有資料不管是經由 NAS、SAN 或是 DAS,最後都是以 SCSI 指令用 block I/O 格式放在磁碟。)



二、資料生命週期管理

我們知道資料的生命週期是從資料的創造、保護、存取、移動、歸檔到刪除。而資料生命週期管理則是依據資料的價值做存放管理，不讓資料雜亂叢生，使資料的整合存取更加有效率。隨著企業對資訊科技的日益倚重，以及 24 小時全年無休(24*7*365)商業運作的增加，企業資料不斷地快速產生及累積，而這些資料的價值也隨著時間的推移而變化。

資料生命週期管理的一個重點是讓資料價值與儲存價值相匹配(data value matched to storage value），因為以投資報酬率來看，不同的資料當然要有不同的管和保護，讓過時的、不重要應用程式的資料擺放在低階的儲存媒體上。資料的價值決定於企業的需求與法規

的需求，對企業生存發展愈不能缺少、愈有幫助的資料，價值就愈大。另外，各國政府隨著社會環境變化(如美國安隆案)，可能訂定必須保留的資料及資料保留期限，那麼該資料就有了必須儲存的價值。而隨著法規要求或是企業需求的改變，相關資料的價值也應該隨著調整。

資料生命週期管理的另一個重點是:不同種類的資料需要不同的管理工具。應用程式的資料依其結構化的程度可以分成三大類:

結構化資料應用程式:交易(Transactions)

◆資料成長非常快

◆應用程式/資料庫的大量資料拖垮伺服器

◆需要”修剪”資料以增進效能，但法規可能規定保留期限而不允許”修剪”

◆需要一個對應用程式透通的交易資料 archiving 方案

半結構化資料應用程式:E-mail

◆E-mail 訊務及附加檔案大量成長

◆需要增加備份次數

◆需要保留訊息以符合法規的要求 :例如 Hitachi Data System 的 Open LDEV Guard 軟體提供 WORM(Write Once Read Many)功能，一但資料完成「寫入」程序後，在一段保存期限內，它允許獲得授權的應用程式檢索和讀取，但不能更改或刪除。

非結構化資料應用程式: Productivity

◆40 % 到 50%是 office 及其他非結構化文件

◆很多過期而沒有人管的文件

◆有需要自動化地移到比較低成本的儲存設備

最後應該要注意的是，資料生命週期管理能夠依資料被存取的情形來移動資料在儲存環境中的位置，甚至被刪除，也就是說它會依據歷史統計來做管理，如果管理人員沒有介入設定管理策略，最後管理出來的資料並就不是企業所要的。因此除了好的設備產品(product)，適當平台 platform，policy(政策)的設定與適當的流程(process)，是非常重用的。

三. 備援服務內容與趨勢

企業或是機構的資訊系統考慮備援，主要是期望能夠做到災難復原(Disaster Recovery)，當發生災難時，資訊系統依舊能夠繼續運作或是在中斷後迅速回復運作。在傳統的備原或是災難復原的領域中，其所關注的焦點在於：Network Connectivity、Hardware、Operation Systems、Critical Data Structures、Mission-Critical Applications，如圖一左側所示。

Traditional disaster recovery site considerations	Additional recovery site considerations that address information security
• Network connectivity • Hardware • Operating systems • Critical data structures • Mission-critical applications	• Anti-virus protection • Firewalls and access control rules • Router control lists • Intrusion detection • VPN and authentication tokens • Content filtering • Forensics and diagnostic tools • Operating system and application security patches

圖一、傳統災難復原與新災難復原所需考量的範疇

目前我們的異地備援服務是已經都將這些部份涵蓋，我們 IDC 所提供的異地備援服務包括有：

1. 資料備份：目前已經投資有防火櫃做為客戶之備份磁帶的保存，以及網路儲存系統做為線上(On-Line)資料備份複製保存之服務。
2. 機房備份：目前主要以桃園富國機房做為異地備援的機房。

3. 系統備份：目前提供伺服主機租賃服務，供客戶重新安裝 Operation System 以及 Application 軟體，做為備份資訊系統。同時我們也提出 Windows 作業系統的線上備份的功能機制，讓客戶在復原時期省卻重新安裝作業系統與應用軟體的時間。
4. 網路備份：提供 X.25、Frame Relay、ATM、IP VPN 等網路之備援切換服務，以作為備援機房與使用者之間的備援通信網路。
5. 辦公室備份：提供客戶在災難發生後，緊急的備援辦公室，做為臨時辦公之用。
6. 人力技術支援：提供客戶在災難發生後，調度 IDC 相關的人力支援客戶加速復原時程，達到企業營運中斷時間縮短之目標。

而在圖一的右側部份，則是列出新的災難復原所需考量的範疇，也就是將資訊安全(Information Security)考量進去，包括有：Anti-Virus protection、Firewall and access control rules、Router control lists、Intrusion detection、VPN and authentication tokens、Content filtering、Forensics and diagnostic tools、Operation system and application security patches 等，這些資訊安全的議題在我們目前的 IDC 加值服務中，部份已經提供，但是卻沒有納入異地備援的服務中，如何整合進入異地備援服務中，提供出那一種類型的服務是目前急需規劃進行的工作。

為什麼異地備援要考慮資訊安全？其實我們講異地備援其實應該說是災難復原(Disaster Recovery)，而進行災難復原不外乎是要做到企業永續服務(Business Continuity)，所以如果我們能夠讓"災難"不發生，其實也就不需要進行災難復原；傳統的"災難"多指是天災，天然

