



俠諾神捕 QnoSniff 專業版 2.0

繁體中文使用手冊

目 錄

一、簡介	4
二、QnoSniff 專業版系統安裝與配置	6
2.1 開始之前的準備	6
2.2 QnoSniff 專業版安裝過程中所需元件	6
2.3 佈署連接範例拓樸	7
2.4 開始安裝	7
三、啟用 QnoSniff 專業版	24
3.1 啟用 QnoSniff 軟體之前路由器的設定	24
3.2 啟用 QnoSniff 專業版軟體	27
四、基本設定	34
五、系統權限管理	40
5.1 觀看許可權	40
5.2 使用者管理	42
5.3 使用者日誌	44
六、群組使用者管理	45
6.1 部門設定	45
6.2 用戶樹狀列表	47
七、系統資源分析	51
7.1 CPU 使用記錄	51
7.2 記憶體 (Memory) 使用記錄	55
7.3 WAN Traffic(廣域網流量) 記錄	56
八、摘要訊息	57
8.1 即時服務總表	58
8.2 網頁瀏覽	59
8.3 電子郵件	61
8.4 檔案傳輸 (FTP)	65
8.5 點對點下載 (P2P)	67
8.6 Telnet	69
8.7 即時通訊	72
九、統計資訊	75
9.1 流量統計報表	75
9.2 部門流量排名總表	77
9.3 使用者流量排名總表	78



十、登出系統.....	79
十一、解除安裝.....	81
附錄：Qno 技術支援資訊.....	85

產品功能說明手冊使用許可協定

《產品功能說明手冊(以下稱"手冊")使用許可協定》(以下稱"協定")是用戶與俠諾科技股份有限公司(以下稱"俠諾")關於手冊許可使用及相關方面的權利義務、以及免除或者限制俠諾責任的免責條款。直接或間接取得本手冊檔案以及享有相關服務的用戶，都必須遵守此協議。

重要須知：俠諾在此提醒用戶在下載、閱讀手冊前閱讀本《協議》中各條款。請您審閱並選擇接受或不接受本《協議》。除非您接受本《協議》條款，否則請您退回本手冊及其相關服務。您的下載、閱讀等使用行為將視為對本《協議》的接受，並同意接受本《協議》各項條款的約束。

【1】知識產權聲明

手冊內任何文字表述及其組合、圖示、界面設計、印刷材料、或電子檔等均受我國著作權法和國際著作權條約以及其他知識產權法律法規的保護。當用戶複製"手冊"時，也必須複製並標示此知識產權聲明。否則，俠諾視其為侵權行為，將適時予以依法追究。

【2】"手冊"授權範圍：

用戶可以在配套使用的電腦上安裝、使用、顯示、閱讀本"手冊"。

【3】用戶使用須知

用戶在遵守法律及本協議的前提下可依本《協定》使用本"手冊"。用戶若是違反本《協議》，俠諾將中止其使用權力並立即銷毀此"手冊"的複本。本手冊"紙質或電子檔案"，僅限於為資訊和非商業或個人之目的使用，並且不得在任何網路電腦上複製或公佈，也不得在任何媒體上傳播；及不得對任何"檔案"作任何修改。為任何其他目的之使用，均被法律明確禁止，並可導致嚴重的民事及刑事處罰。違反者將在可能的最大程度上受到指控。

【4】法律責任與免責聲明

【4-1】俠諾將全力檢查文字及圖片中的錯誤，但對於可能出現的疏漏，用戶或相關人士因此而遭受的直接或間接的經濟損失、資料損毀或其他連帶的商業損失，俠諾及其經銷商與供應商不承擔任何責任。

【4-2】俠諾為了保障公司業務發展和調整的自主權，俠諾擁有隨時自行修改或中斷軟體 / 手冊授權而不需通知用戶的權利，產品升級或技術規格如有變化，恕不另行通知，如有必要，修改或中斷會以通告形式公佈于俠諾網站。

【4-3】所有設置參數均為範例，僅供參考，您也可以對本手冊提出意見或建議，我們會參考並在下一版本作出修正。

【4-4】 本手冊為解說同系列產品所有的功能設置方式，產品功能會按實際機種型號不同而有部份差異，因此部分功能可能不會出現在您所購買的產品上。

【4-5】 俠諾保留此手冊檔案內容的修改權利，並且可能不會即時更新手冊內容，欲進一步瞭解產品相關更新訊息，請至俠諾官方網站流覽。

【4-6】 俠諾（和/或）其各供應商特此聲明，對所有與該資訊有關的保證和條件不負任何責任，該保證和條件包括關於適銷性、符合特定用途、所有權和非侵權的所有默示保證和條件。所提到的真實公司和產品名稱可能是其各自所有者的商標，俠諾（和/或）其各供應商不提供其他公司之產品或軟體等。在任何情況下，在由於使用或檔案上的資訊所引起的或與該使用或運行有關的訴訟中，俠諾和/或其各供應商就因喪失使用、資料或利潤所導致的任何特別的、間接的或衍生性的損失或任何種類的損失，均不負任何責任，無論該訴訟是合同之訴、疏忽或其他侵權行為之訴。

【5】 其他條款

【5-1】 本協議高於任何其他口頭的說明或書面紀錄，所定的任何條款的部分或全部無效者，不影響其他條款的效力。

【5-2】 本協議的解釋、效力及糾紛的解決，適用於臺灣法律。若用戶和俠諾之間發生任何糾紛或爭議，首先應協商解決。若協商未果，用戶在完全同意將糾紛或爭議提交俠諾所在地法院管轄。大陸地區則以「中國國際經濟貿易仲裁委員會」為仲裁機構。

一、簡介



QnoSniff 專業版 2.0 是一款工作於 PC 上的網路流量資訊記錄軟體，透過和俠諾系列路由器的整合，對網路資料進行側錄、過濾、分析，著重現今管理用戶所關切的應用內容，並呈現出易於檢視與閱讀的資料格式，生成統計圖表與報表，提供企業或網路管理人員參考。

企業或網路管理人員經常遇到以下困擾：員工上網都在作什麼？

員工上網不外乎用收發電子郵件、瀏覽網頁與搜尋資料、用 MSN/Skype 等即時通訊（IM）跟朋友閒聊、用 BT 等點對點傳輸（P2P）下載檔案。其中，電子郵件 E-mail 與 IM 是洩密與病毒入侵的管道，而 P2P 更是頻寬的殺手與間諜軟體的溫床。不但如此，IM 浪費上班人力在聊天，工作不斷被外界朋友打斷，耗損的生產力更難以估計。然而 IM 可以節省通信成本，甚至增加溝通效率，許多企業已不得不開放。

上班時間聊天軟體使用過多，影響工作效率、濫用頻寬進行下載，導致正常應用的擁塞、公司機密通過聊天軟體等工具洩漏，QnoSniff 專業版是針對企業用戶經常遇到的問題量身定制的，首先要做的，就是解決企業的網路問題。通過對網路資訊的監控與記錄，QnoSniff 專業版可以有效幫助企業管理人員解決由網路應用衍生出的各種問題。無論是上網記錄，郵件記錄還是聊天記錄，下載文件，QnoSniff 專業版都可以分析整理的井井有條，檢查起來非常方便。

QnoSniff 專業版不僅僅是為了管理而管理，它同時為企業用戶帶來了全新的【主動管理】的理念。傳統的管理模式是被動管理，員工總是到被管理人員關注並通知甚至警告之後，才會約束自己的行為，由此容易讓員工產生抵觸情緒，而且會帶來一些管理問題。

而 QnoSniff 專業版針對此情況，通過提供流量統計排名功能，讓員工可以隨時自己去查看各種網路應用的使用流量排名，例如聊天、下載等，當“榜上有名”時，員工看到就會進行自我約束，從而形成一種自我管理的概念。

流量統計排名同樣也會將服務類型進行排序，以協助網管人員找到本地網路中用戶的網路使用習慣，進而指導網路的設計和規劃，更好的管理網路，實現企業工作效率的最大化。

值得一提的是，QnoSniff 專業版還提供了 PDF 轉檔以及電子郵件寄送功能，可以隨時生成離線檔案，發送給相關人員進行查看。

二、QnoSniff 專業版系統安裝與配置

本章節介紹用戶在安裝之前的準備，以及整體的安裝過程與 QnoSniff 的基本系統設置。

2.1 開始之前的準備

※ 安裝 QnoSniff 專業版的 PC，建議的最低系統需求：

- 1、Intel P4 2.0GHz 以上 / AMD 同等級以上 CPU。
- 2、操作系統：Windows 平台 (不包含 Windows 2000 以下版本)。
- 3、空的硬碟空間 100G 以上。
- 4、系統記憶體 RAM 2GB MB 以上。

※ 必要的搭配佈署

- 1、需與俠諾路由器一同搭配運作。
- 2、俠諾路由器需要有 Mirror Port 實體鏡像埠口功能。
- 3、安裝 QnoSniff 專業版軟體的 PC 需要透過網卡與網路線，連接俠諾路由器的 Mirror Port 埠口。
- 4、「必須」將路由器的 Mirror Port 功能啟用。
- 5、「必須」必須要將路由器的 SNMP 功能啟用。
- 6、「必須」將路由器 License Key 功能的 QnoSniff 選項開啟 (不論是試用還是正式版)。

2.2 QnoSniff 專業版安裝過程中所需元件

QnoSniff 安裝包內會有以下 QnoSniff 運作所需用的所有元件，但是若您的電腦已經有安裝過這些元件

，可能會需要移除 PC 內原本的原件版本，或是重新安裝 / 升級成新的元件版本。

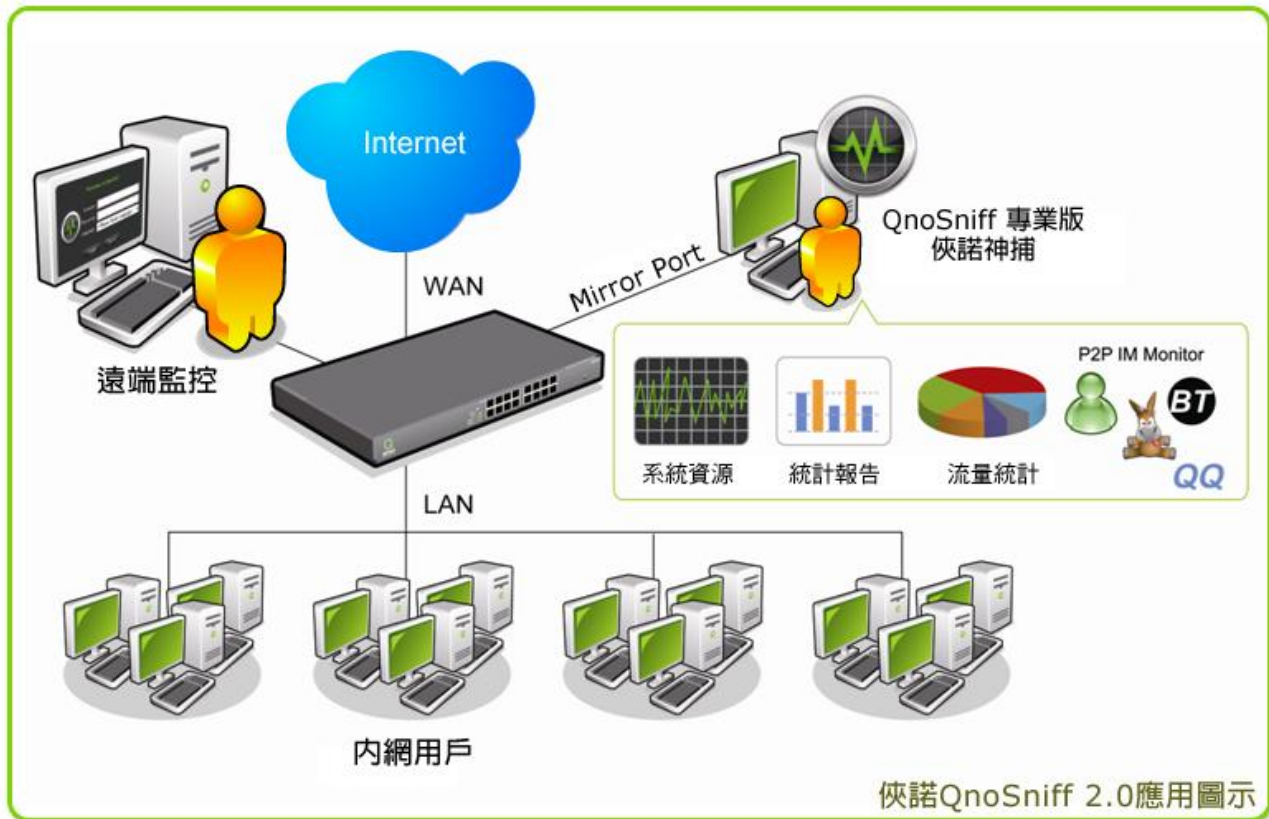
*Apache Server

*WinPcap

*.Net Framework

*PHP


2.3 佈署連接範例拓樸



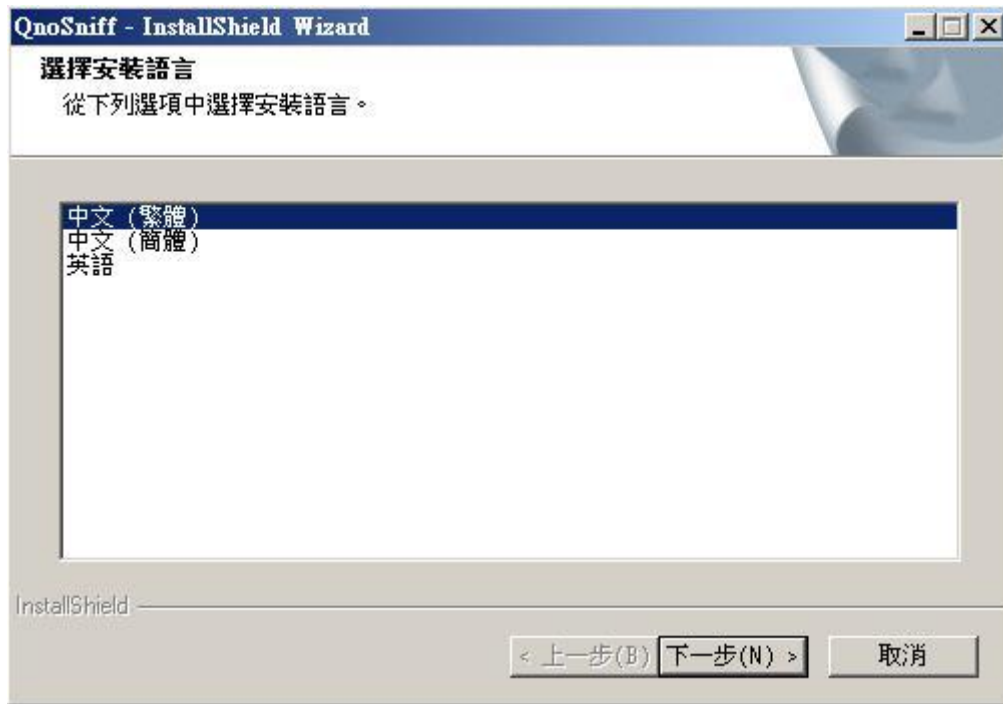
2.4 開始安裝

請參照以下步驟安裝到您的 PC 上

1. 將 QnoSniff 專業版軟體的光碟，放入您電腦的 CD 或 DVD 的讀取裝置中。

2. 用滑鼠點選安裝檔案  進行安裝。(註：系統需要以最高權限管理用戶身分進行安裝)

3. 【語系選擇】開始安裝程序後，首先會跳出選擇語系頁面，請選擇您所使用的語系



選擇「下一步」繼續安裝，選擇「取消」則取消安裝程序。

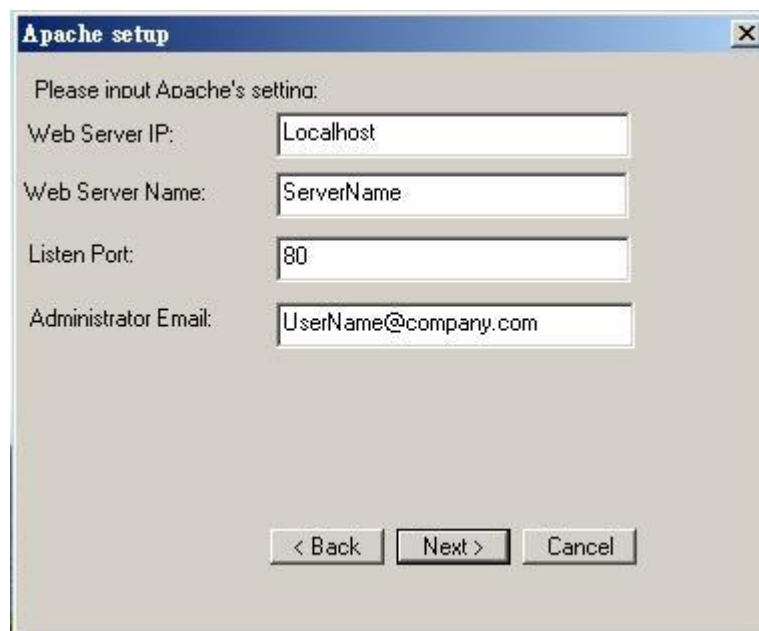
4. 【歡迎頁面】進入到歡迎安裝頁面，選擇「下一步」繼續安裝，選擇「取消」則取消安裝程序。



5. 【授權合約】出現授權合約，請在仔細閱讀後，點選「我接受授權合約的條款」，才能按「下一步」繼續進行安裝。



6. 【Apache Server 安裝】出現 Apache 伺服器的安裝設定頁面，安裝此伺服器是用來讓安裝 QnoSniff 專業版的 PC 能夠開啟 Web 服務，使管理者或用戶能夠進行遠端監控與存取，按「Next」繼續進行安裝程序



Web Server IP 表示 Web 伺服器的 IP 位址，安裝程序預設值會填寫 Localhost，即 127.0.0.1

Web Server Name 表示 Web 伺服器的名稱

Listen Port 表示 Apache 伺服器收送的通訊埠口，安裝程序預設值填寫 80 Port

Administrator Email 表示 Administrator 權限的 Email，方便告知使用者重要訊息

設定完成後，請按「Next」繼續進行安裝程序

※由於 Port 80 常常會與許多的應用程式使用衝突，也常常會是電腦病毒或蠕蟲攻擊的對象，所以強烈建議您做修改（例如改成 8080）

7. 【客戶資訊】接著出現客戶資訊頁面，麻煩請輸入您的使用者名稱以及公司名稱，此兩者皆須輸入內容才能夠按「下一步」繼續進行安裝程序



The screenshot shows a Windows-style dialog box titled "QnoSniff - InstallShield Wizard". The main heading is "客戶資訊" (Client Information) with the instruction "輸入您的資訊。" (Enter your information.). Below this, it says "請輸入您的名字和所在公司的名稱。" (Please enter your name and the name of the company you are in.). There are two input fields: "使用者名稱(U)：" (Username) and "公司名稱(C)：" (Company Name). At the bottom, there are three buttons: "< 上一步(B) | 下一步(N) >" (Previous/Next) and "取消" (Cancel). The "InstallShield" logo is visible in the bottom left corner of the dialog.

