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）

TOPS/Order 系統資訊安全機制實習出國報告書

行政院研考會/省(市)研考會編號欄

服務機關：中華電信北區分公司

出 國 人　職　稱：助理工程師

姓　名：郭　家　昌

出國地點：美國

出國期間：92 年 9 月 21 日至 92 年 10 月 4 日

報告日期：92 年 12 月

系統識別號:C09203307

公 務 出 國 報 告 提 要

頁數: 48　含附件: 否

報告名稱:

TOPS/ORDER系統資訊安全機制實習

主辦機關:

中華電信台灣北區電信分公司

聯絡人／電話:

盧婉屏／2344-3261

出國人員:

郭家昌　中華電信台灣北區電信分公司　行銷處　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 09 月 21 日 -民國 92 年 10 月 04 日

報告日期: 民國 92 年 12 月 23 日

分類號/目: H6／電信　H6／電信

關鍵詞: 資訊系統，資訊安全，異地備援

內容摘要: TOPS/Order是一個使用人的多，使用時間長的重要系統。也就是說系統運作自上線以來即是7天24小時全年無休。在面對全天候的服務需求下，能否妥善地管理保護及儲存資訊將是經營企業的重要課題。TOPS/Order的運作依靠企業網路來維繫運作，如何提供一安全的網路環境，強化系統主機的安全防護能，是決定系統能否正常提供服務的重要因素。所以，本次出國實習的主要目標在於： 1.體認國外在網際網路的安全機制的新理論和實際應用。 2.體認國外在主機系統上資通安全的新技術及實際應用。 3.體認國外對於資料備援和回復的新技術及工具，並適切地將國外的經驗引進TOPS系統。本報告依據實習經驗及國外搜集之資料，並依TOPS/Order現行維運模式，勾勒出系統的資料安全及系統安全模式，並據此模式建議未來改進方向。

本文電子檔已上傳至出國報告資訊網

摘要

TOPS/Order 是一個使用人的多，使用時間長的重要系統。也就是說系統運作自上線以來即是 7 天 24 小時全年無休。在面對全天候的服務需求下，能否妥善地管理保護及儲存資訊將是經營企業的重要課題。TOPS/Order 的運作依靠企業網路來維繫運作，如何提供一安全的網路環境，強化系統主機的安全防護能，是決定系統能否正常提供服務的重要因素。所以，本次出國實習的主要目標在於：

1. 體認國外在網際網路的安全機制的新理論和實際應用。
2. 體認國外在主機系統上資通安全的新技術及實際應用。
3. 體認國外對於資料備援和回復的新技術及工具，並適切地將國外的經驗引進 TOPS 系統。

本報告依據實習經驗及國外搜集之資料，並依 TOPS/Order 現行維運模式，勾勒出系統的資料安全及系統安全模式，並據此模式建議未來改進方向。

目錄

圖表目錄

1、前言

近年來政府大力推動自由化，電信事業在這方面的推動，可以說是成效最為顯著的。面對電信業務自由化的競爭，第一、二類各項電信業務的開放，如何提高服務品質、增進服務效率、以「卓越的技術，穩健中求發展，專業的服務，來滿足客戶的需求」，必須作出更有競爭力的決策，均需仰賴各式有效而即時的資訊。資訊對於組織或企業之重要性一如大腦對於人類的功能，在面對資訊爆炸的世代及一星期七天、一天二十四小時全天候的服務需求下，能否妥善地運用管理及儲存資訊將是經營企業的重要課題。因應這樣的需求，SAN 架構及異地備援的方案也應運而生。引進 SAN 能使用儲存設備的運用管理更具效率，異地備援能使資料安全的保障更完整，因此，這成為我們這次研習的主題之一。

隨著電腦運用的普及與網際網路的蓬勃發展，已帶給人類急速而巨大的衝擊，也改變了人類生活模式，資訊自動化以電子傳輸來取代企業處理人工步驟引入了各個階層和領域，各種形形色色的網路相關應用更是一日千里的發展，多媒體傳輸的媒介、行銷管道、商務軟體的平台等。新通信型態的需求有增無減，我們應從語音、資料、電視、計算、娛樂與電子商務，創造出新的服務與產品。對於客戶愈來愈主動，

期能獲得快速又有性能、高品質、低價格的電信服務，公眾電信服務的價值正逐漸轉型為提供創造性的網路多元服務，以涵蓋語音、資料、影像與多媒體等。但因網路的方便性與其透通性，造成了各類資訊及資料在安全及管理上的許多問題。因為，資料無價，這引起了有心人士想藉機破壞，得取重要資料。因此，網路及伺服系統安全與管理更加重要。首先我們必須解決傳統所面臨的複雜網路與功能整合之需求，並加進新的工具與管理作法已達安全及管理的方便性。為了強化 TOPS/Order 安全機制，我們實習了 TOPS/Orde 主機的相關安全應用模組，體驗如何利用模組來強化 TOPS/Order 系統安全。

2、實習目的及行程概要

2.1 實習目的

TOPS/Order 系統屬於中華電信的核心系統之一，與眾多資訊系統如（LEAMIS、TENAS、SSLOSS）界接，共同維持中華電信固網市話業務的營運，同時亦需保持系統的高彈性，應付未來業務多樣化的趨勢。TOPS 是一個使用人的多，使用時間長的重要系統。也就是說系統運作自上線以來即是 7 天 24 小時全年無休。在面對全天候的服務需求下，能否妥善地管理保護及儲存資訊將是經營企業的重要課題。TOPS/Order 的運作依靠企業網路來維繫運作，如何提供一安全的網路環境，強化系統主機的安全防護能，是決定系統能否正常提供服務的重要因素。

所以，本次出國實習的主要目標在於：

4. 體認國外在網際網路的安全機制的新理論和實際應用。
5. 體認國外在主機系統上資通安全的新技術及實際應用。
6. 體認國外對於資料備援和回復的新技術及工具，並適切地將國外的經驗引進 TOPS 系統。

2.2 行程概要

本次實習自 92 年 9 月 21 日起 至 10 月 4 日止，為期 14 天，實習地點為美國丹佛市、洛杉磯及舊金山等地，行程簡述如表一：

日期	行程及課程說明	地點
9/21	行程	台北->丹佛市
9/22~9/24	實習 SAN 應用，異地備援(DR)與儲存設備之安全	丹佛市
9/24	行程	丹佛市->洛杉磯
9/25~9/26	實習 Security solution on HP Unix OE	洛杉磯
9/27	行程	洛杉磯->舊金山
9/28~10/2	實習 Utility Data Center, Data Center Security Management Solution on System and Network	舊金山
10/3~10/4	行程	舊金山->台北

表一 實習行程表

3、實習過程

3.1 SAN 應用，異地備援(DR)與儲存設備之安全

3.1.1 SAN 架構及應用

傳統上，儲存體(Storsge)是直接界接於伺服器上，我們稱之為 DAS 架構，參考圖 3-1-1。若是將儲存體視作資源(Resource)，則各伺服器上的儲存體資源將是獨立的，無法共享。一但部份儲存體資源發生不足時，會很難立即調度其他伺服器上的空閒儲存體資源來支援。唯一的解決方法就是立即採購，無形上會造成投資效益的不彰。

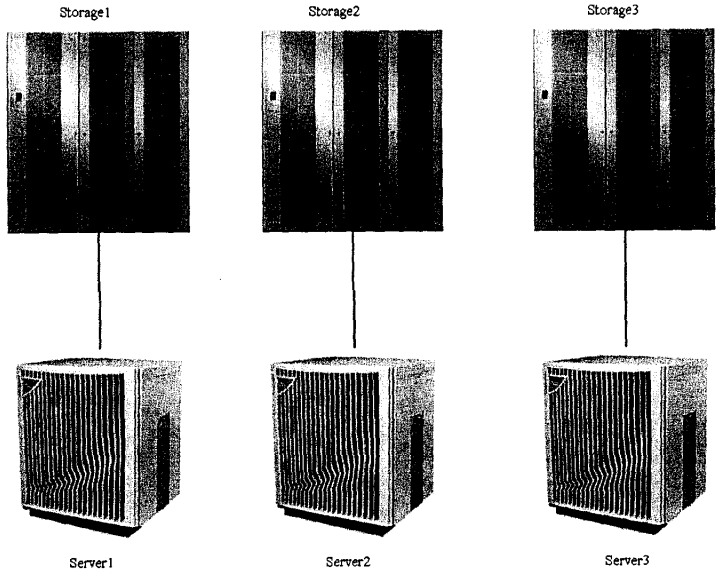

圖 3-1-1 DAS 架構

為了提高儲存體的使用效率及使用彈性，使用 SAN(Storage Area Networks)的架構，參考圖 3-1-2，可以將所有的儲存體資源在邏輯上視作一個共同使用的儲存體區(Storage Pool)，並透過專屬的高速網路與各伺服器介接，各伺服器及應用程式可視實際需求自儲存體區要求適當的儲存體來使用。

