新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2007/6/11 - 2007/6/17 第30期

## 网络记录器 / IR系列报导

# 技术浅谈与应用 - Sniffer 模式改良後的适用环境

新软系统所推出的网络记录器拥有两种架设方式－桥接模式（Bridge Mode）与旁接模式（Sniffer Mode）。企业可依其需求选择适用的架设方式。

当企业的网络记录器采用旁接模式架设时，需要将网络记录器的连接端口与 Core Switch 的镜射埠（Mirror Port）衔接。藉由 Core Switch 会将所有经过之封包，一个不漏的复制给镜射端口的特性，记录企业网络往来之信息。不用更动企业网络架构，即可完成网络记录器的架设。

就因为网络记录器的旁接模式架设快速、方便、随插即用，所以有许多企业采用这种方式架设网络记录器。但是，部分 Core Switch 的镜射埠只有单向传送封包之设计（只送不收）而无法双向传送。导致管理人员无法直接透过 Core Switch 浏览网络记录器的记录。

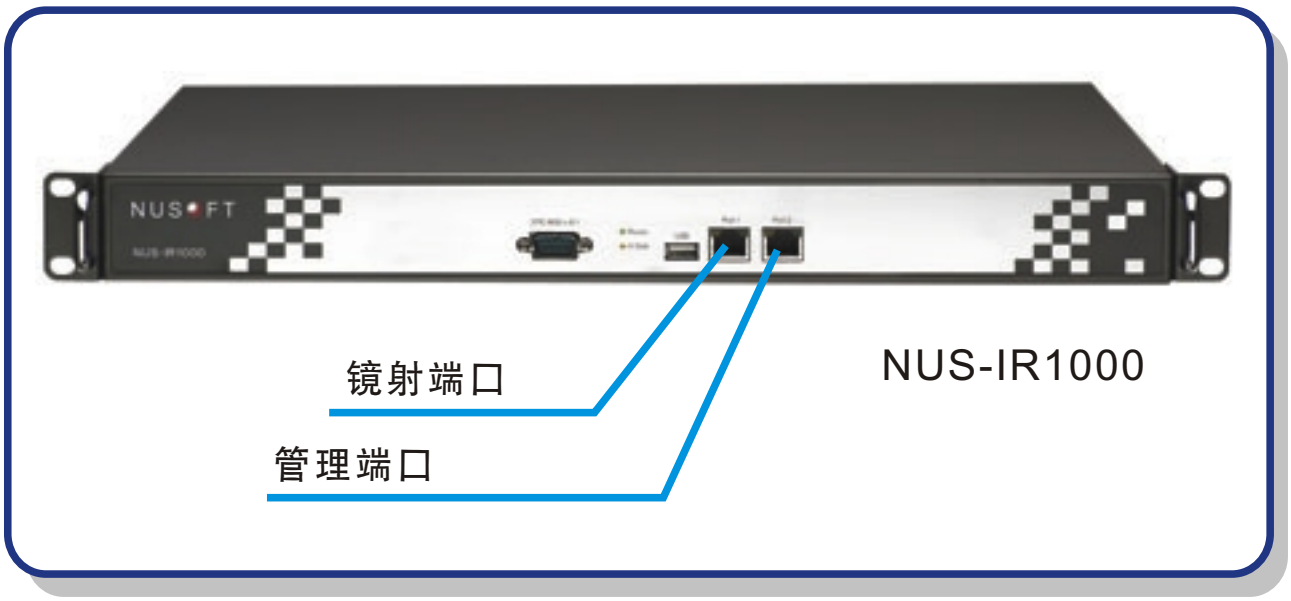
虽然绝大部分 Core Switch 的镜射端口可定义成双向传送，而不会有上述的问题发生。但为了让网络记录器能完全适用于各种企业网络架构，因此新软系统针对此类问题，特别增加了“网络配置模式设定”。针对这些只有单向传送封包镜射端口的 Core Switch 而改良。

