

第十三單元

網路流量分析

1. 實驗目的

利用相關 OSS (Open Source Software) 獲得網路流量，並進行分析。

2. 實驗設備

- 安裝 Linux 系統之電腦
- ntop (<http://www.ntop.org>)
- Ipraf (<http://iptraf.seul.org>)
- Sniffit (<http://reptile.rug.ac.be/~coder/sniffit/sniffit.html>)

3. 背景資料

ntop 簡介

ntop 係由義大利 Pisa 大學教授 Luca Deri 於 1997 年開始研發，基於 GNU GPL 的精神，以開放原始碼方式免費提供網路社群使用，協助網路管理工作。ntop 的發展原係為因應對網路頻寬使用狀況的掌握，正如同運用 unix 系統中的 top 指令以瞭解系統資源使用狀況一樣，top 對每一台可見的主機，均對其資訊傳輸活動加以記錄，在網路管理工作上並具有網路流量檢測、網路設定監控等功能。

網路流量檢測

1. **資料傳送及接收**：依據不同的 IP 通訊協定分別統計其傳送及接收的資料量與封包數量。
2. **IP 多址廣播**：對發出或接收多址廣播 (multicast) 的主機分別記錄其傳輸量及封包數量。
3. **TCP 連線記錄**：目前已建立的網路連線及其相關流量資料。
4. UDP 資料傳輸量及其通訊埠。
5. TCP 與 UDP 服務項目。
6. 顯示作業系統名稱、主機 IP 位址。
7. 分析個別主機的頻寬使用率。

另外，ntop 亦對網路整體流量進行分類統計，包括下列項目：

- **流量分佈情形**：區分為本網路主機之間、本網路與外部網路之間、外部網路

與本網路之間的網路流量統計。

- **封包分佈情形**：依據封包大小、廣播型態及 IP 與非 IP 等加以分類及統計。
- **協定使用及分佈情形**：本網路各主機傳送與接收資料所使用的通訊協定種類與資料傳輸量。

網路設定監控

網路使用者必須遵守網路管理所制定的規範，共同維護網路的正常運作，管理者從 ntop 收集的流量資訊中加以分析，可以發現下列違反規定的情形：

1. IP 重複使用情形。
2. 擅自設定路由功能或子網路遮罩設定錯誤情形。
3. **網路應用程式設定錯誤情形**：例如 outlook 被設定為每五分鐘向郵件主機查詢一次新郵件，ntop 客戶端每十秒鐘向主機校正時鐘一次等情形，均可能造成頻寬無謂的浪費。
4. **網路服務濫用情形**：例如機關規定瀏覽外部網站必須經由 proxy 主機，而使用者故意規避的情形，其他如自行建置 HTTP 及 FTP 伺服器之情形。
5. **使用者設定不必要的通訊協定**：例如在無 Novell 伺服器的環境中發現 IPX 通訊協定之情形。
6. **過度耗用頻寬的情形**：例如持續傳輸大型檔案，長時間佔用頻寬，以致於影響他人作業之情形。

Iptraf 簡介

Iptraf 是一套可在 Linux console 端記錄網路上所有封包的一套軟體，它可以收集各種的 TCP/UDP 封包，還有記錄各個封包的連線狀態，以及記錄區域網路的狀態，這一套軟體在 Fedora Linux 的預設套件裡有就有包含了，如果沒有請執行：

```
[root@net122 root]#wget
```

```
ftp://linux.sinica.edu.tw/fedora/linux/core/1/i386/os/Fedora/RPMS/iptraf-2.7.0-8.i386.rpm
```

```
[root@net122 root]rpm -ivh iptraf-2.7.0-8.i386.rpm
```

Iptraf 的運作特色如下所示：

- 一個 IP 通訊的監示系統，可以監測所有通過網路的封包，並且將它們全部列出來，包含了 TCP 旗標資訊、封包及大小、ICMP 的記錄、OSPF（最短優先路徑）封包型態。
- 一般的及詳細的 IP、TCP、UDP、ICMP 及 non-IP 和其他 IP 封包型態的記錄，其他的包含了 IP checksum errors、interface activity、packet size counts。
- 記錄及監控了 TCP 及 UDP 等應用服務的進出封包資訊。
- 記錄一個區域網路內的各種情況，以及某一個主機所傳送的所有資訊封包。