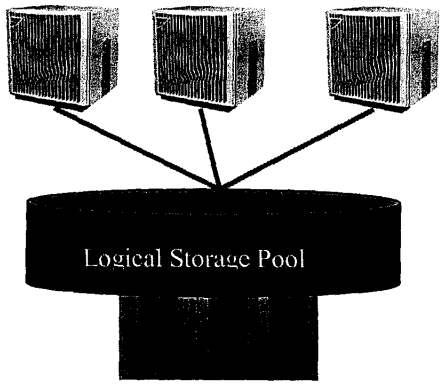

圖 3-1-2 SAN 邏輯架構

SAN 組成架構可大致分成三部份(如圖 3-1-3)：

伺服器(Servers)，除了自己的內建磁碟之外，需求大量儲存體時。通常，需有專屬的高速網路界面來接取 SAN。

SAN 交換器(SAN Switches)，是整個 SAN 的核心，為數台高速的網路交換設備所組成的網路，通常速度可達 1Gb/s 或 2Gb/s，媒界可以光

纖或乙太網路，為了提高網路的穩定，會使用全部網狀(Full Mesh)的連結方式來建置網路，用以連接 SAN 中的伺服器及儲存體。

儲存體區(Storage Pool)，可以是各廠牌所製造的儲存體，如 Hitachi 或 EMC 等等，只要能支援 SAN 的溝通協定即可。儲存體是保存資料的地方，因此，儲存體通常會使用 RAID 技術來作保護。SAN 網路可利用適的設定，通常稱作 zoning，使各伺服器看到所需的儲存體空間，而這些儲存體空間可以是散佈在不同的儲存體設備上，因此各應用系統可依不同的需求取得適當的儲存體空間。當儲存體空間不足時，也可以自現有的儲存體空間來調度或外購額外的儲存體設備。使得系統維運擴充的彈性較大，也較有效率。

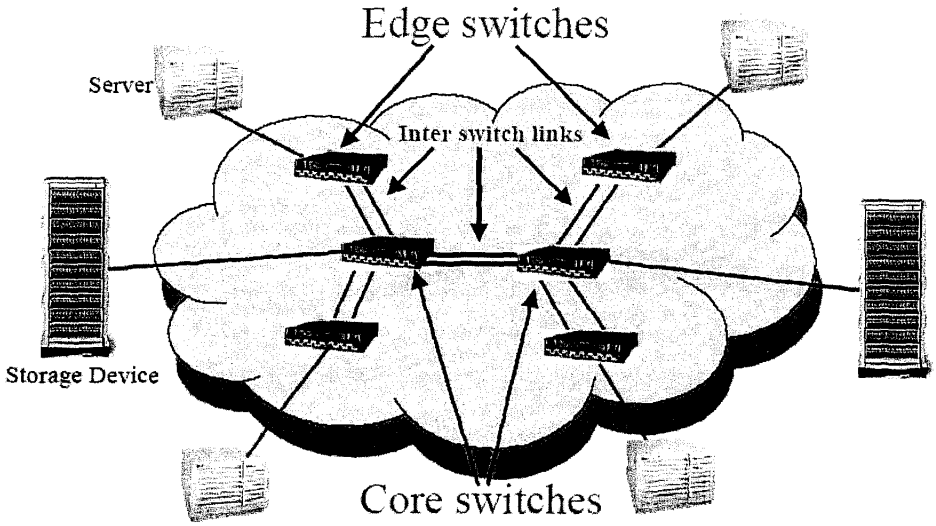

圖 3-1-3 SAN 實體架構

SAN 的特性及應用可歸結如下：

整合伺服器及儲存體，減少資源重覆投資所造成的浪費，減少系統管理上的成本。

因 SAN 是一專屬的網路，不會與正常企業網路共享頻寬，可減少網路的擁塞機會。

增加應用系統的效能，減少系統備份的次數及資料復製時對網路的衝擊。

能獨立地調度伺服器資源及儲存體資源。

為了提高系統的高可用度，使用全部網狀的網路連接方式，可以避免單一路由失效時，沒有替代路由可使用。在伺服器及儲存體方面，界接 SAN 網路亦同時使用雙路由連接設計。

SAN 架構提供了異地備援實施的可能性，這也是 SAN 的最佳應用。

3.1.2 異地備援的架構及實施

異地備援即是將企業所需要的資料，分開兩地存放並且即時運轉提供服務，以便當一地的設備發生運轉問題，另一地建置的設備可以立即接手取代繼續運轉。如此一來，至少所提供的資訊服務不會因地理位置所發生的天災人禍等不可抗拒事件而中斷。

企業實施異地備援的計畫首先對其應用系統進行評估，分清哪些是關鍵的系統，並對其運行環境進行評估，判斷發生災難的可能性有多少。若發生，關鍵系統中斷運行的時間有多長？中斷後對企業的影響有多大？有多少？哪些資料會丟失，有沒有解決的辦法和措施等。資料儲存系統的架構須考量異地備援架構，若考慮在另一地為資料進行備援，將生產系統上資料更新即時備份到遠端的備份系統上，這些動作並不透過伺服器本身，而是經由儲存設備之間的交互作用來完成，這會使備援的效率提高，且不會影響生產系統的正常運作，這技術稱之儲存體為主的即時備援技術(Disk-Based Backup Tech.)。一般而言，儲存設備廠商均支援這項技術，例如 Hitachi 的 TureCopy 及 HP 的 BusinessContinuity 等等。儲存體為主的即時遠端資料備份分同步方式和非同步方式兩種，以下利用 Hitachi 的 TureCopy 來作說明：

TrueCopy 同步方式工作原理如圖 3-1-4，其工作原理簡述如下：

- 一個寫入 I/O 從主機進入本地儲存設備。
- 本地儲存設備將此 I/O 寫至遠端儲存設備。
- 遠端儲存系統收到後，向本地儲存發出確認信號。
- 本地儲存受到確認信號後，向主機發出 I/O 操作完畢。

同步方式的優點在於其基本上可以保證資料的一致性、完整性和資料

不丟失，但由於發送和確認等環節有一些延遲，故可能對應用系統的性能有一些影響。隨著距離的加大，時間延遲也會越大，對性能的影響也越大，故同步方式一般用於同區域或小區域內的災難復原系統。TrueCopy 的同步方式可以支援開放系統(Unix，NT 等)和主機 OS/390 系統。

同步方式的優點是保証資料基本不丟失，其缺點為：

- 本地主機的性能要受一些影響
- 只能用於短距離
- 不能用於大區域的災難復原系統

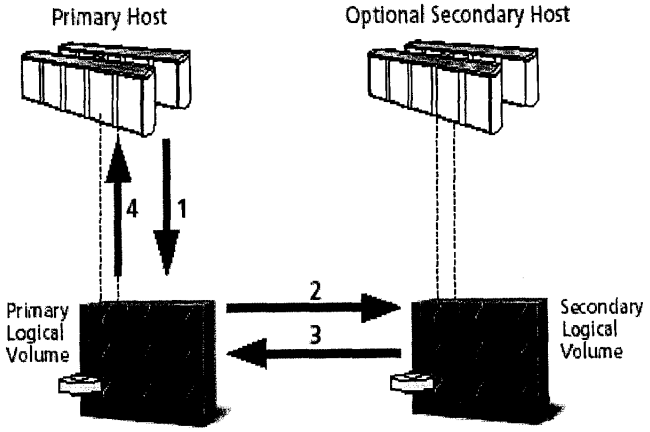

圖 3-1-4 TrueCopy 同步方式工作原理

TrueCopy 非同步方式(TCA)：TrucCopy 非同步方式是以硬體為基礎的非同步遠端資料備份技術。這一技術將應用的更新同資料的傳輸分

開，從而使得做遠距離的即時資料備份也不會對生產主機的性能造成影響。TrueCopy 非同步方式工作原理如圖 3-1-5，其工作原理簡述如下：

- 一個寫入 I/O 從主機進入本地儲存設備。
- 本地儲存受到確認信號後，向主機發出 I/O 操作完畢。
- 本地儲存設備將此 I/O 寫至遠端儲存設備。
- 遠端儲存系統收到後，向本地儲存發出確認信號。

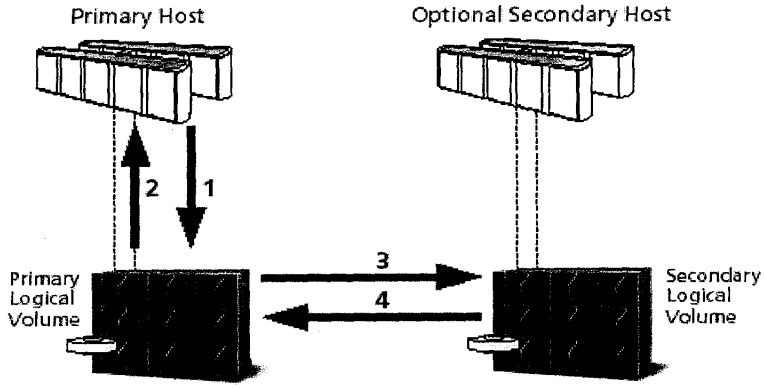

圖 3-1-5 TrueCopy 非同步方式工作原理

TCA 還有兩種重要的技術，時間戳記技術(TimeStamp) 及一致性群組 (Consistency Group)：

(1)時間戳記技術(TimeStamp)：如圖 3-1-6，TrucCopy 非同步方式對每個磁區的更新都會打上一個時間戳記。遠端的存儲系統會根據時間戳記進行排序，從而保證備份資料的完整。當災難發生時，TCA 會迅