8. 【安裝類型】選擇安裝類型，選擇全部是指安裝所有程式的功能；選擇自訂是指可以選擇程式的部分功能安裝，以下顯示圖例選擇安裝類型為全部為例，目前在 QnoSniff 專業版 2.0 版本並沒有其他全部安裝與自訂安裝部分元件的差異，所以選擇其中一個類型皆可。



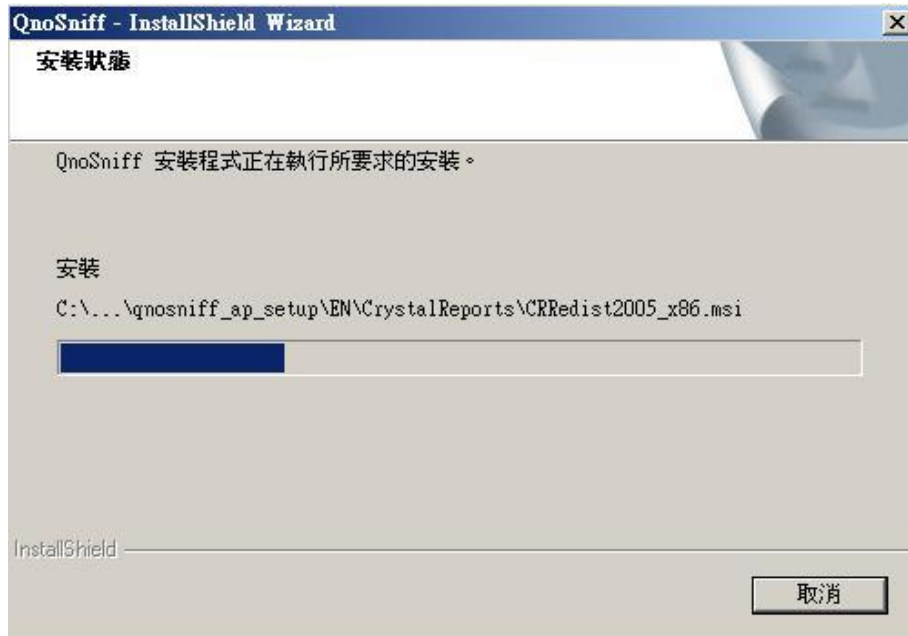
9. 【程式安裝路徑】程式預設安裝路徑為 C:\QnoSniff，您可以按下「變更」按鈕更改安裝的檔案夾路徑，完成後按「下一步」進入開始安裝頁面。



10. 【開始安裝】進入 QnoSniff Web 版本本體程式安裝程序，請按下「安裝」開始。

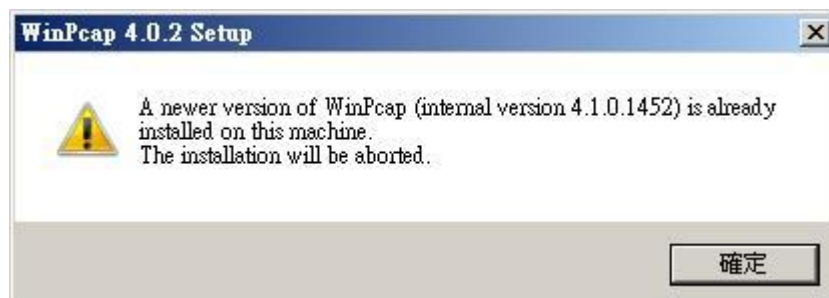


安裝程式中

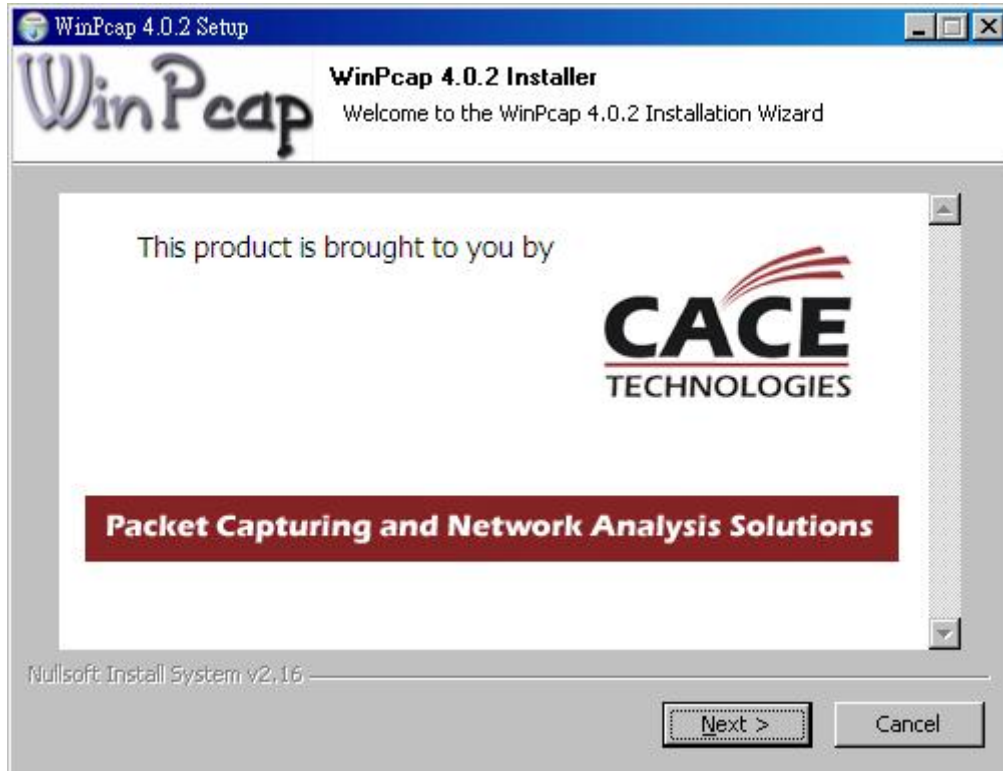


11. 【安裝 WinPcap】在以上的程序結束後，會接著安裝 WinPcap 元件，若您的 PC 上已經有安裝 WinPcap，並且比 QnoSniff 專業版安裝包內的 WinPcap 版本更新的話，會出現警告訊息表示不用再安裝並中斷

WinPcap 的安裝程序



若您的 PC 沒有安裝過 WinPcap 的話，會進行 WinPcap 的安裝程序；若您的 PC 所安裝的版本是較舊的，則安裝程序會要求您先移除舊的 WinPcap 版本在安裝較新的版本。



請按下「Next」進行 WinPcap 安裝程序



請在仔細檢視完 WinPcap 的授權合約之後，按下「I Agree」進行 WinPcap 安裝

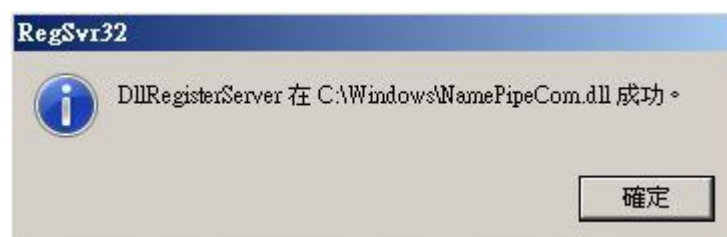


安裝結束後幾秒會出現 Completing Winpcap (安裝完成) 畫面



按下「Finish」繼續安裝其他元件

12. 【註冊 Apache 元件成功】在完成 WinPcap 安裝後，會進行 Apache 元件的註冊並跳出註冊成功訊息



請按下確定繼續其他元件的安裝程序

13. 【Apache 服務啟動】當已註冊完元件，Apahce 會啟動服務，此時若您的 PC 有開啟內建防火牆或是防毒軟體的防火牆，應該會詢問您是否需要開啟此服務可以通過防火牆，請您在此時要選擇「允許」或是「解除封鎖」，如果您的防毒軟體或防火牆已經預先將此服務阻擋，麻煩請在例外條例中開啟允許此服務啟動



14. 【安裝 .Net Framework 2.0】若您的 PC 已經有安裝.Net Framework，則安裝程序會直接跳過這一段的安裝，如果沒有，則會進行.Net Framework 2.0 的安裝

15. 【安裝 QnoSniff 專業版-本地安裝版本】接著安裝 QnoSniff 專業版 本地安裝（應用程式）的本體程式安裝



按下一步進行安裝程序



確認安裝 QnoSniff Command Console，按下一步進行



16. 【QnoSniff 本地安裝版 安裝完成】當所有安裝元件與程序完成後，會到安裝完成頁面，請按下「關閉」至結束整體安裝頁面



請按下完成離開 QnoSniff 專業版整體安裝程序。

三、啟用 QnoSniff 專業版

本章介紹如何開始啟用 QnoSniff 專業版，以及搭配路由器的相關設定。

3.1 啟用 QnoSniff 軟體之前路由器的設定

在啟用 QnoSniff 專業版軟體之前，需要與連接監控 PC 的路由器上，「啟動」QnoSniff 專業版的功能，所以請您先登入路由器的設定頁面



The screenshot shows the QnoSniff router configuration interface. The top navigation bar includes the QNO logo, a language dropdown set to '繁體中文', and a '登出' (Logout) button. The main content area is titled '廣域網狀態' (WAN Status) and contains a table with columns for WAN1, WAN2, WAN3, WAN4, and DMZ. Below this is a '寬帶埠口配置狀態' (WAN Port Configuration Status) table with columns for port numbers 1 through 15 and DMZ.

接口位置	廣域網1	廣域網2	廣域網3	廣域網4	DMZ
IP位址	61.222.81.77	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
預設閘道	61.222.81.65	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
DNS 伺服器	168.95.1.1 0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	---
連線數	32	0	0	0	0
下載頻寬使用率(%)	0	0	0	0	0
上傳頻寬使用率(%)	0	0	0	0	0
動態網域解析服務	Dyndns Disabled 3322 Disabled Dtdns Disabled Qnoddns Disabled	Dyndns Disabled 3322 Disabled Dtdns Disabled Qnoddns Disabled	Dyndns Disabled 3322 Disabled Dtdns Disabled Qnoddns Disabled	Dyndns Disabled 3322 Disabled Dtdns Disabled Qnoddns Disabled	---
QoS頻寬管理	0 條規則	0 條規則	0 條規則	0 條規則	---
手動連線		釋放 更新	釋放 更新	釋放 更新	---

埠口號	1	2	3	4	5	6	7	8
接口位置	區域網							
狀態	啟用	啟用	啟用	啟用	啟用	啟用	連線	啟用

埠口號	9	10	11	12	13	14	15	DMZ
接口位置	區域網			廣域網4	廣域網3	廣域網2	廣域網1	DMZ
狀態	啟用	啟用	啟用	啟用	啟用	啟用	連線	啟用

選擇「系統工具」=>「License Key」



License Key

系統時間： 2009-09-21 時間伺服器(NTP)位址

License Key Number : - - - -

功能名稱	試用版	正式版	註冊時間	狀態與訊息
QnoSniff	<input type="button" value="試用"/>			
Inbound Load Balance	<input type="button" value="試用"/>			

會有兩個選擇

【1】試用：

按下「試用」按鈕，會開啟為期 15 天的試用，當超過 15 天後，QnoSniff 專業版會停止運作，您無法再繼續使用，此時若您確實對 QnoSniff 專業版有所需求，就需要進行購買正式版產品金鑰 (License Key)，再輸入金鑰按下「Submit」之後，若您的金鑰是合法正確的，就能夠繼續使用 QnoSniff 專業版 (正式版)。

【2】直接購買正式版產品金鑰：

若您覺得不需要進行試用，想直接使用正式版 QnoSniff 專業版功能，就需要進行購買正式版產品金鑰 (License Key)，再輸入金鑰按下「Submit」之後，若您的金鑰是合法正確的，就能夠馬上使用 QnoSniff 專業版的正式版本。

※請注意：

- 1.開啟 QnoSniff 專業版功能試用後，不能暫停試用，試用時間會一直倒數。
- 2.若您的產品金鑰 (License Key) 輸入錯誤超過三次，License Key 的輸入頁面會整個鎖住，無法再進行任何設定與輸入動作，此時要請您與購買產品的代理商聯絡，由俠諾原廠幫忙處理。

開啟 Mirror Port 功能：

到實體埠口管理



啟用鏡像埠口(Port1) (須先確認此埠口沒有被關閉)，按下確認按鈕使設定生效

☑ 啟用鏡像埠口(Port 1)							
埠口號	接口位置	關閉	優先權	連線速率	半雙/全雙工模式	自動偵測功能	VLAN
1	LAN	<input type="checkbox"/>	Normal ▼	100M ▼	全雙 ▼	<input checked="" type="checkbox"/>	VLAN1 ▼
2	LAN	<input type="checkbox"/>	Normal ▼	100M ▼	全雙 ▼	<input checked="" type="checkbox"/>	VLAN1 ▼
3	LAN	<input type="checkbox"/>	Normal ▼	100M ▼	全雙 ▼	<input checked="" type="checkbox"/>	VLAN1 ▼

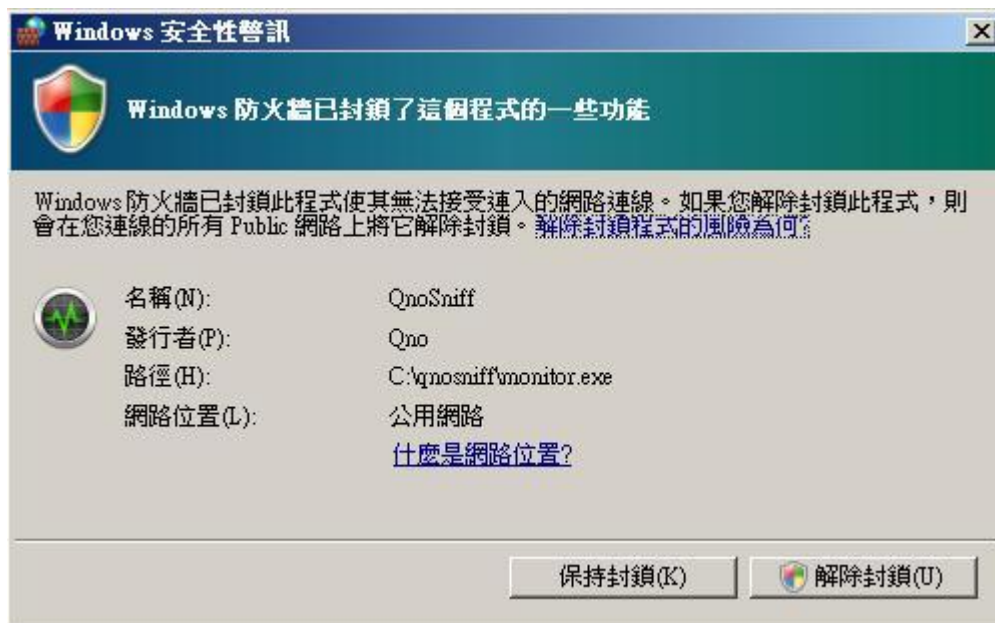
並且確定路由器的 Mirror Port 有用網路線，連接至有安裝 QnoSniff 專業版軟體的 PC 網卡

3.2 啟用 QnoSniff 專業版軟體

完成路由器啟用 QnoSniff 專業版功能動作之後，請您到安裝完 QnoSniff 專業版軟體的 PC，在桌面上會出現



QnoSniff 專業版的 Icon 圖示，請用滑鼠點選開啟



若您的防火牆或是防毒軟體有開啟，在 QnoSniff 專業版啟用時，會需要您將 QnoSniff 應用程式設定在防火牆或是防毒軟體的防火牆例外條例中（解除封鎖），QnoSniff 專業版才能夠正常連線使用。

啟用後會跳出以下登入畫面



預設的帳號是 administrator (須全部小寫)

預設的密碼是 admin (須全部小寫)

語系選擇：

繁體中文請選擇 Traditional Chinese

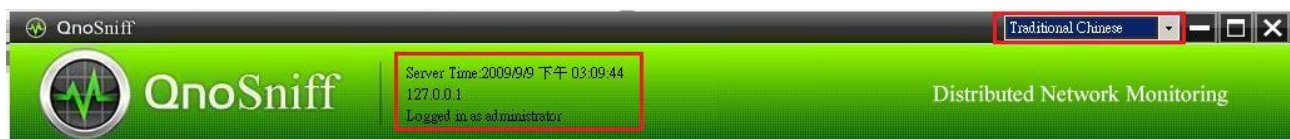
簡體中文請選擇 Simplified Chinese

英文請選擇 English

選擇完後按下確定進入 QnoSniff 專業版 AP 版主控台



左上方會有現在的系統時間、登入 IP、登入身分，右上方可以直接做語系的切換



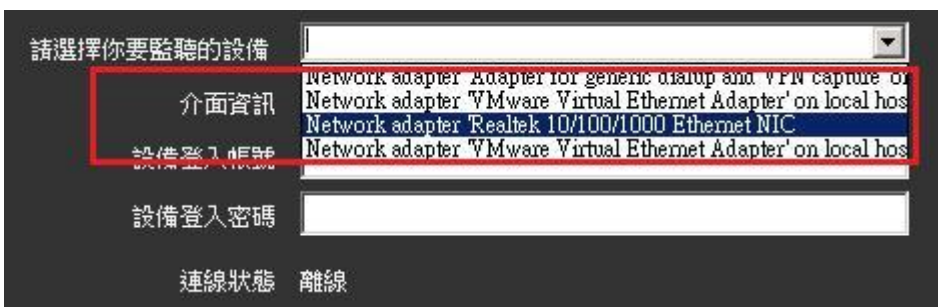
在左方選單左共有 7 個主要選單項目



要能夠正常啟用 QnoSniff 功能，須先至基本設定中進行設置



【1】 監聽來源設定：設定要進行接受監聽封包 / 流量的網卡，QnoSniff 專業版會預先抓取在您電腦上的網路介面資訊，您可以從下拉式選單中做挑選，此網卡也必須確認有用網路線連接到 路由器 Mirror Port 埠口。



【2】 選擇正確的監聽設備之後，下面的介面資訊 IP 與 MAC 會自動顯示您選擇的設備所帶的值

【3】 設備登入帳號 / 密碼：輸入您連接 PC 的前方路由器帳號密碼名稱，輸入完畢後按下儲存會進行連線作認證動作

【4】如果您按下儲存後，會跳出「操作失敗」訊息，可能會有以下原因

- 1.輸入的路由器帳號密碼錯誤，請再確認一次。
- 2.與路由器之間的網路連線可能有問題（需確認連接至 Mirror Port）。
- 3.路由器上的 QnoSniff 專業版功能並沒有正常啟動，請再依前一章節確認一次。

【5】在輸入完路由器帳號密碼按下儲存後，會進行 QnoSniff 專業版與路由器之間的連線認證，連線成功會顯示連線成功訊息，並且會顯示 QnoSniff 專業版版本為試用版還是正式版本（如下圖）。

請選擇你要監聽的設備	Network adapter 'Realtek 10/100/1000 Ethernet NIC (Microsoft's Packet Scheduler)' on local host	
介面資訊	IP 192.168.0.4	MAC 00-24-8C-BA-BA-8C
設備登入帳號	admin	
設備登入密碼	●●●●●●	
連線狀態	正式版本	

【6】遠端存取設定：QnoSniff 有提供 Web 遠端存取功能，所以若有需要用到遠端存取，必須要設定遠端存取所使用的通訊埠，系統預設為 80 Port，您可以依自己不同需求自更改，修改完後按下確認使設定生效，除了軟體本身所設定的通訊埠外，您 PC 上的防火牆與防毒軟體等，也必須將此通訊埠開放出來，才能使遠端存取生效，另外在路由器上，也必須將您指定的遠端存取通訊埠做設定，內容如下：

- 1.進入道路由器設定頁面中，並選擇「進階功能配置」=>「DMZ / 虛擬伺服器」=>「虛擬伺服器」



2.在虛擬伺服器功能中，將您已經設定成 QnoSniff 專業版遠端存取的通訊埠，指定到安裝 QnoSniff 專業版的 PC，舉例來說若您安裝 QnoSniff 軟體的 PC IP 為 192.168.1.100，遠端存取的通訊埠為 80 Port，就必須選擇通訊埠為 HTTP [TCP/80 ~ 80]，內部 IP 位址為 192.168.1.100，接口位置選擇 Any，選擇啟用後加入到對應列表，並按下確定鍵使設定生效。



虛擬伺服器

通訊埠： HTTP [TCP/80~80]

通訊埠設定

內部IP位址： 192 . 168 . 1 . 100

接口位置： ANY

啟用：

更新特殊應用程式

HTTP [TCP/80~80]->192.168.1.100->任意

刪除點選的項目

新增

※請注意！

- 1.若您所指定的遠端存取通訊埠不在路由器既定的通訊埠列表 / 下拉式選單中，您需要在通訊部設定中增加此通訊埠內容。
- 2.若您有指定要從那個 WAN IP 做遠端存取，而不是所有的 WAN，接口位置的部分就不用選擇 Any，而是選擇您所指定的 WAN IP 介面是那一一個。
- 3.若 QnoSniff 專業版的遠端存取通訊埠，已經有被路由器使用（例如路由器的遠端管理通訊埠也是 80 Port），在設定上需要把這兩個 Port 再做修改不能相同。

當您已經將遠端存取通訊埠口從軟體本身、PC 防火牆或防毒軟體、路由器都已設定完成，可以試著從遠端登入檢視 QnoSniff 專業版的 Web 介面做測試

先至路由器首頁確認您的廣域網 (WAN) IP

接口位置	廣域網1
IP位址	61.222.81.77
預設閘道	61.222.81.65
DNS 伺服器	168.95.1.1 0.0.0.0
連線數	2
下載頻寬使用率(%)	0
上傳頻寬使用率(%)	0
動態網域解析服務	Dyndns Disabled 3322 Disabled Dtdns Disabled Qnoddns Disabled
QoS頻寬管理	0 條規則
手動連線	