- 過濾 TCP、UDP 及其他協定列出的資訊，用來允許去觀察特定的協定封包，這樣對於管理及除錯會有很大的幫助。
- 擁有記錄的功能。
- 支援 Ethernet、FDDI、ISDN、SLIP、PPP 及 loopback 介面型態。
- 利用 Linux 核心嵌入的未加工的界面，允許在各式各樣的支援的網路卡片上使用 Iptraf。
- 全螢幕、選單式的操作介面。

Iptraf 支援了以下的協定：

- IP
- TCP
- UDP
- ICMP
- IGMP
- IGP
- IGRP
- OSPF
- ARP
- RARP

接著使用指令的模式來進行記錄的動作，其格式如下：

```
iptraf { [ -f ] [ -q ] [ { -i iface | -g | -d iface | -s iface | -z iface | -l iface } [ -t timeout ] [ -B [ -L logfile ] ] } [ -h ] }
```

選項部份包含：

- **-i iface**：當開始使用 Iptraf 來監測時，所要指定的網路介面為何，或者可以使用 -i all 的模式來監控所有的網路介面。
- **-g**：將 Iptraf 直接啟動在簡易監測的模式下（介面封包數量）。
- **-d iface**：將 Iptraf 直接啟動在詳細監測的模式下（介面封包數量）。
- **-s iface**：將 Iptraf 直接啟動在監測封包數的模式下，並用協定的種類來分類。
- **-z iface**：將所有的封包依照大小來進行分類的動作。
- **-l iface**：和 -i 的選項相同，只不過這個模式是利用 MAC 位址的模式來進行監控。
- **-t timeout**：指定 Iptraf 在一定的時間內監控。
- **-B**：將標準的輸出重導到/dev/null 中，關閉標準的輸入模式，以及指定這個程式在背景執行。

- **-L logfile**：指定事件記錄的檔案的名稱及位置，預設的檔案名稱是以詳細（detail）或是簡易（general）及網路卡名稱來命名，如果沒有指定位置的話，會放置在/var/log/iptraf 目錄中。
- **-f**：清除所有被鎖住的計數器，這個參數只被用來修復被毀壞的系統。
- **-h**：顯示出所有指令的語法。

Sniffit 軟體簡介

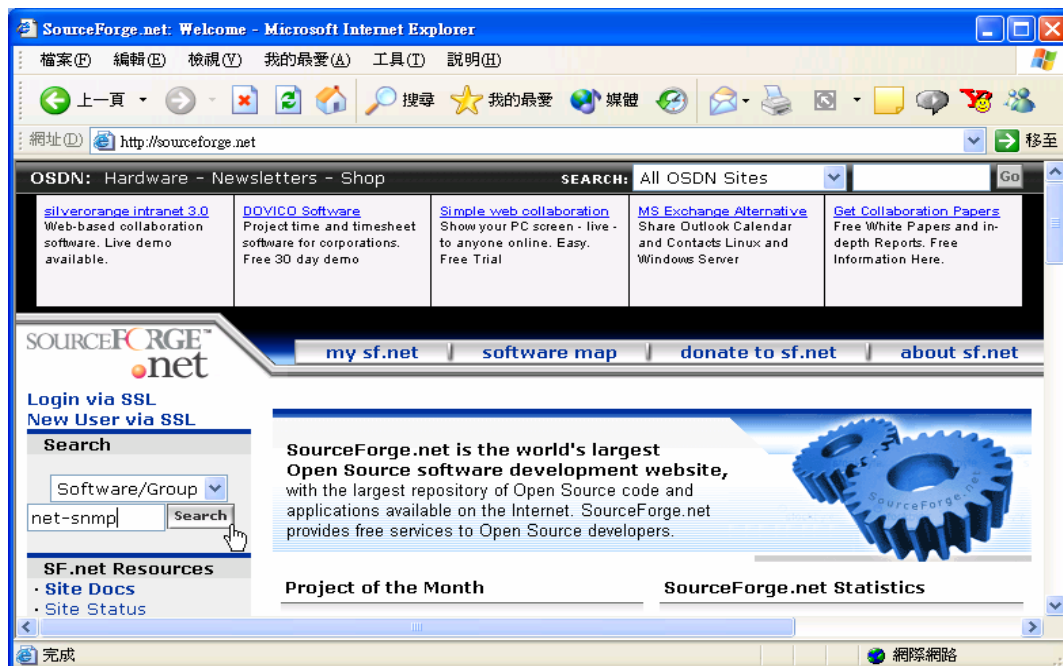
Sniffit 是由比利時工程師所撰寫出來的 shareware 軟體，主要是針對 TCP/IP 協定的不安全性做一番探討。這套軟體的功能是對正在進行 TCP/IP 協定的機器進行竊聽，意即竊聽兩機器間的通訊封包並將它記錄下來，但是，必須是在此封包有經過執行 sniffit 程式的機器上才行；換句話說，sniffit 只能夠竊取同一個網域的機器封包，除非這個外來的封包有經過你的機器才行，否則不大可能去竊取到非本網域之外的機器封包。