速將備份資料凍結，不再接收發送來的資料，保證備份資料是災難發生前一個時刻一份完整的資料備份，從而保證應用能夠快速復原。TCA 的傳輸路徑可由多種選擇，其中一種是可以通過 IP 路徑進行傳輸，既節省了投資，又可以進行超遠距離（可達數千公里）的資料備份。TCA 有一套複雜的演算法來保證備份資料的順序。本地與遠端的存儲系統之間還有一條 Heart Beat，供 TCA 來偵測本地的系統是否正常工作，一旦發現異常則立即凍結備份資料，保證資料不被破壞。

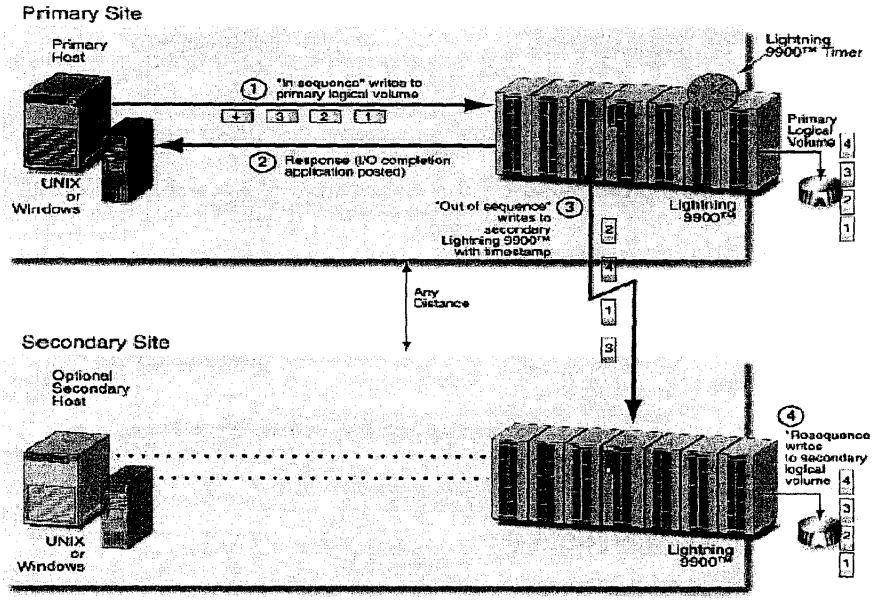

圖 3-1-6 時間戳記技術

(2)一致性群組（Consistency Group）：如圖 3-1-7，這是由一系列群組成，可以把它看一個大群組，每個對這個大群組的更新都會安排一個順序號。TCA 會對接收到的資料進行排序，保證備份資料的完整

性。例如：一個資料庫建立在多個群組(如 Oracle Log and Data LUN)，可以將這些群組定義成一個一致性群組(C/C Group 0)。則該資料庫群組的更新會有順序的出現在遠端備份系統上，成為一份完整的備份資料。

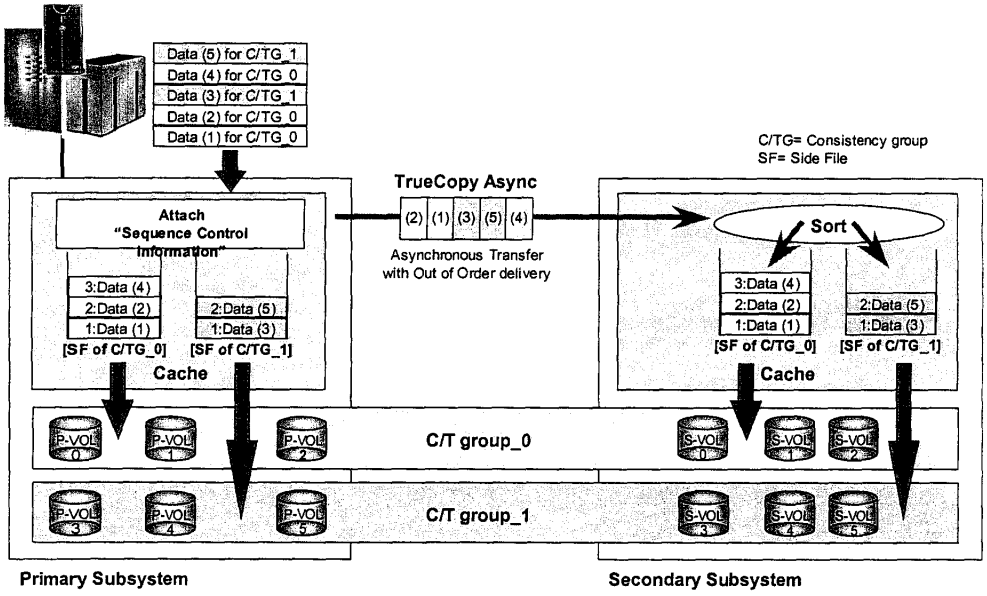

圖 3-1-7 一致性群組

TCA 的優點簡述如下：

- 備份的資料是完整的，可立即用於復原 (Restart)
- 可支援遠距離的資料備份
- 可支援多條線鏈路的傳輸
- 對本地主機幾乎沒什麼影響

TCA 的缺點在於備份資料可能會滯後生產資料，滯後時間的長短取決於線路的帶寬和應用產生的資料量。

3.3.3 實習結論

異地備份及備援所需考慮的要素，除了高可用性(High Availability)的備援硬體設備以外，合適的備援方案選擇、各地之間夠用的網路通訊及資料複製通道建置、應用軟體及服務可容許的停機時間、有效的備援複製、複製時間點與備援啟動時間差等等，都需要良好的規劃。還有往往最重要也最容易被忽略的，即是一個方便、自動化、及有效的整體管理工具，否則事後的維護工作與管理投資成本，將隨資料容量的快速成長而形成另一個巨大且沉重的包伏。

異地備援規劃所涵蓋的範圍，除了基本的儲存設備以外，還有網路環境、應用軟體環境的備援。如何有效的管理及運用，便成為另一重要且另人頭痛的課題。因此、較具有整體性考量及遠見的資訊設備服務供應商，已融合儲存設備管理 Storage Area Management、網路環境管理 Network Area Management、資料運用管理 Data Management 及應用軟體管理 Application Management，將所有原先繁複且分開的多種管理控制介面整合成單一控管介面，提出 Federated Storage Area Management 意即『協同式儲存區域管理』方案。應用這樣的方案，可方便快速的將原先分開卻又息息相關的多種管理介面整合在一起，讓資訊管理人員有效的從許多分散在各環境的狀態訊息內，連結分析出有用的控管訊息，在第一時間內找出問題點的源頭，甚至可進

一步的提供預測資訊，讓管理人員可預測及事先分配服務環境的需求，大幅度的降低整體管理成本，並將資訊設備的投資運用發揮到最佳，使得投資成本與服務水準快速並容易地達成良好平衡，發揮出最完善的投資效益比。

3.2 Security solution on HP Unix OE

開放式的分散式資訊系統的組成元件包括了儲存體、伺服器、網路、使用者終端(Clients)。架構一安全的資訊系統，須考量每一元件的安全設計及建置，及彼此間相互運作的安全性。例如須架設防火牆(Firewall)，來保障網路進出的安全。本節實習的重點在於提高不可停機的資料庫伺服器的安全性設計，並作一介紹。

3.2.1 以流程觀點看系統安全管理

建置安全的系統環境是一件持續進行的過程。由於環境的變化，新的安全威脅與日俱增，維持系統保持一定的安全水準是一件動態的、具挑戰的工作。圖 3-2-1 顯示出動態維持系統安全流程中的每一階段：

(a)防護階段(Prevention)：

此階段著重於提高作業系統本身和應用程式的安全控管能力。另

外也提供了額外輔助工具來作安全防護工作，例如資料加密、資料認証、防火牆設置、制定及執行安全防護政策等。根據統計，2/3 的安全漏洞皆由那些在某些時段的使用者登入系統時所造成，因此，定義安全政策可有效防範及追蹤。

