新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2006/12/25 - 2006/12/31 第9期

网络记录器 / IR系列报导

技术浅谈与应用 - 新软网路记录器:适用建置任何网络架构

由新软公司所推出之 IR 系列产品，双模式（旁接模式、桥接模式）的配置支持广受企业好评。特别是旁接模式（Sniffer Mode）的运用，快速、简易、随插即用的特性，已成为企业普遍采用的主流模式。

由于企业采用旁接模式（Sniffer Mode）和 Core Switch 搭配使用时，常因下列情形，造成系统管理人员无法于远程管理网络记录器的困扰：

1. Core Switch 的镜射端口（Mirror Port）于设定上，常常对于封包只接收而不响应（单向传送封包），以致于当管理人员透过 Core Switch 的镜射端口登入网络记录器时，往往造成联机无响应的情况发生。
2. 若将网络记录器未用到的另一个端口，接回 Core Switch，藉此达到封包响应的目的，将会导致封包传输路径造成循环（Loop）情形，以致于瘫痪整个网络。

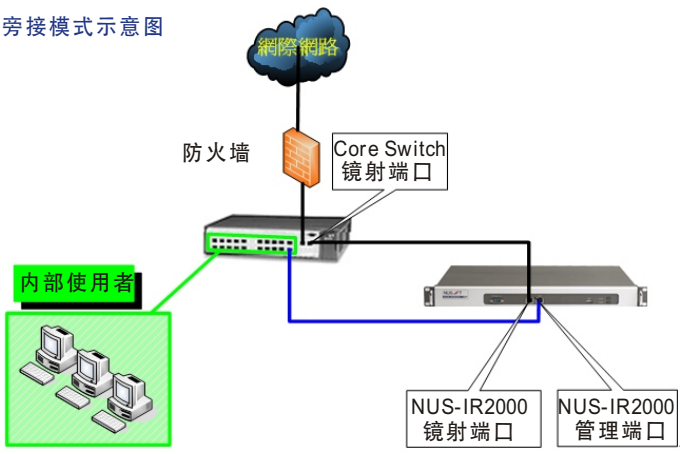
有鉴于此，新软公司针对企业所面临的上述问题研发出改善机制。可根据企业实际采用的网络记录器配置模式，搭配相对应的软件机制，有效避免上述问题的发生。

以 NUS-IR2000 为例，当系统管理人员设定系统为：

1. 桥接模式：系统对于 NUS-IR2000 之两端口，允许同时收发封包，保有原来设备的软硬件特性。
2. 旁接模式：系统将会把 NUS-IR2000 之两端口分别独立设置为：镜射端口（指定为Port1）与管理端口（指定为 Port2），其功能执掌如下：
   a. 镜射端口：加入封包发送限制，使其专职于封包接收而不响应（包括 ARP 封包）。
   b. 管理端口：允许同时收发封包，可提供系统管理人员之管理联机。

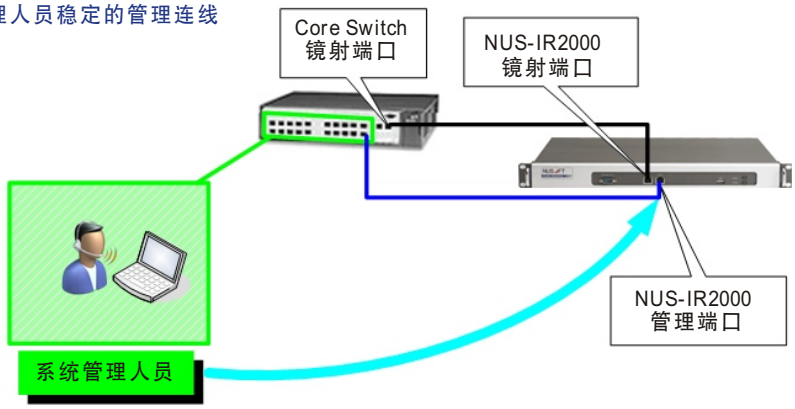
若系统管理人员因 Core Switch 设备的单向传送功能限制，而必须将管理端口接回至Core Switch 设备时（如 图一），由于 NUS-IR2000 端口独立的设计，能有效避免了路径循环的发生。

图 一 旁接模式示意图

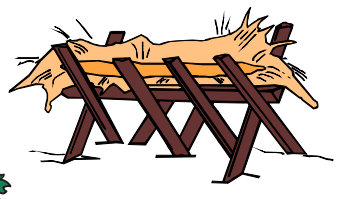


而限制镜射端口回应封包的机制，可让管理人员联机登入 NUS-IR2000 时，Core Switch 会将所有管理联机导向至管理端口，透过管理端口正常的封包收发机制，提供管理人员稳定的管理联机（如 图二）。藉此改善因部分 Core Switch 设备只能单向传送封包的功能缺陷，所导致管理人员无法正常登入 NUS-IR2000 之窒碍问题。

