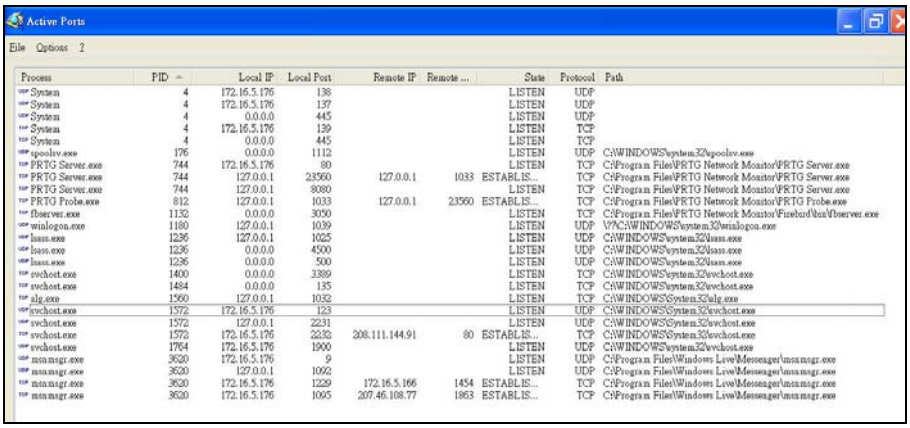
COMPUTERWORLD 10 大免費網路軟體工具介紹

在管理者進行網路管理時常會需要使用一些軟體工具協助工作的進行，增加工作效率。推薦 10 項免費網路軟體工具給大家使用，這些軟體在 www.computerworld.com 被列爲 10 大網管工具。這 10 項工具雖是免費軟體，但所提供的功能不輸給專業的商業軟體，其軟體功能包含資訊安全、設備管理、網路偵測、流量統計等。經本中心測試整理，10 項免費網路軟體工具如下：

1、Active port：網路運作狀況監控軟體
2、MRTG（Multi Router Traffic Grapher）：伺服器及網路設備運作狀況監控軟體
3、Nessus：系統弱點掃描軟體
4、Netstumbler：無線網路工具軟體
5、Nmap：系統弱點掃描軟體
6、Putty：SSH / Telnet 連線軟體
7、SNMP Traffic Grapher：網路設備流量監控軟體
8、The Dude：監控伺服器跟網路設備軟體
9、Wireshark：網路封包分析軟體
10、ZipTie：管理網路設備設定軟體

1、軟體名稱	Active port
軟體簡介	Active port 是一套本機網路運作狀況監控軟體，可以讓使用者了解可以看到系統上的執行程式所使用的網路埠（Port），並且詳細的列出相關 TCP/IP 或者 UDP 網路連線資訊。主要應用爲 1、檢查系統程式是否正常啓動網路服務，如 IIS 程式是否已啓動 80 port。2、檢查使用者電腦有無不明程式使用網路連線出去。PS：由於 Active port 是偵測本機上開啓的 port，可能會被某些防毒軟體判斷爲病毒程式。
軟體性質	免費軟體
作業系統平台	Windows NT/2000/XP
語言界面	英文
軟體下載網址	http://www.download.com/Active-Ports/3000-2085_4-10062969.html
軟體操作說明	一、安裝完 Active port 後，執行 Active port 程式。  二、Active port 執行畫面如下。

<table>
<tr><td></td><td>


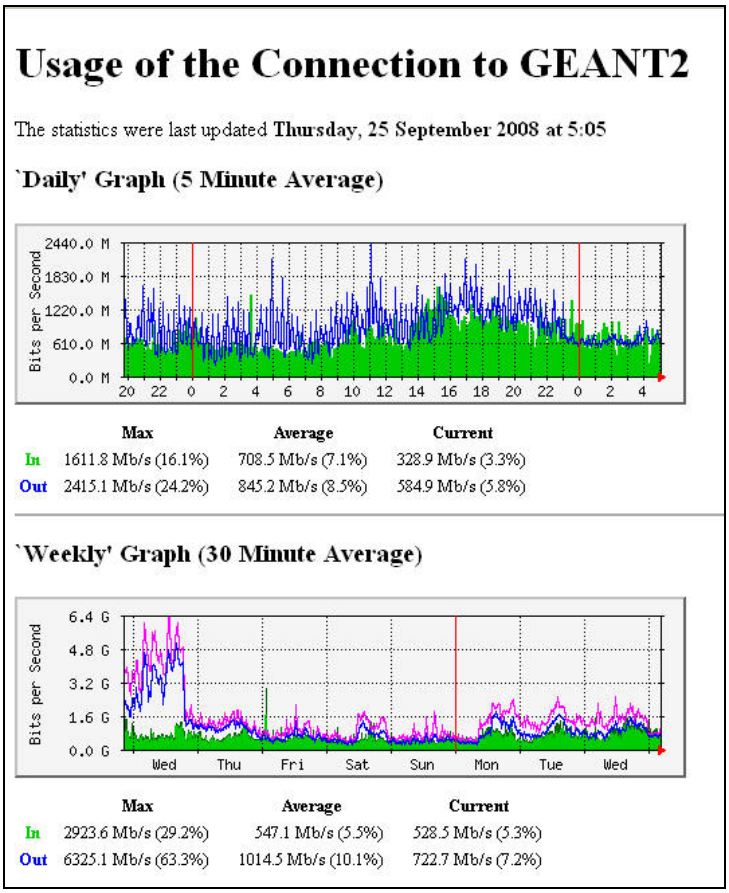
三、可於 Active port 中看到本機上正在建立連線的程式、本機 IP、本機開啓的 port、連線至遠端的 IP 及 port、連線狀態、協定。