4. 實驗方法

安裝 ntop

首先要取得下列 ntop 的套件，建議從 <http://sourceforge.net/> 去 search 下載，接著再開始安裝。

- net-snmp-5.0.9.tar.gz
- ntop-2.2-0.i386.rpm
- rrdtool-1.0.41-1.8.0.ntop.i386.rpm



直接下載：

```
[root@net122 root]# wget
```

```
http://heanet.dl.sourceforge.net/sourceforge/net-snmp/net-snmp-5.0.9.tar.gz
```

```
[root@net122 root]# wget
```

```
http://heanet.dl.sourceforge.net/sourceforge/ntop/rrdtool-1.0.41-1.8.0.ntop.i386.rpm
```

```
[root@net122 root]# wget
```

```
http://heanet.dl.sourceforge.net/sourceforge/ntop/ntop-2.2-0.i386.rpm
```

安裝 net-snmp :

```
[root@net122 root]#tar xvfz net-snmp-5.0.9.tar.gz
```

```
[root@net122 root]# cd net-snmp-5.0.9
```

```
[root@net122 net-snmp-5.0.9]# ./configure ; make; make install
```

安裝 rrdtool 、 ntop :

```
[root@net122 root]#rpm -ivh --nodeps rrdtool-1.0.41-1.8.0.ntop.i386.rpm
```

```
[root@net122 root]#rpm -ivh --nodeps ntop-2.2-0.i386.rpm
```

相關動作 :

```
[root@net122 root]# ln -sf /lib/libssl.so.0.9.7a /lib/libssl.so.2
```

```
[root@net122 root]# ln -sf /lib/libcrypto.so.0.9.7a /lib/libcrypto.so.2
```

```
[root@net122 root]# mkdir /var/ntop
```

```
[root@net122 root]#usr/bin/ntop @/etc/ntop.conf -A
```

接著會要求輸入管理者的密碼，輸入密碼後結束，當以後要在 web 上修改資料時，其管理者為”admin”，請輸入自己的密碼。

```
Please enter the password for the admin user: xxxxxxxx
```

```
Please enter the password again: xxxxxxxx
```

```
17/Feb/2004 14:59:09 Admin user password has been set
```

啟動 ntop :

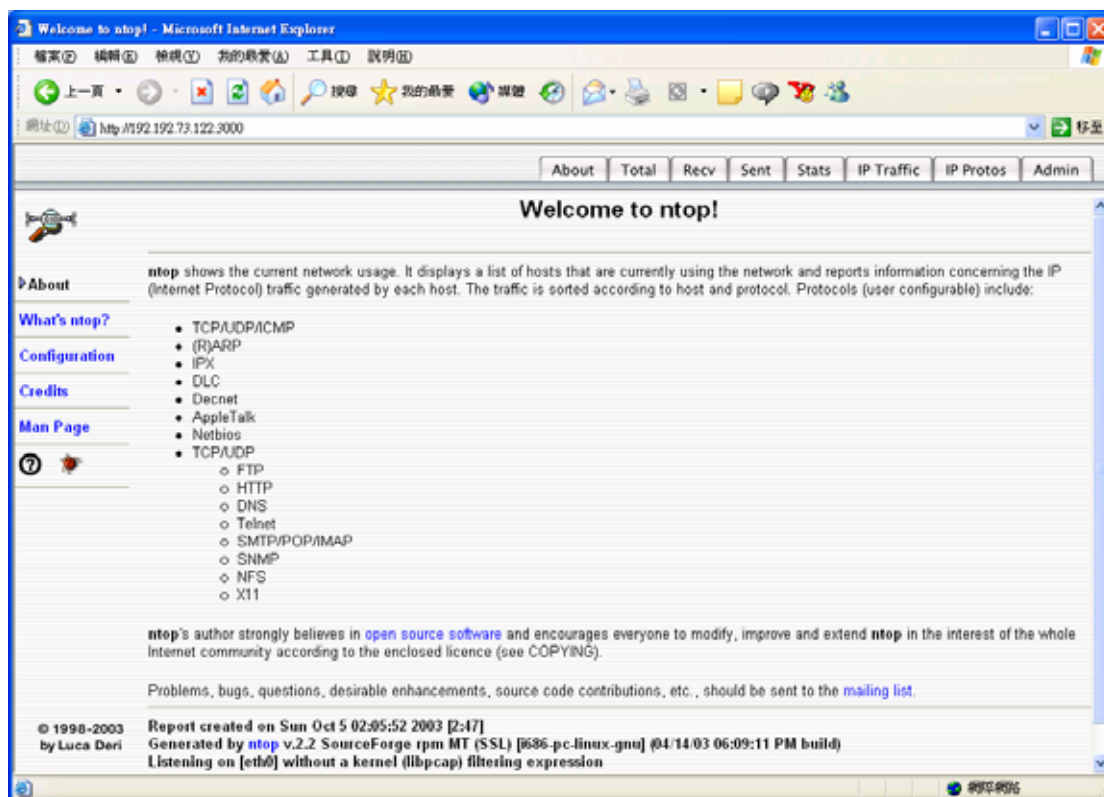
```
[root@net122 init.d]# /etc/rc.d/init.d/ntop restart
```

```
[root@net122 root]# /etc/init.d/ntop restart
Stopping ntop: [ 失敗 ]
Starting ntop: [ 確定 ]
[root@net122 root]# █
```