(b)偵測階段(Detection)：

此階段著重於入侵偵測，包含偵測駭客攻擊、病毒攻擊等，皆屬於這個範圍。一般而言，可於系統中設置入侵偵測系統、病毒掃描系統等工具來持續監測系統活動的狀況、分析收集到的記錄來發現問題並依設定程序來回報問題、發出警訊。一般常見攻擊方式如阻斷服務(Denial of Service)、植入木馬程式(Trojan Horse)、各式病毒(Virus)及蠕蟲(Worm)等。

(c)調查階段(Investigation)和解決階段(Diagnosis & Resolution)

當於偵測階段發現異常時便會觸發調查和解決階段。此時會根據收集到的資訊作一問題的描述，並依事先設定好的解決方法來修正問題，並留下記錄供日後追蹤。而這些過程及經驗會成為下一個防護階段的安全防護基準線(Baseline)。通常，這兩個階段合稱安全事件回應(Incident Response)。

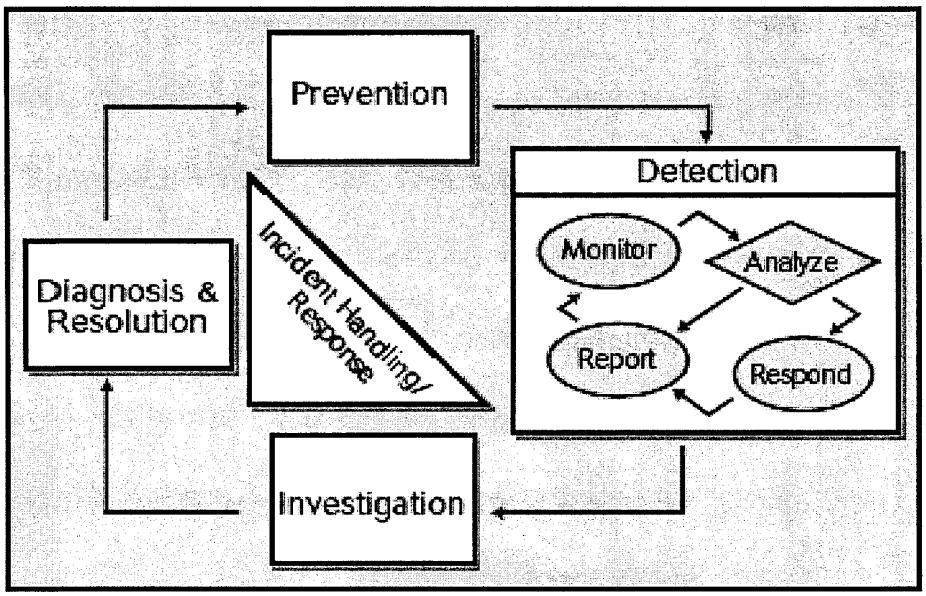

圖 3-2-1 系統安全流程

3.2.2 HP-UX 上的安全防護模組

(a)入侵偵測系統(IDS/9000)

為了偵測某些可疑的行為是否是惡意的攻擊，IDS 所監測的電腦網路系統必須提供某些原始資料(raw data)給 IDS。資料來源蒐集模組就是把這些原始資料當作輸入，並且提供關於 IDS 所監控的電腦網路的資訊。這些關於電腦網路系統的安全資料包含了作業系統中的稽核紀錄、網路封包的標頭檔、以及所提供服務型態等。

根據不同的資料蒐集的型態，可將它分為「網路型入侵偵測系統」(Network-based IDS)與「主機式入侵偵測系統」(Host-based IDS)

以作區分。

(a)網路型入侵偵測系統

網路型入侵偵測系統以原始網路封包作為資料來源，通常將網路卡設定於混亂模式下來攔截所有過往的網路通訊，以進行偵測及分析。主要的檢測方式，最簡單的即是檢測網路封包內的標頭(header)以及其使用的指令及語法，從中判定是否包含駭客行為，所以被入侵者能在偵測到有攻擊行為的同時，就進行反制動作或提早預警。

(b)主機式入侵偵測系統

主機式入侵偵測系統發展始於 80 年代早期，通常只觀察、稽核系統日誌檔是否有惡意的行為，用以防止類似事件再發生。在 Windows NT/2000 的環境下，通常可以藉由監測系統，事件及安全日誌檢視器中所記載的內容來加以過濾、比對，從中發現出可疑的攻擊行為；在 UNIX 環境下，則監測系統日誌。當有事件發生時，主機式入侵偵測系統即做入侵行為的比對，若有符合，則由回應模組通知系統管理員，以對攻擊行為進行適當的反應。

HP 所提出的 IDS/9000 即是針對主機式入侵偵測所提出的解決方案，所包括的偵測範圍可分為四類：

A、系統核心部份：

- 未經授權的存取
- 病毒偵測
- 權限的防制
- 後門程式的防護
- root 權限的保護

B、HP-UX 作業系統：

- 暫存區溢滿攻擊
- 以嘗試錯誤方式猜測密碼

C、使用者安全防護：

- 失敗的登入次數
- 使用者的環境設定檔是否被未正常地修改
- 非法取得執行殼(shell)

D、檔案保護：

- 唯讀檔案是否被修改
- 是否有權限進行檔案的增加及刪除

依據以上的偵測範圍，IDS/9000 會內建相對應的防護範本(Template)，例如當某個帳號失敗的登入次數超過臨界值時，Repeated failed logins 即被觸發，並執行已事先設定好的動作。

另外，IDS/9000 採用即時式的偵測及告警。告警的內容會嘗試解析可能攻擊者的使用者名稱或 IP 位址，並依內建的攻擊模式範本來判斷攻擊的種類，若超過定。如圖 3-2-2。

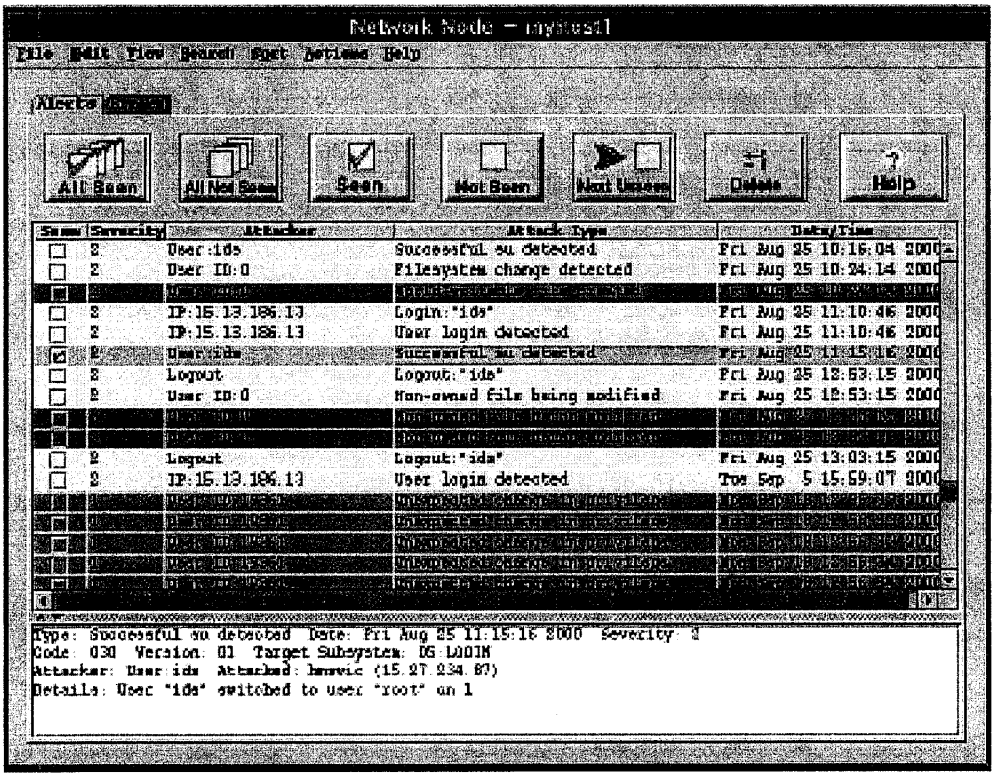

圖 3-2-2 IDS/9000 範本例

IDS/9000 的管理採用集中式的畫面管理模式。

使用主機式入侵系統會有下列的優點：

(a)確定駭客是否成功入侵：因為主機式入侵偵測系統所根據的檢測來源是系統的稽核紀錄檔，而在事件(event)完成後才會將該項紀錄記載至事件稽核紀錄中，因此攻擊是否成功可以從中判斷得知。

(b) 監測特定主機系統的活動：主機式入侵偵測系統是安裝在各系統主機上的監控程式，主要便是針對各系統主機進行監測。

(c) 較適合有加密及網路交換器(switch)的環境：由於網路環境的限制，因此針對有加密過的封包或有交換器的網路環境，網路型入侵偵測系統無法對封包內容進行解讀或蒐集的動作，而主機式入侵偵測系統則無此項限制。