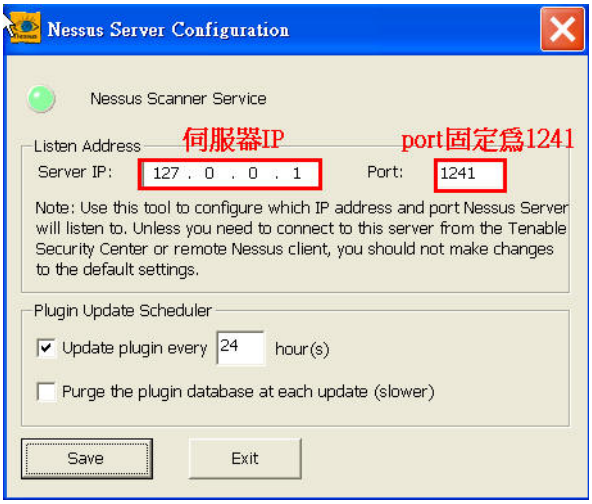
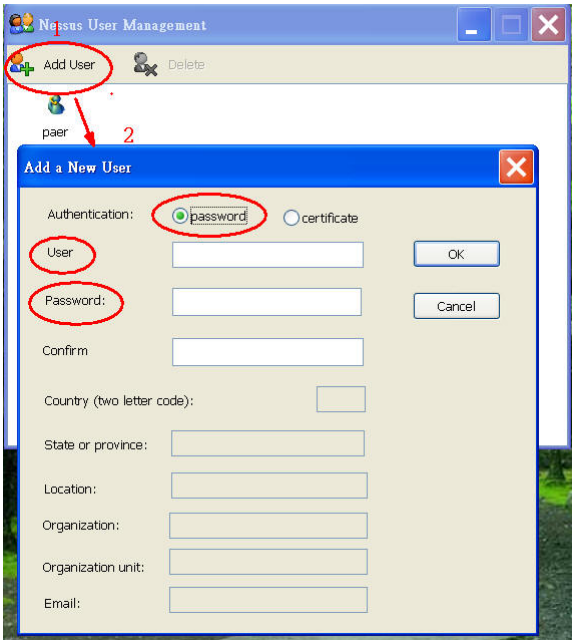
Process	PID	Local IP	Local Port	Remote IP	Remote Port	State	Protocol
msnmsgr.exe	3620	172.16.5.176	9			LISTEN	UDP
msnmsgr.exe	3620	127.0.0.1	1092			LISTEN	UDP
msnmsgr.exe	3620	172.16.5.176	1229	172.16.5.166	1454	ESTABLISHED	TCP
msnmsgr.exe	3620	172.16.5.176	1095	207.46.108.77	1863	ESTABLISHED	TCP
svchost.exe	1764	172.16.5.176	1900			LISTEN	UDP

四、亦可看到建立連線的程式所在目錄。

Protocol	Path
UDP	C:\Program Files\Windows Live\Messenger\msnmsgr.exe
UDP	C:\Program Files\Windows Live\Messenger\msnmsgr.exe
TCP	C:\Program Files\Windows Live\Messenger\msnmsgr.exe
TCP	C:\Program Files\Windows Live\Messenger\msnmsgr.exe

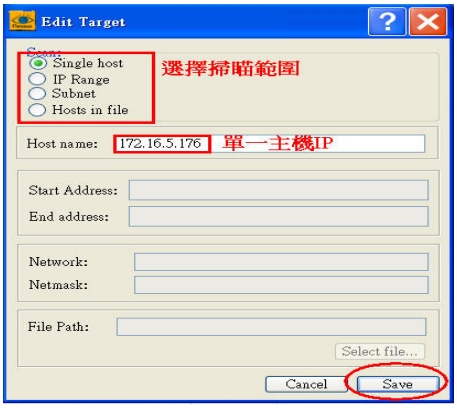
</td></tr>
<tr><td>2、軟體名稱</td><td>MRTG（Multi Router Traffic Grapher）</td></tr>
<tr><td>軟體簡介</td><td>MRTG 是一套伺服器及網路設備運作狀況監控程式。MRTG 是透過 SNMP 協定來了解設備運作資訊的，MRTG 程式向主機詢問相關的資料後，主機傳遞數值給 MRTG 程式，然後 MRTG 再繪製成網頁上的圖表。透過 MRTG 的圖表可以讓管理者清楚看到設備運作上的變化（如：網路卡整體流量、CPU 使用率、RAM 使用率趨勢等），使管理者更能掌控資訊資源使用情況，以做適當的管理及應變。</td></tr>
<tr><td>軟體性質</td><td>免費軟體</td></tr>
<tr><td>作業系統平台</td><td>Linux、Windows</td></tr>
<tr><td>語言界面</td><td>英文</td></tr>
<tr><td>軟體下載網址</td><td>http://oss.oetiker.ch/mrtg/pub/?M=D</td></tr>
<tr><td>軟體操作說明</td><td>一、MRTG 安裝方式較複雜，於 linux 上安裝 MRTG 請參考 http://oss.oetiker.ch/mrtg/doc/mrtg-unix-guide.en.html，於 Windows 上安裝 MRTG 請參考 http://oss.oetiker.ch/mrtg/doc/mrtg-nt-guide.en.html。
二、安裝完成後，設定監控一個網路設備（該設備須開啓 snmp 功</td></tr>
</table>

	能）。 三、MRTG 可提供網頁介面讓使用者看到網路設備的流量趨勢圖（可分爲 日、周、月流量圖）。 
3、軟體名稱	Nessus
軟體簡介	Nessus 是一個針對伺服器作業系統以及所提供服務的弱點所設計出來的掃描的軟體，功能強大且執行速度快，它主要是針對系統上的安全漏洞做檢查，使用者可依據自己的需求設定 Nessus 要偵測的漏洞。Nessus 其實可以視爲一種攻擊工具，掃描程式以 NASL 寫成 script，而每種弱點都寫成一隻 plugin，這種 plugin 的架構在維護更新攻擊測試程式是迅速方便的。在掃描的結果方面，Nessus 提供了很詳細的資訊，會將弱點分成低、中、高，三個等級，並且也有描述解決方式，供管理者方便去更新軟體漏洞。因此常被資安業者拿來使用，政府部門也有在推行 Nessus 的使用，以加強政府單位的資安檢測能力。（參考資料：http://www.pcdiscuss.com/forum/archiver/tid-22597.html）
軟體性質	免費軟體
作業系統平台	Nessus 3 支援 - Linux: Fedora 7, 8 and 9, Red Hat Enterprise 3, 4 & 5 (i386 and x86-64), CentOS 3, 4 & 5, SuSE 9.3 & 10, Debian 4(i386, amd64), Ubuntu 7.10