接著可以開啟瀏覽器，輸入 `http://<your_IP>:3000`，ntop 會使用 port 3000；若是使用 SSL 連線，可以修改設定檔/etc/ntop.conf，ntop 則是使用 port 3001 的 SSL

連線。

在此輸入 `http://192.192.73.122:3000`，進行連線。ntop 的連線畫面如下圖所示。



■ 啟動 ntop 設定檔

啟動 ntop 的相關設定檔存在 `/etc/ntop.conf` 目錄，內容如下：

```
#設定 ntop 執行時的使用者 Sets the user that ntop runs as.
#一般來說都是 ntop
--user ntop

# 設定 ntop 的目錄
--db-file-path /usr/share/ntop

# 設定網路界面，預設是 eth0，若這台主機有做 NAT 功能，可指定為 eth1
#查看虛擬 ip 的流量。
#--interface eth0

# 設定在 port mirroring 或 SPAN 時， ntop 不要信任 MAC 的位址
#--no-mac

#使用 syslog 記錄訊息
#--use-syslog

#設定 ntop 只去追蹤本地主機，同一個 Hub 下的機器
#--track-local-hosts

#設定 HTTP webservice 連線時的 port，預設是 port 3000
--http-server 3000

#設定 HTTPS webservice 連線時的 port，可同時使用 http 及 https 來連線
--https-server 3001

#設定本地的網路
#--local-subnets xx.xx.xx.xx/yy

# 設定使用 domain.
#--domain mydomain.com

# 允許使用 rrd
# --reuse-rrd-graphics

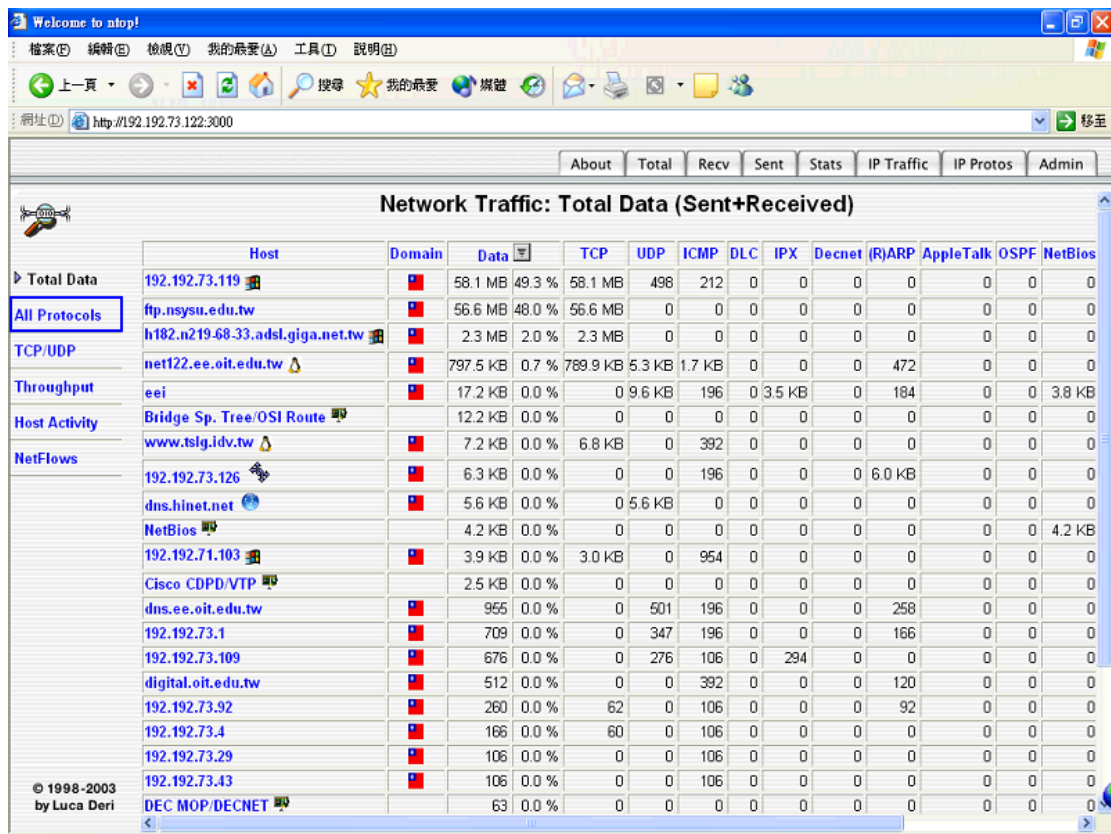
#設定 ntop 以 daemon 方式執行
--daemon
```