以上述為例，在瀏覽器的連接網址上打 <http://61.222.81.77:80> (冒號後面是所設定的遠端存取通訊埠口)

若您的設定與連線皆正常的話，一樣會跳出登入頁面



Welcome to QnoSniff

Account :

Password :

Language : --Please Select Language--

Apply Cancel

預設的帳號是 administrator (須全部小寫)

預設的密碼是 admin (須全部小寫)

語系選擇：

繁體中文請選擇 Traditional Chinese

簡體中文請選擇 Simplified Chinese

英文請選擇 English

選擇完後按下確定進入 QnoSniff 專業版 Web 版主控台



※請注意！

1.若您的虛擬伺服器設定有特別指定某一個 WAN 介面，請在輸入網址連結的時候，參照首頁該 WAN 介面的 IP 位址，若您的介面是選擇 Any，則是使用任何一個 WAN IP 皆可。

2.QnoSniff 專業版本地安裝版與 Web 版本（遠端存取版本）所表現的資料內容相同，設定部分只在基本設定上有差異如下：

本地安裝版本可以進行遠端存取埠口更改，Web 版不行

本地安裝版本可以進行資料庫硬碟儲存路徑更改，Web 版不行

本地安裝版本可以將部分資料直接轉成 PDF 檔案，Web 版不行

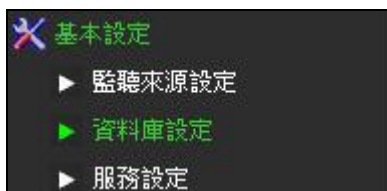
(不過 Web 版 E-mail 功能可以直接將資料轉成 PDF 檔寄送出去)。

四、基本設定

本章主要是在正常啟用 QnoSniff 軟體功能之後，對於軟體一些基本的設置包括資料庫的儲存路徑，以及儲存方式與限制條件等進行設定。

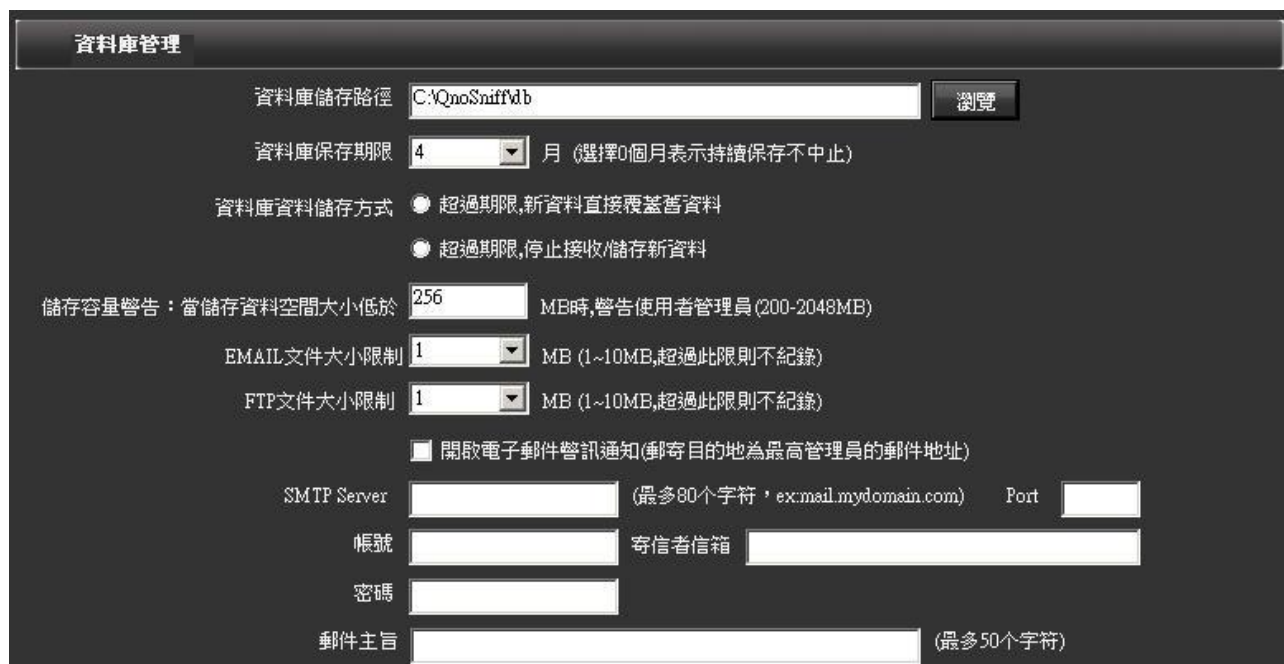
基本設定主要分成三個子功能選單：

1. 監聽來源設定
2. 資料庫設定
3. 服務設定



監聽來源設定在前一章節已經說明過，便不再重複

資料庫設定：



項目	說明
<p>資料庫儲存路徑</p>	<p>預設是在您安裝 QnoSniff 專業版軟體的硬碟分割中，若您需要變更資料庫的儲存路徑，請按下右方的「瀏覽」按鈕，在新跳出的視窗尋找合適正確的資料庫儲存路徑。</p>  <p>※資料庫大小會因為隨著時間一直累積資料量而增大，所以請特別注意您的硬碟盛餘空間的使用狀況</p>
<p>資料庫保存期限</p>	<p>設定資料庫的資料儲存動作期限 1 至 6 個月，超過此期限，可以選擇以下兩種處理方式</p> <ol style="list-style-type: none"> <li data-bbox="469 1637 884 1682"> <input checked="" type="radio"/> 超過期限,新資料直接覆蓋舊資料 <p>當超過限制的時間條件時，新的資料會從最舊的資料陸續把舊資料覆蓋掉，舊資料不會保存，占用硬碟空間也不會再持續變大。</p> <li data-bbox="469 1872 884 1917"> <input checked="" type="radio"/> 超過期限,停止接收/儲存新資料 <p>當超過限制的時間條件時，會停止接收、儲存新資料，舊的資料不會被刪除，但是</p>

	<p>也不會有新的資料產生，並須將期限做調整或是重置計算期限時間，才能夠再開始收集新資料與儲存新資料</p> <p>3. (選擇0個月表示持續保存不中止)</p> <p>若您不想中斷資料持續儲存，也不想刪除舊資料，在選擇時間期限時就必須要選擇成「0 個月」表示持續保存資料不中斷</p>
<p>儲存容量警告</p>	<p>1.硬碟剩餘儲存空間大小偵測與預警：</p> <p>設定當儲存資料庫的該硬碟剩餘空間低於___MB 時 (200~2048MB)，警告使用者管理員</p> <p>2.E-mail 文件大小限制：為避免過多的 E-mail 資料儲存迅速佔用甚至浪費硬碟空間，可設定 E-mail 記錄大小 1~10 MB 的限制，若 E-mail 整體大小 (包含附件) 超過所設定限制，該封 E-mail 的紀錄仍然會保留，但是由於最多就只有保留您所設定的大小，所以可能會產生附件檔案超過的部分被截取掉，導致無法正常開啟檔案的現象，但是檔案名稱的紀錄還是會保留住。</p> <p>3.FTP 文件大小限制：為避免過大的 FTP 文件資料儲存迅速佔用甚至浪費硬碟空間，可設定 FTP 傳輸文件大小 1~10MB 的限制，若 FTP 文件大小 (不論上傳下載) 超過所設定限制，該筆 FTP 傳輸記錄仍然會保留，但是由於最多就只有保留您所設定的大小，所以可能會產生附件檔案超過的部分被截取掉，導致無法正常開啟檔案的現象，但是檔案名稱的紀錄還是會保留住。</p>
<p>開啟電子郵件警訊通知：</p>	<p>啟用此功能之後，當資料儲存剩餘空間低於您所設定的大小，系統就會發送 E-mail 電子郵件通知您，提醒您的剩餘儲存空間已經低於您所設定的警戒值；另外之後在每個頁面上的 E-mail 資料報表功能，也必須透過此 SMTP Server 轉發信件，所以若您沒有正確設定 SMTP Server 內容，E-mail 資料報表功能無法正常。</p> <p>SMTP Server：請填入 SMTP 伺服器的網域名稱 (例：ms12.hinet.net)</p> <p>Port：發送電子郵件所使用的通訊 Port (例：25)</p>

	<p>帳號 : 發送電子郵件的帳號 (例 : tony.chen)</p> <p>密碼 : 發送電子郵件所使用的密碼</p> <p>寄信者信箱 : 發送電子郵件所使用的電子郵件信箱 (例 : tony.chen@ms12.hinet.net)</p> <p>郵件主旨 : 所發送電子郵件的主旨</p>
--	--

服務設定：針對 Http (網頁訪問) 紀錄的模式，與所需進行 QQ IM 通訊監控的帳號進行設置。

HTTP 特定網站設定，需要詳細記錄的網站與 IP：

QnoSniff 專業版針對於 HTTP / 網頁 / 網站訪問的記錄，預設只會記錄在主要網域 (Domain) 「/」以前的網址，例如 <http://tw.yahoo.com/>，若有去其他子頁的記錄，則不會顯示出來，也會記錄成 tw.yahoo.com

除非是把您需要特別將整個網站連結的細節都記錄下來的網站名稱，加入到「需要詳細記錄的網站 / IP」，才會將完整的網址細節連結記錄下來，例如

<http://tw.news.yahoo.com/article/url/d/a/090911/17/1qwgx.html>。

將想詳細記錄網址的主要網域名稱輸入網站/IP 空白欄位中，按下「新增」按鈕，並按下「儲存」後才會生效。



IM QQ 號碼設定：



IM:QQ號碼設定

QQ號碼

QQ密碼

使用者名稱 (限20個字元以內)

跳到 頁 每頁顯示 筆

編號	使用者名稱	QQ號碼	編輯
----	-------	------	----

QnoSniff 專業版針對 IM 類別中的 QQ 監控，「必須」要將須監控的 QQ 帳號與密碼收集起來並且輸入，才能進行監控與記錄 QQ 活動。

將想監控的 QQ 帳號、密碼以及識別此帳號的使用者名稱輸入在相對應的空白欄位中，按下「新增」按鈕，並按下「儲存」後才會生效。

例如想要監控的 QQ 帳號是 12355639，12355639 此帳號的密碼是 34568989，使用者識別為 Sales1，就依序填入空白欄位中，按下「新增」按鈕，並按下「儲存」後才會生效。

五、系統權限管理

本章介紹 QnoSniff 專業版系統管者與系統使用者登入帳號的權限與系統相關操作的日誌記錄。

5.1 觀看許可權

觀看許可權主要在設置某一個「帳號身分」在登入 QnoSniff 專業版系統之後，是否能觀看甚至編輯各類通訊協定所記錄的資料與統計圖表。

系統權限管理

觀看許可權

帳號身分:

通訊協定	HTTP	Email	IM	FTP	P2P	Telnet	統計圖表
權限設定	無權限	無權限	無權限	無權限	無權限	無權限	無權限

新增 取消

帳號身分	觀看權限	編輯權限	成員個數	編輯
administrators		CHART,TELNET,P2P,IM,HTTP,EMAIL,FTP	1	
admin		CHART,TELNET,P2P,IM,HTTP,EMAIL,FTP	1	修改
user		CHART,TELNET,P2P,IM,HTTP,EMAIL,FTP	0	修改
defineuser		CHART,TELNET,P2P,IM,HTTP,EMAIL,FTP	0	修改 刪除

帳號身分：

此空白欄位請輸入您預歸類為某類帳號身分的命名，例如 Common User，administrator 帳號身分為最高權限管理者與使用者，預設是對所有通訊協定類別以及統計圖表等資料皆有觀看及編輯權限，並且無法進行修改與刪除。

請注意，系統的權限有五種，由高到低為：administrator、admin、user、defineuser 和自定義用戶。新增的身份帳號都為自定義用戶，

權限比其他四種低。修改帳號身份時，使用者只能修改自己的，以及比自己權限低的身身份帳號。

通訊協定：

由於 QnoSniff 專業版的記錄資料最主要是以通訊協定為主，所以是以各類通訊協定所記錄的資料，各別進行觀看與編輯的權限設定，以及最後的統計圖表等。

※請注意！

這邊設定各類通訊協定的觀看與編輯權限，是在摘要訊息內的限制(該類通訊協定細部列表)，在統計圖表中，也會有各位通訊協定的分類，但是目前並無法從中再做權限設定，只是針對「所有的」統計資料及圖表做觀看或編輯的限制設定。

權限設定：

對每一個通訊協定項目與統計圖表的存取權限設定

無權限－代表不能觀看與不能編輯，該類用戶登入後該選項會消失

觀看權限－代表僅能觀看該項訊息資料內容，無法進行資料刪除修改

並且只能無法使用郵寄、PDF 按鈕功能

編輯權限－代表可以對該項訊息資料觀看、刪除與使用郵寄與 PDF 功能

新增：

輸入完帳號內容後按下新增，會跳出「新增使用者成功」，並將該筆資料增加至下方列表

修改：

若您需要進行修改已有的帳號內容，請按下下方列表中該筆資料右方的「修改」按鈕，該筆資料會內容會出現在上方各個對應欄位內，您就可以依此進行修改，修改完成後請按下「修改」按鈕(原本新增按鈕在修改狀態下會變成修改)，系統會詢問您是否確認修改該筆資料，再按下是修改資料動作即完成。

取消：

取消會將您正在設定帳號過程中已輸入的資料清空，或是取消修改動作。

5.2 使用者管理

當您設定完您想分類的帳號身分類別後，就要在每個身分類別下增加帳號，所以在「觀看許可權」所設定的帳號身分是一種在權限邏輯上的帳號分類，至於在「使用者管理」所設定的帳號，則是登入系統所使用的真實帳號、密碼以及該帳號的使用語系等設定，同樣地，根據使用者登錄帳號身份的不同，使用者只能修改自己的，以及新增或修改比自己權限低的帳號身份。最高管理員 administrator 可以增加 administrator 身份的帳號，其他非 administrator 身份的用戶則不能做此操作。

使用者管理

帳號

密碼

重新輸入密碼

身份

電子郵件

顯示語言

帳號	身份	電子郵件	顯示語言	編輯	
administrator	administrators	May_Zhou@email.LingAn.co...	Traditional Chinese	修改	
admin	admin	admin@yahoo.com.cn	Simplified Chinese	修改	刪除
abc	test	abc@com.jp	Traditional Chinese	修改	刪除

帳號： 輸入登入的帳號名稱

密碼： 輸入此帳號登入的密碼

重新輸入密碼： 須再輸入相同密碼再確認一次

身分： 從下拉式選單中挑選屬於何種身分帳號，預設會有 administrator、admin、user、defineuser，您所新增或修改的身分帳號也會出現在下拉式選單中提供選擇。

- 電子郵件： 輸入該帳號的電子郵件信箱內容，在使用者使用「郵寄」功能時，資料會寄到所設定電子郵件信箱當中。
- 顯示語言： 設定此用戶在登入頁面後，預設的系統顯是語系為繁中、簡中或英文。
- 新增： 輸入完帳號內容後按下新增，會跳出「新增使用者成功」，並將該筆資料增加至下方列表
- 修改： 若您需要進行修改已有的帳號內容，請按下下方列表中該筆資料右方的「修改」按鈕，該筆資料會內容會出現在上方各個對應欄位內，您就可以依此進行修改，修改完成後請按下「修改」按鈕（原本新增按鈕在修改狀態下會變成修改），系統會詢問您是否確認修改該筆資料，再按下是修改資料動作即完成。
- 取消： 取消會將您正在設定帳號過程中已輸入的資料清空，或是取消修改動作。

※請注意！

administrator 與 admin 身分帳號在預設的時候，系統會各別預先設定一個「administrator」與「admin」的「登入帳號」，而且這兩個帳號下的電子郵件信箱（E-mail）預設也是虛擬、不正確的，請您務必記得修改成該帳號所對應的正確電子郵件信箱內容，資料列表的 E-mail 功能才能將報表檔案，正確發送至您所設定的電子郵件信箱。

5.3 使用者日誌

使用者日誌會顯示所有使用者登入、登出、編輯與修改資料等資訊，QnoSniff 專業版只有 administrator 與 admin 兩種身分帳號的使用者，登入後才會看到使用者日誌列表，其他的身分帳號得使用者是看不到的。