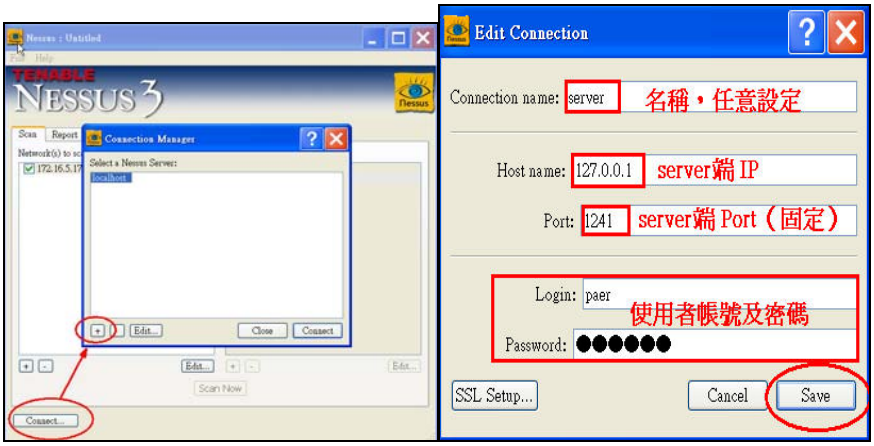
	(i386) and 8.04 (i386, amd64) - FreeBSD: FreeBSD 7 (i386) - Solaris: Solaris 9 & 10 (sparc) - Mac OS X: Mac OS X 10.4 and 10.5 (intel & ppc) - Windows: Windows XP, 2003, Vista and 2008
語言界面	英文
軟體下載網址	http://www.nessus.org/download/
軟體操作說明	一、安裝程式後（server 及 client 端軟體皆須安裝，兩者可安裝在同一台主機），先執行「Nessus server configuration 程式」設定 server 端。 二、設定 server 端 IP 及 port。  三、設定 server 端使用者名稱及密碼，提供 client 端登入用。 

四、將「Nessus server configuration 程式」設定儲存後關閉，然後執行「Nessus client 程式」，加入掃瞄目標。

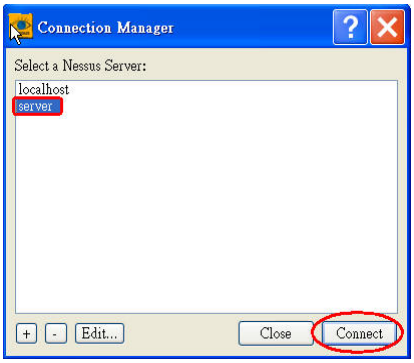
五、選擇掃瞄目標及範圍。



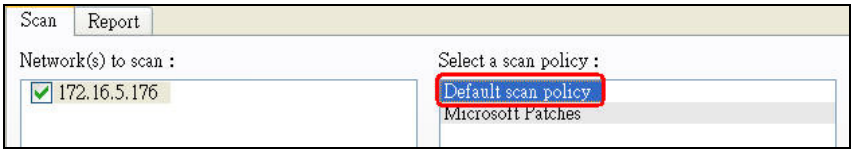
六、設定完掃瞄目標後，開始設定 connetion manager。connetion manager 即 Nessus server，由於 Nessus server 安裝於本機上，故設定爲本機 IP 即可。



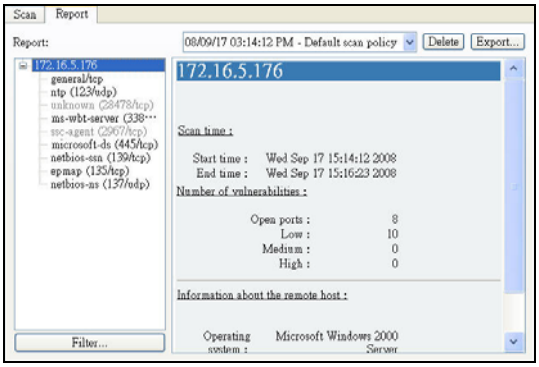
七、設定 connetion manager 完成後，按下 connect 鍵，即連線至伺服器端。

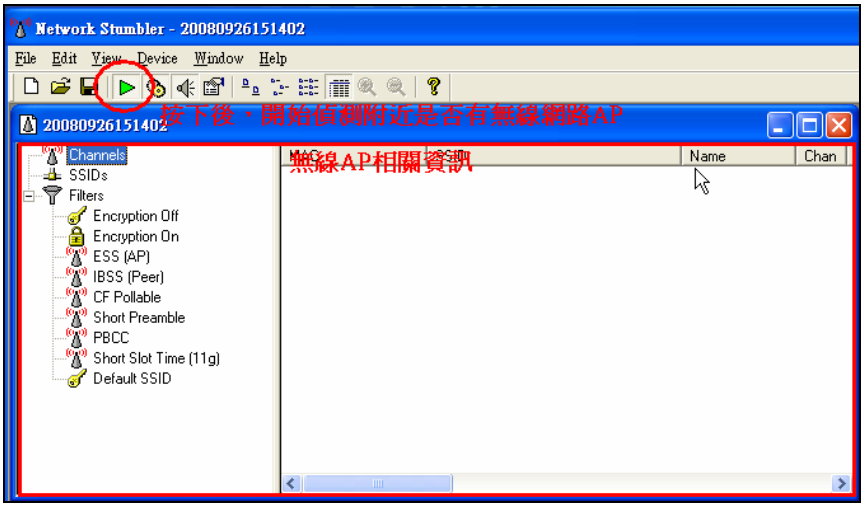
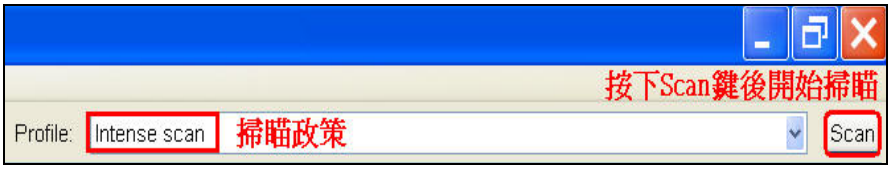


