新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2006/12/25 - 2006/12/31 第9期

網路記錄器 / IR 系列報導

技術淺談與應用 - 新軟網路記錄器: 適用建置任何網路架構

由新軟公司所推出之 IR 系列產品，雙模式（旁接模式、橋接模式）的配置支援廣受企業好評。特別是旁接模式（Sniffer Mode）的運用，快速、簡易、隨插即用的特性，已成為企業普遍採用的主流模式。

由於企業採用旁接模式（Sniffer Mode）和 Core Switch 搭配使用時，常因下列情形，造成系統管理人員無法於遠端管理網路記錄器的困擾：

1. Core Switch 的鏡射埠（Mirror Port）於設定上，常常對於封包只接收而不回應（單向傳送封包），以致於當管理人員透過 Core Switch 的鏡射埠登入網路記錄器時，往往造成連線無回應的情況發生。
2. 若將網路記錄器未用到的另一個埠口，接回 Core Switch，藉此達到封包回應的目的，將會導致封包傳輸路徑造成迴圈（Loop）情形，以致於癱瘓整個網路。

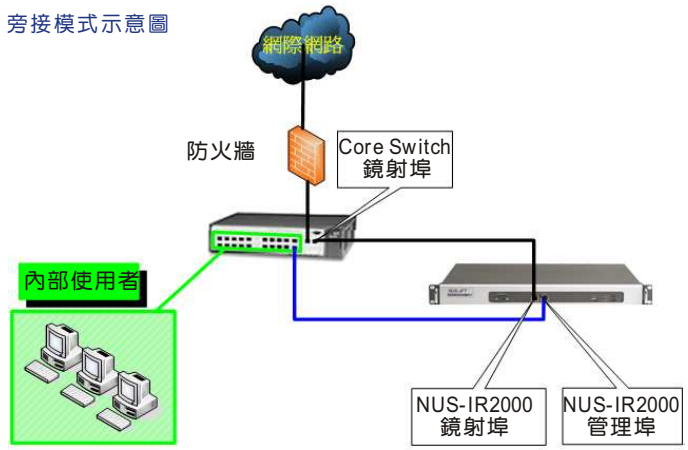
有鑑於此，新軟公司針對企業所面臨的上述問題研發出改善機制。可根據企業實際採用的網路記錄器配置模式，搭配相對應的軟體機制，有效避免上述問題的發生。

以 NUS-IR2000 爲例，當系統管理人員設定系統爲：

1. 橋接模式：系統對於 NUS-IR2000 之兩埠口，允許同時收發封包，保有原來設備的軟硬體特性。
2. 旁接模式：系統將會把 NUS-IR2000 之兩埠口分別獨立設置為：鏡射埠（指定為 Port1）與管理埠（指定為 Port2），其功能執掌如下：
   a. 鏡射埠：加入封包發送限制，使其專職於封包接收而不回應（包括 ARP 封包）。
   b. 管理埠：允許同時收發封包，可提供系統管理人員之管理連線。

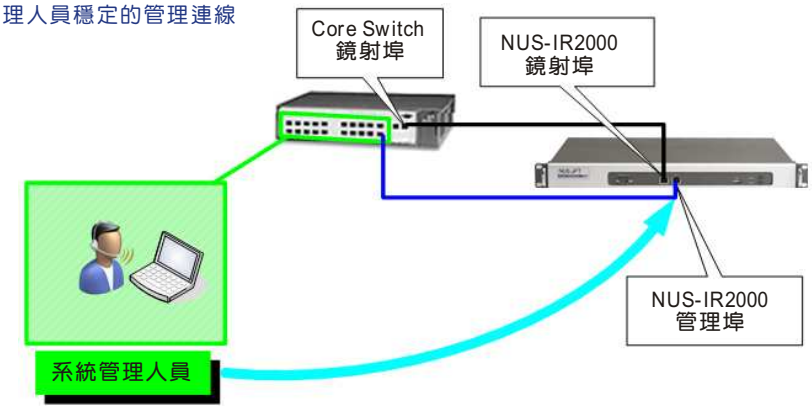
若系統管理人員因 Core Switch 設備的單向傳送功能限制，而必須將管理埠接回至 Core Switch 設備時（如 圖一），由於 NUS-IR2000 埠口獨立的設計，能有效避免了路徑迴圈的發生。

圖 一 旁接模式示意圖

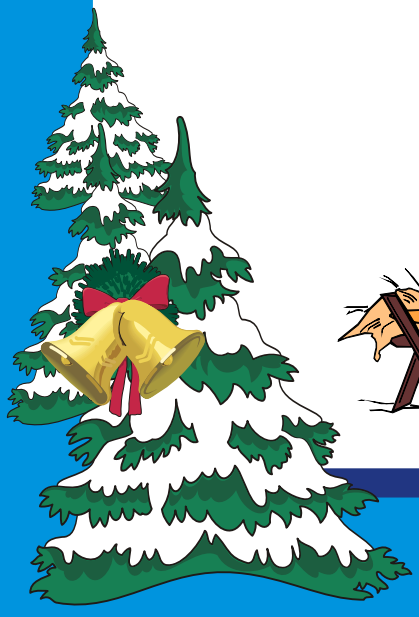


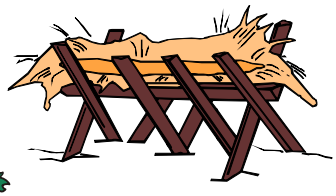
而限制鏡射埠回應封包的機制，可讓管理人員連線登入 NUS-IR2000 時，Core Switch 會將所有管理連線導向至管理埠，透過管理埠正常的封包收發機制，提供管理人員穩定的管理連線（如 圖二）。藉此改善因部分 Core Switch 設備只能單向傳送封包的功能缺陷，所導致管理人員無法正常登入 NUS-IR2000 之窒礙問題。