(d) 不需另外增加硬體設備：主機式入侵偵測系統僅需在所需要監測的特定主機上安裝監測系統即可達成，因此不需要增加額外的硬體設備。

(b)IPSec/9000

就現況而言，所有進出系統的資料皆由 IP 網路來傳送，如果能在資料送出網路前將資料底部的 IP 層保護起來，則網路基本上是安全的。根據這樣的觀念，IPSec 被發展為保護 IP 層，如此一來，應用系統間的資料傳送是安全且透通的。

IPSec 使用加解密(Cryptography)的方式來提供私密性及認証服務。加解密技術可分為對稱式(Sytmetric)及非對稱式(Asymmetric)兩種：

(a)對稱式加解密技術

對稱式使用單一金鑰(Key)來執行加解密，傳送端(Sender)及接收端(Receiver)皆須擁有同一金鑰，因此，這金鑰是被兩端共享的，稱之為共享金鑰(Shared Key)，如圖 3-2-3。

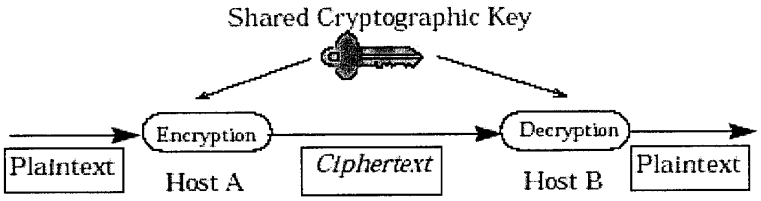

圖 3-2-3 對稱式加解密

對稱式加解密技術中採用共享金鑰雜湊函數來進行資料的認証工作(Authentication)。這種共享金鑰雜湊函數的特性是單向的，一個輸入值一定對應一個輸出值，它是不可能用同一輸出值去反求另一個輸入值。整個運作流程如圖 3-2-4。傳送端在傳送資料時利用共享金鑰得出認証值，連同欲傳送的資料送至接收端。這時接收端利用同一共享金鑰雜湊接收到的資料而得到另一認証值，並與傳送端送來的認証值作一比較。當兩者相同時，系統認為資料傳送過程中並未被修改，是安全的。

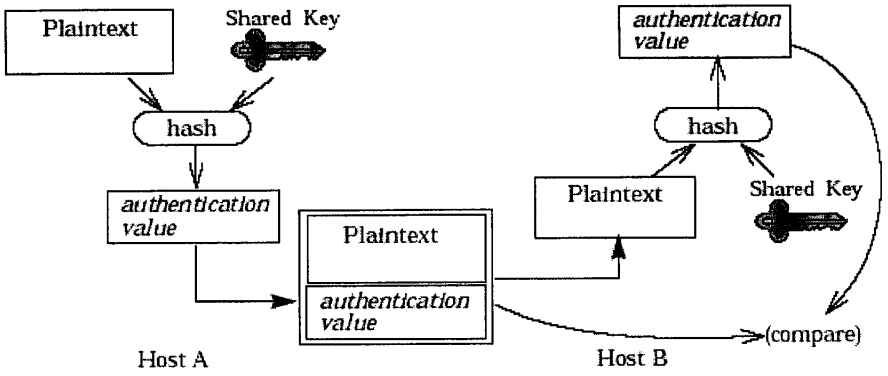

圖 3-2-4 對稱式金鑰認証

(b) 非對稱式加解密技術

非對稱式則使用一對相關聯但各自不同的金鑰，在傳送端稱之為公開金鑰，資料傳送前先用公開金鑰加密。在接收端稱之私有金鑰，接收端在收到資料後會用私有金鑰解密，如圖 3-2-5。因私有金鑰僅接收端知道，可保証資料傳送時的安全。

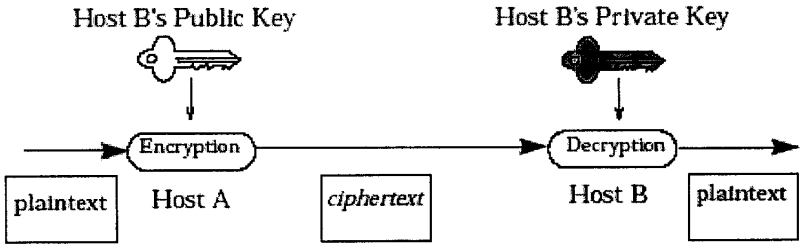

圖 3-2-5 非對稱式加解密

HP IPSec/9000 採用對稱式加解密來建構 IPSec 環境，整體架構可用圖 3-2-6 來表示。基本上，當每個主機安裝 IPSec/9000 後，彼此之

間的通訊通道會是安全的。

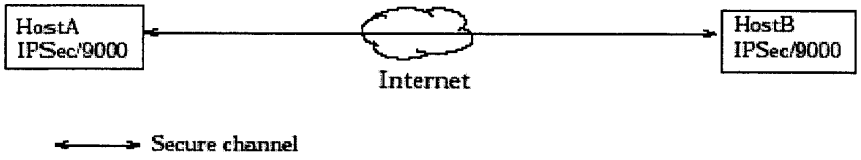

圖 3-2-6 IPSec/9000 整體架構

(C)SSH

HP SSH 可替代某些指令，如 rlogin、rsh、rcp 等，同時，它提供了多種加密方法，使用雜湊函數來驗証資料的正確性，使用公開金鑰及私有金鑰來提供一個安全及快速的資料加解密管道。SSH 的架構及實作如圖 3-2-7。

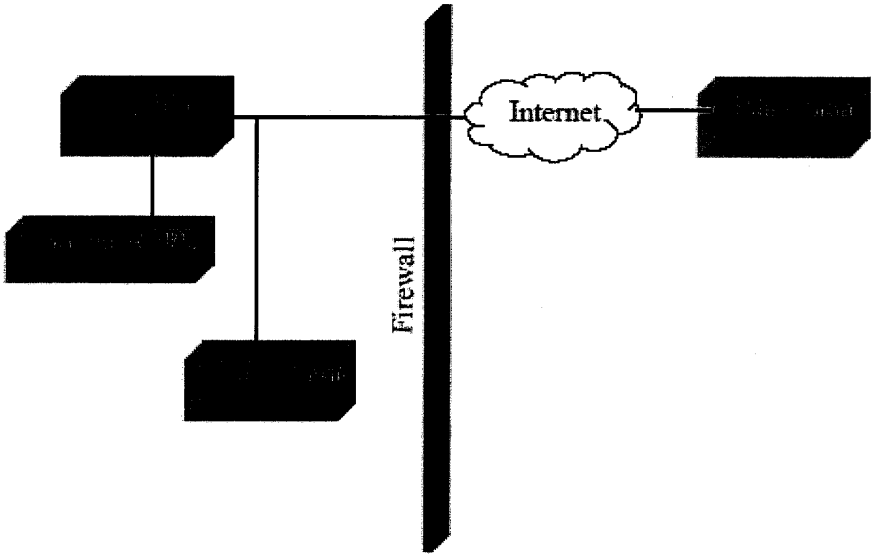

圖 3-2-7 SSH 的架構

SSH 的特性如下：

- 提供穿隧(Tunneling)能力，對於 TCP 服務如 telnet 等能被包裝於 SSH 隧道內，所有傳送的資料皆被加密。
- 支援 SSH-1 及 SSH-2 兩種規格，但建議使用 SSH-2 可減少植入攻擊的機會。
- SSH 的安裝及使用是很簡單的，搭配 TCPWrapper 可以進一步減少伺服器傾聽要求的流量。
- SSH 支援的認証模式包括密碼驗証、公開金鑰、Kerberos 及系統本身提供的方式。就本地使用者而言，使用密碼驗証來作認証，對遠地使用者而言，可使用公開金鑰機制來作認証。因 SSH 是採用加密方式來處理資料，所以也不怕密碼會被攔阻及被攻擊。對於公開金鑰的使用而言，SSH 在各個伺服器上會有一把公開金鑰，私有金鑰則保留在客戶端上。就安全上而言，這樣的安全機制會比僅有密碼保護來得安全。

(4)Kerberos 機制

Kerberos 是一種協定，它的功能在提供使用者認証時，使用者的密碼是不經由明碼傳送，因此，它是安全的。通常，它是集中於一個稱之 KDC 的 Kerberos 伺服器來執行使用者認証的工作。在 HP-UX 上內

建的網路服務，包括 ftp、rcp、rlogin、telnet 和 rmesh 等均支援此種協定。另外，HP-UX 亦提供相關 API、GSS-API 等供相關應用系統使用。

圖 3-2-8 說明 Kerberos 協定的運作流程。KDC 主要含有兩個元件，一為認証伺服器(Authentication Server)，一為權杖派發伺服器(Ticket Granting Server)。應用程式終端及應用程式伺服器則是在 Kerberos 運作下的應用系統。KDC 產生權杖並用 KDC 金鑰加密後給使用者，使用者利用此權杖再取得服務權杖，並獲認証核可，取得應用系統的服務。