八、連線至伺服器端後，「Select a scan policy：」集出現可選擇的伺服器端之掃瞄政策。選擇掃瞄政策（政策可由使用者自行調整）後，按下 Scan Now 鍵後，開始針對 172.16.5.176 進行掃瞄動作。

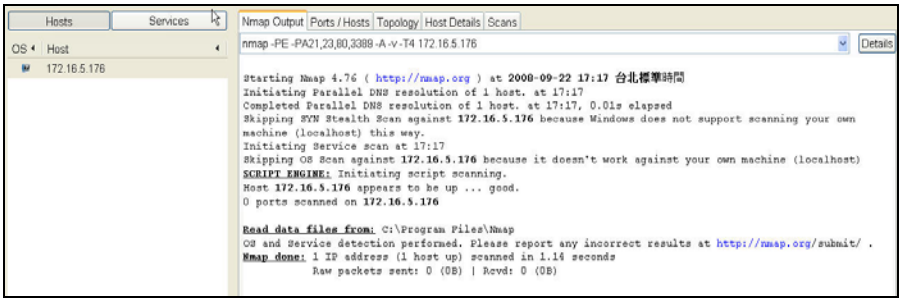


九、掃瞄結束後，將結果於 Report 欄列出。

	
4、軟體名稱	Netstumbler
軟體簡介	Netstumbler 是一款免費的無線網路工具軟體，它可以檢查公司的無線網路中是否存在不安全的連接，也可以用來判斷無線信號的強弱。這個軟體執行於 Windows 上的 802.11b/a/g 網路，而且可以隨著無線網路協定和標準的改變而不斷進行更新昇級。Netstumbler 不但可以自動偵測無線電訊號，並且可以找出 Access Point 的 MAC 位址、無線網路的名稱、SSID、製造廠商、目前所使用的頻道、有沒有使用 WEP 加密技術、信號強度、乃至噪訊比。 （參考資料：http://forum.slime.com.tw/thread175120.html）
軟體性質	免費軟體
作業系統平台	Windows
語言界面	英文
軟體下載網址	http://www.netstumbler.com/downloads/
軟體操作說明	一、安裝完成後，啓動程式。  二、程式啓動會自動偵測附近有無無線 AP，若有無線 AP 存在，會將 AP 相關資訊列出。

	
5、軟體名稱	Nmap
軟體簡介	Nmap 是一套免費的開放原始碼工具，它可以探測網路服務或做安全稽核，例如探測網路上的主機有開啓什麼樣的服務，正在執行的作業系統版本等。Nmap 可以針對一個網段進行掃描，也可針對單一主機進行更高階的掃描。在進行網路安全檢測時，常使用 Nmap 及 Nessus 來進行測試工作。
軟體性質	免費軟體
作業系統平台	Nmap 4.68 支援 Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS
語言界面	英文
軟體下載網址	http://nmap.org/download.html
軟體操作說明	一、安裝完成後，執行程式  。 二、填入「掃瞄目標」及選擇「掃瞄政策」後開始掃瞄。  

