~ 中小企業網路安全利器 ~
智能型交換器打造智慧服務新紀元

/台灣思科系統提供

面對網際網路已成為企業營運的必備元素之一，網路安全議題更是不容忽視的重要環節，因此，網管人員必須花費許多的精力來維護網路安全，而非將時間應用在實際的網路設定與管理工作上。根據美國聯邦調查局（FBI）於四月份針對政府機關、企業、財務、醫療機構、大學等 503 家美國公司單位的調查結果顯示，其中曾被電腦駭客入侵的比例已高達 91%，雖然如此，這些單位卻因害怕揭露後會遭受各界質疑，因此僅有 34%向主管當局揭露，而平均因被入侵而受損金額則為 200 萬美元。

由於台灣經濟架構多以中小型企業為主，因此，Cisco 除了持續針對大型企業推出網路安全解決方案，更依據中小型企業的網路安全需求，推出多項智慧型服務內容，其中包括豐富的強化型安全服務，如：在整個廣域與區域網路建立多個控制點，讓顧客獲得更完善的安全防護。而網路安全的最佳應用方針，即是 Cisco 語音、視訊及數據整合架構 (Architecture for Voice, Video and Integrated Data ，AVVID)，其可協助中小型企業及其分公司大幅提升防護能力的同時，成功運用各種網際網路中的商業應用模式。

善用智慧型交換器建構安全網路環境

目前的智慧型乙太網路交換器除了強化原有安全機制外，業界更針對相關軟體進行改良，使中小型企業可建置一套大型企業級的安全區域網路（Local-Area Network，LAN）基礎建設，提供完備安全功能以及操作簡易的嵌入式 Web 型管理軟體。以 Cisco 為例，其相關軟體改進的項目如下：

- **更安全的網路管理機制**
  - Secure Shell (SSH) 與 SNMPv3 能協助管理員在執行 telnet 連線，以及透過簡易網路管理協定（簡單網路管理協定—小辭典）(Simple Network Management Protocol，SNMP)所傳送出的資料流進行加密，以加強保護力，防止外部未經授權的使用者存取密碼以及組態資訊。
- **功能更強大的使用者驗證機制**
  - IEEE 802.1x 驗證型安全機制讓網管人員能透過端點連接埠的層級，控制使用者對網路之存取權限。
  - 動態位址分配服務協定(Dynamic Host Configuration Protocol，DHCP)介面追蹤器能向 DHCP 伺服器提供實體交換器，以及連接

埠的位置，供使用者進行追蹤。

- 一套完整的連接埠、虛擬區域網路（virtual LAN）、以及路由器介面等類型的存取控制表單（Access Control Lists，ACLs），可讓網管人員根據多重標準以限制網路存取權限，並改進使用者分隔功能。

- **增進網路安全管理功能**
  - 目前的交換器叢集機制中，除了能提供高頻寬的網路連接技術外，同時也擁有全新網管技術，如：Cisco 智慧型叢集管理軟體(Cluster Management Suite，CMS)，其可讓使用者運用標準的 Web 瀏覽器，同時設定與修復多部 Catalyst 桌上型交換器。而安全精靈（Security Wizard）則使管理人員只要透過幾個簡單步驟，即可限制使用者在特定伺服器或網路區段的存取權限。

中小企業競爭力 V.S.網路安全

在今年初台灣加入 WTO 之後，有高達 95％的中小企業，更強烈感受到競爭舞台已由區域性轉向全球市場，為了維持企業本身的高度競爭優勢，提升競爭力便成為勢在必行之途。除了透過 e 化以增加組織擴張的彈性外，企業整體的網路安全更是台灣中小企業極須思考及佈建的首要關鍵。若將安全功能直接嵌入網路設備，便可讓任何網路系統都可擁有一定程度的安全保護能力，並藉由控制啟動各個網路設備的安全功能，網路管理人員就可以針對系統開放程度、花費成本和管理考量等不同因素來決定公司網路所需的安全等級。所以，網路安全怎可等閒視之！