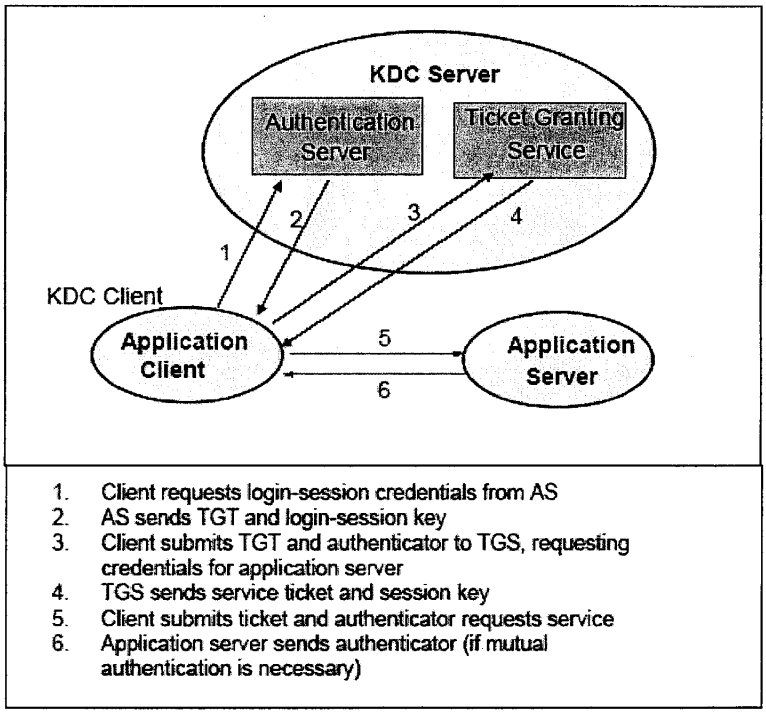

圖 3-2-8 Kerberos 協定

Kerberos 伺服器是 HP-UX 所提供的模組，有下列的特性：

- 密碼不會直接在網路上傳送，僅傳送加密後的權杖。
- 終端使用者及應用系統可彼此作認証，因此，終端使用者及應用系統均可確認通訊的對像是安全合法的。
- 提供單一簽入的功能(Single Sign-on)。當使用者用密碼登入時，伺服器自動將密碼轉換成認証權杖及服務權杖。當取得服務權杖後，使用者便可使用應用系統提供的服務。
- 密碼同步化，改變密碼時，所有的環境均同時變更，減少管理的複雜度。
- KDC 提供資料複製的功能，能提供備援，提高 Kerberos 伺服器的可用度。

3.3.3 實習結論

維持系統安全是一項持續的過程，有效且安全的系統通訊環境是保障企業成長及利益的根本。若沒有適當的安全防護，則有可能：

- 資料在傳遞的過程中被修改。
- 資料的來源可能是假的。
- 大量的故意攻擊或入侵。

在分散式的系統環境中，網路是 IT 基礎設施的一環，也因此使系統

暴露在易受攻擊的環境中。建立強壯且有效益的安全機制來保護系統的正常運作。而這安全機制會包括認証、使用權的指定和資料的一致性等。

3.3 Utility Data Center, Data Center Security Management Solution on System and Network

關於 IT 基礎架構(Infrastructure)的演進，是朝向三個目標努力：

- 提昇基礎架構的靈活性(Agility)，以快速反應企業的多變需求。
- 建構企業各部門間協同運作(Collaboration)的環境。
- 增加企業的投資報酬率(ROI)。

為達成這些目標，IT 技術的需求及整合方向為：

- 對應用系統而言，IT 基礎架構將是虛擬化，IT 將集中以服務提供(service-centric)為導向。
- 各 IT 資源會整合成資源區(Resource Pool)，如磁碟儲存體區、記憶體區等，各應用系統會依實際需求自資源區(Resource Pool)取得所需的資源。
- 強化系統的管理及維運自動化。

圖 3-3-1 說明了 IT 基礎架構的演進過程及未來趨勢。

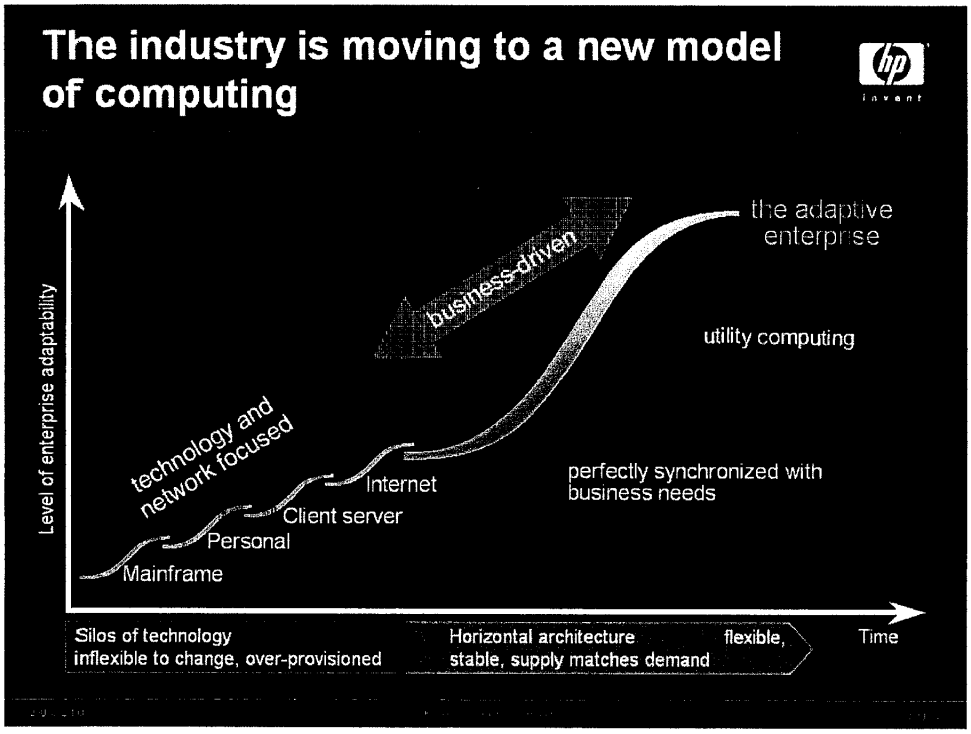

圖 3-3-1 IT 基礎架構的演進過程

3.3.1 Utility Data Center 概念

傳統上，IT 系統本身應包含伺服器、儲存體、網路、應用軟體等。若以服務提供導向(Service-Centric)模型看待系統，系統本身所有的伺服器、儲存體、網路、應用軟體是虛擬化、分開的，但是會專注於系統能提供的功能及附加價值，它能動態地提供服務所需求的 IT 資源，如圖 3-3-2，以服務需求者的角色來看，所有的 IT 資源階是虛擬的，尤其一但應用軟體也是虛擬化，格網運算(Grid Computing)的時代將是更有機會實現。依據這種模型，將會有 IT 供應者將建置

大型、集中化的 Data Centers，提供使用者依據本身需求向 IT 供應者取得適當的 IT 資源以得到資訊及通訊服務。當使用者不再需要 IT 資源時，IT 供應者可回收其資源並重新配置。藉由這種資源的配置與回收，可提高 IT 資源的使用率。

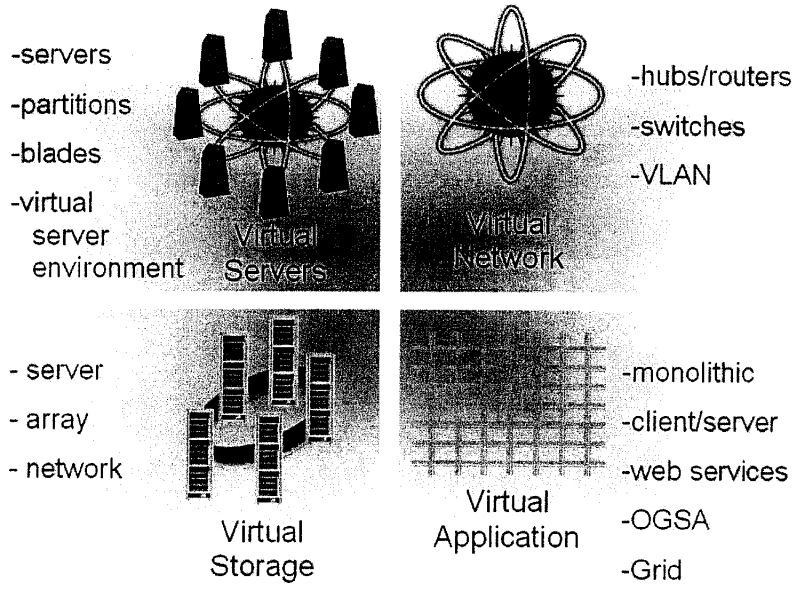

圖 3-3-2 IT 資源虛擬化

以一個例子來說明。當企業需求並計劃發展一個客戶關懷系統時。系統分析人員分析需求，制定服務水準(service level)，如系統可靠度、回應時間、系統容量等。依據這些指標，可計算所需的 IT 資源，制定服務範本(Service Template)。這些服務範本的 IT 資源包括了