三、顯示掃瞄結果。



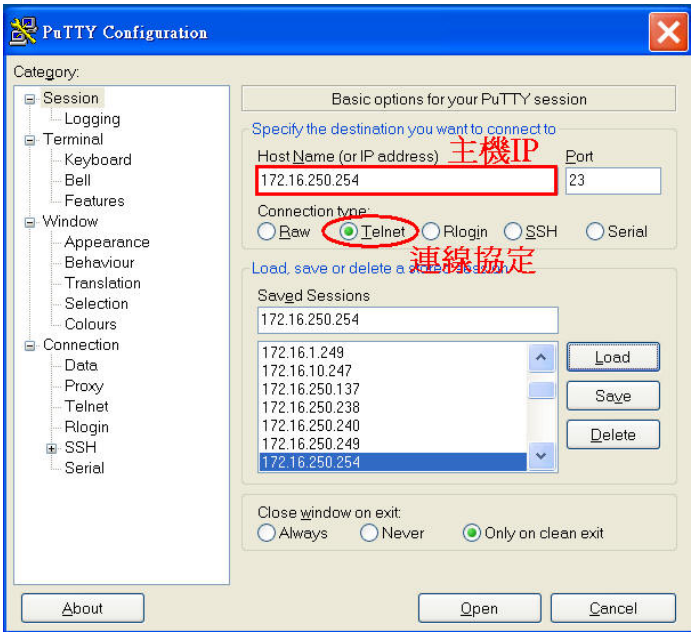
四、可以由使用者自訂掃瞄指令（Command）。指令格式說明如下：

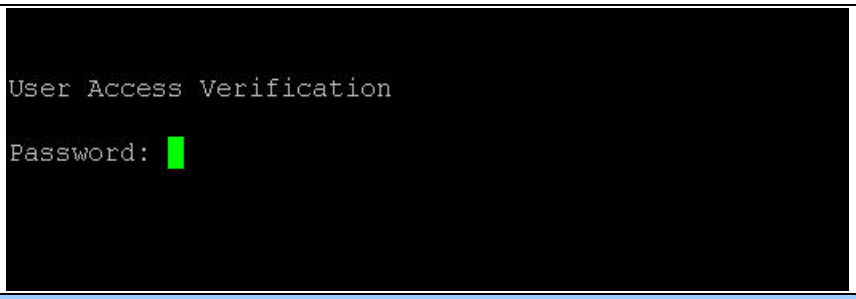
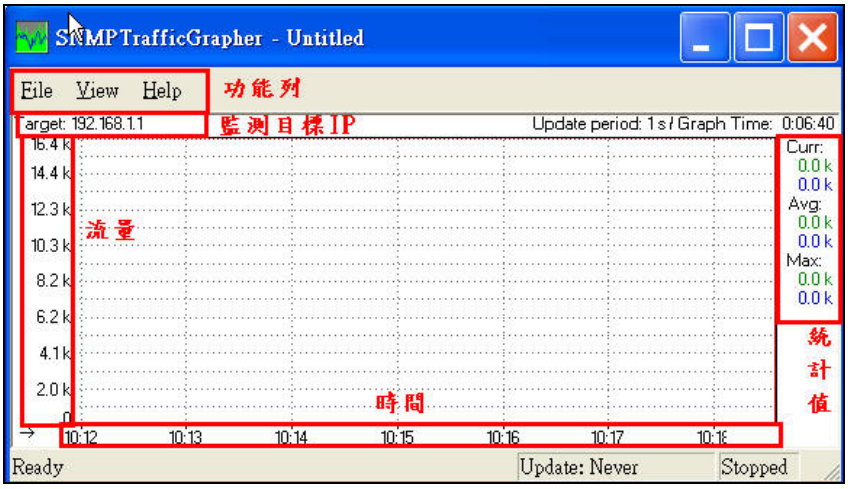
Nmap 指令語法：nmap [Scan Type(s)] [Options]

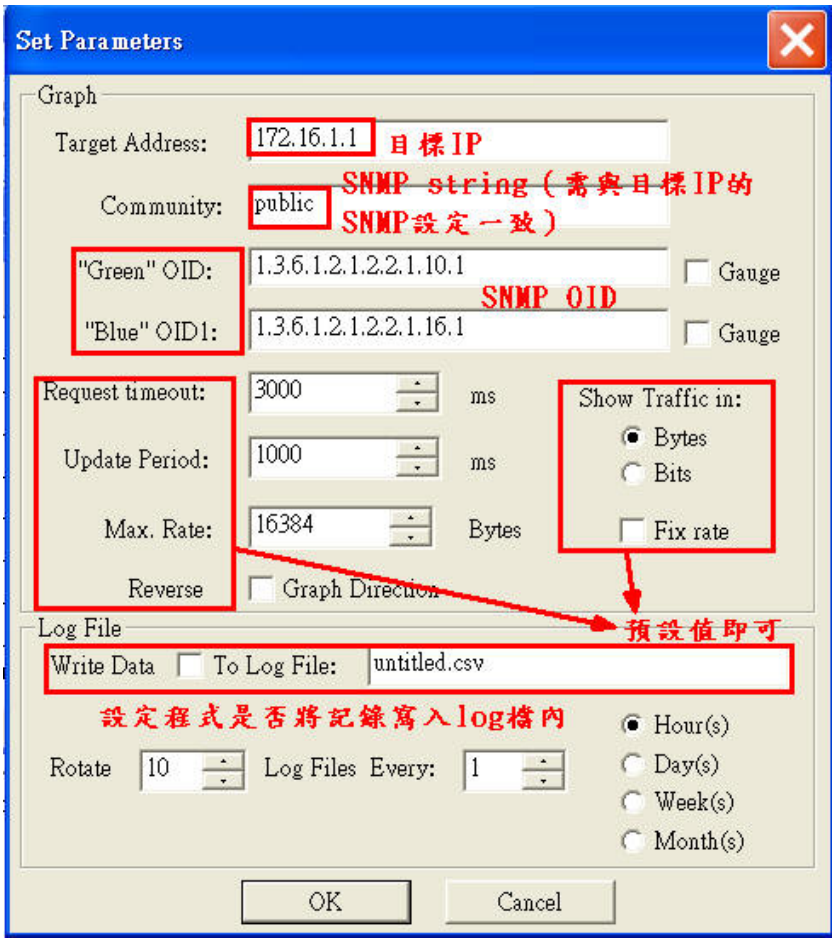
- 功能選項可以組合使用。一些功能選項只能夠在某種掃瞄模式下使用。nmap 會自動識別無效或者不支援的功能選項組合
- 使用 nmap －h 可快速列出功能選項的列表

掃瞄範例如下：

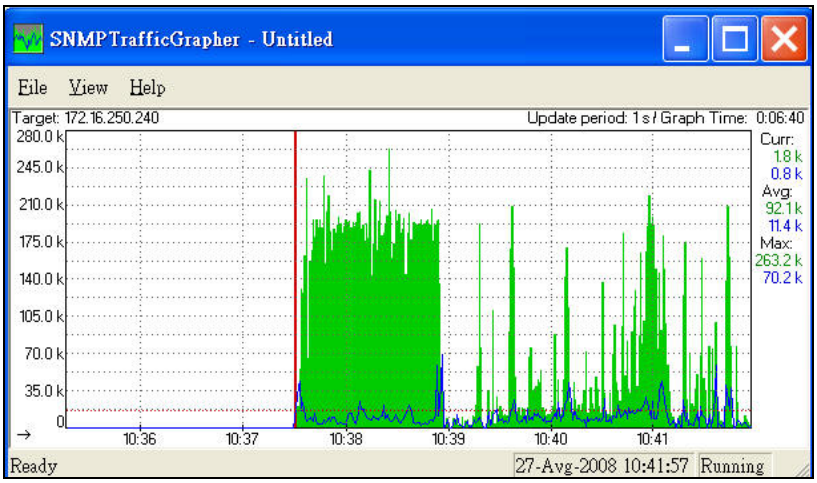
- nmap -v target.example.com
  掃瞄主機 target.example.com 的所有 TCP 埠。-v 細節模式 。
- nmap -sS -O target.example.com/24
  掃瞄對 target.example.com 所在網絡上的所有 255 個 IP 地址的秘密 SYN 掃瞄。同時還探測每台主機操作系統的指紋特徵。
- nmap -sX -p 22,53,110,80 210.69.*.1-127
  對 B 類 IP 地址 210.69 中 255 個可能的 8 位子網的前半部分發起聖誕樹掃瞄。確定這些系統是否打開了 sshd、DNS、pop3d、和 HTTP 埠。注意聖誕樹掃瞄對 Micro$oft 的系統無效，因爲協定的 TCP 層有缺陷。
- nmap -v --randomize_hosts -p 80 *.*.2.3-5
  只掃瞄指定的 IP 範圍，有時用於對這個 Internet 進行取樣分析。nmap 將尋找 Internet 上所有後兩個字節是.2.3、.2.4、.2.5 的 IP 地址上的 WEB 服務器。如果你想發現更多有意思的主機，你可以使用 127-222，因爲在這個範圍內有意思的主機密度更大。
- nmap -sT -O localhost
  校驗哪些埠正在監聽 。
- nmap -sP -O 10.0.0.0/24
  掃瞄哪些埠正在監聽 。