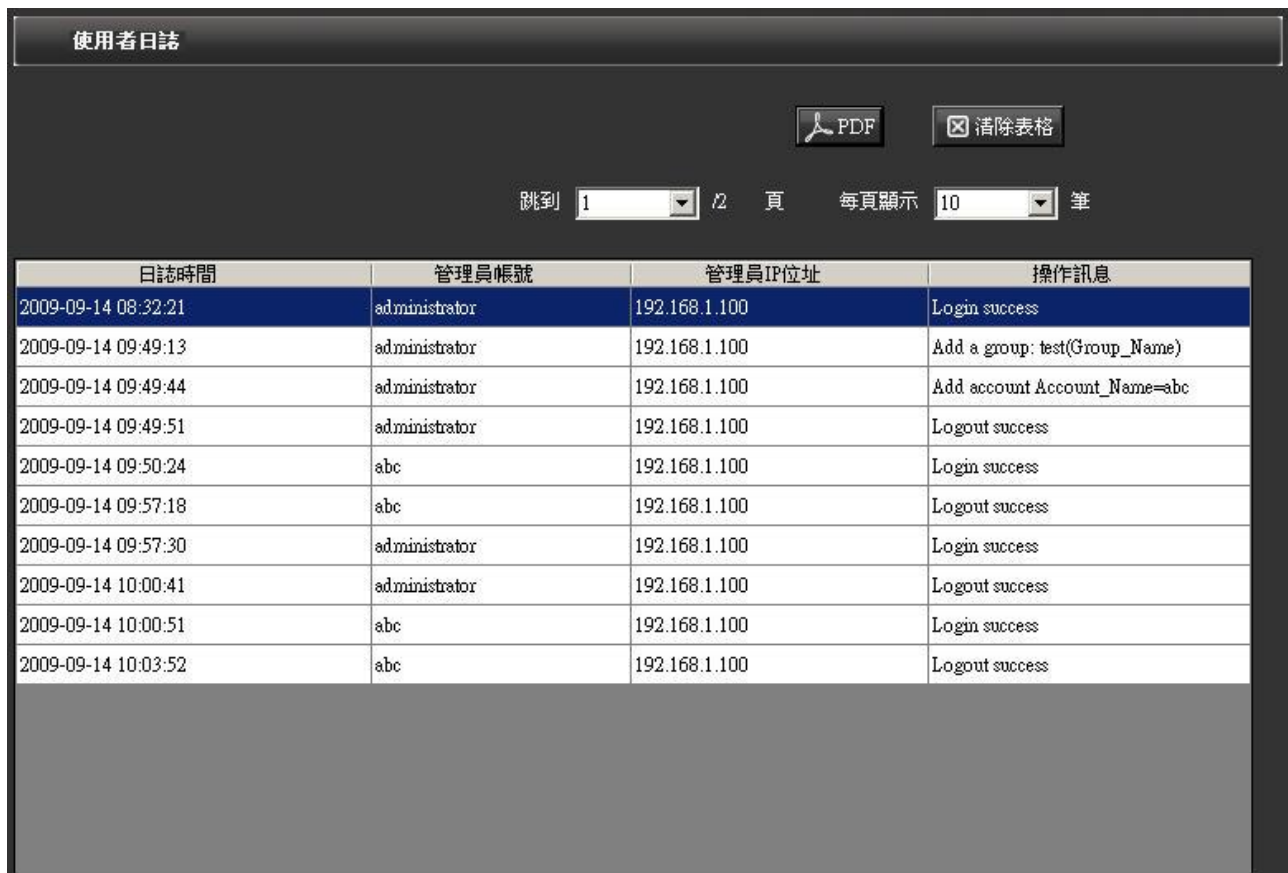
PDF：

若有需要將日誌轉換成 PDF 檔做保存或參考，請按下 PDF 按鈕做匯出動作

清除表格：

若記錄已經過多並且多半是舊有記錄不需再保留，可以按下清除表格按鈕清除所有日誌記錄

每頁顯示___筆，跳到___頁：可以自定義日誌列表一頁可顯示幾筆資料，並可以直接跳到另外一頁

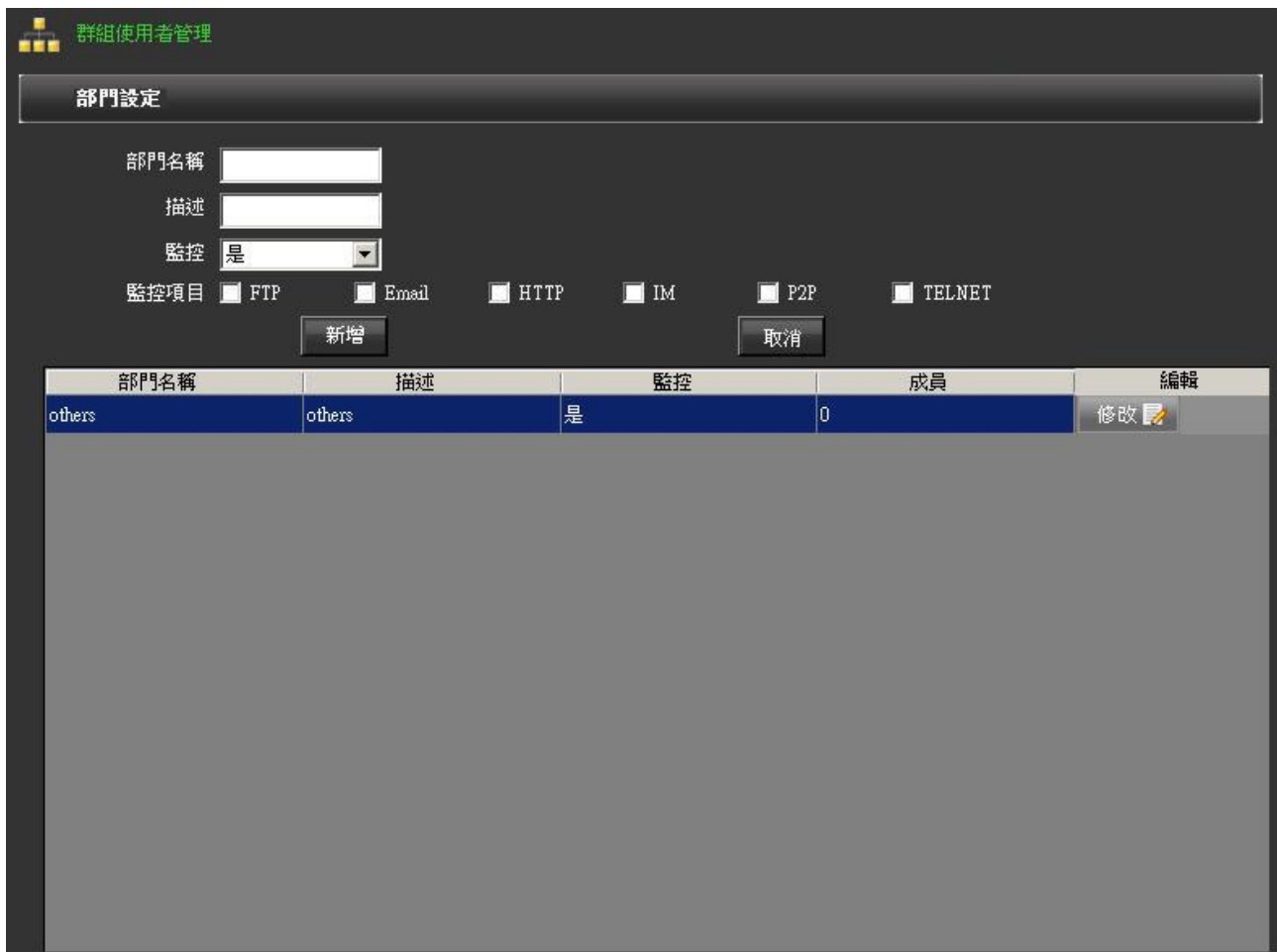


日誌時間	管理員帳號	管理員IP位址	操作訊息
2009-09-14 08:32:21	administrator	192.168.1.100	Login success
2009-09-14 09:49:13	administrator	192.168.1.100	Add a group: test(Group_Name)
2009-09-14 09:49:44	administrator	192.168.1.100	Add account Account_Name=abc
2009-09-14 09:49:51	administrator	192.168.1.100	Logout success
2009-09-14 09:50:24	abc	192.168.1.100	Login success
2009-09-14 09:57:18	abc	192.168.1.100	Logout success
2009-09-14 09:57:30	administrator	192.168.1.100	Login success
2009-09-14 10:00:41	administrator	192.168.1.100	Logout success
2009-09-14 10:00:51	abc	192.168.1.100	Login success
2009-09-14 10:03:52	abc	192.168.1.100	Logout success

六、群組使用者管理

本章節講述 QnoSniff 專業版中的群組架構設定，使用群組的好處是方便統一管理，該群組下的成員不需一一進行設置與調整，可以將設定一次套用該群組所有成員，並且您可以依網路真實的使用狀況進行群組劃分，使 QnoSniff 專業版所記錄分析的資料，更符合您內網用戶的網路使用現況。

6.1 部門設定



群組使用者管理


部門設定

部門名稱

描述

監控

監控項目 FTP Email HTTP IM P2P TELNET

部門名稱	描述	監控	成員	編輯
others	others	是	0	修改 

- 部門名稱： 將您預分類出來的部門命名名稱，例如 Sales、RD。
- 描述： 針對該部門做簡單的註釋與敘述以識別。
- 監控： 選擇是否針對此部門進行監控記錄。

- 監控項目：** 選擇該部門會受 QnoSniff 專業版監控並記錄的通訊協定類別，若您的某些部門是不方便進行監控或具機密性質的，例如總經理或董事長的 E-mail 或 IM 即時通訊，您就可以在此做不監控的選擇設定。
- 新增：** 輸入完帳號內容後按下新增，會跳出「新增使用者成功」，並將該筆資料增加至下方列表
- 修改：** 若您需要進行修改已有的帳號內容，請按下下方列表中該筆資料右方的「修改」按鈕，該筆資料會內容會出現在上方各個對應欄位內，您就可以依此進行修改，修改完成後請按下「修改」按鈕（原本新增按鈕在修改狀態下會變成修改），系統會詢問您是否確認修改該筆資料，再按下是修改資料動作即完成。
- 取消：** 取消會將您正在設定帳號過程中已輸入的資料清空，或是取消修改動作。

6.2 用戶樹狀列表

用戶樹狀列表是用來便於展開您所設定的所有群組與使用者，QnoSniff 專業版必須要將受監控的用戶加入樹狀列表與其下方的用戶列表才有辦法進行監控動作。



編號	部門名稱	監控	開始監控時間	IP地址	MAC位址	用戶名稱	電腦名稱/MAC位址	編輯
----	------	----	--------	------	-------	------	------------	----

用戶名稱： 輸入用戶的名稱，例如 SalesPC1。

IP 地址： 輸入用戶的 IP 位址，例如 192.168.3.100。

MAC 位址： 可以手動輸入，也可以用下拉式選單選擇自動學習到的 IP。

MAC 位址： 輸入用戶的 MAC 位址，例如 00-1A-B6-02-3F-9A。(請注意格式必須以“-”相隔)

部門名稱： 從下拉式選單中挑選您已經設定完成並且欲加入的群組。

監控： 針對此單一用戶是否進行監控。

請注意，即使該用戶所歸屬的群組已經納入要監控範圍，但是在單一用戶的監控選項是選擇「否」（不監控），則此單一用戶就不會納入監控範圍，監控的動作選項會以單一用戶的選擇決定。

IP-MAC 學習： 若您的手邊已經有建立好的內網用戶對照表，自然可以一一將這些資料依序輸入，但是這仍然會花費不少時間，QnoSniff 專業版有提供一個更方便的工具讓您使用，就是 IP-MAC 自動學習。

當您按下 IP-MAC 學習按鈕後，會跳出另一個視窗畫面，是 QnoSniff 專業版幫您學習到的內網用戶資料，包含電腦名稱（如果沒有學習到電腦名稱會顯示 MAC）、IP 位址、MAC 位址，用戶名稱是您可以自己填寫的，部門則是用下拉式選從現有設定好的部門群組做選擇，最後選擇該用戶是否監控，當列表的用戶都設定好之後，就可以勾選「全選」並按下「保存」，就可以一次就將眾多的內網用戶分好群組、設定是否監控、以及用戶名稱等設定完成，相較於一個個輸入會方便許多。

若您的發覺某些用戶資料，在進入視窗畫面當時並沒有學習到，您可以再按下「重新整理」按鈕來更新學習到用戶列表內容。

※請注意！

已經設定好並加入用戶以及樹狀列表的用戶，不會再出現在 IP-MAC 學習清單當中，若您的用戶在設定加入列表完成後更改 IP，則已經設定好資料仍然會以原本的 MAC 為主，並自動更新成目前最新的 IP 位址為該用戶的 IP 資料。



全選 <input type="checkbox"/>	編號	電腦名稱/MAC位址	IP地址	MAC位址	用戶名稱	部門名稱	監控
<input type="checkbox"/>	1	00-00-00-00-00-10	192.168.1.186	00-00-00-00-00-10		others	是
<input type="checkbox"/>	2	00-00-39-83-C8-D7	192.168.0.134	00-00-39-83-C8-D7		others	是
<input type="checkbox"/>	3	00-00-6C-6A-E4-A0	192.168.2.186	00-00-6C-6A-E4-A0		others	是
<input type="checkbox"/>	4	00-00-6C-8B-DB-99	192.168.2.182	00-00-6C-8B-DB-99		others	是
<input type="checkbox"/>	5	00-00-74-65-4B-E3	192.168.0.123	00-00-74-65-4B-E3		others	是
<input type="checkbox"/>	6	00-00-E8-7C-89-42	192.168.0.163	00-00-E8-7C-89-42		others	是
<input type="checkbox"/>	7	00-01-29-4C-16-E5	192.168.2.180	00-01-29-4C-16-E5		others	是
<input type="checkbox"/>	8	00-01-4A-CC-1C-FF	192.168.2.92	00-01-4A-CC-1C-FF		others	是
<input type="checkbox"/>	9	00-02-3F-0A-D5-34	192.168.2.118	00-02-3F-0A-D5-34		others	是
<input type="checkbox"/>	10	00-02-DD-50-E1-28	192.168.2.160	00-02-DD-50-E1-28		others	是
<input type="checkbox"/>	11	00-03-93-AC-35-DC	192.168.1.216	00-03-93-AC-35-DC		others	是
<input type="checkbox"/>	12	00-04-61-4A-87-87	192.168.2.110	00-04-61-4A-87-87		others	是
<input type="checkbox"/>	13	00-05-5D-69-6B-6E	192.168.0.237	00-05-5D-69-6B-6E		others	是
<input type="checkbox"/>	14	00-08-54-A7-05-91	192.168.0.9	00-08-54-A7-05-91		others	是
<input type="checkbox"/>	15	00-08-A1-8D-0D-B9	192.168.2.108	00-08-A1-8D-0D-B9		others	是
<input type="checkbox"/>	16	00-09-6B-47-72-48	192.168.1.214	00-09-6B-47-72-48		others	是
<input type="checkbox"/>	17	00-0A-48-05-7D-E6	192.168.2.124	00-0A-48-05-7D-E6		others	是
<input type="checkbox"/>	18	00-0A-48-13-95-44	192.168.2.10	00-0A-48-13-95-44		others	是
<input type="checkbox"/>	19	00-0A-79-BD-96-4C	192.168.0.198	00-0A-79-BD-96-4C		others	是
<input type="checkbox"/>	20	00-0A-79-F5-3C-25	192.168.2.179	00-0A-79-F5-3C-25		others	是
<input type="checkbox"/>	21	00-0A-E4-0B-76-49	192.168.1.175	00-0A-E4-0B-76-49		others	是

完成加入的用戶列表

※請注意！

IP-MAC 自動學習方法，是當按下 IP-MAC 學習按鈕，會針對內網 LAN 端所有子網 (Subnet) 用戶電腦發出 ARP 詢問並且進行學習，所以若您的內網 PC 若是放在防火牆裡面，很有可能會學習不到該用戶資料。

用戶樹狀列表

組部門

- others (1)
 - test001
- Sales1 (1)
 - test002

用戶名稱:

IP地址:

MAC位址:

部門名稱:

監控:

編號	部門名稱	監控	開始監控時間	IP地址	MAC位址	用戶名稱	電腦名稱 /MAC位址	編輯	
1	others	是	2009-09-14 13:28:40	192.168.14.1	00-AA-AB-A...	test001	test001	修改	刪除
2	Sales1	是	2009-09-14 13:30:48	192.168.14.3	00-AB-CC-D...	test002	test002	修改	刪除

※用戶成功加入列表的時間，並且必須選擇監控選項為「是」的時間，就是開始監控時間。

七、系統資源分析

本章節是介紹以 QnoSniff 專業版，抓取監控 PC 所連接路由器的路由器系統資訊，其中包括路由器的 CPU 使用率、記憶體 (Memory) 使用率、以及每個廣域網 (WAN) 的上傳及下載流量。

7.1 CPU 使用記錄

不論是路由器的 CPU 使用記錄，還是記憶體使用率或廣域網 (WAN) 的流量，QnoSniff 專業版要能正常抓到正確的數值，必須確認路由器有開啟 SNMP 功能，所以先進入路由器的管理頁面「系統工具」=>「SNMP 網路管理」，確認有將 SNMP 網路管理功能啟用。



SNMP網路管理

啟用

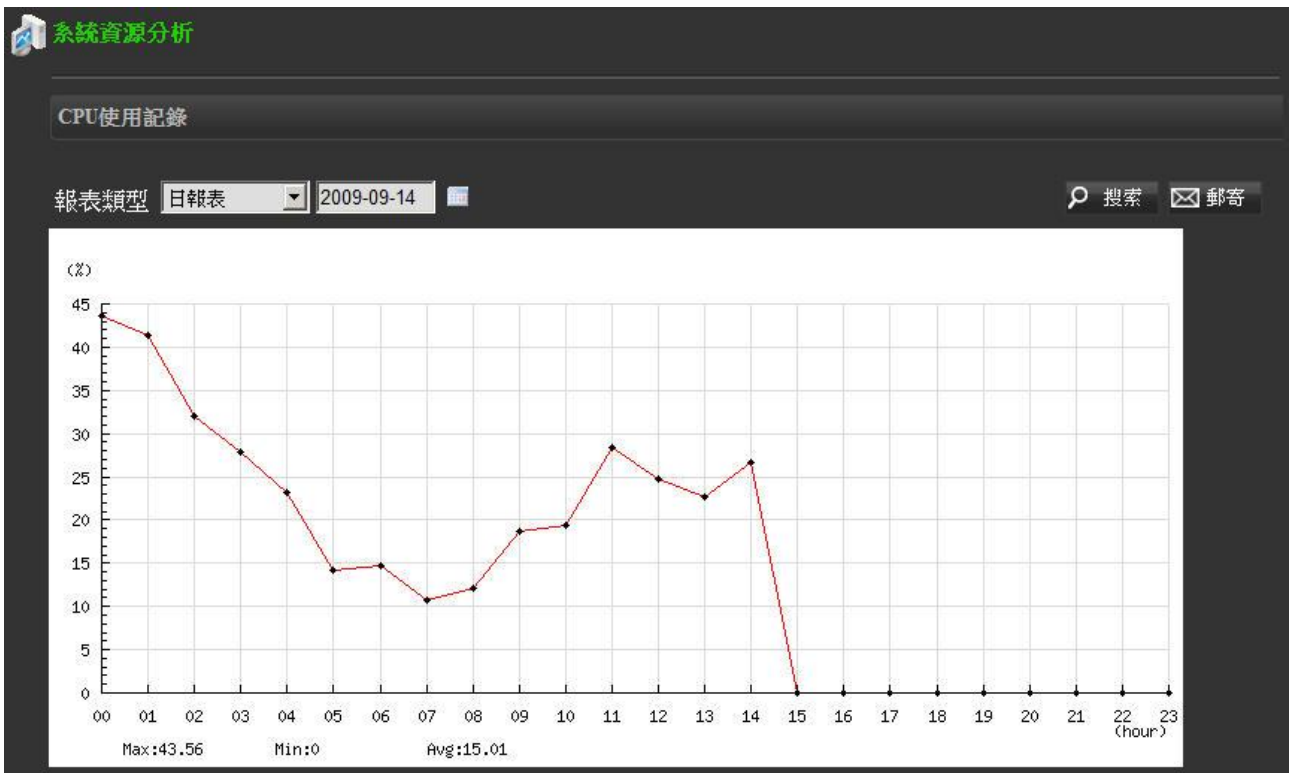
系統名稱:	<input type="text" value="8_WAN_QVM_Router"/>
連絡方式:	<input type="text"/>
系統地址:	<input type="text"/>
Get Community Name:	<input type="text" value="public"/>
Set Community Name:	<input type="text" value="private"/>
Trap Community Name:	<input type="text" value="public"/>
Send SNMP Trap to:	<input type="text"/>

回到 QnoSniff 專業版系統資源分析的 CPU 使用記錄頁面，左方的時間選擇會有日報表、週報表、月報表



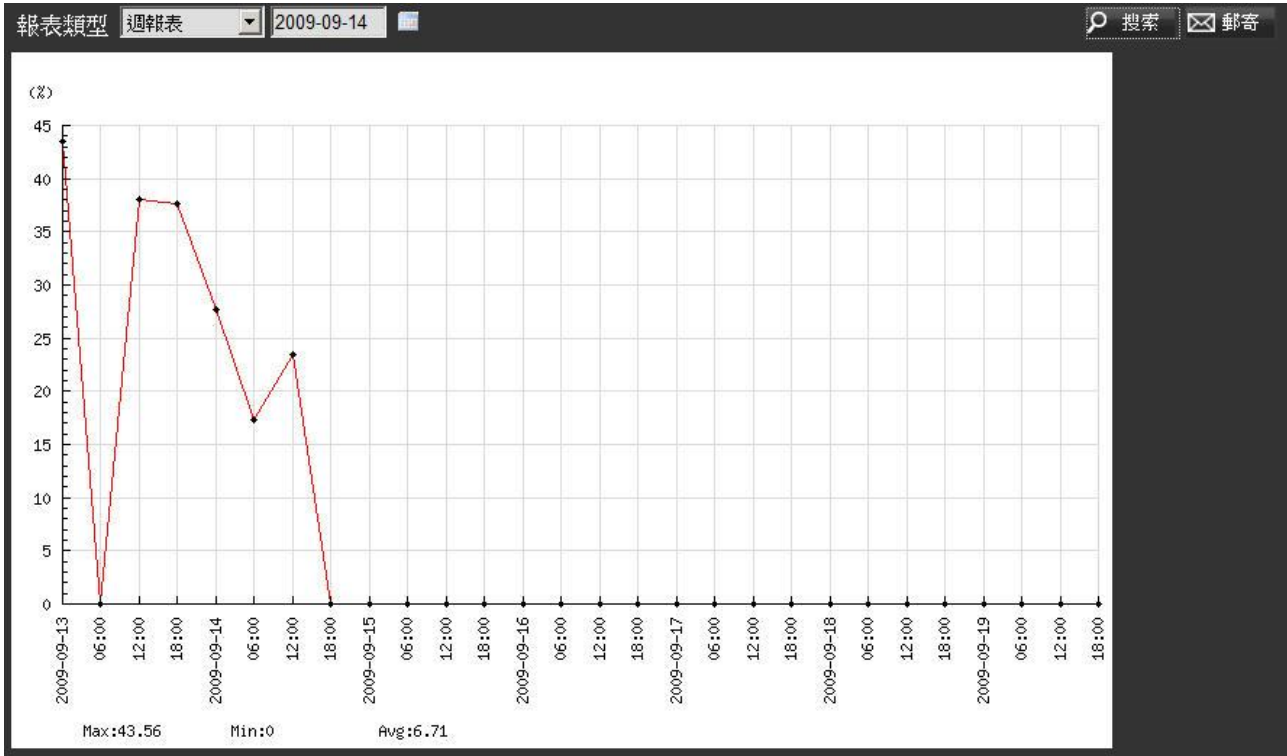
及自訂日期，右方有電子月曆可以直接點選，出現的圖表除了折線圖外，還會在圖表下方顯示這段時間內的最大值、最小值、平均值，另外報表與月曆點選的時間關係如下：

【1】 選擇日報表：月曆日期選擇到那一天，就是指那一天的 CPU 使用率狀況 (0 ~ 24 小時)，例如選擇到 2009/9/14，就表示資料圖示是顯示 2009/9/14 當天的 CPU 使用記錄