■ ntop 應用

首先點選在【Total】中的『All Protocol』選項，如下圖所示的畫面會列出這個網路中所有的流量統計，這個網段為 192.192.73.0/24，ee.oit.edu.tw 為網域名稱。這是在/etc/ntop.conf 中設定—interface eth0 界面的狀態。

在下圖中的最上列為所統計的項目：

Host	Domain	Data	TCP	UDP	ICMP	DLC	IPX	Decnet	(R)ARP	AppleTalk
			OSPF	NetBios	IGMP	OSI	IPv6	STP	Other	



如下圖所示的畫面是在/etc/ntop.conf 中設定—interface eth1 界面的狀態。內部的虛擬 IP 主機只有兩台，分別是 192.168.1.119 和 192.168.1.254。


Network Traffic: Total Data (Sent+Received)													
	Host	Domain	Data	TCP	UDP	ICMP	DLC	IPX	Decnet	(R)ARP	AppleTalk	OSPF	Net
▶ Total Data	192.168.1.119		28.6 KB 50.2 %	0	252	28.3 KB	0	0	0	0	0	0	0
All Protocols	192.168.1.254		28.3 KB 49.8 %	0	0	28.3 KB	0	0	0	0	0	0	0

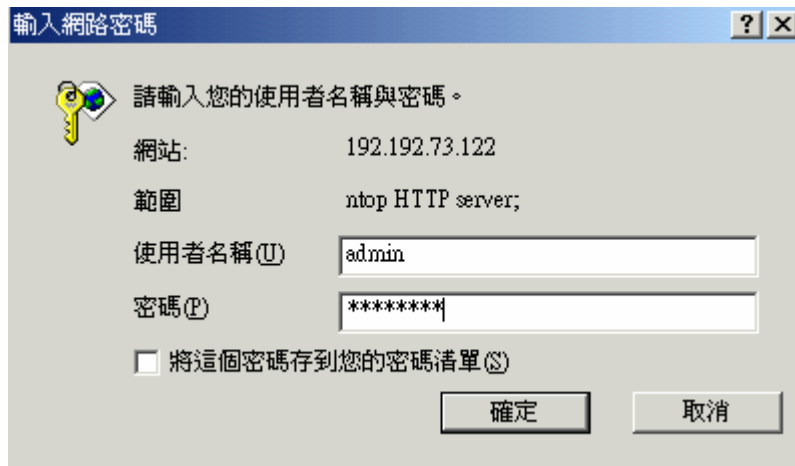
Note: These counters do not include broadcasts and will not equal the 'Global Protocol Distribution'

Report created on Thu Sep 25 12:46:41 2003 [2:29]
Generated by ntop v.2.2 SourceForge rpm MT (SSL) [i686-pc-linux-gnu] (04/14/03 06:09:11 PM build)
Listening on [eth1] without a kernel (libpcap) filtering expression
Web report active on interface eth1
© 1998-2003 by Luca Deri