災難當然非人為可以控制，但是現在的"災難"已經擴展到像是病毒、蠕蟲、駭客入侵/攻擊、人為錯誤等等資訊安全事件，其實是可以避免或控制的。因此消極地進行災難復原規劃，不如積極地進行風險控制，所以目前的異地備援/災難復原服務也將資訊安全的服務一併納入，以完整的業務永續(Business Continuity)為服務目標。就像我們對抗感冒一樣，在未感冒前可以採用"施打疫苗"的方式來避免感染，在感染感冒後採用"服用藥物"的方式來治療感冒；所以資訊安全的管理就像是"施打疫苗"的預防措施，而異地備援/災難復原則是"服用藥物"的補救方法，誠如我們常見的一句話「預防勝於治療」，所以資訊安全的管理服務是在企業進行業務永續(Business Continuity)時的最佳疫苗。

我們來比較一下資訊安全與災難復原/異地備援的不同，如同表一之比較表說明。

表一、資訊安全與災難復原的比較表

Information Security	Disaster Recovery
著重在確保資訊的可用度、保密性與一致性(Availability, Confidentiality, Integrity)，避免非授權的存取、使用與修改	著重在災難中復原(Recovery)，進行 resources redundant & backup, emergency response, and recovery
期望藉由許多程序管理降低安全威脅發生的機會(**降低風險**)	期望縮短災難發生對營業中斷的影響時間(**加速復原**)

為了做到高可用度(High Availability)，多數做法為進行 redundant & backup 及相對的復原計劃，因此 Information Security 計劃中多涵蓋 Disaster Recovery	

我們可以從表一中了解其實在資訊安全的領域中，災難復原是涵蓋其中的，因為資訊安全的目標是確保資訊系統的可用度、保密性與一致性，在可用度方面來看，災難復原是確保高可用度的一種方法，所以當大家在重視災難復原的這些工作時，我們反省一下其問題來源我們會發現，其實我們需要重視的應該是資訊安全的議題。如果我們做好資訊安全的控制，就可以降低甚至於避免災難發生的機會，自然就無需啟用到災難復原計劃，這才是企業永續營運最佳的目標。

所以我們發現現在的 IDC 服務方向是朝資訊安全管理服務(Security Management Service)來發展，由資訊安全管理服務來涵蓋災難復原服務，達到服務面更廣更大更完整的方式來說服客戶委外由專業的 IDC 服務業者來負責。這些工作不外乎包括：防火牆架設與管理、入侵偵測與預防、弱點分析及修補、資訊的存取控制、事件的預警與告警通報作業、緊急應變計劃與程序、內外部稽核等等，我們分別依據各個服務內容來探討客戶需求以及服務業者所可能提供的服務方案：

1. 防火牆架設與管理：防火牆的架設與管理的工作主要是在於資訊安全政策上的訂定，確立內外部的通信開放部份與不開

放部份以及開放對象等等政策。管理的部份包括資訊安全政策的異動管理以及防火牆的設備維運管理等等工作。目前在資訊安全管理服務(Security Management Service)裡面，多數委外服務的公司是以防火牆架設與管理委外部份為最多。國外的服務案例有的是防火牆由企業自備，而維運管理委外；也有是防火牆由資訊安全委外服務商(Security Service Provider)提供，包括軟硬體的維運管理。目前我們已經提供此類的服務，我們採用 NetScreen 的防火牆，並由我們統一提供維運與管理服務，定期產生報表供客戶參考資訊安全事件記錄。

2. 入侵偵測與預防：由於新的駭客入侵已經不是單純透過防火牆就可以阻隔的，而是透過資訊系統本身的漏洞滲透進入，因此唯有透過入侵偵測(IDS, Intrusion Detection System)，或是入侵預防(IPS, Intrusion Prevention System)等設備，才能偵測出入侵事件或是阻隔入侵攻擊。早期的技術多半是採用網路型(Network-base IDS)或是主機型入侵偵測(Host-base IDS)，其作法只能偵測出可能的攻擊事件，並無法即時阻隔攻擊，因此目前比較新的技術都強調入侵預防的作法，然而入侵預防的技術的缺點是怕遭遇到誤判情形，將正常封包阻隔；另外一個缺點則是因為入侵預防其作法像防火牆一般，需要逐一封包檢視，因此效能是其瓶頸，如何提昇處理效能是入侵預防設備的挑戰。目前我們 IDC 機房也有提供入侵偵測服務，我們採用 ISS(Internet Security System)公司的產品來作網路型入侵偵測服務，入侵預防的產品與服務正在測試開發階段，預計與其他資訊安全的服務做一配套包裝後提出新服務。
3. 弱點分析及修補：弱點分析(Vulnerability Assessment)服務主

要是著眼於發現資訊系統所潛在的弱點或漏洞，並提供修補或加強的建議方法，以類似健康檢查的顧問諮詢來強化資訊系統的安全。目前我們 IDC 機房也有提供弱點分析及修補服務，我們採用 ISS(Internet Security System)公司的產品來作弱點分析及修補服務，如何有效的建立資訊資產資料庫以及弱點分析資料庫，以提昇弱點分析服務的正確性是本服務下一階段的挑戰。