圖 二 提供管理人員穩定的管理連線



文 賴鴻文 tony@nusoft.com.tw





市場行銷報導 - 市售網路側錄設備功能探討

隨著網際網路的快速發展，多元化的網路服務有助於企業提昇整體競爭力，而在企業追逐於網路 e 化的同時，伴隨而來的卻是企業網路資源慘遭公器私用，對於企業網路來說無疑是揮之不去的夢魘。因此，各家業者紛紛推出網路側錄設備，藉此協助企業杜絕網路資源遭濫用之情形。但由於各家業者研發各項產品時，受限於研發實力及理念錯誤，造成所設計研發之產品功能參差不齊擁有許多缺陷。

市售網路側錄設備與新軟公司之 NUS-IR2000 比較如下：

	新軟公司 NUS-IR2000	一般市售網路側錄設備
產品定位	獨立的硬體平台設計，不論是硬體效能的展現或是系統穩定性發揮皆在水準之上。以完整的記錄功能及絕佳的記錄效能孕育而生，定位於網路記錄器，專職於網路記錄及流量分析。	分為兩大主流： 1. 硬體平臺：以現有的防火牆平臺為主，加入簡易的記錄功能魚目混珠。 2. 監控軟體：使用監控軟體仿真，無法掌握整體效能及系統穩定性。
網頁瀏覽記錄	可深入分析記錄網頁瀏覽封包，不僅支援以 HTTP Proxy 模式瀏覽網頁之記錄，更能詳實記錄網站標題、完整的URL、網頁內容、使用者等相關資訊。	不支援以 HTTP Proxy 模式瀏覽網頁之記錄，且以不完整的 URL 記錄資訊宣稱記錄成效。
郵件記錄	不僅有效記錄收/寄件者、郵件內容、主旨、附加檔案等相關資訊，更支援多國語系，使管理人員不需手動調整語系，就能一目了然信件內容。	不支援多國語系，需透過手動調整語系才能正常顯示信件內容，且一次僅能顯示單一語系。
網路郵件記錄	廣泛支援記錄多達 11 家網路上最常用的網路信箱，並以獨特的自動更新特徵技術，維持記錄的準確性。	採用網頁快照方式記錄，常常記錄不明的網頁內容（如 登入畫面、彈跳廣告等）。
即時通訊對話記錄	支援記錄網路上常用的即時通訊軟體，並依通訊對象分類記錄。多國語系的支援更能使管理人員可輕鬆瀏覽資訊記錄。	依發話時間記錄對話內容，當通訊人數眾多時，無法分辨與何人對話。
檔案傳輸記錄	不僅可詳實記錄檔案傳輸之主機位置、登入之帳號/密碼、檔案名稱等資訊，更能將所傳輸之檔案備份之設備中，待管理人員取回稽查。	無法記錄登入主機之帳號/密碼，且無法將所傳輸之檔案備份於設備中，提供稽核人員審查，容易造成記錄死角。

	新軟公司 NUS-IR2000	一般市售網路側錄設備
搜索功能	1. Mail / Web Mail：可根據信件內容、收/寄件者、主旨、附加檔案名稱等資訊，輸入關鍵字加以搜索。 2. IM：可根據使用者名稱、使用者帳號、參與者、對話內容、傳輸檔案名稱、認證名稱等資訊，輸入關鍵字加以搜索。 3. HTTP：可根據網站標題、使用者名稱、網頁內容，輸入關鍵字加以搜索。	1. Mail：無法針對信件的內容，附加檔案的檔名檢索。 2. Web Mail：常用網頁快照方式記錄 Web Mail，導致無法利用收件者、寄件者、主旨、信件內容…方式搜尋。 3. IM：大多僅能對聊天的帳號搜尋。無法針對聊天的內容、傳遞的檔案加以搜尋。 4. HTTP：通常只能針對 URL 搜尋，而不能搜尋網頁內容與網頁標題。
流量統計	可根據特定時段進行所有服務的流量分析，包括八大服務記錄類型以外之各類型資訊。	僅能針對單一時間點內的記錄做分析，且無法分析預設服務以外的各類型資訊，不僅無法符合企業多元化的網路服務需求，更不能藉此協助企業排除危害網路使用者。
備份機制	可根據需求自行分配各種記錄的儲存期限，並自動將過期資訊記錄允予刪除，以維持資訊記錄的時效性。 支援遠端手/自動備份，並可於管理介面直接瀏覽備份資料。	1. 不支援遠端備份，多半採用光碟燒錄輸出方式進行備份，不僅侵蝕企業維護成本，更在備份資料的尋找及審查上造成不便。 2. 須於上班時間內由專人進行備份工作。在備份時往往需停止記錄動作，於備份完成時在進行記錄工作。
異常流量偵測	主動察覺企業內部每位使用者的使用流量，當內部發生異常之大流量時，可發出警訊通知管理人員及使用者，使用橋接模式配置時，可進一步阻擋流量。	僅提供警訊通知系統管理人員，無法提供具體的異常流量阻擋功能。

文 賴鴻文 tony@nusoft.com.tw