■ 設定過濾規則

在使用 ntop 時會列出一長串雜七雜八的主機流量統計，但有時只是想查看某幾台電腦的使用情形而已，所以，透過 filter expression（過濾規則）即可達到所要的功能。

點選在【Admin】中的『ChangeFilter 』選項，這裡的 user 是 admin，密碼是之前所設定的密碼。



輸入網路密碼

請輸入您的使用者名稱與密碼。

網站: 192.192.73.122

範圍: ntop HTTP server;

使用者名稱(U): admin

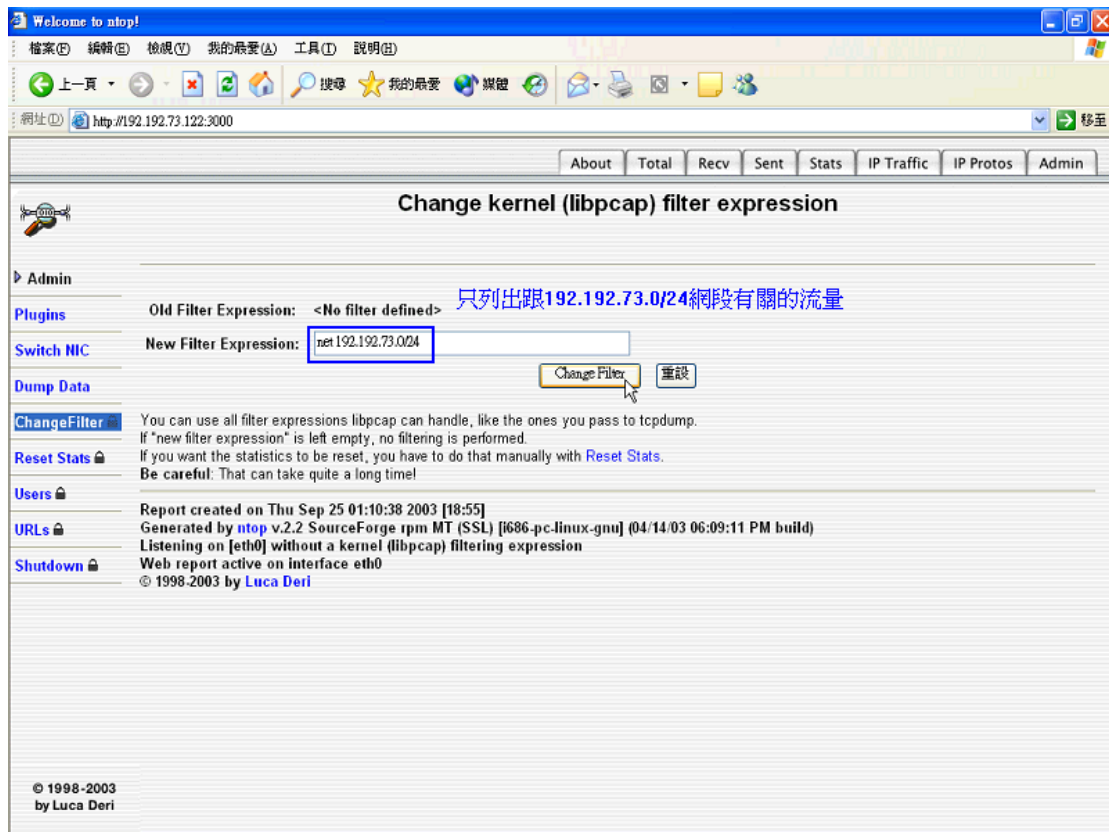
密碼(P): *****

將這個密碼存到您的密碼清單(S)

確定 取消

之後填入 net 192.192.73.0/24，這表示只要列出 net 192.192.73.0/24 這個網段有關的流量統計即可。關於過濾規則，可以參考 tcpdump 的 filter expression，以下只是它的簡單介紹：

- host 192.192.73.122 列出主機 192.192.73.122 的主機流量
- net 192.192.73.0/24 列出網段 192.192.73.0/24 的主機流量
- port ftp-data 列出使用 ftp 傳輸的主機流量



設定完規則後，出現的主機數就變少了。不過，為什麼還是有不屬於 192.192.73.0/24 網段的主機出現呢？這是因為只要是與這個網段做連線、傳輸時，它一樣也會列出來。

如下圖所示是主機 192.192.73.119 正跟 ftp.nsysu.edu.tw 做 FTP 下載，資料有 38.2MB，所以可以清楚知道 192.192.73.119 正佔用著頻寬。接著直接點選 Host 中的 192.192.73.119，會出現更仔細的狀態說明，如主機資訊、交通狀況、封包狀態、協定使用率...等。

Welcome to ntop!

