

網路記錄器 / IR 系列報導

技術淺談與應用 - 網路記錄器的硬碟容量可以使用多久？ 如何得知硬碟容量快額滿了？

隨著網路科技的發達，企業每天透過網路傳輸的資料量相當龐大，網路儼然已成為企業最重要的溝通管道之一。在企業大量使用網路傳遞資訊的同時，對於具相當規模的企業來說，旗下員工每天的網路行為所產生之資料量往往都過於龐大，導致一般網路側錄設備其所內建的硬碟容量經常不敷使用。同時機器所記錄之資料也缺少分類的機制，當內建硬碟容量接近飽和時，系統便會自動將最舊的資料刪除，如此無差別的硬碟儲存管理方式，對於硬碟儲存容量不僅沒有做到有效分配的控管，也不符合企業須長時間保存資料的要求。

新軟系統針對一般市售網路側錄設備此缺點，特別在新軟網路記錄器（IR 系列產品）上加入對於封包的傳遞做擷取、分析及歸類的獨特過濾技術，除了能夠詳細過濾封包的來源並加以歸類之外，同時在資料儲存上具有獨家的「儲存期限」機制；透過此機制，網管人員可依企業的需求在各項服務上設定欲儲存的時間值，而 IR 即會依據網管人員所設定的「資料儲存時間」與該服務的「每日平均流量」，計算各項網路服務的「預估儲存空間大小」及該服務的「硬碟容量佔用百分比」，藉由此方式來有效分配各項記錄於 IR 內建硬碟的使用率。

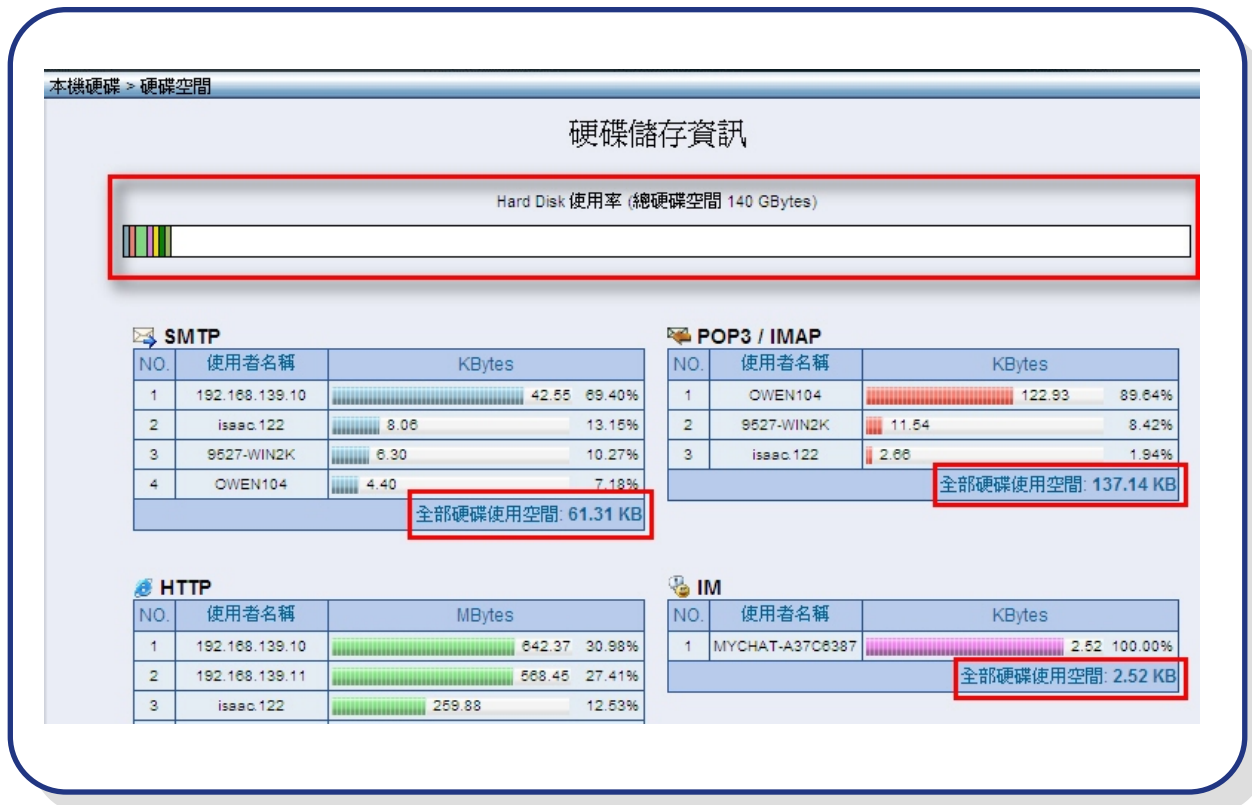
服務名稱	目前儲存時間範圍 (y/m/d)	平均流量 / 天	儲存時間 (0: 不記錄)	預估儲存空間* (百分比)
SMTP	07/12/06 ~ 07/12/10	12.26 KB	60 天	735.72 KB (0.00%)
POP3 / IMAP	07/12/06 ~ 07/12/10	27.43 KB	7 天	191.99 KB (0.00%)
HTTP	07/12/06 ~ 07/12/10	414.39 MB	60 天	24.86 GB (16.54%)
IM	07/12/07 ~ 07/12/10	1 KB	7 天	4.41 KB (0.00%)
Web SMTP	07/12/06 ~ 07/12/10	1 KB	7 天	1 KB (0.00%)
Web POP3	07/12/06 ~ 07/12/10	314.85 KB	7 天	2.20 MB (0.00%)
FTP	07/12/10 ~ 07/12/10	1 KB	7 天	1 KB (0.00%)
TELNET	07/12/10 ~ 07/12/10	85.32 KB	8 天	682.58 KB (0.00%)
全部				24.87 GB (16.54%)