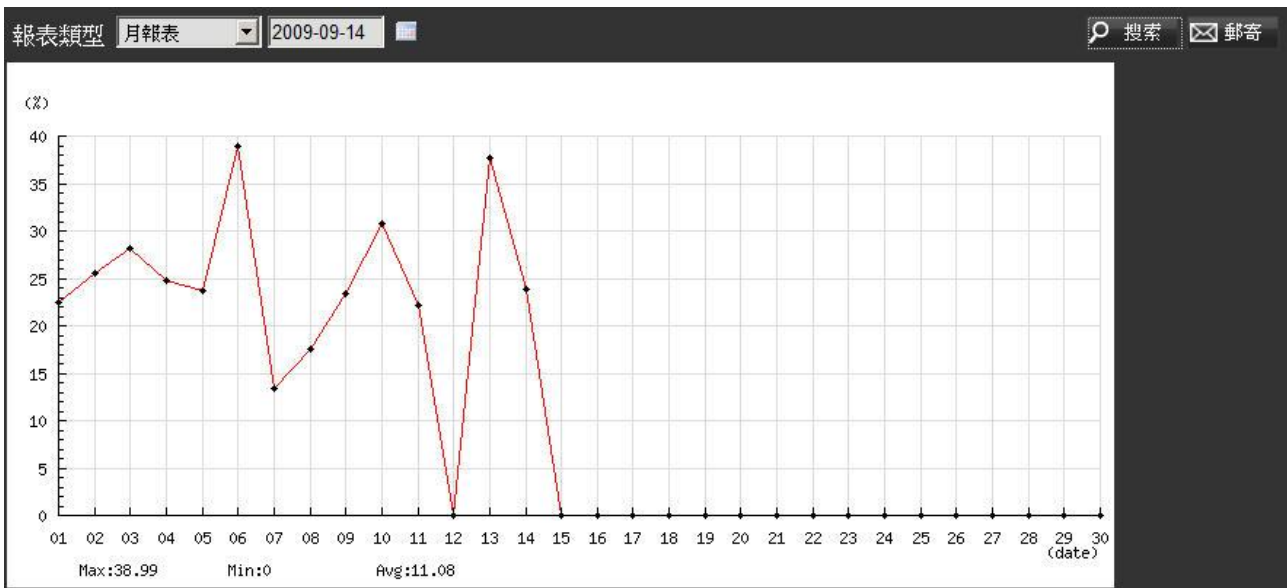
【2】 選擇週報表：月曆日期選擇到那一天，就是指那一天所在的那週 CPU 使用率狀況，例如選擇

到 2009/9/14，就表示資料圖示是顯示 2009/9/14 到 2009/9/20 這一週的 CPU 使用記錄

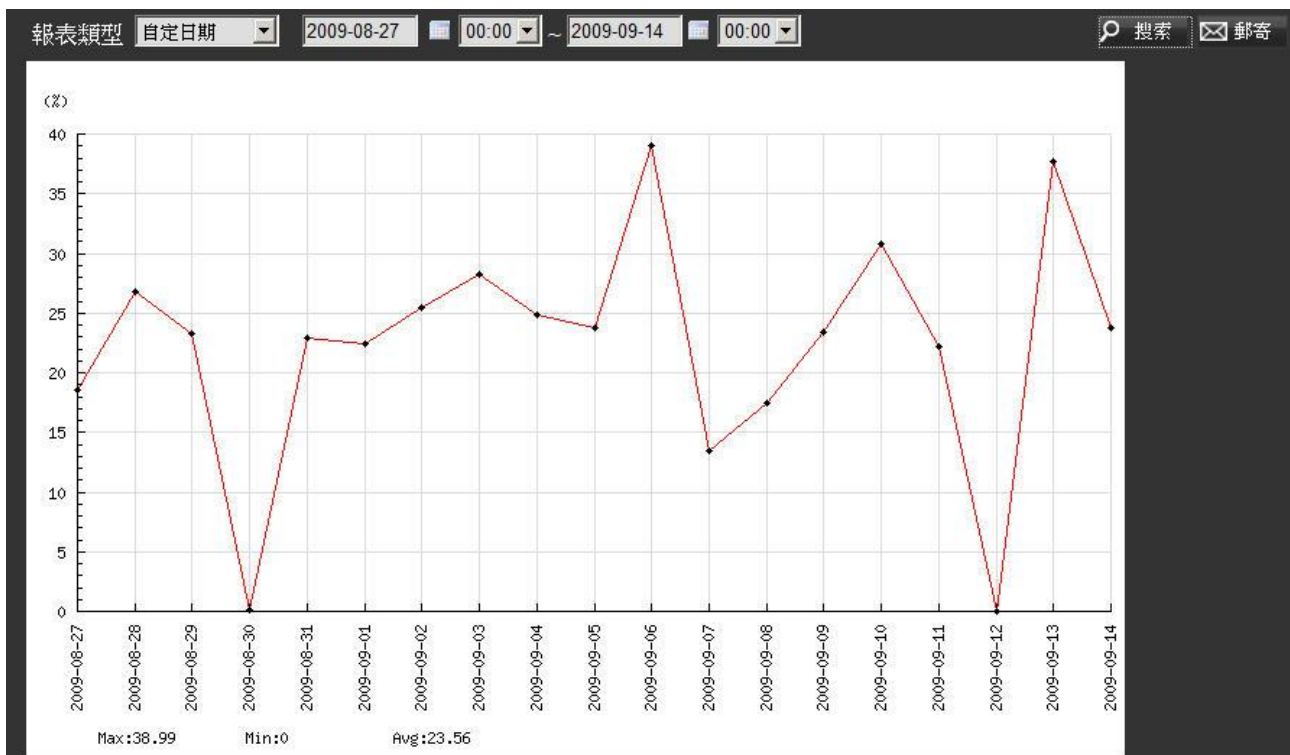


【3】 選擇月報表：月曆日期選擇到那一天，就是指那一天所在的那一個月 CPU 使用率狀況，例如選擇

到 2009/9/14，就表示資料圖示是顯示 2009 年 9 月份整個月的 CPU 使用記錄



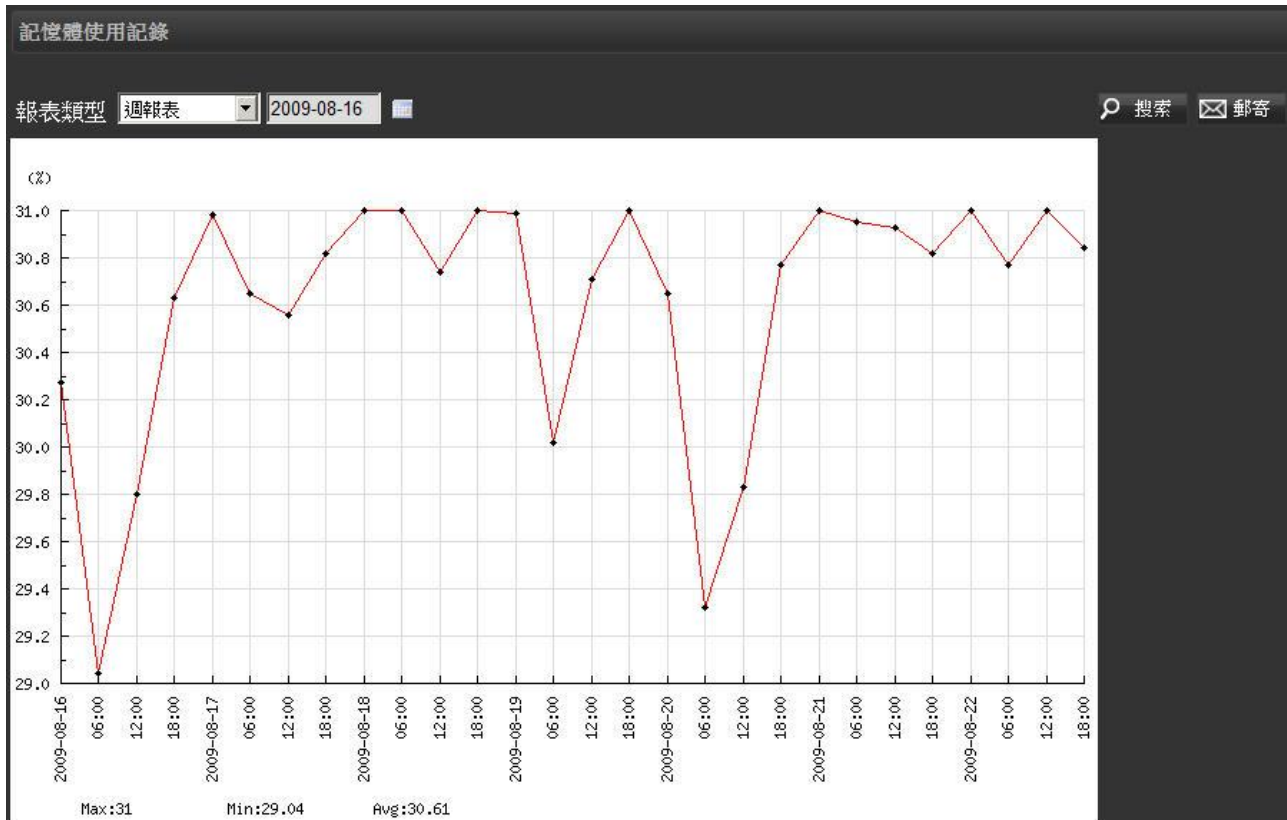
【4】選擇自訂日期：可以跨月自己選擇一段時間做資料查詢，當選擇到這個選項時，會跳出兩個月曆以及 24 小時制時間，時間間隔最多不能超過 32 天，並且由於是自定義查詢條件（非預設值），所以在呈現資料的時間上會相對比較久。



請注意：以上查詢時間區段確認後，請記得按下「搜索」按鈕，因為該畫面數據資料只會在從別的頁面首次跳到此頁時會更新，當您查詢的時間區段有變異，麻煩請再按下「搜索」按鈕以讓資料可以更新到符合您新定義的時間區段，另外本地安裝版會有 PDF 與郵寄功能，Web 版會有郵寄功能，有需要亦可善加利用。

7.2 記憶體 (Memory) 使用記錄

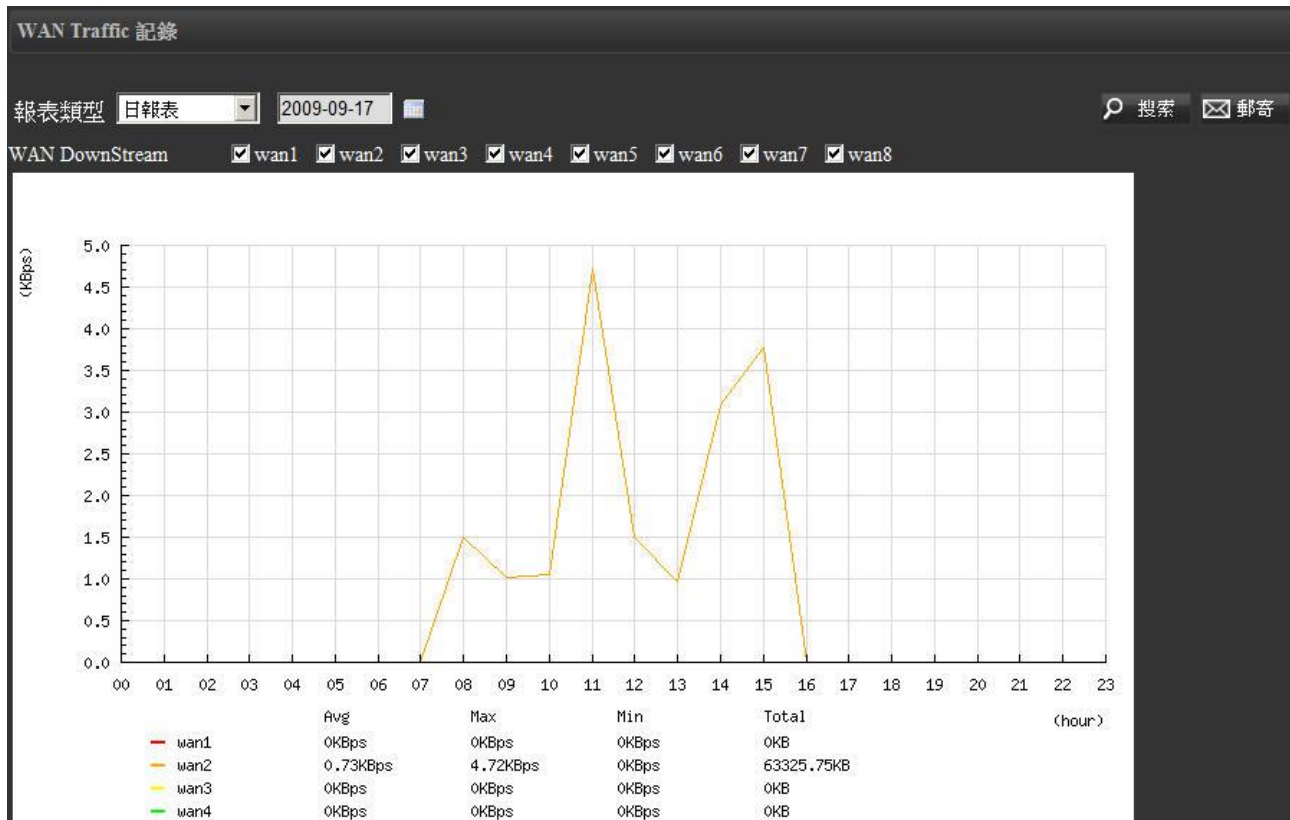
這部分的列表圖示，是指路由器的系統記憶體使用狀況，是以使用了多少百分比來顯示。



時間區段的選擇與上述 CPU 使用記錄的方式相同，您可以依您的需要切換不同時間區段，來檢視不同時間區段的路由器系統記憶體使用狀況。

7.3 WAN Traffic(廣域網流量) 記錄

WAN 的流量有分 Upstream (上傳) 與 Downstream (下載)，您可以選擇您想觀察的某個 WAN 埠口，進行流量使用狀況顯示。



最下方仍然會出現您所選擇 WAN 口的流量平均值、最大值、最小值數據 (在您所定義的時間區段之內)。

八、摘要訊息

接下來進入 QnoSniff 專業版的核心功能－各類通訊協定流量監控與記錄。

QnoSniff 專業版目前可監控的通訊協定最主要分為以下幾大類：

- (1) 網頁瀏覽 (HTTP)
- (2) 電子郵件 (SMTP 與 POP3)
- (3) 檔案傳輸 (FTP)
- (4) 點對點下載 (P2P)
- (5) TELNET
- (6) 即時通訊 (IM)

針對不同的服務與流量內容各別進行監控與記錄，接下來我們來一一介紹。

8.1 即時服務總表

即時服務總表用途，是用來顯示在您瀏覽當天，內網所有用戶的網路流量狀況，所以資料量的累積只有一天，當您在隔天登入檢視此頁，所檢視的就是隔天的內網用戶使用狀況。

部門選擇
Total

跳到 1 / 23頁 每頁顯示 10 筆 重新整理 郵寄

序號	用戶名	電腦名稱/MAC位址	部門名稱	聊天紀錄	網頁瀏覽	文件傳輸	收發郵件	TELNET	所占頻寬(KB)	IP地址	開始監控時間
1	1-246	6D1FD77257824C9	1.x-test22	0	0	0	0	0	2393954.75	192.168.1.246	2009-08-04 19:19:57
2	0-128	00-13-D4-F5-C1-0A	0.x-test	0	0	0	0	0	1961456.45	192.168.0.128	2009-08-07 11:43:10
3	1-154	WINXP	1.x-test22	0	0	0	0	0	1709536.08	192.168.1.154	2009-08-04 19:19:57
4	0-197	00-24-1D-22-14-1F	0.x-test	0	0	0	0	0	1586278.95	192.168.0.197	2009-08-07 11:43:10
5	1-160	00-21-9B-15-AF-34	others	0	0	0	0	0	1549887.0	192.168.1.160	2009-08-07 11:48:52
6	1-220	00-1F-D0-CB-42-DB	1.x-test22	0	0	0	0	0	1481963.94	192.168.1.220	2009-08-04 19:19:57
7	0-154	USER-0F521D1ACS	0.x-test	0	0	0	0	0	980939.42	192.168.0.154	2009-08-07 11:43:10
8	1-250	YOSHIKUN-9C8A55	others	0	0	0	0	0	791268.27	192.168.1.250	2009-08-07 11:48:52
9	1-81	00-13-D4-F0-E6-6B	1.x-test22	0	0	0	0	0	785006.42	192.168.1.81	2009-08-04 19:19:57
10	1-2	00-0E-A6-53-09-35	others	0	0	0	0	0	768624.13	192.168.1.2	2009-08-07 11:48:52

在這個列表當中會列出當下用戶各個網路通訊協定類別的流量使用情形，包括聊天記錄 (IM)、網頁瀏覽、文件傳輸、收發郵件、Telnet 的記錄數量與流量大小 (所占頻寬)，每個用戶記錄在各個通訊協定類別的數量都有超連結，可以直接用滑鼠點選進入該用戶的該項通訊協定記錄查詢細部的記錄內容如下圖 (以滑鼠點選檔案傳輸為例)。

摘要訊息

檔案傳輸

搜索條件1 日期範圍 從 2009-09-14 到 2009-09-14

搜索條件2 IP地址 192.168.1.129 搜索 文件名稱編碼 BIG5

搜索條件3 用戶名 郵寄 刪除

前頁 上一頁 跳到 1 頁 每頁顯示 10 筆 下一頁 下頁

全選	日期時間	IP地址	用戶名	電腦名稱/MAC位址	FTP主機	FTP帳號名	方向	文件名稱	文件大小 (KB)
<input type="checkbox"/>	2009-09-14 00:06:11	192.168.1.129	1-129	YOSHIKUN-B61993	202.47.28.150	Anonymous	Download	SiteStat.xml	0.118
<input type="checkbox"/>	2009-09-14 00:06:12	192.168.1.129	1-129	YOSHIKUN-B61993	202.47.28.150	Anonymous	Download	catalog.z	3.604

8.2 網頁瀏覽

網頁瀏覽指的是用戶的網頁訪問記錄，在網路通訊協定方面監控的是 HTTP。

摘要訊息

網頁瀏覽

搜索條件1 日期範圍 從 2009-09-01 到 2009-09-14

搜索條件2 IP地址

搜索條件3 用戶名

搜索 郵寄 刪除

前10頁 上一頁 跳到 1 頁 每頁顯示 10 筆 下一頁 下10頁

全選	日期時間	IP地址	用戶名	電腦名稱/MAC位址	Website	Website IP Address	數量
<input type="checkbox"/>	2009-09-01 00:00:02	192.168.0.103	0-103	00-1E-68-C7-A3-62	HTTP://WWW.104INFO.COM.TW/	202.8.15.245	1
<input type="checkbox"/>	2009-09-01 00:00:05	192.168.0.152	0-152	888TIGER-B9BF86	HTTP://TW.PAGE.MALL.YAHOO.COM/	116.214.7.144	1
<input type="checkbox"/>	2009-09-01 00:00:08	192.168.0.108	0-108	00-16-E6-49-DF-D4	HTTP://IMG.HARVEST.6WAVES.COM/	174.120.12.67	1
<input type="checkbox"/>	2009-09-01 00:00:09	192.168.0.167	0-167	HOME	HTTP://PATCH.RAYCITY.COM.TW/	210.64.126.120	1
<input type="checkbox"/>	2009-09-01 00:00:15	192.168.0.152	0-152	888TIGER-B9BF86	HTTP://TW.PAGE.BID.YAHOO.COM/	163.30.157.1	1
<input type="checkbox"/>	2009-09-01 00:00:19	192.168.2.21		00-1D-7D-D3-0F-71	HTTP://UM14.ESET.COM/	89.202.149.34	1
<input type="checkbox"/>	2009-09-01 00:00:20	192.168.0.200	0-200	888TIGER-2C79DB	HTTP://PHP.WEATHER.SINA.COM.CN/	202.106.182.237	1
<input type="checkbox"/>	2009-09-01 00:00:20	192.168.2.23		00-1F-C6-25-58-2E	HTTP://04065145061.CHANNEL30.FACEBOOK.COM/	203.69.138.42	2
<input type="checkbox"/>	2009-09-01 00:00:21	192.168.2.137		DOC-PC	HTTP://TW.YAHOO.COM/	119.160.246.242	1
<input type="checkbox"/>	2009-09-01 00:00:22	192.168.0.103	0-103	00-1E-68-C7-A3-62	HTTP://APPS.FACEBOOK.COM/	69.63.178.14	1