4. 資訊的存取控制：所謂的資訊的存取控制主要是管制需要有經過授權的人方可依據其權限存取特定資料。此部份的技術多屬於應用系統上的認證授權，比較難以 ASP 模式委外，因此此部份較少有服務的特定模式，僅有少部份是專案式客製化處理。除了應用系統上的認證授權外，資訊的存取控制也可以在前端的網路設備上進行控管，如 Access Control List (ACL)的設定，此部份倒是可以進行委外的部份；我們目前亦有提供路由器或交換器等網路設備上進行 ACL 的存取控制功能的設定。
5. 事件的預警與告警通報作業：資訊安全的預防以及即時偵測通報是非常重要的，一個是防範於未然，一個是即時的反應處理，所以事件的預警與告警通報作業是目前多數資訊安全委外服務的必要服務項目。事件的預警包括資訊系統新弱點/漏洞的通知，以及新的資訊安全攻擊手法的通知；告警通報則是包括遭受入侵/攻擊之事件通告，以及國際間其他最新入侵/攻擊之事件通告。目前我們 IDC 並沒有完整的此項服務，因為我們需要建立 SOC(Security Operation Center)方能做到即時的入侵/攻擊之事件通告，以及與其他國家的 SOC 連線

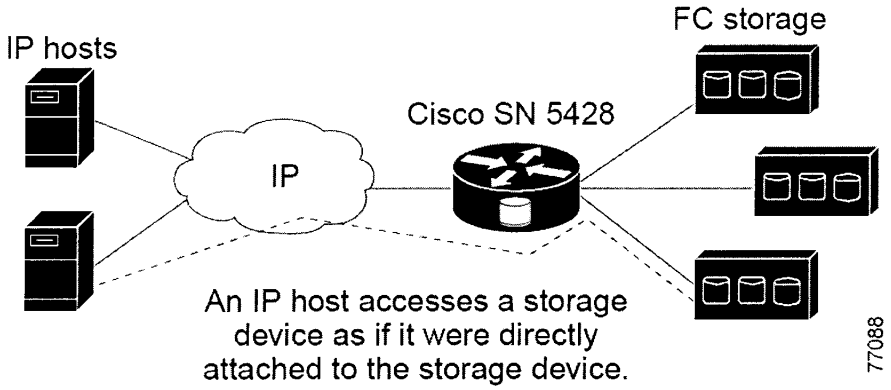
方能取得最新的入侵/攻擊事件通告；目前我們的服務僅提供資訊系統新弱點/漏洞的通知，以及新的資訊安全攻擊手法的通知。

6. 緊急應變計劃與程序：有了即時的事件通報，還需要有一套完整的因應計劃與程序，才能在發生資訊安全事件時能不手忙腳亂，有條理的做出反應並加速處理，以降低事件影響時間與範圍。
7. 內外部稽核：資訊安全的各項工作是否落實，唯有藉由稽核來確保，方能達到資訊安全的各項政策之要求。稽核的方式有分內部稽核與外部稽核兩種，內部稽核是較經濟的一種作法，至於外部稽核的成本較高，但是卻也可能發現更多的改善空間以更落實資訊安全的工作。目前我們 IDC 並沒有幫客戶進行稽核的工作，僅有是配合客戶的稽查人員進行答覆稽核的作業。

當然除了資訊安全的預防措施外，還是需要有事發後補救的措施，所以異地備援/災難復原還是需要的。然而目前的異地備援/災難復原的趨勢為何？主要還是以資料儲存技術的演進為主，主要的趨勢有：iSCSI 的相關硬體陸續成熟上市、IDE 硬碟陣列的推出、Windows NAS Server 的推出、以及跨廠牌的儲域網路系統(Storage Area Network, SAN)管理功能等等。

1. iSCSI 的相關硬體陸續成熟上市：Intel 的 iSCSI 網卡的上市，以 Gigabit Ethernet 的速度傳送資料，同時也簡化了網路儲存的架構，再搭配 Cisco 的 SN 5000 系列的 Storage Router 就可以讓前端的伺服主機存取位於 TCP/IP 網路後端的 Storage，感覺就像是 Direct Attach Storage 一樣，如圖二。這樣就可以