$\text{預估儲存空間} = \text{平均流量} \times \text{儲存時間}$


(圖一) 預估儲存時間 = 使用者設定的【儲存時間】× 系統分析的【平均流量】

當 IR 內部的各項服務記錄一旦過了網管人員所設定的儲存時間期限，系統則會自動將超過保存期限的資料刪除。倘若，在尚未到達資料儲存時間之前，硬碟儲存空間就已經額滿，則 IR 系列產品會依照資料儲存的時間先後順序，從時間最久的記錄資料做刪除的動作，空出儲存空間，如此一來不僅 IR 產品內建的硬碟儲存空間能不斷地重複儲存使用，同時系統側錄機制也能夠持續地維持運作。

那網管人員要如何得知硬碟的使用狀況呢？很簡單~！網管人員只要從 IR 內部的『硬碟空間』管理介面上即可清楚得知內建硬碟的使用狀況。在『硬碟空間』的管理介面中，除了可以看到各項服務所使用的硬碟空間之外，更能透過畫面上的硬碟儲存資訊及橫條圖，清楚得知內建硬碟的總空間大小與硬碟的使用率。藉由這樣一目瞭然的硬碟儲存資訊介面，不僅讓網管人員輕鬆地得知 IR 系列產品內建硬碟的空間使用情形，同時能清楚地看到各項服務的員工使用排行榜，進而掌握企業的網路使用概況。



(圖二) 各項服務的硬碟使用率與總使用率情形

文  黃贊中 isaac@nusoft.com.tw

市場行銷報導 - 流量排行榜可以幫網管人員解決哪些問題？

拜近年的網際網路快速發展之賜，並透過企業 e 化的結合，使企業整體競爭力不斷提升，網路科技的百家爭鳴時期就此因應而生。但在過度依賴網路便捷性的同時，可經常發現網路資源遭到有心人士的不當濫用、員工網路摸魚等問題層出不窮。雖然，坊間出現許多號稱可協助網管人員監督企業網路使用的網路側錄設備，不過這些網路側錄設備僅能提供網路總流量記錄之類的陽春功能，對於網管人員欲藉此揪出濫用企業網路資源害蟲的需求，根本無濟於事！