搜索條件 1 日期範圍： 選擇您想要查詢資料所在的日期時間範圍。

搜索條件 2、搜索條件 3： 您可以依照以下條件進行篩選查詢

IP 位址、用戶名、電腦名稱/MAC 位址、WebSite 網址名稱

※請注意！

包括即時服務總表以及之後的其他通訊協定類別資料列表，搜索的條件若是三個都有設定，則搜尋結果必須三個條件都要符合；若是設定兩個，則兩個條件都要符合；如果只有設定一個，那麼只要符合所設定的一個條件即可。

搜索： 定義好篩選搜尋條件後，須按下此「搜索」按鈕更新資料列表

郵寄：	每個登入帳號都會有屬於該帳號的電子郵件信箱（在「系統權限管理」=>「使用者管理中設定」），郵寄功能是可以將您目前所檢視的頁面畫面，直接以 PDF 檔案格式呈現並郵寄到您目前登入帳號所歸屬的電子郵件信箱當中。
刪除：	選擇刪除列表中的記錄，選擇的方式則是用列表左方的方格勾選
PDF (本地安裝版本才有)：	若您是在安裝 QnoSniff 專業版軟體的 PC 上，可以按下 PDF 按鈕將所呈現的畫面資料轉變成 PDF 檔案，儲存在別的硬碟空間或位置上。
前 10 頁：	按此按鈕資料列表會直接跳到前 10 頁的資料，舉例來說，若您現在是在第 201 筆資料列表畫面，而您所選擇是每頁顯示 10 筆資料，在按下前 10 頁的按鈕之後，會跳到第 101 筆資料列表畫面。
上一頁：	選擇您現在正在瀏覽頁面本頁的前一頁資料列表。
下一頁：	選擇您現在正在瀏覽頁面本頁的後一頁資料列表。
下 10 頁：	按此按鈕資料列表會直接跳到後 10 頁的資料，舉例來說，若您現在是在第 1 筆資料列表畫面，而您所選擇是每頁顯示 10 筆資料，在按下下 10 頁的按鈕之後，會跳到第 101 筆資料列表畫面。
跳到____頁	您可以自己定義每頁所顯示的資料筆數，10 筆、30 筆、50 筆、100 筆；也可以透過下拉式選單，直接跳選想檢視的頁數。
每頁顯示____筆	

資料列表欄位

日期 / 時間：	用戶訪問該筆資料網站的時間
IP 位址：	用戶的 IP
用戶名：	用戶的名稱
電腦名稱或 MAC 位址：	用戶的電腦名稱或 MAC 位址（解析不到電腦名稱會直接顯示成 MAC）
Website：	用戶所訪問的網站名稱
Website IP Address：	用戶所訪問的網站 IP 位址
數量：	訪問該網站的次數（每 15 分鐘累加一次）

※請注意！

有時候網站的網域名稱雖然相同（例如：tw.yahoo.com），但是所對應的 IP 位址是是不同的，這種狀況會將資料顯示成另一筆資料；而用戶訪問同一網站的次數，每隔 15 分鐘才會再累加一次，也就是說在這 15 分鐘以內，不論訪問該網站幾次（包括主要網域名稱「/」之後的網址），都只會算成一次。

8.3 電子郵件

電子郵件指的是用戶收送電子郵件的流量記錄，在網路通訊協定上所監控的是標準 SMTP 與 POP3。

電子郵件

搜索條件 1 日期範圍 從 2009-09-01 到 2009-09-02

搜索條件 2 IP地址

搜索條件 3 用戶名

前10頁 上一頁 跳到 1 頁 每頁顯示 10 筆 下一頁 下10頁

全選	日期/時間	IP地址	用戶名	電腦名稱/ MAC位址	寄件者	收件者	主題	大小 (KB)	下載附件	信件內容
<input type="checkbox"/>	2009-09-01 09:50:30	192.168.2.54		00-15-F2-D1-36-06	emmalovetina@hotmail.com	"" <emmalovetina@hotmail.com>;		5.71	Outlook Open	Content
<input type="checkbox"/>	2009-09-01 12:37:36	192.168.0.189	0-189	ACER-BF0AC3988F	Gourmets-lisa<lisa@gourmetspartner.com.tw>	'Sean' <sean@gourmetspartner.com.tw>,connie@gourmetspartner.com.tw	正在寄送電子郵件: Document, 01 SEPT SALES	43.61	Outlook Open	Content
<input type="checkbox"/>	2009-09-01 14:34:41	192.168.0.174		00-16-E6-37-BE-FE	s124015849lakers0709@yahoo.com.tw	s124015849lakers0709@yahoo.com.tw	優的	3.19	Outlook Open	Content
<input type="checkbox"/>	2009-09-01 21:38:52	192.168.2.54		00-15-F2-D1-36-06	tinahu7512@yahoo.com.tw	"Universidad Autónoma de Barcelona" <infouab@pmasters.es>;	RE : Carta aceptación del Master en Gestión de la Industria de la Moda y el Diseño (Mango)	21.71	Outlook Open	Content

搜索條件 1 日期範圍： 選擇您想要查詢資料所在的日期時間範圍。

搜索條件 2、搜索條件 3： 您可以依照以下條件進行篩選查詢

IP 位址、用戶名、電腦名稱/MAC 位址、寄件者電子郵件信箱、收件者電子郵件信箱、電子郵件主題

搜索： 定義好篩選搜尋條件後，須按下此「搜索」按鈕更新資料列表

郵寄： 每個登入帳號都會有屬於該帳號的電子郵件信箱（在「系統權限管理」=>「使用者管理中設定」），郵寄功能是可以將您目前所檢視的頁面畫面，直接以 PDF 檔案格式呈現並郵寄到您目前登入帳號所歸屬的電子郵件信箱當中。

刪除： 選擇刪除列表中的記錄，選擇的方式則是用列表左方的方格勾選

PDF (本地安裝版本才有)： 若您是在安裝 QnoSniff 專業版軟體的 PC 上，可以按下 PDF 按鈕將所呈現的畫面資料轉變成 PDF 檔案，儲存在別的硬碟空間或位置上。

前 10 頁：	按此按鈕資料列表會直接跳到前 10 頁的資料，舉例來說，若您現在是在第 201 筆資料列表畫面，而您所選擇是每頁顯示 10 筆資料，在按下前 10 頁的按鈕之後，會跳到第 101 筆資料列表畫面。
上一頁：	選擇您現在正在瀏覽頁面本頁的前一頁資料列表。
下一頁：	選擇您現在正在瀏覽頁面本頁的後一頁資料列表。
下 10 頁：	按此按鈕資料列表會直接跳到後 10 頁的資料，舉例來說，若您現在是在第 1 筆資料列表畫面，而您所選擇是每頁顯示 10 筆資料，在按下下 10 頁的按鈕之後，會跳到第 101 筆資料列表畫面。
跳到____頁	您可以自己定義每頁所顯示的資料筆數，10 筆、30 筆、50 筆、100 筆；也可以透過下拉式選單，直接跳選想檢視的頁數。
每頁顯示____筆	

資料列表欄位

日期 / 時間：	該筆電子郵件收送的時間。
IP 位址：	收送該筆電子郵件的用戶 IP 位址
用戶名：	收送電子郵件的用戶名稱
電腦名稱或 MAC 位址：	收送電子郵件的電腦名稱或是 MAC 位址（當電腦名稱解析不到時會直接顯示 MAC 位址資訊
寄件者：	該封電子郵件的寄件者
收件者：	該封電子郵件的收件者
主題：	該封電子郵件的主題
大小：	該封電子郵件的大小（整封郵件包含內文與附件）
下載附件：	「Outlook Open」按鈕是用來以 Outlook 或 Windows Mail 程式來打開郵件，在按下「Outlook Open」按鈕之後，您可以先儲存整個郵件，再用到儲存郵件的地方用 Outlook 程式打開，或是直接以 Outlook 程式執行開啟，附件檔案此時便會在該程式中正常顯示，所以此時就可以針對附件進行開啟或儲存動作。

※請注意！

若您是用遠端登入 Web 版本，若是按下「Outlook Open」並選擇直接開啟郵件，郵件會以您預設瀏覽網頁格式 (HTML) 的程式直接開啟，以下圖為例就是直接用 Firefox 直接開啟郵件內容。(右上方仍可選擇以那種語系解析信件內容，共有 English 英文、Traditional Chinese 繁體中文、Simplified Chinese 簡體中文)



信件內容：

「Content」按鈕是以 QnoSniff 專業版內建的程式開啟，所以信件內文只能呈現純文字內容，附件檔案部分指會顯示檔案名稱，並無法針對附件進行開啟或儲存動作，這是用來讓使用者快速瀏覽某些只有文字敘述的電子郵件內容。

另外右上方目前可以選擇繁體中文、簡體中文與 UTF-8 編碼來解析信件內容，若您的信件因為語系不同而出現亂碼，您可以試著調整看看語系來看內容是否能正常顯示。



8.4 檔案傳輸 (FTP)

QnoSniff 專業版的檔案傳輸目前指的是標準 FTP 通訊協定，包括主動模式與被動模式，若是採取其他加密型態的檔案傳輸 (如 SFTP、FTPS、FTPES 等)，是不在 QnoSniff 專業版的監控範圍內。



全選 <input type="checkbox"/>	日期時間	IP地址	用戶名	電腦名稱/MAC位址	FTP主機	FTP帳號名	方向	文件名稱	文件大小 (KB)
<input type="checkbox"/>	2009-09-16 00:33:19	192.168.2.11		00-20-ED-40-2F-99	61.220.58.41	Anonymous	DownLoad	version.ini	0.191
<input type="checkbox"/>	2009-09-16 00:43:42	192.168.2.59		888TIGER-8CEAE2	210.64.12.133	Anonymous	DownLoad	god_crc.txtZ	10.597
<input type="checkbox"/>	2009-09-16 00:43:43	192.168.2.59		888TIGER-8CEAE2	210.64.12.133	Anonymous	DownLoad	MfcControl.dll	557.568
<input type="checkbox"/>	2009-09-16 00:44:14	192.168.2.59		888TIGER-8CEAE2	210.64.12.133	Anonymous	DownLoad	Thumbs.db	61.868
<input type="checkbox"/>	2009-09-16 00:44:15	192.168.2.59		888TIGER-8CEAE2	210.64.12.133	Anonymous	DownLoad	LargeSel.rom	780.533
<input type="checkbox"/>	2009-09-16 00:44:22	192.168.2.59		888TIGER-8CEAE2	210.64.12.133	Anonymous	DownLoad	GainJP.wav	643.292
<input type="checkbox"/>	2009-09-16 00:44:28	192.168.2.59		888TIGER-8CEAE2	210.64.12.133	Anonymous	DownLoad	Stadium.ogg	229.764

搜索條件 1 日期範圍：選擇您想要查詢資料所在的日期時間範圍。

搜索條件 2、搜選條件 3：您可以依照以下條件進行篩選查詢

IP 位址、用戶名、電腦名稱/MAC 位址、FTP 主機、FTP 帳號名稱、方向、文件名稱

搜索：定義好篩選搜尋條件後，須按下此「搜索」按鈕更新資料列表

郵寄：每個登入帳號都會有屬於該帳號的電子郵件信箱 (在「系統權限管理」=>「使用者管理中設定」)，郵寄功能是可以將您目前所檢視的頁面畫面，直接以 PDF 檔案格式呈現並郵寄到您目前登入帳號所歸屬的電子郵件信箱當中。

刪除：選擇刪除列表中的記錄，選擇的方式則是用列表左方的方格勾選

PDF (本地安裝版本才有)：若您是在安裝 QnoSniff 專業版軟體的 PC 上，可以按下 PDF 按鈕將所呈現的畫面資料轉變成 PDF 檔案，儲存在別的硬碟空間或位置上。

前 10 頁：按此按鈕資料列表會直接跳到前 10 頁的資料，舉例來說，若您現在是在第 201 筆資料列表畫面，而您所選擇是每頁顯示 10 筆資料，在按下前 10 頁的按鈕之後，會跳到第 101 筆資料列表畫面。

上一頁：選擇您現在正在瀏覽頁面本頁的前一頁資料列表。

下一頁：	選擇您現在正在瀏覽頁面本頁的後一頁資料列表。
下 10 頁：	按此按鈕資料列表會直接跳到後 10 頁的資料，舉例來說，若您現在是在第 1 筆資料列表畫面，而您所選擇是每頁顯示 10 筆資料，在按下下 10 頁的按鈕之後，會跳到第 101 筆資料列表畫面。
跳到____頁	您可以自己定義每頁所顯示的資料筆數，10 筆、30 筆、50 筆、100 筆；也可以透過下拉式選單，直接跳選想檢視的頁數。
每頁顯示____筆	

資料列表欄位

全選：	可以透過勾選此方格，將此頁面多筆資料一起做勾選，進行刪除動作。
日期 / 時間：	該筆 FTP 上傳下載動作記錄的時間與日期。
IP 位址：	該筆 FTP 上傳下載動作記錄的內網 IP 位址。
用戶名：	該筆 FTP 上傳下載動作記錄的內網用戶名稱。
電腦名稱 / MAC 位址：	該筆 FTP 上傳下載動作記錄的內網電腦名稱或 MAC 位址。
FTP 主機：	該筆 FTP 上傳下載動作記錄的 FTP 主機 IP 位址。
FTP 帳號名：	該筆 FTP 上傳下載動作記錄的 FTP 登入帳號名稱。
方向：	該筆 FTP 上傳下載動作記錄的方向，是屬於上傳 (UpLoad) 還是下載 (Download)。
文件名稱：	該筆 FTP 上傳下載動作記錄的目標檔案名稱，點選超連結可以儲存或是直接用相關程式開啟檔案內容。

※請注意！

若您已經有在「基本設定」=>「資料庫設定」=>「文件大小限制」有做設定 (例如 10MB)，FTP 上傳/下載動作的目標檔案若是超過此大小，是無法將完整檔案收集至資料庫當中的，資料庫只會收集至您所設定的大小限制 (但是檔案大小欄位的資料顯示，還是會顯示真實的傳輸大小)，所以您在開啟檔案若是發生錯誤，很有可能就是因為有此限制，造成檔案不完整而無法開啟。

文件大小(KB)：	該筆 FTP 上傳下載動作記錄的目標檔案大小。
-----------	-------------------------

※請注意！

資料庫只會儲存您所設定 FTP 文件大小限制，超過此大小的部分不會儲存，但是文件大小會顯示完整的檔案資料大小，所以不會造成流量大小誤判

8.5 點對點下載 (P2P)

QnoSniff 專業版可以針對某些現在熱門的 P2P 下載軟體行為，進行監控記錄，目前可以判斷這些流量為 P2P 的流量模式以及流量大小是多少，QnoSniff 專業版未來規劃有可能會陸續加上 P2P 軟體種類的流量識別。

點對點下載

搜索條件 1 日期範圍 從 2009-08-16 到 2009-08-18 搜索

搜索條件 2 IP地址 [] 郵寄 刪除

前10頁 上一頁 跳到 1 頁 每頁顯示 10 筆 下一頁 下10頁

全選 <input type="checkbox"/>	日期時間	IP地址	用戶名	電腦名稱/MAC 位址	上傳速率 (KB/S)	下載速率 (KB/S)	上傳大小 (KB)	下載大小 (KB)
<input type="checkbox"/>	2009-08-17 13:57:13	192.168.0.4	0-004x	F1	0.0	0.0	0.0	1.03
<input type="checkbox"/>	2009-08-17 13:57:13	192.168.0.4	0-004x	F1	4.41	1.43	3966.5	1290.27
<input type="checkbox"/>	2009-08-17 13:57:13	192.168.0.112	0-112	DOBE	0.0	0.0	0.41	0.88
<input type="checkbox"/>	2009-08-17 13:57:13	192.168.0.128	0-128	00-13-D4-F5-C1-0A	0.0	0.0	2.79	2.85
<input type="checkbox"/>	2009-08-17 13:57:13	192.168.0.128	0-128	00-13-D4-F5-C1-0A	0.02	0.03	20.37	23.85
<input type="checkbox"/>	2009-08-17 13:57:13	192.168.0.128	0-128	00-13-D4-F5-C1-0A	0.1	0.12	86.66	109.54
<input type="checkbox"/>	2009-08-17 13:57:13	192.168.0.162	0-162	00-25-11-2D-61-8F	0.0	0.0	1.53	0.92
<input type="checkbox"/>	2009-08-17 13:57:13	192.168.0.234	0-234	SAYA	0.0	0.0	2.43	2.9
<input type="checkbox"/>	2009-08-17 13:57:13	192.168.0.234	0-234	SAYA	0.02	0.02	16.39	20.21
<input type="checkbox"/>	2009-08-17 13:57:13	192.168.0.234	0-234	SAYA	0.16	0.24	146.08	213.69

搜索條件 1 日期範圍：

選擇您想要查詢資料所在的日期時間範圍。

搜索條件 2：

您可以依照以下條件進行篩選查詢

IP 位址、用戶名、電腦名稱/MAC 位址

搜索：

定義好篩選搜尋條件後，須按下此「搜索」按鈕更新資料列表

郵寄：

每個登入帳號都會有屬於該帳號的電子郵件信箱（在「系統權限管理」=>「使用者管理中設定」），郵寄功能是可以將您目前所檢視的頁面畫面，直接以 PDF 檔案格式呈現並郵寄到您目前登入帳號所歸屬的電子郵件信箱當中。

刪除：

選擇刪除列表中的記錄，選擇的方式則是用列表左方的方格勾選

PDF (本地安裝版本才有)：

若您是在安裝 QnoSniff 專業版軟體的 PC 上，可以按下 PDF 按鈕將所呈現的畫面資料轉變成 PDF 檔案，儲存在別的硬碟空間或位置上。

前 10 頁：

按此按鈕資料列表會直接跳到前 10 頁的資料，舉例來說，若您現在是在第 201 筆資料列表畫面，而您所選擇是每頁顯示 10 筆資料，在按下前 10 頁的按鈕之後，會跳到第 101 筆資料列表畫面。

上一頁：

選擇您現在正在瀏覽頁面本頁的前一頁資料列表。

下一頁：	選擇您現在正在瀏覽頁面本頁的後一頁資料列表。
下 10 頁：	按此按鈕資料列表會直接跳到後 10 頁的資料，舉例來說，若您現在是在第 1 筆資料列表畫面，而您所選擇是每頁顯示 10 筆資料，在按下下 10 頁的按鈕之後，會跳到第 101 筆資料列表畫面。
跳到____頁	您可以自己定義每頁所顯示的資料筆數，10 筆、30 筆、50 筆、100 筆；也可以透過下拉式選單，直接跳選想檢視的頁數。
每頁顯示____筆	

資料列表欄位

全選：	可以透過勾選此方格，將此頁面多筆資料一起做勾選，進行刪除動作。
日期 / 時間：	該筆被判斷為 P2P 上傳/下載行為動作的時間與日期。
IP 位址：	該筆被判斷為 P2P 上傳/下載行為動作的內網 IP 位址。
用戶名：	該筆被判斷為 P2P 上傳/下載行為動作的內網用戶名稱。
電腦名稱 / MAC 位址：	該筆被判斷為 P2P 上傳/下載行為動作的內網電腦名稱或是 MAC 位址。
上傳速率 (KB/S)：	該筆被判斷為 P2P 上傳/下載行為動作的平均上傳流量速率。
下載速率 (KB/S)：	該筆被判斷為 P2P 上傳/下載行為動作的平均下載流量速率。
上傳大小 (KB)：	該筆被判斷為 P2P 上傳/下載行為動作的目前上傳檔案大小。
下載大小 (KB)：	該筆被判斷為 P2P 上傳/下載行為動作的目前下載檔案大小。

8.6 Telnet

QnoSniff 專業版所針對的是標準 Telnet 網路通訊協定標準，如果您的用戶使用 Telnet 有改變用其他的通訊埠口進行連線，或是加密型的 SSH，QnoSniff 專業版目前是不支援此類的非標準協定或加密協定。