輕鬆地用主機端的單純 Copy 指令做到遠端資料備份，因為本機看到的磁碟區塊，已經是遠端的磁碟機。



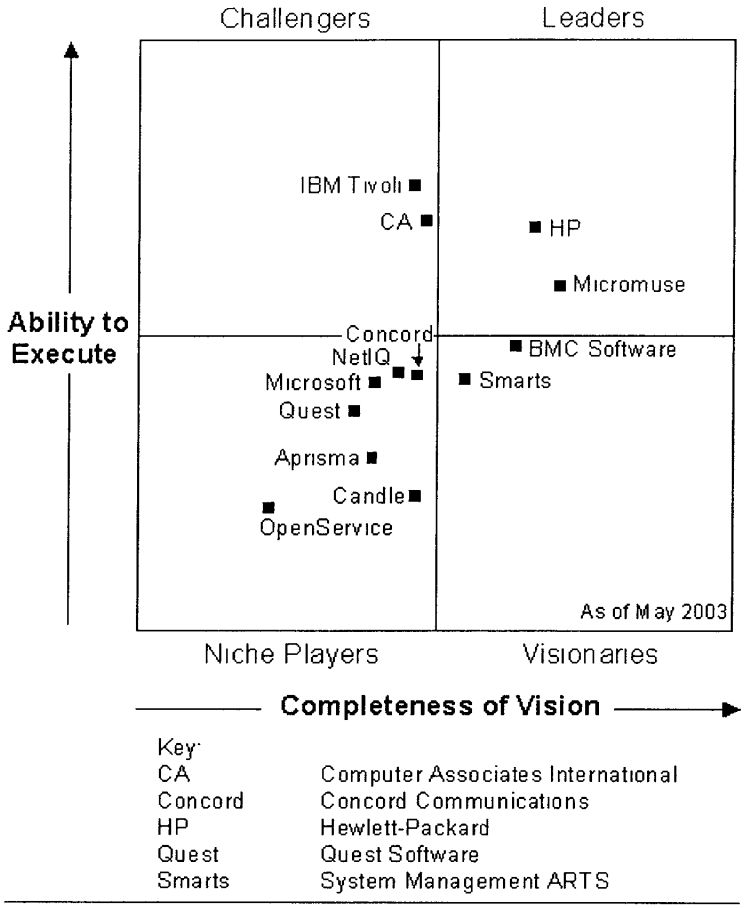
圖二、iSCSI Router 介接使用架構圖。

2. IDE 硬碟陣列的推出：SCSI 硬碟成本較高，隨著 IDE 新傳輸介面標準的推出以及低成本的優勢，IDE 硬碟陣列的推出形成一個介於 SCSI 硬碟陣列與磁帶機之間的一種儲存媒體，也因此改變了許多儲存應用的架構，像是以往磁帶備份的時間過長的問題可以改為備份至 IDE 硬碟陣列中，以加速備份所需時間。另外一種應用為將較為少存取的資料由效能較佳的 SCSI 硬碟陣列中搬移至 IDC 硬碟陣列中，可以降低系統運作成本。
3. Windows NAS Server 的推出：軟體業界的巨人投入 NAS 的儲存領域中，使得原本比較廉價的 NAS 備份市場掀起了不小的漣漪，由於視窗式的圖像操作與為人熟悉的作業系統，造成一股使用 Windows NAS Server 進行資料備份的風潮。
4. 跨廠牌的儲域網路系統(SAN)管理功能：一直以來各廠牌的儲域網路系統(SAN)設備是採用不同的架構與技術來生產，因此不同廠牌間的儲域網路系統是無法對接管理，或是做相互的

資料複製。目前幾家大廠如 EMC、HDS、HP(Compaq)已經取得共識，彼此交換管理的呼叫介面(API, Application Interface)來使用，因此可以達到初步的管理功能，可以監控不同廠牌的儲域網路系統狀態以及配發儲域網路系統的資源給前端伺服主機使用。

四. MICROMUSE NETCOOL 網管軟體

Micromuse Netcool 網路管理軟體的優勢在於提供開放式的架構，可與許多現成的軟體模組相容，並收集管理網路環境中的資訊，包括管理應用程式、語音、數據網路作業設備、網際網路與廣域網路以及電腦系統。Netcool 常被用來整合其它已建置並使用中的管理工具，成為”manager of managers”，被市場調查組織 Gartner 評定為企業事件管理軟體(Enterprise Event Management)領導廠商，如圖 4－1 所示。



Source: Gartner Research (May 2003)

圖 4 - 1 Enterprise Event Management Magic Quadrant, 2003

Netcool/OMNIbus 是 Micromuse 的旗艦級操作支援系統(OSS)應用，可即時收集、過濾及彙整現有網路環境中，超過一千種不同設備及廠牌所發出的即時告警訊息，並將訊息以有意義、直接及點選的方式，快速呈現於螢幕上，Netcool/OMNIbus 管理架構圖

如圖 4-2 所示。

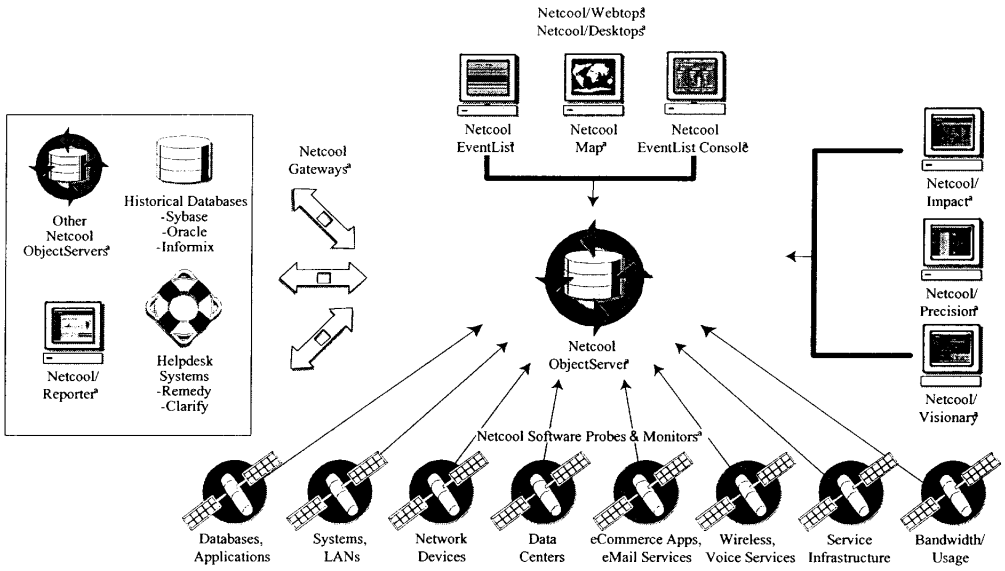


圖 4-2 Netcool/OMNIbus 管理架構圖

Netcool/OMNIbus 組件

Netcool/OMNIbus 共有四個基本的結構性元素：Probe、ObjectServer、Desktop 和 Gateway。簡言之，Probe 將資料送至 Netcool/OMNIbus 系統，它能從 1000 多種管理資料源收集事件，並將此資料快速標準化，這些事件可在 ObjectServer 中存儲、查看和操作。ObjectServer 為快速的資料庫，能夠去除重複事件、找出事件的關聯狀況，並執行其他處理。Desktop 使操作員能查看、操作和執行資料，為 Netcool 的圖形操作前