图 二 提供管理人员稳定的管理连线



文 赖鸿文 tony@nusoft.com.tw

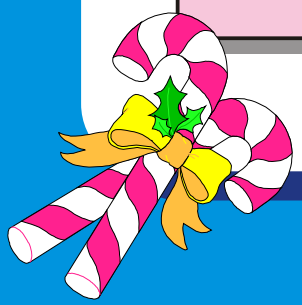


市场营销报导 - 市售网络侧录设备功能探讨

随着因特网的快速发展，多元化的网络服务有助于企业提升整体竞争力，而在企业追逐于网络 e 化的同时，伴随而来的却是企业网络资源惨遭公器私用，对于企业网络来说无疑是挥之不去的梦魇。因此，各家业者纷纷推出网络侧录设备，藉此协助企业杜绝网络资源遭滥用之情形。但由于各家业者研发各项产品时，受限于研发实力及理念错误，造成所设计研发之产品功能参差不齐拥有许多缺陷。

市售网络侧录设备与新软公司之 NUS-IR2000 比较如下：

	新软公司 NUS-IR2000	一般市售网络侧录设备
产品定位	独立的硬件平台设计，不论是硬件效能的展现或是系统稳定性发挥皆在水平之上。以完整的记录功能及绝佳的记录效能孕育而生，定位于网络记录器，专职于网络记录及流量分析。	分为两大主流： 1. 硬件平台：以现有的防火墙平台为主，加入简易的记录功能鱼目混珠。 2. 监控软件：使用监控软件仿真，无法掌握整体效能及系统稳定性。
网页浏览记录	可深入分析记录网页浏览封包，不仅支持以 HTTP Proxy 模式浏览网页之记录，更能详实记录网站标题、完整的 URL、网页内容、使用者等相关信息。	不支持以 HTTP Proxy 模式浏览网页之记录，且以不完整的 URL记录信息宣称记录成效。
邮件记录	不仅有效记录收/寄件者、邮件内容、主旨、附加档案等相关信息，更支持多国语系，使管理人员不需手动调整语系，就能一目了然信件内容。	不支持多国语系，需透过手动调整语系才能正常显示信件内容，且一次仅能显示单一语系。
网络邮件记录	广泛支持记录多达 11 家网络上最常用的网络信箱，并以独特的自动更新特征技术，维持记录的准确性。	采用网页快照方式记录，常常记录不明的网页内容（如登入画面、弹跳广告等）。
实时通讯对话记录	支持记录网络上常用的实时通讯软件，并依通讯对象分类记录。多国语系的支持更能使管理人员可轻松浏览信息记录。	依发话时间记录对话内容，当通讯人数众多时，无法分辨与何人对话。
档案传输记录	不仅可详实记录档案传输之主机位置、登入之账号/密码、文件名称等信息，更能将所传输之档案备份之设备中，待管理人员取回稽查。	无法记录登入主机之账号/密码，且无法将所传输之档案备份于设备中，提供稽核人员审查，容易造成记录死角。



	新软公司 NUS-IR2000	一般市售网络侧录设备
搜索功能	1.Mail / Web Mail：可根据信件内容、收/寄件者、主旨、附加文件名称等信息，输入关键词加以搜索。 2.IM：可根据使用者名称、使用者账号、参与者、对话内容、传输文件名称、认证名称等信息，输入关键词加以搜索。 3.HTTP：可根据网站标题、使用者名称、网页内容，输入关键词加以搜索。	1. Mail：无法针对信件的内容，附加档案的档名检索。 2. Web Mail：常用网页快照方式记录 Web Mail，导致无法利用收件者、寄件者、主旨、信件内容…方式搜寻。 3. IM：大多仅能对聊天的账号搜寻。无法针对聊天的内容、传递的档案加以搜寻。 4. HTTP：通常只能针对 URL 搜寻，而不能搜寻网页内容与网页标题。
流量统计	可根据特定时段进行所有服务的流量分析，包括八大服务记录类型以外之各类型信息。	仅能针对单一时间点内的记录做分析，且无法分析预设服务以外的各类型信息，不仅无法符合企业多元化的网络服务需求，更不能藉此协助企业排除危害网络使用者。
备份机制	可根据需求自行分配各种记录的储存期限，并自动将过期信息记录允予删除，以维持信息记录的时效性。 支持远程手/自动备份，并可于管理接口直接浏览备份数据。	1. 不支持远程备份，多半采用光盘烧录输出方式进行备份，不仅侵蚀企业维护成本，更在备份数据的寻找及审查上造成不便。 2. 须于上班时间内由专人进行备份工作。在备份时往往需停止记录动作，于备份完成时在进行记录工作。
异常流量侦测	主动察觉企业内部每位使用者的使用流量，当内部发生异常之大流量时，可发出警讯通知管理人员及使用者，使用桥接模式配置时，可进一步阻挡流量。	仅提供警讯通知系统管理人员，无法提供具体的异常流量阻挡功能。

文 赖鸿文 tony@nusoft.com.tw