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

上一頁 搜尋 我的最愛 媒體

網址 http://192.192.73.122:3000

About Total Recv Sent Stats IP Traffic IP Protos Admin

Network Traffic: Total Data (Sent+Received)

	Host	Domain	Data	FTP	HTTP	DNS	Telnet	NBios-IP	Mail	DHCP-BOOTP	SNMP	NNTP	NFS	X11
Total Data	192.192.73.119		38.6 MB 44.1 %	38.2 MB										
All Protocols	ftp.nsysu.edu.tw		38.2 MB 43.7 %	38.2 MB										
TCP/UDP	h182.n219.68.33.adsl.giga.net.tw		8.3 MB 9.5 %	0	2.2 KB	0	0	0	0	0	0	0	0	0
Throughput	net122.ee.oit.edu.tw		2.4 MB 2.7 %	0	2.2 KB	6.6 KB	0	0	0	0	0	0	0	0
Host Activity	tslg.idv.tw		7.2 kB 0.0 %	0	0	0	0	0	0	0	0	0	0	0
NetFlows	192.192.73.109		3.6 kB 0.0 %	0	0	0	0	3.4 kB	0	0	0	0	0	0
	192.192.73.1		1.6 kB 0.0 %	0	0	0	0	1.4 kB	0	0	0	0	0	0
	dns.ee.oit.edu.tw		1.1 kB 0.0 %	0	0	172	0	1002	0	0	0	0	0	0
	192.192.73.126		196 0.0 %	0	0	0	0	0	0	0	0	0	0	0
	192.192.73.4		124 0.0 %	0	124	0	0	0	0	0	0	0	0	0
	192.192.73.43		124 0.0 %	0	124	0	0	0	0	0	0	0	0	0
	192.192.73.92		62 0.0 %	0	62	0	0	0	0	0	0	0	0	0

Note: These counters do not include broadcasts and will not equal the 'Global Protocol Distribution'

Report created on Thu Sep 25 01:30:31 2003 [38:48]
 Generated by ntop v.2.2 SourceForge rpm MT (SSL) [i686-pc-linux-gnu] (04/14/03 06:09:11 PM build)
 Listening on [eth0] with kernel (libpcap) filtering expression "net 192.192.73.0/24"
 Web report active on interface eth0
 © 1998-2003 by Luca Deri

© 1998-2003 by Luca Deri

■ 傳輸率 (Throughput)

接著查看 192.192.73.119 跟 ftp.nsysu.edu.tw 之間的下載速率：

Welcome to ntop!

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

上一頁 搜尋 我的最愛 媒體

網址 http://192.192.73.122:3000

About Total Recv Sent Stats IP Traffic IP Protos Admin

Network Traffic: Total Data (Sent+Received)

	Host	Domain	Data			Packets		
			Current	Avg	Peak	Current	Avg	Peak
Total Data	192.192.73.119		3.6 Kbps	573.5 Kbps	5.4 Mbps	6.3 Pkts/sec	79.2 Pkts/sec	778.1 Pkts/sec
All Protocols	ftp.nsysu.edu.tw		0.0 bps	564.8 Kbps	5.4 Mbps	0.0 Pkts/sec	75.6 Pkts/sec	756.4 Pkts/sec
TCP/UDP	h182.n219.68.33.adsl.giga.net.tw		9.9 Kbps	33.1 Kbps	120.0 Kbps	7.0 Pkts/sec	16.1 Pkts/sec	59.8 Pkts/sec
Throughput	net122.ee.oit.edu.tw		1.3 Kbps	7.8 Kbps	50.1 Kbps	0.7 Pkts/sec	4.3 Pkts/sec	26.6 Pkts/sec
Host Activity	192.192.73.126		0.0 bps	0.0 bps	696.8 bps	0.0 Pkts/sec	0.2 Pkts/sec	1.9 Pkts/sec
NetFlows	192.192.73.109		0.0 bps	0.0 bps	234.8 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.2 Pkts/sec
	192.192.73.1		0.0 bps	0.0 bps	0.0 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.1 Pkts/sec
	dns.hinet.net		0.0 bps	0.0 bps	0.0 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.0 Pkts/sec
	00:02:44:13:46:DF		0.0 bps	0.0 bps	0.0 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.0 Pkts/sec
	00:E0:4C:70:1B:D9		0.0 bps	0.0 bps	0.0 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.0 Pkts/sec



Peak values are the maximum value for any 10 second interval.
 Average values are recomputed each 60 seconds, using values accumulated since this run of ntop was started.