端工具套件。Gateway 則將資訊傳送到其他資料庫、伺服器和外部應用，使 ObjectServer 資料能與其他 ObjectServer、RDBMS 檔案（Oracle、Sybase、Informix）、網路管理系統（如 HP OpenView）及其它作業支援系統（OSS）共用。

Netcool/OMNIbus 能即時監控組成網路的所有元件以及受這些元件影響（相關元件停頓時）的所有服務。它還產生（通過檔案閘道）歷史資料，以便實現 SLA 監控和相容性。借助篩檢程式，操作員可以設計自己的 Service View 和 Service Report。

Netcool/Precision 自動故障分析套件

Netcool/Precision 自動故障分析套件包括兩個主要產品。第一個產品提供網路探索(Network Discovery)、狀態監視和自動安裝。第二個產品提供故障分析、故障確認以及網路損害評估。

網路探索：如果我們不能清晰、準確、及時地瞭解網路，那麼，網路的管理，不管是故障管理，還是其他 FCAPS，都是一句空話。Netcool/Precision 將網路探索技術與現有應用資

料的存取結合在一起，將從多種協定、發現技術和資料源的大量資料中提取出來的多層拓撲資訊彙集成一個單一的資料源。

狀態監視：狀態監視主要是確定網路設備和元件的狀態。Netcool/Precision 為整個網路設施提供了一種分佈、可配置的狀態輪詢功能。它的狀態監視模組通過 ICMP ping、SNMP 輪詢、ATM OAM 以及命令行查詢等方式的組合來監視網路。它的配置參數可以按照設備分類或特定設備進行設置，從而讓 NOC 可以區別對待關鍵設備和週邊設備。

自動安裝：只需針對 Netcool 套件進行一些簡單的設置，就可以借助其網路知識自動完成以下工作：

- 按照用戶提供的簡單策略配置它的狀態監視器；
- 檢查那些基於 SNMP 的指定設備，確認其 trap 指令可以傳送到 Netcool ObjectServer；
- 另外，Netcool/Precision 還包括一個軟體，它可以對報告的網路故障進行分析，診斷故障類型（例如，基本故障或次要故障等），並進行網路級的故障損害評估。Netcool/Precision 可以通過自動的基本

測試來確認它的診斷、控制輪詢和報警的規模，並按照故障對網路的影響確定故障的優先順序。

Netcool/Impact

Netcool/Impact™軟體可以針對 Netcool 所收集的故障資料，迅速確定其對 IT 業務流程、網路服務以及電子商務系統的影響。它可以針對特定的事件確定其將會對業務流程、服務和客戶產生什麼影響。Netcool/Impact 的主要功能包括三個方面，即影響分析、回應與調整以及策略管理。

影響分析：當網路或系統發生問題時，它的影響不只是引起網路技術人員的頭疼。某個特定路由器介面或特定伺服器硬體驅動器的問題可能影響到的用戶或業務流程的數量可能是很難預料的。

Netcool/Impact 可以從網路設施和業務兩個角度對故障影響進行分析。當某個事件指出某台主機出現停機時，操作員可能希望對該機器所服務的所有用戶，或選定的部分用戶發出告警。另外，當管理員解決了問題之後，Netcool/Impact 還會發出另一個通知，告知服務已經恢復。

回應：Netcool/Impact 具有迅速確定負責解決特定問題的待命技術人員的能力。當某個事件到達時，Netcool/Impact 將通過 E-Mail、簡訊或其他方式通知具體負責的技術人員。如果該技術人員不能解決該事件，Netcool/Impact 會按照職責鏈將該事件進一步通知向上一級責任人。

故障管理策略：Netcool/Impact 可以讓組織對到達事件的處理策略進行定義和強化。一個簡單的策略可能只是向特定的管理員發送一個 E-Mail，並對日誌欄位進行更新。策略的定義方法很簡單，只要將其與描述不同類型問題解決職責的檔或圖表聯繫在一起即可。這些檔和圖表可以是微軟的 Word 檔、HTML 檔或其他資訊檔，它們將不同的事件類型與操作員必須執行的一系列行動聯繫在了一起。

Netcool® for Security Management™

在資訊安全整合監控與管理方面，Micromuse Netcool 延伸原來在網路障礙與服務管理的整合能力，提供及時資訊安全事件管理。目前能夠整合的資訊安全設備有:

防火牆

Checkpoint Firewall-1 NG

Cisco Systems' PIX 6

Cisco PIX on FWSM
Nokia IP Series
NetScreen Global Pro
Cyberguard
Sonicwall
Secure Computing Sidewinder G2