6、軟體名稱	putty
軟體簡介	putty 是一套免費的 SSH / Telnet 程式，它可以連接上支援 SSH /Telnet 連線的站台，在這些站台上下各種操作指令。（SSH 是一種加密通訊息協定，可以將 Telnet 的內容加以加密保護，避免資料內容被第三者截取。）並提供站台記錄功能。
軟體性質	免費軟體
作業系統平台	較早的版本僅支援 Windows 平台，在最近的版本中開始支援各類 Unix 平台
語言界面	英文/中文
軟體下載網址	http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
軟體操作說明	一、執行 putty 程式。  二、輸入要 SSH /Telnet 連線的站台 IP，及選擇連線協定。  三、按下 open 鍵。  四、連線至站台上操作。

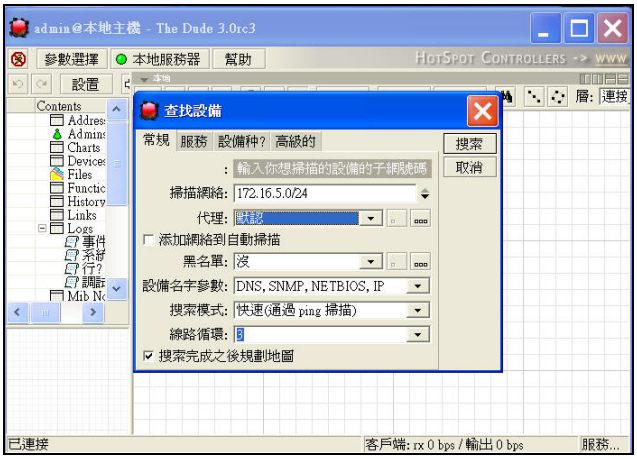
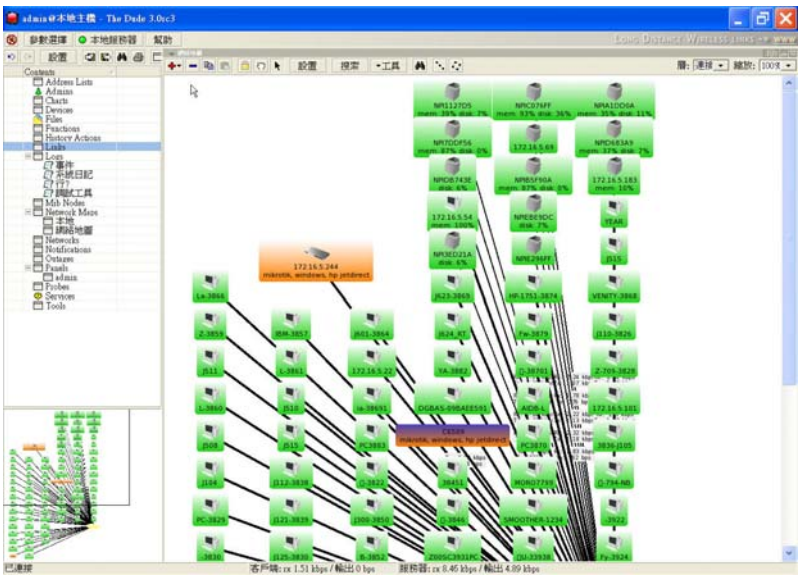
	
7、軟體名稱	SNMP Traffic Grapher
軟體簡介	SNMP Traffic Grapher 爲一套流量監控軟體，可以即時顯示網路介面的流量。程式小執行速度快，相對於 MRTG 每分鐘統計一次的流量資料，SNMP Traffic Grapher 所展現的流量資訊是以每秒速度來更新，因此展現的流量狀態更爲即時，適合用觀察短時間流量狀態變化時使用。PS: 使用 SNMP Traffic Grapher 需熟悉監控設備之 SNMP 相關設定及 OID 值。
軟體性質	免費軟體
作業系統平台	Windows
語言界面	英文
軟體下載網址	http://leonidvm.chat.ru/
軟體操作說明	一、SNMP Traffic Grapher 不需安裝，直接按下執行程式。  二、開啓程式後，執行畫面如下。  三、設定監控流量之目標，選擇功能列上的「view」內的「setting」。 四、設定「setting」中的各項參數，設定如下圖所示：