新型的旁接模式会将网络记录器的连接端口重新定义：

Port 1－定义为镜射端口，专职接收 Core Switch 所传送的企业网络信息，而不会响应任何封包（包含 ARP）。

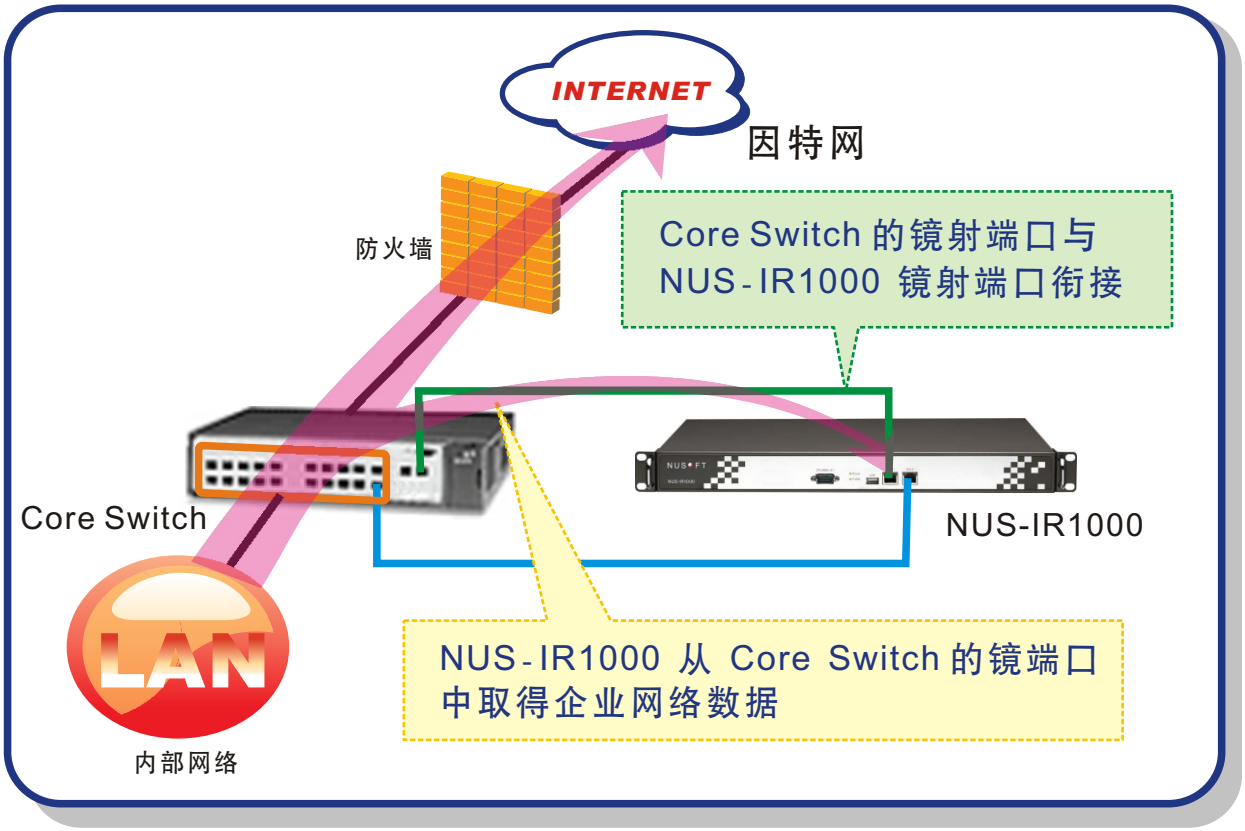
Port 2－定义为管理端口，管理人员可从此浏览网络记录器之记录。


圖一 NUS-IR2000、NUS-IR1500 旁接模式时连接端口之定义

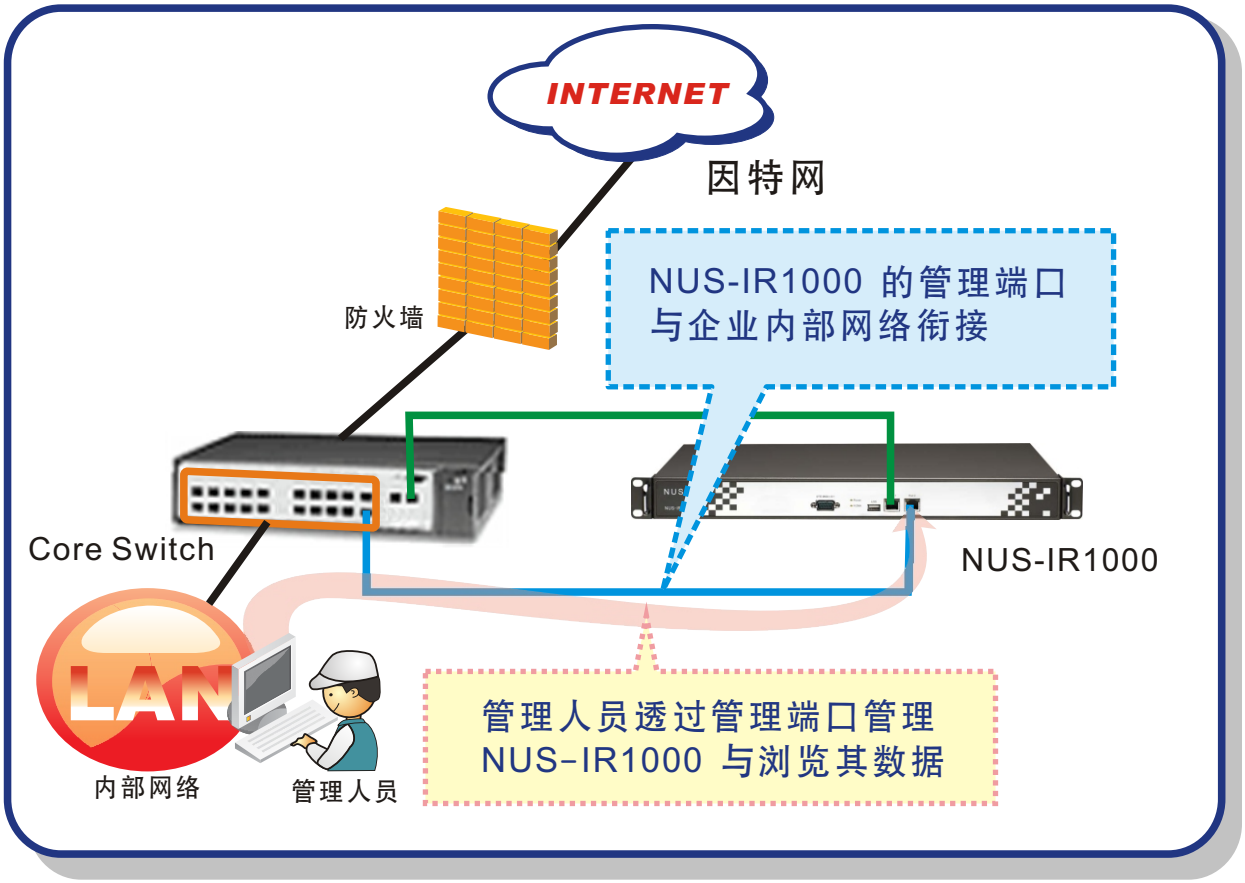



圖二 NUS-IR1000 旁接模式时接端口之定义

管理人员可将网络记录器的镜射端口与 Core Switch 的镜射端口衔接，接收企业网络信息。再将管理端口联接至企业网络。如此一来，网络记录器可正常记录企业网络信息，管理人员也可从企业网络的任何地方浏览网络记录器所记录的数据。




图三 NUS-IR1000 利用 Core Switch 的镜射端口取得企业网络数据




图四 管理人员利用管理端口管理 NUS-IR1000 与浏览其数据

| | | 旁接模式 | 桥接模式 |
|---|---|---|---|
| 架设方式 | | 镜射端口与Core Switch衔接<br>管理端口与企业网络衔接 | 直接安插在企业内部网络<br>与防火墙之间 |
| 管理機制 | 异常流量侦测 | 仅能提出警告，无法阻挡 | 可提出警告，并可阻挡 |
| | P2P管理 | 无法使用 | O |
| | IM认证/管理 | 无法使用 | O |
| 适用环境 | | 当企业不想更动原有企业网络架构时适用。<br>必须拥有Core Switch。 | 当企业需要使用网络记录器的管理机制时适用。 |

表一 网络记录器架设模式差异

文 程智伟 rayearth@nusoft.com.tw

## 市场营销报导-全方位搜寻记录，帮您轻松找到所要数据

企业e化的结果，可为企业带来丰厚的商机。但随之而来的员工网络摸鱼、商业机密泄露...，却严重损及企业之竞争力。因此，为了保护企业机密、防止员工滥用企业网络资源，国内外各家厂商纷纷推出了网络侧录相关设备，来为企业网络使用情况把关。这些厂商的网络侧录设备虽然可以详细记录员工上网之情况，但往往忽略掉一个关键重点－事后数据调阅搜寻的方便性。