網路入侵偵測

Cisco IDS v3.0 (PostOffice)
Cisco IDS v4 (RDEP)
ISS SiteProtector
ISS Workgroup Manager
ISS Real Secure Network Sensor v7
ISS Real Secure Server Sensor
Niksun NetDetector
Niksun NetVCR
Enterasys Dragon
Snort IDS 1.9 and v2
Network Flight Recorder

主機入侵偵測

Entercept
Cisco/Okena

防毒

Symantec
McAfee
Trend Viruswall (SMTP)
Trend Viruswall (Exchange)
CA eTrust (HTTP)

網路掃描器

Network Associates' Sniffer Distributed™
Nessus (under development)

網路

Cisco Routers
Cisco Netflow Collectors

內容過濾

Websense Content Inspection

硬體VPN設備

Cisco
Nortel Contivity
Asita Technologies

網際網路服務和通信協定

HTTP and HTTPS
SMTP
POP3
IMAP
DHCP
DNS
FTP
ICMP
NNTP
NTP

認證和授權

Operating system user access controls
Radius
Cisco IOS Access Control Lists

CiscoSecure ACS (under development)
RSA ACE/Server (under development)
TACACS+ Syslog

實體安全系統

Johnson Controls Metasys Cardkey

安全政策管理

Solsoft

應用程式保護

Sana Security Primary Response

應用程式Proxies

Netapp Netcache v5
Squid

資料一致性

Tripwire

作業系統

Unix Syslog
Linux Syslog
Windows NT Event Log
Windows 2000 Event Log

應用程式

Microsoft IIS
Microsoft Exchange
Apache
Oracle

五、 IPSec VPN 與 SSL VPN

1. IPSec VPN

IPSec VPN 技術主要是用於 Internet VPN 架構下，國外網際網路頻寬費用較為廉價，因此許多企業採用 Internet 來架構其企業內部網路(Intranet)，其所仰賴的安全機制即是 IPSec VPN。目前非常多的路由器或是防火牆皆支援 IPSec VPN 功能，只是國內的 Internet 環境還是不像國外那般比 Intranet VPN 網路低廉許多，所以還是較少客戶採用。唯目前的兩岸間的 Intranet VPN 頻寬費用昂貴，因此存在著採用 IPSec VPN 的市場，我們 IDC 倒是可以考慮提供多部 NetScreen 防火牆租賃來構成 IPSec VPN 的服務，以較為經濟的費用滿足台商兩岸的通信需求。

遠端接取有龐大的市場，而這市場包含了下列幾種使用者:

◆筆記型電腦使用者:有許多公司已經用了 IPsec VPN 解決方案，讓這些人員可以安全地遠端接取，VPN 用戶端軟體安裝在這些筆記型電腦上，保護用戶接取安全。

◆其他外出員工:不少用戶沒有筆記型電腦，但是仍然偶

而需要接取 intranet、e-mail 或其他應用。

◆商業夥伴:很多商業夥伴、顧問以及顧客需要接取到公司資訊，有些公司建立了昂貴的 extranet 網站來服務這類使用者。一個理想的遠端接取解決方案應該要對外部使用者做好存取控制。

遠端接取的主要需求包括:

◆可以從任何地方接取，譬如說無線熱門點(wireless hot spot)、網路咖啡廳。

◆支援任何人—銷售人員、在家上班員工、外出員工及商業夥伴等。

◆可以接取到任何應用程式。

◆保護在傳輸中的資料、保護用戶端免於遭受攻擊。

◆容易使用(例如 web 瀏覽器)

◆容易整合到客戶的現有安全基礎架構

IPsec VPN 適合 site-to-site 不適合遠端接取與 extranet

◆IPsec VPN 必須在 IP 網路上建立 tunnel 來連接外地使用者到公司防火牆會閘道器,然後再接到公司內部網路。這通常須要在 tunnel 兩端使用相同的軟硬體,且幾乎都是同一家廠商,然而很少有公司願意或能夠強制要求商業伙伴來使用,由此可知 IPsec VPN 不適合 extranet。

◆至於遠端接取的市場, 對於 tunnel 數需求不多的, IPsec VPN 還可以適用;但對於有上千個遠端使用者分散在不同地點時,分送和管理這些用戶端軟體是非常吃力的。

◆IPsec VPN 使用者可以進到公司內部整個網路,他可能不需要連到公司內每一台伺服器而已, 但是該使用者將發現他都可以使用,無形中增加了安全風險。

◆IPsec VPN 無法穿越防火牆

2. SSL VPN

SSL VPN是一個極新的技術,主要的應用面是在於提供企業員工以非常簡易且快速地透過Internet來安全地存取企業內部的資訊系統。它強調只是透過Https方式,即可非常安全地進行各項傳統的資訊系統應用連線,不像以往需要安裝Tunnel軟體來做安全連線。

SSL (Secure Socket Layer)是介於應用層及傳輸層之間，從應用層傳送到SSL層的資料先被加密後，再送到傳輸層；從傳輸層送來的資料先到達SSL層解密後，再送達應用層。在不變動原有的TCP/IP架構之下，達到資料加密功能。Netscape及Microsoft之Web及**瀏覽器**產品中已內建SSL功能。SSL的運作如下:

- **開始進行交易時，顧客瀏覽器會傳送加密請求給企業的伺服器。**
- **企業伺服器會將公開金鑰與認證資料傳給顧客。**
- **顧客核對認證資料確定企業身份後，隨機產生秘密金鑰，用企業的公開金鑰加密後傳給企業。**
- **企業利用其秘密金鑰進行解密取出此金鑰後，送出交易代號給顧客。**

而SSL VPN是運用SSL和proxy來提供認證和加密,用戶只要透過Browser就可接取公司內部的網站或做檔案分享。SSL VPN採用user-level認證,所以能夠對個別使用者做存取控制。SSL VPN的運作如圖3-1所示:

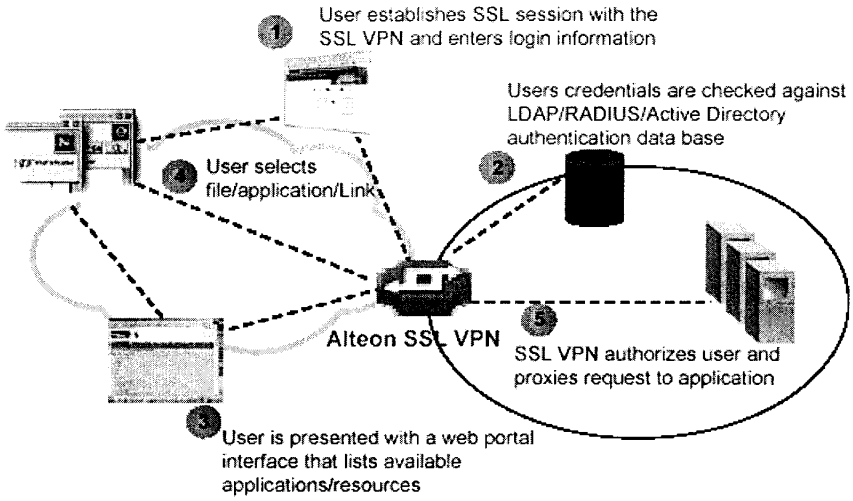


圖 3-1 SSL VPN的運作過程 (source : Nortel Networks)

SSL VPN 的優點:

◆在用戶端方面,只要使用**瀏覽器就可以進行** SSL VPN 連線,簡易方便。

◆整體持有成本降低。

◆快速建置。

◆可以從任何 PC 連上線。

◆不用改變防火牆。

第六章 實習心得與建議

1. 基本上，IDC 的經營是一資金密集、技術密集、人力密集的產業，同時也造成網路設備、主機設備、電力空調高密度使用的特殊環境，也因此突顯網路監控(Network)、資訊安全(Security)、環境設施(Facility)整體管理的重要性，類似 Micromuse Netcool 兼具監控與管理之整合系統在市場上已陸續出現，我們將密切觀察評估，並適時引進系統，以彌補因客戶眾多且進出頻繁與機房分散可能產生之風險，並提升 IDC 之服務品質。

2.考慮導入 SSL VPN 技術：

a. 初期建立以 SSL VPN Base 的 IDC 維運網路，供 IDC 維運主管人員於非上班時間安全地進入 IDC 網路，進行遠端遙控障礙修復等工作，以彌補人力之不足。

b. 建置並提供 SSL VPN 服務:

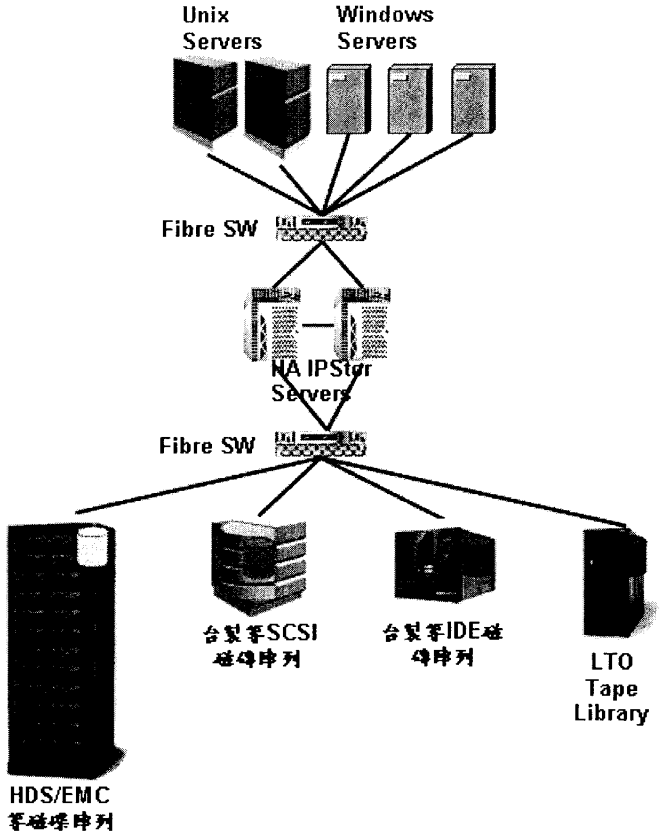
SSL VPN 是一個極新的技術，主要的應用面是在於提供企業員工以非常簡易且快速地透過 Internet 來安全地存取企業內部的資訊系統。它強調只是透過 Https 方式，即可非常安全地進行各項傳統的資訊系統應用連線，不像以往需要安裝 Tunnel 軟體來做安全連線，此對兩岸台商、 商務人事或企業客戶或可適時解決