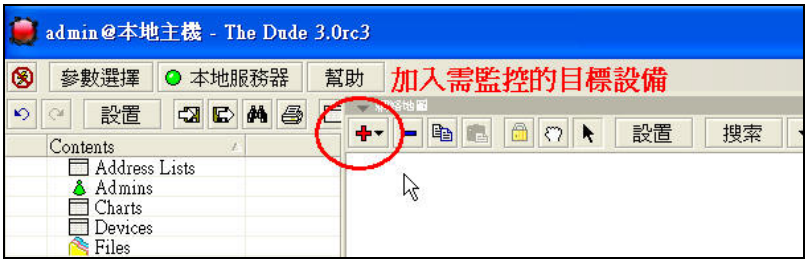


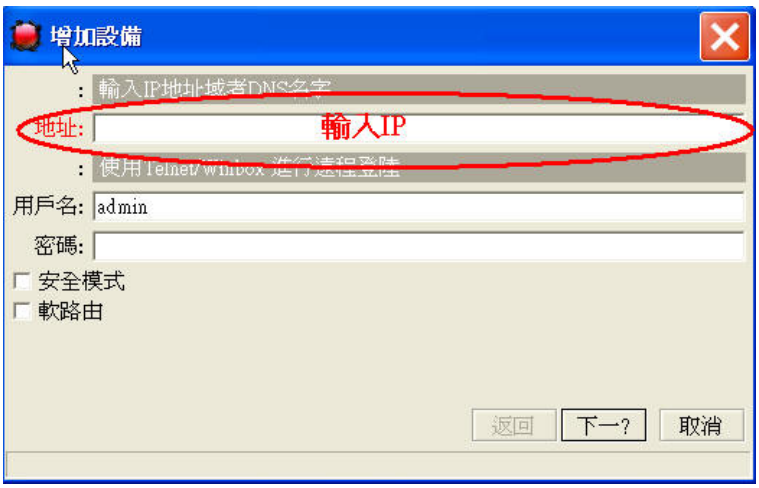
五、按下「OK」鍵後，程式立刻開始監控目標設備流量。監控畫面如下：

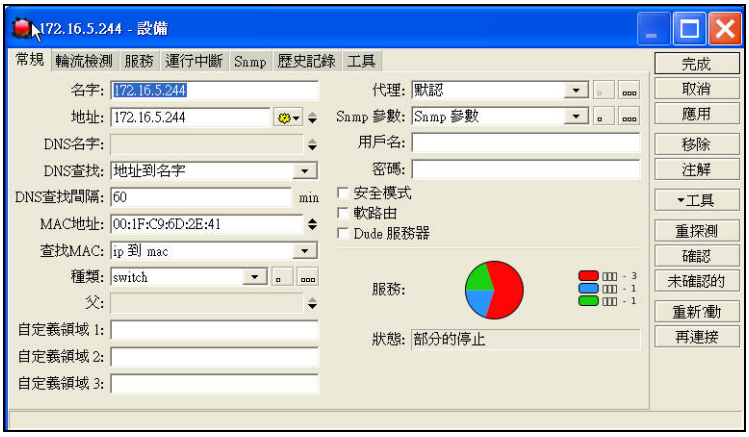


8、軟體名稱	The Dude
軟體簡介	The Dude 是一種網路管理工具，具備圖形化的操作介面，主要功能爲監控伺服器跟網路設備。這套軟體的優點在於可自動搜尋網路上的主機跟設備，包括各個使用 PC、各種功能伺服器、印表機、Router 等，凡是使用到 ip 的裝置都能被偵測到，會自動繪製成網路拓樸

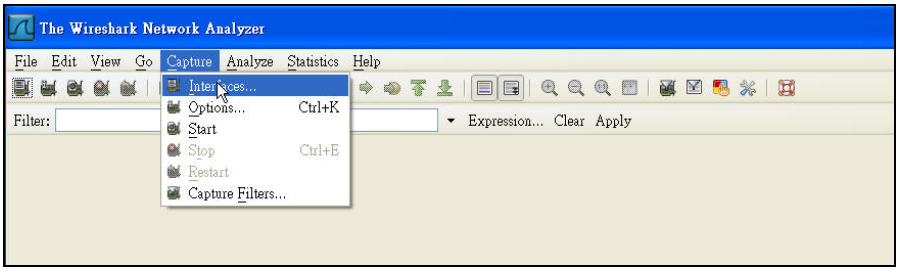
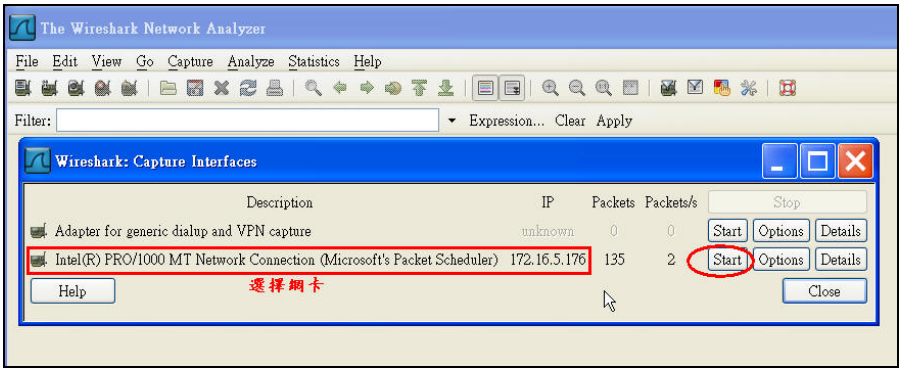
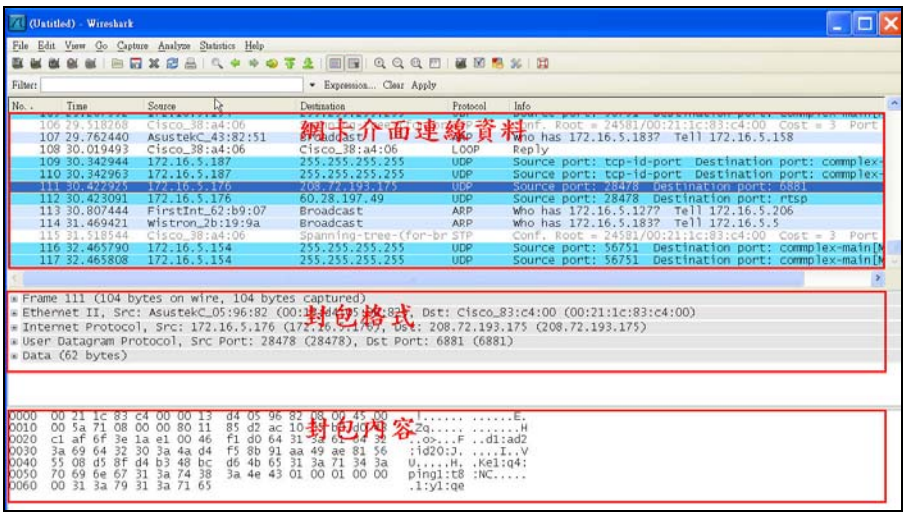
	圖，並支援 snmp 協定，可監控流量及網路服務。The Dude 也提供一些網路管理工具如：ping 、traceroute 等。The Dude 對於實際的檢查、測試功能也不馬虎，不但能查詢各電腦處理器和記憶體使用率、也能檢查硬體週邊的緩衝記憶體以及排程用量
軟體性質	免費軟體
作業系統平台	Windows XP/2000
語言界面	中文/英文
軟體下載網址	http://www.mikrotik.com/thedude.php
軟體操作說明	一、安裝完成後，執行程式。 二、可以自動搜尋網路上的主機跟設備。  三、自動搜尋後，可自動繪製成網路拓樸圖。  四、也可以單獨加入需監控的設備。