應用程式、資料庫管理系統、儲存體和網路。使用 Utility Data Center 管理工具，可以自動地配置及設定 IT 資源，並安裝應用程式及提供服務。日後當服務需求增加時，若需更多的 CPU 時間，記憶體容量、儲存體空間或網路頻寬時，Utility Data Center 管理工具會自資源區中取得適當的資源配置給提供服務的應用系統。除此之外，應用系統的升級及發佈(Deployment)也會變的更有彈性，在過程中也不會影響系統正常運作。當與傳統的應用系統發佈相比較，會有下列的不同點：

- 在 Utility Data Center 中 IT 資源是被集中管理、分配使用的。
- 異質資源在面對不同的服務需求時是可共同被分配，並隨時變更服務等級。
- 在面對不同的服務需求時，IT 人員能有效率地利用現有資源來建置及維護應用系統。

3.3.2 Utility Data Center 架構

用功能面來看 Utility Data Center 架構，可參考圖 3-3-3，在硬體層的上端，主要集中於建置一個 utility 控制器，負責各項服務所需資源的配置，內含 Utility Data Center 管理工具，因此，資源的自動配置是 utility 控制器的基本功能，同時也包含了入侵偵測、使用

者認証等安全控管機制。作業系統的支援包括了 UNIX、Windows 等等，以符合異質資源整合的需求，同時也搭配了 HP OpenView 等系統/網路監管工具，作為 utility 控制器的一部份。

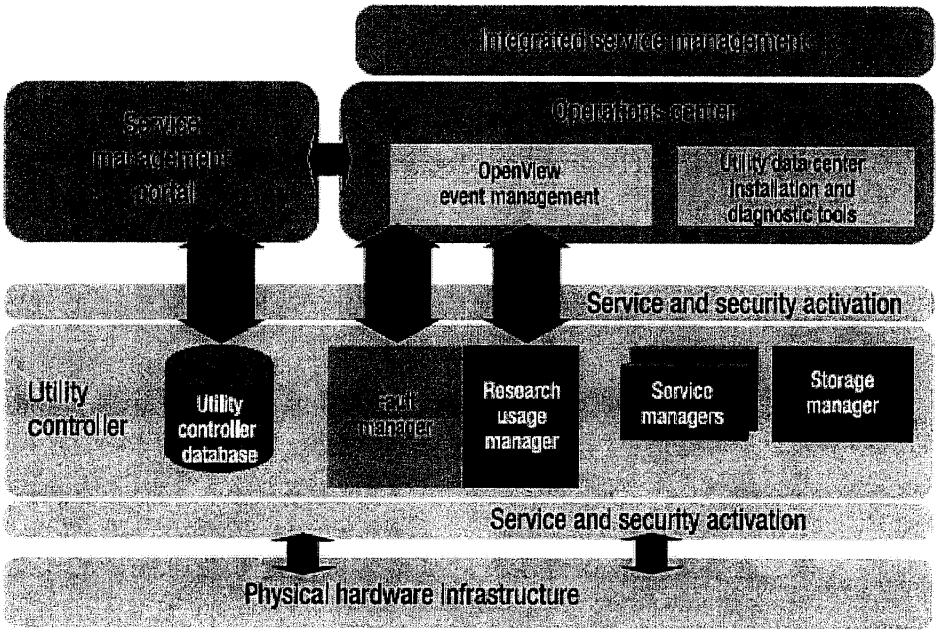

圖 3-3-3 Utility Data Center 的功能性架構

，Utility Data Center 的實際運作可以區分成四個層，每層之間的連結透過高速乙太網路設備，詳如圖 3-3-4(A)。說明如下：

(a) 資料庫層(Database Tier)：這層是整個 Utility Data Center 的運作的基礎。它提供了大量利用 RAID 技術和快照技術(Snapshot)的儲存體空間、磁帶櫃、儲存體網路(SAN)設備及高速乙太網路交換設備等。如果需要的話，關連式資料庫也可存在這層。

(b) 應用層(Application Tier)：這層含有伺服器、儲存體，乙太網路交換設備等觀念。透過高速乙太網路交換設備連接資料庫層，可以將部份的資料處理在應用層處理。另外，部份核心的應用系統也架設在應用層，如 ERP 系統。應用層中的儲存體，最主要的用途在作資料的快取和暫存。

(c) 網頁層(Web Tier)：這層含有伺服器、儲存體，乙太網路交換設備等觀念。在網頁層中的伺服器及儲存體提供使用者利用網頁瀏覽所需的資料，並透過高速乙太網路交換設備來進出存取層。

(d) 存取層(Access Tier)：這層含有伺服器、儲存體，乙太網路設備等觀念。存取層提供了所需要的安全性考量。例如使用者的認証、存取權的控管、網路之間 VPN 的建置及入侵偵測、病毒防治等更強化的安全控管機制等等。

配合 Utility Data Center 所包含四層間的實際運作設計，在硬體實際配置如圖 3-3-4(B)，因每層階有伺服器、儲存體、乙太網路設備等架構觀念，在實體上 Utility Data Center 將這些架構需求虛擬成資源區，如伺服器區、儲存體區、乙太網路交換設備區等等，虛擬化的一項好處是設備的架設跳線是一次滿足。事實上，這四層中的設備皆是由 Utility Data Center 中的資源區所取得的。取得的方式是利用 Utility 控制器，經由適當的設定分配給這四層。為了提高資源區

的可用度，故障切換(Failover)及資料復製(Data Replication)會應用至資源區中作保護。為了提高效率，也可引進負載平衡技術，設置成一個資源區--負載平衡區(Load Balancer Pool)。

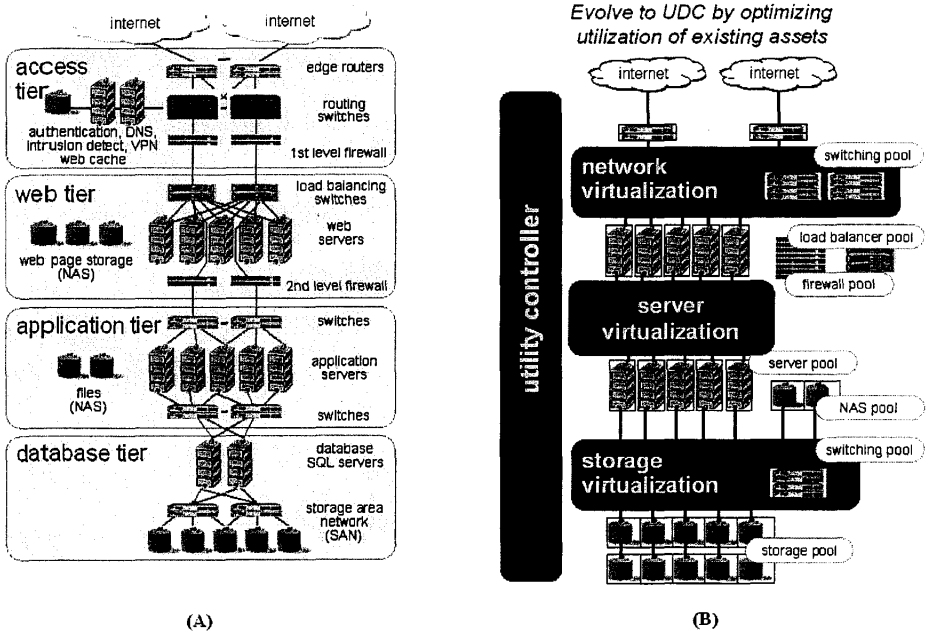

圖 3-3-4 Utility Data Center 運作架構及實體組成

3.3.3 Utility Data Center 的安全性設計

使用防火牆來保護 Utility Data Center 所提供的服務時，可能會引發使用者在使用部份經授權的服務時，也能得到未經授權服務的存取機會，這是一項潛在的安全性問題。為了解決這項問題，對 Utility

Data Center 所提供的每一項服務均有自己的自有網路區(Private Network Zone)，彼此互相獨立。使用者被授權使用其中一項服務時，它的授權會同時包括從防火牆外部存取權及該服務所擁有的自有網路區中的存取權，這包含了該服務所有的伺服器硬體及其他資源如儲存體、網路等。

自有網路區是建立在 Utility Data Center 的資源虛擬化及管理上。Utility Data Center 使用 FML 來表示資源及資源之間彼此關聯架設(Wiring)的工作。所有的設定格式是使用標準的 XML 語法。Utility Data Center 使用農場(Farm)來表示某項服務所需的資源及資源之間彼此關聯架設，也就是說，農場所代表的就是某項資源的系統環境。圖 3-3-5 表示了一個 Utility Data Center 農場的例子。這個例子包括了一個防火牆(FW)，在防火牆後端設置了數量可調變的 web 伺服器群。而這個農場所有的系統環境設定如圖 3-3-6。從其中可得知最少所需執行 web 服務的機器是 4 台，最多則是 20 台，初始值是 10 台。還有另外扮演兩種角色的機器，一是資料庫伺服主機，一是檔案伺服器。