要知道，在稍具规模的企业里，网络侧录设备可记录到的数据成千上万，管理人员根本无从一一浏览查看；无法轻松调阅搜寻的记录数据，对把关企业网络使用情况是无任何帮助的。因此，新软系统在研发网络记录器（NUS-IR2000、NUS-IR1500、NUS-IR1000）之初，就针对数据调阅、数据搜寻这部份的功能多加着墨。

**新软网络记录器数据调阅、搜寻（以NUS-IR2000为例）**

当员工透过企业网络上网时，NUS-IR2000除了会记录其上网数据之外，其内建的分析引擎会将数据的各种特征记录在NUS-IR2000的数据库中，方便管理人员日后查询与调阅。

电子邮件（SMTP、POP3）－ NUS-IR2000除了可搜寻收件者、寄件者、主旨、时间...之外，还拥有其它厂商所没有的**信件内容**与**附加文件名称搜寻**。要知道，信件内容与其附加文件才是信件的主体。倘若无法搜寻，则在信件调阅时，容易错失重要信件。

网页邮件－ 一般网络侧录设备是把网页邮件以网页快照的方式记录，因此系统无法判断信件的收件者、寄件者、主旨...。在这先天不良的条件下，管理人员仅能使用URL、Web Mail Server...等无关紧要的搜寻条件调阅信件。反观NUS-IR2000利用网页邮件分析引擎，将网页邮件以一般电子邮件方式记录。所以NUS-IR2000的网页邮件调阅搜寻方式与一般电子邮件相同，管理人员调阅起来轻松快速。

网页浏览－ NUS-IR2000在其网页浏览的搜寻接口中特别增加了**网站名称**（URL）与**网页内容**这两种搜寻条件。管理人员可透过这两种搜寻条件在庞大的网页记录数据中找寻所要的记录。而用不像一般网络侧录设备，仅能透过时间这个搜寻条件来缩小记录范围，查阅数据相当困难。

实时通讯软件－ 在实时通讯记录中，最重要的当然就是员工**聊天内容**与其**传输之文件**。倘若管理人员无法针对这两个关键

重点搜寻，那网络侧录设备记录在多的聊天内容也无实质作用；需要找寻的数据，很有可能是在众多网络聊天中的一两句话，仅用 使用者名称、账号、参与者...根本找不到所要资料。因此，NUS-IR2000 特别强化了这方面的搜寻功能，协助管理人员管理实时通讯软件。

FTP 文件传输－ 唯有完整的搜寻条件，管理人员方能轻松找到所需之数据。NUS-IR2000 的 FTP 文件传输可以针对文件名称、FTP 主机名称、使用者名称、文件大小、联机方向、时间...方式搜寻记录，想要快速找到想要的文件再也不是难事。

Telnet / BBS－ 在 Telnet 记录搜寻中，Telnet 主机名称的搜寻是重要的关键之一。如果想要找到员工特定的 Telnet 记录，能从 Telnet 主机名称的方向找寻，数据调阅将可事半功倍。

| 网络服务 | 可搜寻的特征 | |
|---|---|---|
| | 新软网络记录器 | 一般网络侧录设备 |
| 电子邮件（SMTP、POP3） | 收件者、寄件者、主旨、信件内容、使用者名称、有无附加文件、附加文件名称、信件传送方向、时间 | 收件者、寄件者、主旨、使用者名称、时间 |
| 网页邮件 | 收件者、寄件者、主旨、信件内容、使用者名称、有无附加文件、附加文件名称、信件传送方向、时间 | 使用者名称、URL、Web Mail Server、时间 |
| 网页浏览 | 网站（网站名称、URL）、使用者名称、网页内容、联机方向、时间 | 时间 |
| 实时通讯软件 | 实时通讯软件类别、使用者名称、帐号、参与者、内容、传送文件名称、实时通讯认证帐号、时间 | 使用者名称、帐号、参与者、时间 |
| FTP 文件传输 | 文件名称、FTP 主机名称（IP）、使用者名称、文件大小、联机方向、时间 | 文件名称、FTP 主机 IP、使用者名称、帐号、联机方向、时间 |
| Telnet / BBS | 使用者名称、Telnet 主机名称、联机方向、时间 | 使用者名称、时间 |

表一 新软网络记录器与一般网络侧录设备在数据调阅、搜寻方面的差异

文 程智伟 rayearth@nusoft.com.tw