<table>
<tr><td></td><td>


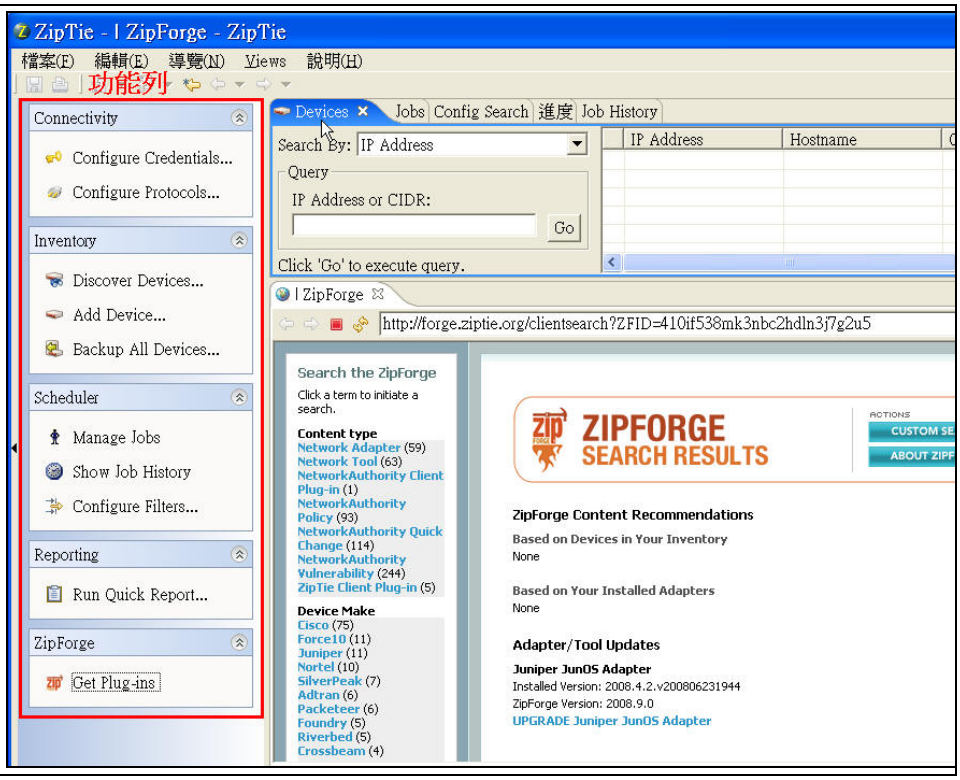


五、可自行調整被監控設備的相關參數。


</td></tr>
<tr><td>9、軟體名稱</td><td>Wireshark</td></tr>
<tr><td>軟體簡介</td><td>Wireshark 是網路封包分析工具。主要作用是收集網路封包，並顯示封包內的詳細傳輸資料。使用 Wireshark 可看到網路中最原始的資料（每個封包的格式、型態等），能協助網管人員了解網路上的真實情況。主要應用於解決網路故障問題、檢測網路安全、測試協定執行情況、查看封包的詳細協定資訊等。Wireshark 也提供通過多種方式過濾封包，多種方式查詢封包，通過過濾以多種色彩顯示封包及建立多種統計分析等功能，加強軟體使用便利性。</td></tr>
<tr><td>軟體性質</td><td>免費軟體</td></tr>
</table>

作業系統平台	Wireshark 1.0.2 支援 Windows / linux / OS X / Solaris
語言界面	英文
軟體下載網址	http://www.wireshark.org/
軟體操作說明	一、安裝完成後，執行程式。 二、選擇要收集封包的介面（即網卡）。   三、開始收集介面上面收送的封包。 
10、軟體名稱	ZipTie

軟體簡介	ZipTie 是一個開放程式碼的軟體，提供使用者有效率地管理網路設備上的設定。它可以備份網路設備上的設定資料，比較網路設備設定是否有更動，搜尋發現指定網路上的所有網路設備，是一個有效清查和管理網路設備設定的工具。
軟體性質	免費軟體
作業系統平台	Windows / Linux / Mac OS X
語言界面	英文
軟體下載網址	http://www.ziptie.org/
軟體操作說明	一、Ziptie 安裝步驟較爲複雜，需先安裝 Sun Java Development Kit (JDK)、Perl 、NMAP 等搭配軟體，Ziptie 本身有兩個安裝軟體，一個是 server 端軟體，另一個是 client 端軟體。以上安裝方式請參閱 http://docs.ziptie.org/doku.php?id=ugdoc:users_guide。 二、安裝完成後，請確認 Ziptie server 端服務已啓動（安裝時可設定是否要自動啓動服務），並開啓 client 端連至 server 端。連至 server 端時需輸入帳號及密碼（預設爲 admin 及 password）、server IP（若在本機則爲 localhost）、port（預設 8080）。  三、Ziptie 操作管理介面如下圖所示，主要功能列位於左邊。詳細操作請參閱 http://docs.ziptie.org/doku.php?id=ugdoc:users_guide。相關使用問題請參考 http://docs.ziptie.org/doku.php?id=doc:faq。



(本文由行政院主計處電子處理資料中心邱弘朝 提供)