TELNET

搜索條件1 日期範圍 從 到

搜索條件2

搜索條件3

前10頁 上一頁 跳到 頁 每頁顯示 筆 下一頁 下10頁

全選 <input type="checkbox"/>	日期時間	IP地址	用戶名	電腦名稱/MAC位址	網站IP地址	網址	Telnet帳號名	內容
<input type="checkbox"/>	2009-08-17 13:47:43	192.168.0.108	0-108	00-16-E6-49-DF-D4	68.180.217.16	68.180.217.16	Guest	Telnet
<input type="checkbox"/>	2009-08-17 13:52:53	192.168.0.108	0-108	00-16-E6-49-DF-D4	68.180.217.16	68.180.217.16	Guest	Telnet
<input type="checkbox"/>	2009-08-17 13:58:23	192.168.0.108	0-108	00-16-E6-49-DF-D4	68.180.217.16	68.180.217.16	Guest	Telnet
<input type="checkbox"/>	2009-08-17 14:04:54	192.168.0.108	0-108	00-16-E6-49-DF-D4	68.180.217.16	68.180.217.16	Guest	Telnet
<input type="checkbox"/>	2009-08-17 14:11:24	192.168.0.108	0-108	00-16-E6-49-DF-D4	68.180.217.16	68.180.217.16	Guest	Telnet
<input type="checkbox"/>	2009-08-17 14:23:08	192.168.0.108	0-108	00-16-E6-49-DF-D4	68.180.217.16	68.180.217.16	Guest	Telnet
<input type="checkbox"/>	2009-08-17 14:29:43	192.168.0.108	0-108	00-16-E6-49-DF-D4	68.180.217.16	68.180.217.16	Guest	Telnet
<input type="checkbox"/>	2009-08-17 14:35:25	192.168.0.108	0-108	00-16-E6-49-DF-D4	68.180.217.16	68.180.217.16	Guest	Telnet
<input type="checkbox"/>	2009-08-17 14:42:12	192.168.0.108	0-108	00-16-E6-49-DF-D4	68.180.217.16	68.180.217.16	Guest	Telnet

搜索條件 1 日期範圍：

選擇您想要查詢資料所在的日期時間範圍。

搜索條件 2、搜索條件 3：

您可以依照以下條件進行篩選查詢

IP 位址、用戶名、電腦名稱/MAC 位址、網站 IP 位址、網站名稱、Telnet 帳號名稱

搜索：

定義好篩選搜尋條件後，須按下此「搜索」按鈕更新資料列表

郵寄：

每個登入帳號都會有屬於該帳號的電子郵件信箱（在「系統權限管理」=>「使用者管理中設定」），郵寄功能是可以將您目前所檢視的頁面畫面，直接以 PDF 檔案格式呈現並郵寄到您目前登入帳號所歸屬的電子郵件信箱當中。

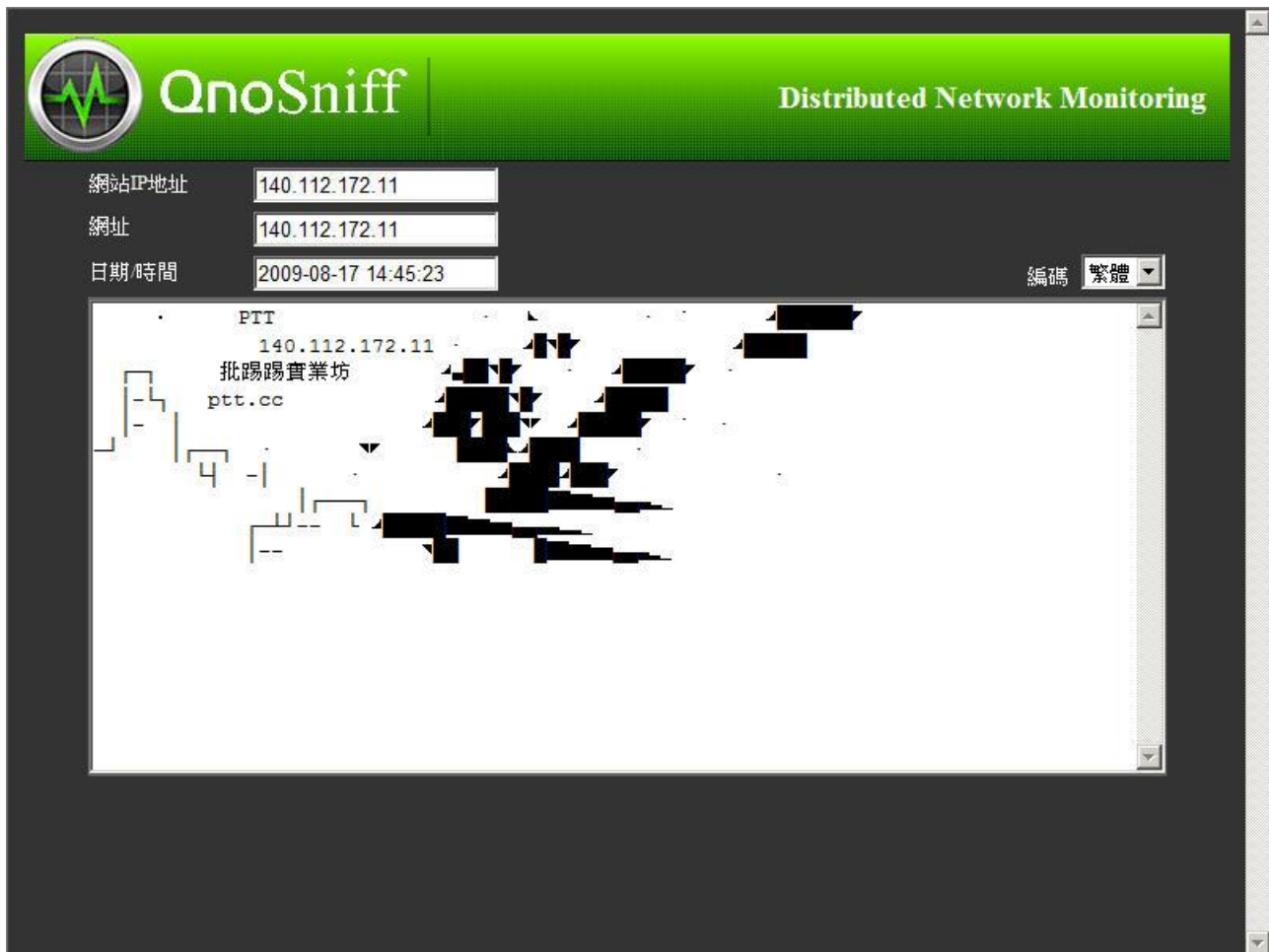
刪除：

選擇刪除列表中的記錄，選擇的方式則是用列表左方的方格勾選

PDF (本地安裝版本才有) :	若您是在安裝 QnoSniff 專業版軟體的 PC 上,可以按下 PDF 按鈕將所呈現的畫面資料轉變成 PDF 檔案,儲存在別的硬碟空間或位置上。
前 10 頁 :	按此按鈕資料列表會直接跳到前 10 頁的資料,舉例來說,若您現在是在第 201 筆資料列表畫面,而您所選擇是每頁顯示 10 筆資料,在按下前 10 頁的按鈕之後,會跳到第 101 筆資料列表畫面。
上一頁 :	選擇您現在正在瀏覽頁面本頁的前一頁資料列表。
下一頁 :	選擇您現在正在瀏覽頁面本頁的後一頁資料列表。
下 10 頁 :	按此按鈕資料列表會直接跳到後 10 頁的資料,舉例來說,若您現在是在第 1 筆資料列表畫面,而您所選擇是每頁顯示 10 筆資料,在按下下 10 頁的按鈕之後,會跳到第 101 筆資料列表畫面。
跳到____頁	您可以自己定義每頁所顯示的資料筆數,10 筆、30 筆、50 筆、100 筆;也可以透過下拉式選單,直接跳選想檢視的頁數
每頁顯示____筆	

資料列表欄位

全選 :	可以透過勾選此方格,將此頁面多筆資料一起做勾選,進行刪除動作。
日期 / 時間 :	該筆 Telnet 記錄動作的時間
IP 位址 :	該筆 Telnet 記錄動作的內網 IP 位址
用戶名 :	該筆 Telnet 記錄動作的內網用戶名稱
電腦名稱 / MAC 位址 :	該筆 Telnet 記錄動作的內網電腦名稱或 MAC 位址
網站 IP 地址 :	該筆 Telnet 記錄的目的地 IP 位址
網址 :	該筆 Telnet 記錄的目的地網址或網域名稱
Telnet 帳號名 :	該筆 Telnet 記錄的登入帳號名稱
內容  :	該筆 Telnet 記錄的詳細內容資訊,按下此按鈕後會出以下內容資訊



網站 IP 位址：您 Telnet 遠端登入的目的地 IP 位址

網址：您 Telnet 遠端登入的目的地的網址或網域名稱

日期 / 時間：該筆 Telnet 登入動作的時間與日期

內容頁面：顯示 Telnet 的登入資訊內容

編碼：有繁體編碼、簡體編碼以及 UTF-8 編碼可以做切換

8.7 即時通訊

QnoSniff 專業版目前可以進行監控與記錄的應用程式如下：

【1】MSN (Live Message / 8.5 / 8.0)

【2】QQ (並須將用戶 QQ 帳號、密碼輸入在「基本設定」=>「服務設定」內的「IM：QQ 號碼設定才能夠進行監控與記錄」，並且目前無法對 QQ 所有「TM」版本進行側錄監控)

【3】Yahoo Message

【4】Google Talk

即時通訊

搜索條件1 日期範圍 從 2009-08-14 到 2009-08-16

搜索條件2 IP地址

搜索條件3 用戶名

搜索 郵寄 刪除

前10頁 上一頁 跳到 1 頁 每頁顯示 10 筆 下一頁 下10頁

全選	日期時間	IP地址	用戶名	電腦名稱/MAC位址	本地帳號	對方帳號	IM類別	記錄
<input type="checkbox"/>	2009-08-14 00:05:40	192.168.1.231	1-231	ACFS-6450580BDF			MSN	6
<input type="checkbox"/>	2009-08-14 00:05:43	192.168.0.193	0-193	00-14-2A-11-38-23			YAHOO MSG	16
<input type="checkbox"/>	2009-08-14 00:07:17	192.168.2.58		00-11-D8-1A-5E-4D			MSN	1
<input type="checkbox"/>	2009-08-14 00:07:29	192.168.1.106	1-106	00-1B-FC-C7-A9-DE			MSN	18
<input type="checkbox"/>	2009-08-14 00:07:51	192.168.2.145		PC			MSN	42
<input type="checkbox"/>	2009-08-14 00:10:38	192.168.0.117	0-117	00-1C-25-33-4D-4D			YAHOO MSG	4
<input type="checkbox"/>	2009-08-14 00:10:47	192.168.2.179		00-0A-79-F5-3C-25			YAHOO MSG	2
<input type="checkbox"/>	2009-08-14 00:12:45	192.168.1.164		00-1E-8C-21-47-19			YAHOO MSG	7
<input type="checkbox"/>	2009-08-14 00:13:57	192.168.1.100	1-100	00-21-85-05-06-67			MSN	34
<input type="checkbox"/>	2009-08-14 00:14:35	192.168.2.145		PC			MSN	5

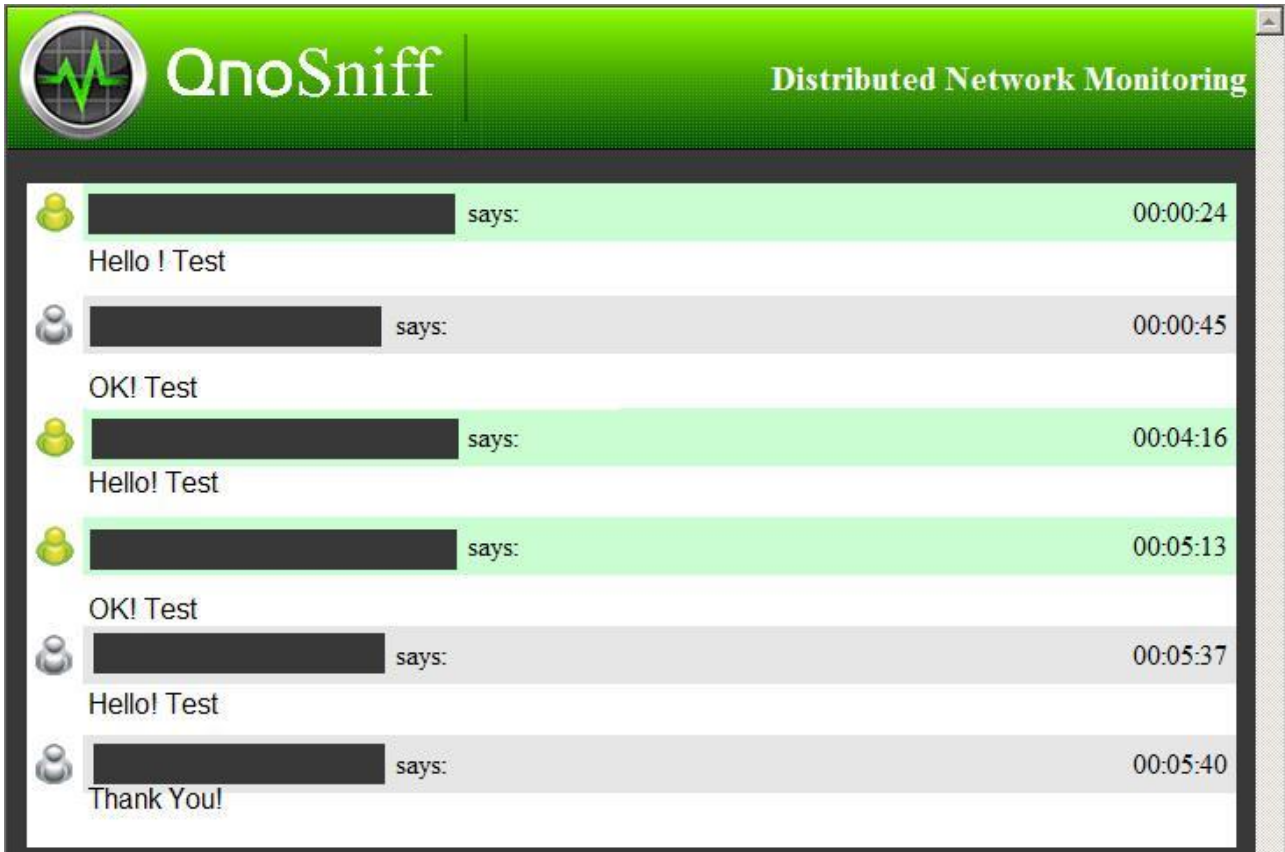
搜索條件 1 日期範圍：	選擇您想要查詢資料所在的日期時間範圍。
搜索條件 2、搜索條件 3：	您可以依照以下條件進行篩選查詢
	IP 位址、用戶名、電腦名稱/MAC 位址、本地帳號、對方帳號、IM 類別
搜索：	定義好篩選搜尋條件後，須按下此「搜索」按鈕更新資料列表
郵寄：	每個登入帳號都會有屬於該帳號的電子郵件信箱（在「系統權限管理」=>「使用者管理中設定」），郵寄功能是可以將您目前所檢視的頁面畫面，直接以 PDF 檔案格式呈現並郵寄到您目前登入帳號所歸屬的電子郵件信箱當中。
刪除：	選擇刪除列表中的記錄，選擇的方式則是用列表左方的方格勾選
PDF (本地安裝版本才有)：	若您是在安裝 QnoSniff 專業版軟體的 PC 上，可以按下 PDF 按鈕將所呈現的畫面資料轉變成 PDF 檔案，儲存在別的硬碟空間或位置上。
前 10 頁：	按此按鈕資料列表會直接跳到前 10 頁的資料，舉例來說，若您現在是在第 201 筆資料列表畫面，而您所選擇是每頁顯示 10 筆資料，在按下前 10 頁的按鈕之後，會跳到第 101 筆資料列表畫面。
上一頁：	選擇您現在正在瀏覽頁面本頁的前一頁資料列表。
下一頁：	選擇您現在正在瀏覽頁面本頁的後一頁資料列表。
下 10 頁：	按此按鈕資料列表會直接跳到後 10 頁的資料，舉例來說，若您現在是在第 1 筆資料列表畫面，而您所選擇是每頁顯示 10 筆資料，在按下下 10 頁的按鈕之後，會跳到第 101 筆資料列表畫面。
跳到____頁	您可以自己定義每頁所顯示的資料筆數，10 筆、30 筆、50 筆、100 筆；也可以透過下拉式選單，直接跳選想檢視的頁數
每頁顯示____筆	

資料列表欄位

全選：	可以透過勾選此方格，將此頁面多筆資料一起做勾選，進行刪除動作。
日期 / 時間：	該筆即時通訊的通訊時間
IP 地址：	該筆即時通訊所使用的內網 IP 位址
用戶名：	該筆即時通訊所使用的用戶名稱
電腦名稱 / MAC 位址：	該筆即時通訊所使用的電腦名稱
本地帳號：	該筆即時通訊在上述所列 IP / 電腦上所使用的帳號
對方帳號：	該筆即時通訊交談的另一個帳號

IM 類別： 該筆即時通訊類別是屬於 MSN、QQ、YahooMessage 或是 Google Talk。

記錄： 該筆通訊記錄來回的訊息總共有幾筆數量，點選該數字的超連結後，會另外跳出詳細即時通訊記錄內容（如下圖）。



※灰色遮蔽的部分在您的軟體上會正常顯示帳號內容，以上圖示只是範例。

日期/時間、IP 位址、用戶名、電腦名稱/MAC 位址、IM 類別、記錄都可接點選該欄位進行排序。

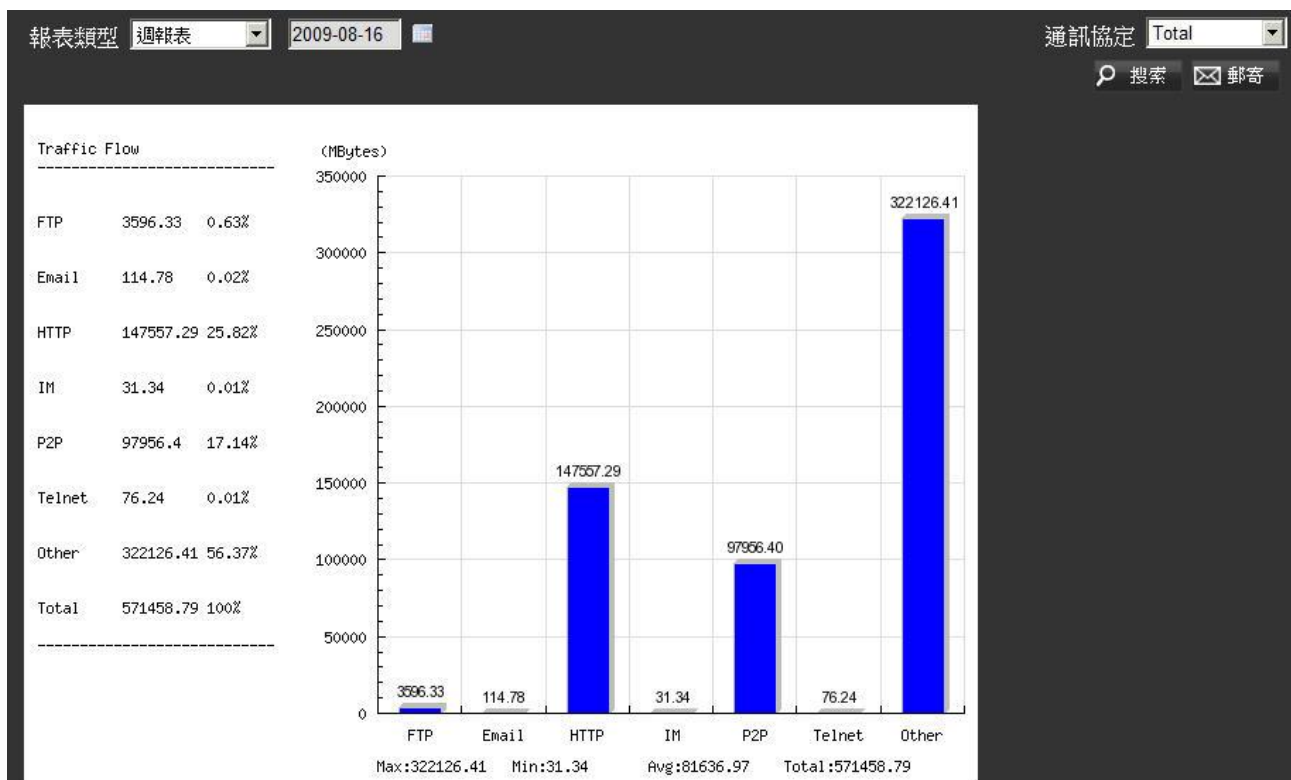
九、統計資訊

本章節介紹 QnoSniff 專業版的流量統計功能，總共有流量統計報表、部門流量排名總表、使用者流量排名總表，可以依據部門別、網路通訊協定類別以及所自訂的時間，充分的呈現內網用戶網路流量以及應用程式使用各種情形；另外流量統計報表數值與圖表的部分，是每隔 15 分鐘才會更新統計的內容與圖示，所以在 15 分鐘以內的資料是不會有所變動的。