當前之資通問題。

3. 另外在儲存網路系統服務：以儲存備援服務方面的技術而言，因為已經是成熟的市場服務，所以目前所見到的服務趨勢比較著重於管理功能部分。而不同廠商的儲存網路系統，各自有其管理的系統與介面，很難做到整合監控與管理。而這些問題已經存在已久，現在我們終於看到部份的成果。目前幾家大廠如 EMC、HDS、HP(Compaq)等多已經取得共識，彼此交換管理的呼叫介面(API, Application Interface)來使用，因此可以達到初步的整合管理功能，可以監控不同廠牌的儲域網路系統狀態，以及配發儲域網路系統的資源給前端伺服主機使用。

像此次參訪實習的 FalconStor 公司就可以跨廠牌的管理不同廠牌的儲存網路系統，然而它所強調的是採兩種方式來介接，一個是單純地當不同廠牌的儲存網路系統為一個磁碟陣列，另外一個做法是以 SED(Service Enable Disk)將原本的儲存切割資訊轉址方式(Redirect)來做整合再利用，所以它能夠以側面角度來與其他品牌來介界接(非正統做法)，而且也可以順利地與多家廠商介接，而不用取得該公司的內部運作架構或細節。不像其他 EMC、HDS、HP(Compaq)等廠商間以交換控制介面來相互連線。但是其缺點就是因為它們採側面方式來介接，有些客戶比較不能接受這種類似走後門的方式，所以這也影響了部份市場的開拓。不過我們倒是可以善加利用這個好處於客戶首次進行的 Data Migration 的過程中，因為這只是一次性工程，客戶應該可以接受這種介接方式，完成後會再恢復為原先架構或是一個嶄新的架構。

至於此次 HDS 的行程中，我們也發現像 HDS 與 EMC 等儲存網路系統大廠，皆推出中低階的產品，並且將原本高階產品的異地備份/複製功能移植到中階產品上，因此具備異地備援的儲存網路系統之費用已經大幅下降。我們可以利用此一現象再投資世界大廠 HDS 或 EMC 的中階儲存網路設備，做為我們儲存服務的儲存空間，將原本舊的儲存空間投資設備(台灣製的 SilverShine 磁碟陣列)做為第二階之儲存空間，或是以效能區隔為 Level 1 與 Level 2，客戶要求高效能的儲存空間服務我們以 HDS 或 EMC 的設備提供，如果中小型客戶所需的僅是尚可的效能空間，那我們就以台灣製的 SilverShine 磁碟陣列做因應，如此以不同的成本經營，也給客戶不同的費用來租賃，相信可以區隔出市場定位，各別在不同的客戶群中尋得目標客戶。再加上可以考慮引進 IDE 的磁碟陣列，來做為 Level 3 的儲存空間服務，定位在做資料備份空間碟，以 IDE 硬碟效能高於磁帶機的宣傳方式，吸引需要快速備份的高階客戶；因為 IDE 硬碟取得成本並不會較磁帶機與磁帶來得高出許多，所以這也是一個可以嘗試的新服務。



圖四、hiStorage 未來服務架構示意圖

所以我們可以利用高階 SCSI 硬碟設備、中階 SCSI 硬碟設備、IDE 硬碟設備、以及磁帶機與磁帶，這四種儲存空間設備來透過 IPStor 的集中管控，進行不同服務等級的儲存空間租賃服務，當然再配合 IPStor 本身的功能可以自動將 I/O 讀取率較低的資料由高階效能的儲存設備搬移至較低階效能的儲存設備，如此一來也可以將各不同效能的儲存設備可以達到有效利用，如圖四。

至於磁碟機上異地備份/複製的部份，在技術方面倒是不見有何新的創新，反而看到的現象是原本廠商專注的高階備援市場轉戰中低階備援客戶市場，因此也見到的有很多異地備份/複製的

軟體直接於 Host 端安裝，然後備份至異地的儲存空間存放。而目前的簡易做法即是用 iSCSI 來達到透過 TCP/IP 網路進行存取異地端的儲存設備。而我們原本合作的 FalconStor 公司的 IPStor 軟體也推出像 FileSafe 與 DataSafe 等軟體，可以直接將 Host 端的資料或作業系統資料進行異地備份/複製。

還有另外我們即將推出的 DataSAFE 服務也是同樣的精神，在客戶端的主機上安裝一個 Agent 程式，然後該程式會定期將所定義的資料或系統資料備份至我們 IDC 機房內的伺服主機上，達到異地備份的功能。我想我們在這一部份的技術趨勢中，倒是已經跟上腳步或是可以說已經領先國內的許多廠商。

3. 中華電信 HiNet IDC 經營迄今，已擁有相當基礎與眾多客戶，這其中，IT 人員的服務態度與技術水準當是獲得客戶信賴的第一要件，他如備援服務新技術引進與週全的網管監控系統亦是當務之急，然擺在眼前，亦有一些瓶頸亟待解決- 即適合 IDC 長期經營的理想大型空間取得問題!

a. 空間條件本來就是 IDC 產品最基本且不可或缺內涵之一。

b. 空間不良、不足或分散，將直接影響 IDC 產品及服務之品質，甚至浪費人力、物力、財力，拉高成本，降低經營效率。

c. 當今在中華電信強調資產活化、人力活化的此時，若能解決前述，當可讓持續成長的 IDC 業務更加蓬勃，除固守並拉大 IDC 市場占有率之外，並加速帶動 CHT 甚或全國加值產業之快速發展。