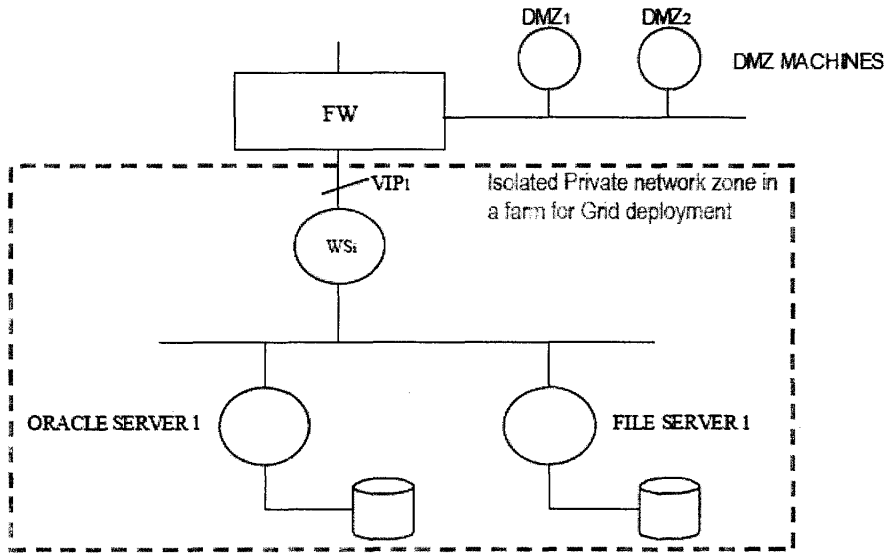

圖 3-3-5 Utility Data Center 範例

```
<farm name="My-3-Tier-Farm", fmlversion="1.1">
<subnet id="subnet1" name="outer" ip="external" vlan="outer-vlan">
</subnet>
<subnet id="subnet2" name="inner" ip="internal" vlan="vlan1">
</subnet>
<subnet id="subnet3" name="data" ip="internal" vlan="vlan1">
</subnet>

<lb id="lb1" name="lb1" type="lb">
        <interface name="eth0" subnet="subnet1" />
        <interface name="eth1" subnet="subnet2" />
        <policy> round-robin </policy>
        <vip name="vip0" subnet="outer">
                <bind id="bind12" name="tier1:eth0"
      virtual-port="8081"
                real-port="8080" />
        </vip>
</lb>

<tier id="tier1" name="WebTier">
        <interface name="eth0" subnet="inner" />
        <interface name="eth1" subnet="data" />
        <role> role1 </role>
        <min-servers> 4 </min-servers>
        <max-servers> 20 </max-servers>
        <init-servers> 10 </init-servers>
</tier>

<tier id="tier2" name="AppTier">
        <interface name="eth0" subnet="subnet2" />
        <interface name="eth1" subnet="subnet3" />

        <min-servers> 2 </min-servers>
        <max-servers> 5 </max-servers>
        <init-servers> 3 </init-servers>
        <role> role3 </role3>
</tier>

<tier id="tier3" name="DBTier">
        <interface name="eth0" subnet="subnet2" />
        <interface name="eth1" subnet="subnet3" />
        <min-servers> 1 </min-servers>
        <max-servers> 1 </max-servers>
        <init-servers> 2 </init-servers>
        <role> role2 </role>
</tier>

</farm>
```

圖 3-3-6 Utility Data Center 農場環境設定

3.3.4 實習結論

Utility Data Center 所提供的技術將資料中心虛擬化，有以下特點：

(a) 資料中心的所有資源是可被虛擬化，利用關聯架設的技術，其資源是可以很彈性地被重復配置及使用。

(b) 新的系統及應用可以在很短的時間內設定啟用。

(c) 伺服器、儲存體、網路的使用率可以接近 100%。

(d) 資源虛擬化及最佳化，可以滿足系統的服務水準需求。

(e) 管理及操作的複雜度減低，相對減低管理及操作的負擔。同時也減少犯錯的機會。

4、感想與建議

4.1 感想

工作職能(Competency)獲得的途徑很多，從書籍、從課堂、從網路...等等，尤其是資訊相關的知識來源，更是隨處都是。我們有機會出國進修，是另一項獲得工作職能的途徑。這一次出國實習，能有機會在國外 IT 領導廠商提供下，從課堂上了解 IT 科技的發展，從實驗室了解他們對追求 IT 科技創新的執著與嚴謹。難怪有人說科技進步的美國，是因為不斷持續的創新，使美國變成超級強國，全球競爭力持續第一。

網路帶來了便利，提高了 IT 在企業發展時成為不可缺少的利器。但是也帶來安全的威脅。企業資訊是企業的命脈，保障資訊安全，便成為企業資訊系統發展及維運的一項重課題。安全防護所針對的是對已知的安全威脅，但是新的攻擊手法會一直推陳出新，因此，建立一套良好的安全管理及更新機制，會幫助我們在系統維運時事半功倍，也能使我們能對於新的安全威脅能採取主動發覺、縮短反應時間。

資訊科技是 21 世紀企業賡續發展的重要基石，如何將中華電信 IT 人才集中、力量集中、分享知識是非常重要的，因為：知識建構優勢，惟有我們創造不可模仿的競爭優勢，我們才有能力創造更光明的電信

未來。

4.2 建議

影響安全的因素可歸結為：

- 未經授權者（駭客）侵入電腦系統，竊取或更改資料甚至更動原系統設定
- 合法使用電腦人員有意或無心，造成資料的毀損、竊取或系統破壞。
- 資料在傳輸中途被截取、竊窺或變更
- 電腦感染與傳遞病毒

依照這樣的結論，TOPS/Order 將會依下列的方向來強化安全方護：

- 網路使用帳號，應由專人統籌管理設定。
- 網路密碼必須定期更換，且不得洩露他人，並於人員異動及職務變更時，註銷帳號或調整其使用權限
- 下載資料或程式必須先確認無病毒感染後，再行下載。
- 連線設備應使用防毒及合法版權軟體，嚴禁更動原系統設定。
- 為防範電腦遭到非法侵入，應該要設置伺服器防火牆。
- 設定警示系統，如 HP OpenView，隨時提醒系統管理或使用人員處理突發狀況。
- 不定時更新系統修補程式。

同時，為因應突發事件，確保 TOPS/Order 系統在遭受破壞，病毒、惡意程式等攻擊造成系統停擺時，能迅速通報及緊急應變處置，並在最短時間內回復，以維持客戶最大權益及公司最大利益，於是依據事前防護、事中預警應變、事後復原鑑識等原則，TOPS/Order 需擬定緊急應變計劃，內容可包括病毒入侵的危機處理程序、駭客入侵的危機處理程序、惡意程式攻擊事件的危機處理程序、系統回復程序等。

TOPS/Order 現已引進 SAN 架構來提供主機與儲存體之間的運用效率，同時也為異地備援的建設打下基礎。在下一個階段可朝向建置異地備援的規劃及建設為主。由於 TOPS/Order 資料庫分成北中南三區，因此，利用現有的設備，達成設備互為利用、互為備援是可以考慮的方向。由於 SAN 也是網路，隨著 SAN 的應用愈來愈多，管理也成了一項重要課題，如何建立網路備援，如何執行日常監控等等，畢竟 SAN 是系統核心中的血管，必須時時保持正常。TOPS/Order 已引進了 OpenView 來作為系統日常監控維護的工具，未來可引進或自行開發適切的模組，將 SAN 的管理納入 OpenView 的維運操作中，這也是可努力的方向。

Utility Data Center 是網格運算的基礎，虛擬化的觀念也可以在日後建置資料中心時引為參考。這對於資源利用率的提昇、系統管理的簡化，都是很大的進程。面對未來愈來愈競爭的環境，虛擬化的彈性

必能快速反應企業的新功能需求，進而創造公司的最大利益。

5、書籍與文獻

- D. Naveh, "The Hitachi SAN Solutin"
- HP, "SAN Technical Planning and Design", U4236S
- R.R. Schulman, "Disaster Recover Issues and Solutions", March 2003
- C. Wang, "HP-UX 11i Security"
- HP, "Installing and Administering IPSec/9000"
- HP, "Network Security Feature of HP-UX 11i"
- HP, "HP-UX 11i System Security, White Paper"
- J. Chitnis, "HP Utility Data Center-Transforming Data Center Economics", Oct. 2003
- S. Patel, "HP Integrity/HP-UX Overview", Oct. 2003
- HP, "hp-ux geographically dispersed clusters", Oct. 2003
- ICSA, "An Introduction to Intrusion Detection Assessment"