9.1 流量統計報表

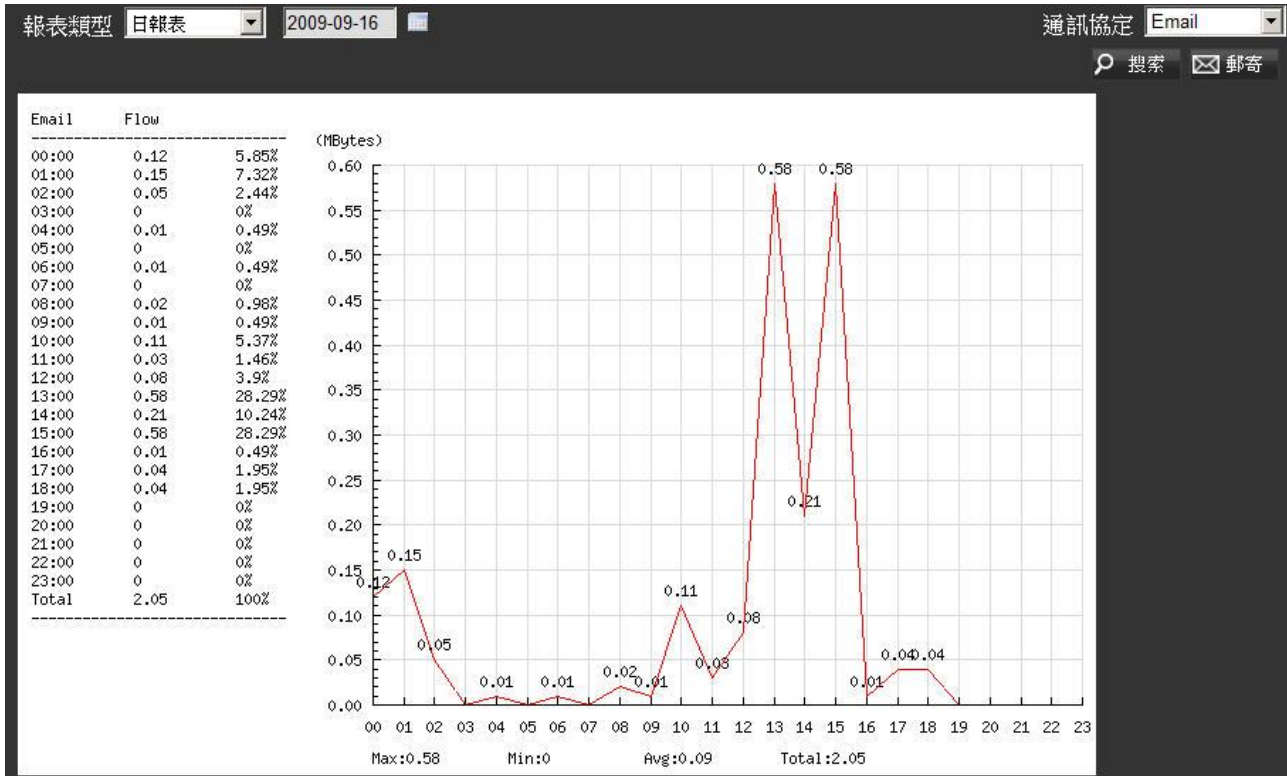
這部分的報表主要是以圖表與統計數字，來顯示各個通訊協定下的流量統計資訊。

左方有 Traffic Flow 列表，在通訊協定選擇「Total」的時後，會顯示各個通訊協定在您所選擇的時間區段內的統計數值與所占總流量的百分比，右方則是圖示，在選擇時間區段以及選擇通訊協定過後，需要再按一下「搜尋」按鈕，以使資料數值能夠更新到您所選擇的時間區段，以及通訊協定所正確對應的資料內容。



若您的通訊協定不是選擇「Total」而是選擇單一通訊協定例如「E-mail」(電子郵件)，左方的 Traffic Flow 列表轉化成時間縱軸的方式，顯示各個時間區段內的流量統計，若您選擇日報表，則是 0-23 小時，每一個小時顯示統計資料；若您選擇週報表，則是七天並且每六個小時為一個時間區段顯示統計資料若您選擇月報表，則

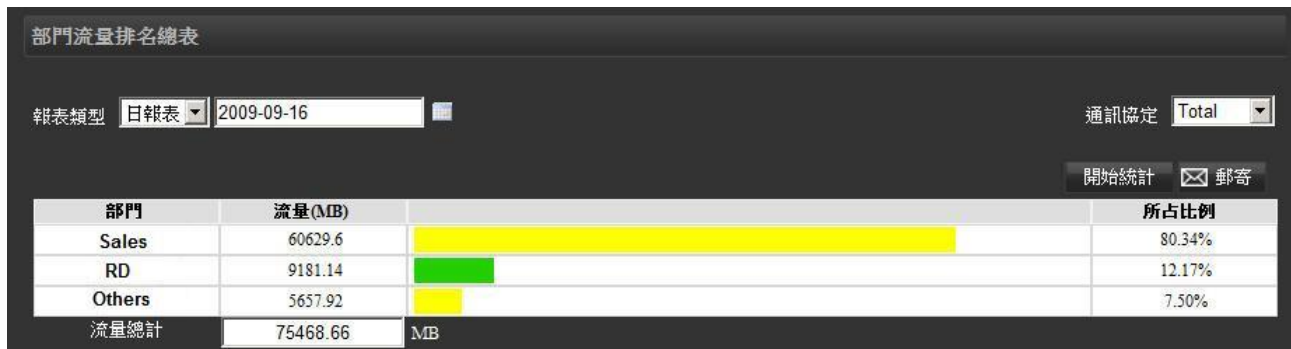
顯示的是該月 1 日到 30 或 31 日，每一日顯示統計資料。



郵寄、PDF (只有本地安裝版本)功能仍然可以在統計列表中使用，直接將查詢的報表 / 圖示資料轉成 PDF 檔案或是直接以 PDF 檔案寄送電子郵件到管理者電子郵件信箱。

9.2 部門流量排名總表

部門流量排名總表，主要是用部門所使用的流量來排序，並且可以針對不同通訊協定，來查詢各個部門的使用流量狀況，例如所有部門的即時通訊流量，從最多到最小的流量統計列表內容。



您可以依照您想檢視的時間區段、網路通訊協定類別，來顯示您所有部門的流量統計狀況以及數值，若您想檢視某個部門、在某個通訊協定下，該部門下的成員流量使用統計明細，可以直接按下部門名稱的超連結，就會顯示出該部門（例如 Sales）以下成員，使用某種通訊協定（例如 E-mail）的流量統計排名與數值、百分比等（如下圖例）。

報表類型

部門 通訊協定

編號	IP地址	用戶名	電腦名稱/MAC位址	流量(MB)	百分比
1	192.168.2.121		00-1E-68-BD-75-F6	0.56	27.05%
2	192.168.1.175		00-0A-E4-0B-76-49	0.54	26.09%
3	192.168.1.115		00-14-2A-41-01-F1	0.18	8.70%
4	192.168.1.110		00-1E-8C-EE-19-2A	0.09	4.35%
5	192.168.2.153		00-0F-B0-95-43-55	0.08	3.86%
6	192.168.2.45		00-1F-D0-31-85-3D	0.07	3.38%
7	192.168.1.39		00-1F-C6-C5-8C-41	0.06	2.90%
8	192.168.1.50		00-0A-E4-F9-B7-97	0.06	2.90%
9	192.168.2.46		00-40-F4-3A-29-B7	0.06	2.90%
10	192.168.2.63		00-11-09-8F-61-82	0.04	1.93%
11	192.168.1.6		00-21-85-39-CD-8F	0.03	1.45%
12	192.168.1.60		Z	0.03	1.45%
13	192.168.2.137		DOC-PC	0.03	1.45%
14	192.168.2.182		00-00-6C-3D-F4-09	0.03	1.45%
15	192.168.1.233		GEOFFREY-PC	0.02	0.97%
16	192.168.2.123		LV-429AE77A94B0	0.02	0.97%







9.3 使用者流量排名總表

使用者流量排名總表，是針對所有單一內網用戶所做的流量統計與排序，也可以依不同時間區段、部門別以及網路通訊協定類別，選擇流量統計內容與排序列表。

使用者流量排名總表

報表類型 2009-09-16

部門 通訊協定

編號	IP地址	用戶名	電腦名稱/MAC位址	流量(MB)		百分比
1	192.168.0.247		00-16-36-16-1D-60	8722.35		11.03%
2	192.168.1.100		PC-200908311526	8320.13		10.52%
3	192.168.1.6		00-21-85-39-CD-8F	3967.12		5.02%
4	192.168.1.233		GEOFFREY-PC	3482.88		4.40%
5	192.168.2.87		00-1C-25-3C-0F-02	2841.29		3.59%
6	192.168.1.192		USER	2622.3		3.32%
7	192.168.2.156		00-40-45-1C-32-BA	2617.13		3.31%
8	192.168.1.160	1-160	00-21-9B-15-AF-34	2043.01		2.58%
9	192.168.2.27		HOMEUSER	1809.87		2.29%
10	192.168.1.67	1-67	TOMMY	1281.05		1.62%
11	192.168.1.175		00-0A-E4-0B-76-49	1255.55		1.59%
12	192.168.1.76	1-76	00-1D-92-E4-3F-9E	962.24		1.22%
13	192.168.1.81	1-81	00-13-D4-F0-EE-6B	949.15		1.20%
14	192.168.2.88		00-19-DB-B6-30-62	873.49		1.10%
15	192.168.1.139		C1D7641E5AD14CD	833.22		1.05%
16	192.168.0.188		00-1D-7D-08-D5-60	822.66		1.04%

一開始進入畫面的時候，會以所有使用者、所有類型的流量統計做排序，包括實際流量統計(MB)以及所占百分比，若您要查詢某部分，或是其他通訊協定，皆可以透過右方的下拉式選單做篩選，則選擇新的查詢條件之後，請您注意一定要再按下「開始統計」按鈕，資料才會開始更新符合您的新篩選條件。

十、登出系統

當您不再使用 QnoSniff 專業版，可以按下「登出系統」選單離開 QnoSniff 專業版操作主頁面。

在遠端登入離開後自然是離開網頁，若是在安裝 QnoSniff 專業版的 PC 上，離開本地安裝版本的主控頁面後，右下角的系統列仍然會有 QnoSniff 專業版的 Icon，表示 QnoSniff 專業版仍然在背景運行抓取資料（綠色圖示表示正常與路由器連線中，灰色的圖示表示未與路由器正常連線）。

若您需要關閉整個 QnoSniff 專業版，包括收集資料功能，就需要在系統列的 Icon 上按滑鼠右鍵，選擇選單中的「Exit Minitor」離開系統，QnoSniff 專業版會再詢問您一次是否要確認關閉整個 QnoSniff 專業版系統，按下確定後，QnoSniff 專業版系統會進行關閉程序，大約在 10~15 秒內，系統列的 Icon 會因為整個系統關閉完成而消失。

請注意：若關閉整個 QnoSniff 專業版，包括資料收集功能，這段關閉的時間之內是沒有資料的，QnoSniff 專業版的資料庫也不會有資料，所以在統計的資料中也不會出現這段時間的資料內容。

在系統列的 Icon 上按下滑鼠右鍵會跳出以下選單：




- 1.Information：有 QnoSniff 專業版的版權資訊、所使用的監聽網路卡設備、QnoSniff 專業版的軟體版本，以及現在儲存資料所占用的大小。
- 2.Login System：若您還未成功登入 QnoSniff 專業版主控台，可以點選此選項進行登入。
- 3.Enable/Disable Auto：可以啟用 (Enable) 或是 關閉 (Disable) 開機後自動啟用 QnoSniff 專業版於背景運行，您若是第一次選擇自動運行，則在下次開機的時候就會生效隨著開機後自動啟用 QnoSniff 專業版。

4.Exit Monitor：離開並關閉整個 QnoSniff 專業版，包括資料收集的功能，按下後系統會跳出以下視窗再次詢問您是否確認離開並關閉整個系統，按下「是」後，QnoSniff 專業版系統會進行關閉程序，大約在 10~15 秒內系統列的 Icon 會因為整個系統關閉完成而消失。

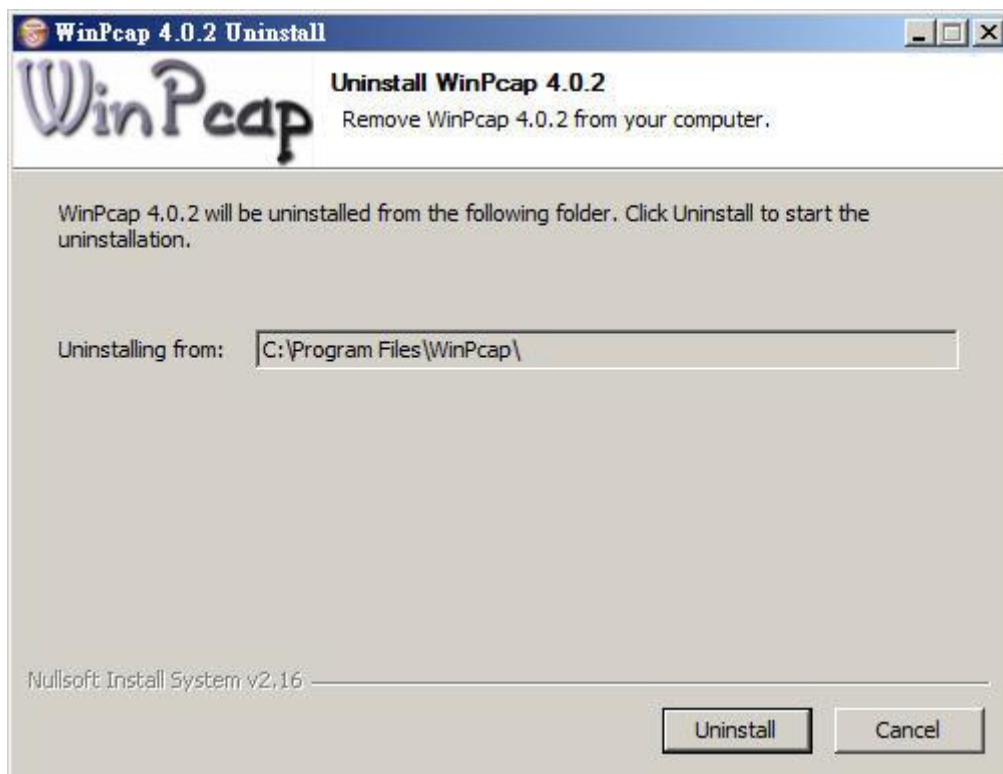


十一、解除安裝

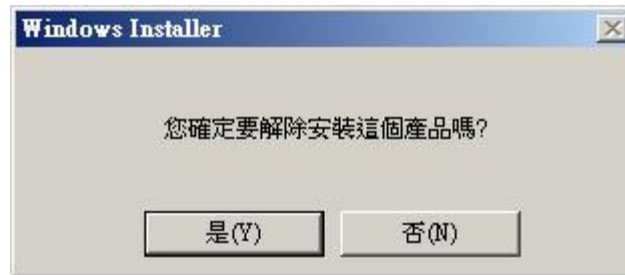
當您想要移除安裝 QnoSniff 專業版，請到系統程式集尋找 QnoSniff 資料夾，該資料夾下有會有「Uninstall」

選項如右圖  選擇 Uninstall 就會開始進行移除程序，或是到「控制台」的「新增或移除程式」，點選 QnoSniff 進行移除程式動作。

移除程序首先會移除 WinPcap 如下圖，若您是直接到控制台選擇移除 QnoSniff 專業版，可能會跳過解除安裝 WinPcap 這一段，但是一樣能達成完全移除的結果。



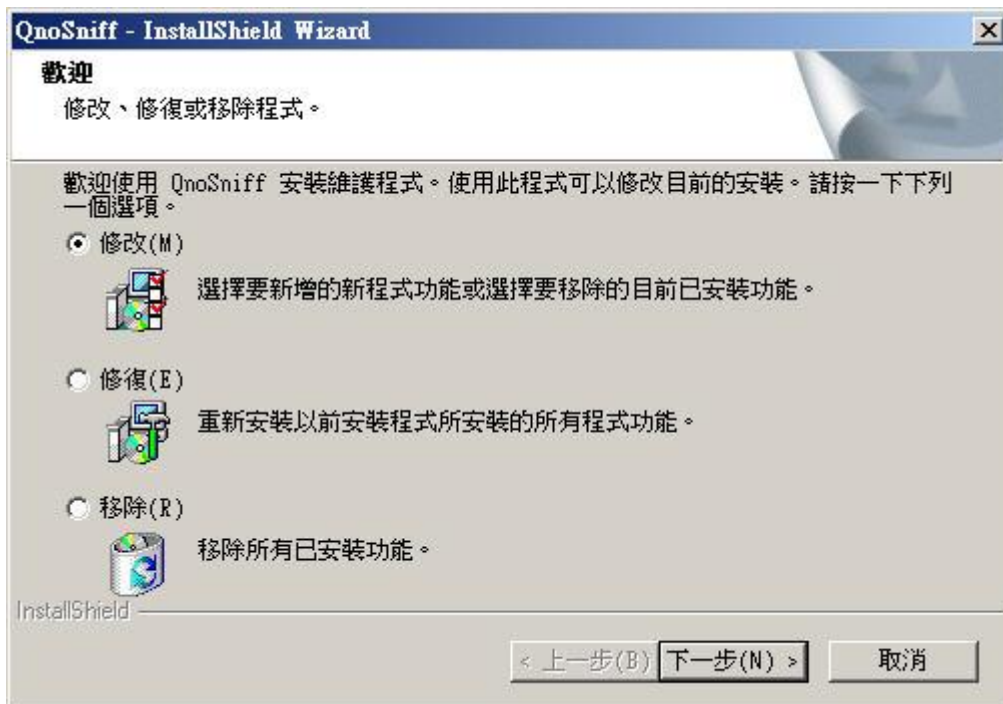
按下 Uninstall 進行移除 WinPcap 元件，移除完成畫面如下，請按下 Finish 繼續移除程序，會跳出是否確認解除安裝主程式訊息，請按下「是」



蒐集解除安裝相關資料中



跳出軟體維護畫面如下，請選擇「移除(R)」並按下一步繼續




詢問是否確認移除，請按「是」便會開始進行主程式解除安裝程序



進行完解除安裝後，會挑出要您重新開機的訊息，若您仍有其他作業尚未完成並且未做儲存動作，可以選擇稍後再自行重新啟動電腦，若無其他疑慮，則可立刻重開機，請注意必須要將電腦重開機後，整個安裝程序才算完成。



重新開機後，請到您之前所安裝 QnoSniff 專業版軟體的硬碟位置 (如 C:\QnoSniff  QnoSniff 檔案資料夾)，您

所收集到的資料庫內容仍然會留在此檔案夾中如下圖



若您之後再重新安裝 QnoSniff 專業版並且安裝在相同的硬碟位置，這些資料仍可以與 QnoSniff 專業版主控台做連結，進行資料檢視與篩選；若是您確認往後都使用不到這些資料庫內容，便可將整個 QnoSniff 資料夾進行刪除，已增加您硬碟的剩餘可用空間。

附錄：Qno 技術支援資訊

更多有關俠諾產品技術資訊，除了可以登錄俠諾寬頻討論區、參照 FTP 伺服器的相關實例；或是進一步聯繫俠諾各經銷商技術部門、或俠諾大陸技術中心取得相關協助。

俠諾科技官方網站：<http://www.Qno.com.tw>

各大經銷商服務聯繫方式：

用戶可以登錄網站先上服務頁面查詢各大經銷聯繫方法 http://www.qno.com.tw/web/where_buy.asp

台灣技術中心：電子郵件信箱：QnoFAE@qno.com.tw