而新軟系統瞭解企業此一需求，於網路記錄器（IR 系列產品）的流量分析功能特別加入『流量排行榜』的設計。流量排行榜是以「使用者的網路流量」與「各項網路服務的使用量」兩種類型以排名的方式排序，並透過簡單明瞭的圖表呈現企業網路的使用情形。透過流量排行榜，不僅可輕鬆掌握企業任何時段的網路使用情形，更能夠得知「是誰」在「哪個時段」使用「何種服務」佔據企業網路頻寬。

流量排行榜分為兩種，各別為「今日排行榜」與「歷史排行榜」：

● 今日排行榜：

今日排行榜最大的特點就是一網管人員可觀察當天任一時段網路流量前 10 名的記錄，並透過新軟獨家的「橫移滑動拉桿」時間軸設計，網管人員可以輕鬆地利用拖曳方式來選擇欲觀察之時段，並從畫面排名結果中得知在這一時段內「何人」使用「何種服務」佔用企業頻寬。甚至可以深入了解該使用者透過此項服務到底做了些不法勾當，導致如此大量佔用企業頻寬。

另外值得注意的是，「今日排行榜」的觀察時間是以每“10 分鐘”為單位，當然，網管人員也可依個人需求調整觀察時間。會有這樣的設計想法主要是因為過長的觀察時間雖然可以累積記錄較多的資料，但反而造成網管人員無法清楚得知該從何處找出問題發生的時間點，同時網路的異常流量也容易被其他服務資訊所掩埋。這就是為什麼新軟網路記錄器的「流量排行榜」機制遠遠優於他牌網路側錄設備的緣故。

一、拖曳橫桿至欲觀察的時間點

二、顯示流量排行，點選欲觀察的使用者名稱或流量

NO.	User Name	8-Recorded / Others	MBytes (Click to view top service)	
1	NUSOFT_NB-PC	1.29 MB / 14.11 KB	1.31	88.45%
2	Reggie	30.56 KB / 73.61 KB	0.10	7.05%
3	MailServer	4.72 KB / 16.64 KB	0.02	1.44%

三、顯示員工的網路使用情形，點選流量最高的服務名稱

NO.	Service Name	Flows	MBytes	
1	HTTP	1.29 MB	1.29	98.53%
2	IM	5.18 KB	< 0.01	0.40%

四、員工佔用公司網路頻寬的惡行馬上原形畢露

Date/Time	Web Site
12/14 08:51	火辣銷魂.avi
12/14 08:51	最新最便宜情色光碟.exe
12/14 08:51	中X銀行員-桌上露毛又露...avi

【圖一】透過今日排行榜，簡單四個步驟即可輕鬆查閱使用者的網路使用情形

● 歷史排行榜：

「歷史排行榜」雖然也可讓網管人員了解企業頻寬的使用情形，但與「今日排行榜」不同的是，「歷史排行榜」所觀察的對象不是「當天的流量」，而是「企業從以往至當天的所有網路使用情況」。網管人員可依需求瀏覽指定時間日期範圍內的所有網路流量資訊，隨時皆能掌握企業頻寬的使用動態。

流量排行方式	新軟網路記錄器	一般網路側錄設備
今日排行榜	可觀察當日任何時段的網路流量排行，並列出流量最高的前10名，使網管人員輕鬆掌握企業頻寬之使用情形。	僅能提供單一特定時間點內的分析記錄，也無法提供預設網路服務之外的分析記錄。網管人員要找出濫用頻寬者如同大海撈針。
歷史排行榜	顯示全時段的所有流量排行，網管人員可完整了解企業整體網路頻寬的運作情況，無一遺漏。	

【表一】新軟網路紀錄器 vs. 一般網路側錄設備的流量分析記錄差異

文 黃贊中 isaac@nusoft.com.tw