Note: Both values are reset each time ntop is restarted.

Report created on Thu Sep 25 01:39:07 2003 [47:24]
 Generated by ntop v.2.2 SourceForge rpm MT (SSL) [i686-pc-linux-gnu] (04/14/03 06:09:11 PM build)
 Listening on [eth0] with kernel (libpcap) filtering expression "net 192.192.73.0/24"
 Web report active on interface eth0
 © 1998-2003 by Luca Deri

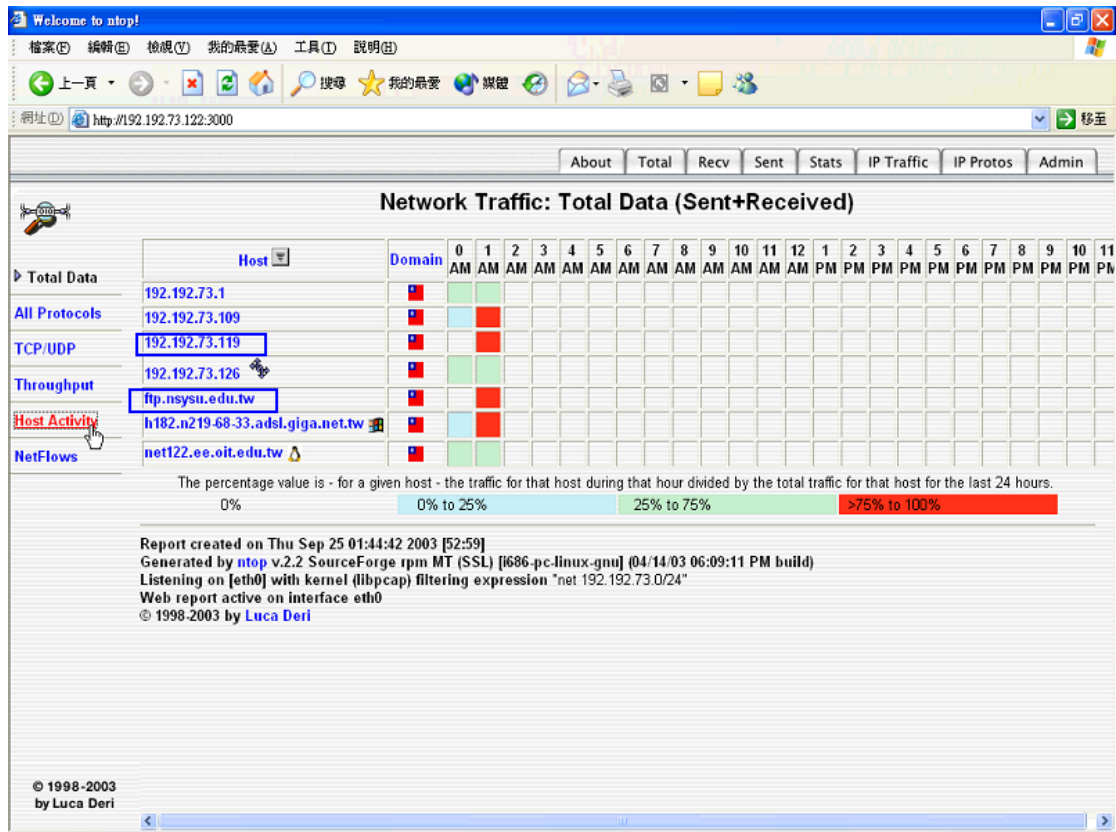
© 1998-2003 by Luca Deri

將圖中的數據抓出來，由下表看出下載的速度相當快，平均有 550 多 Kbps。

Host	Domain	Data			Packets		
		Current	Avg	Peak	Current	Avg	Peak
192.192.73.119		9.2 Kbps	550.5 Kbps	5.4 Mbps	6.8 Pkts/sec	76.2 Pkts/sec	778.1 Pkts/sec
ftp.nsysu.edu.tw		0.0 bps	541.8 Kbps	5.4 Mbps	0.0 Pkts/sec	72.5 Pkts/sec	756.4 Pkts/sec

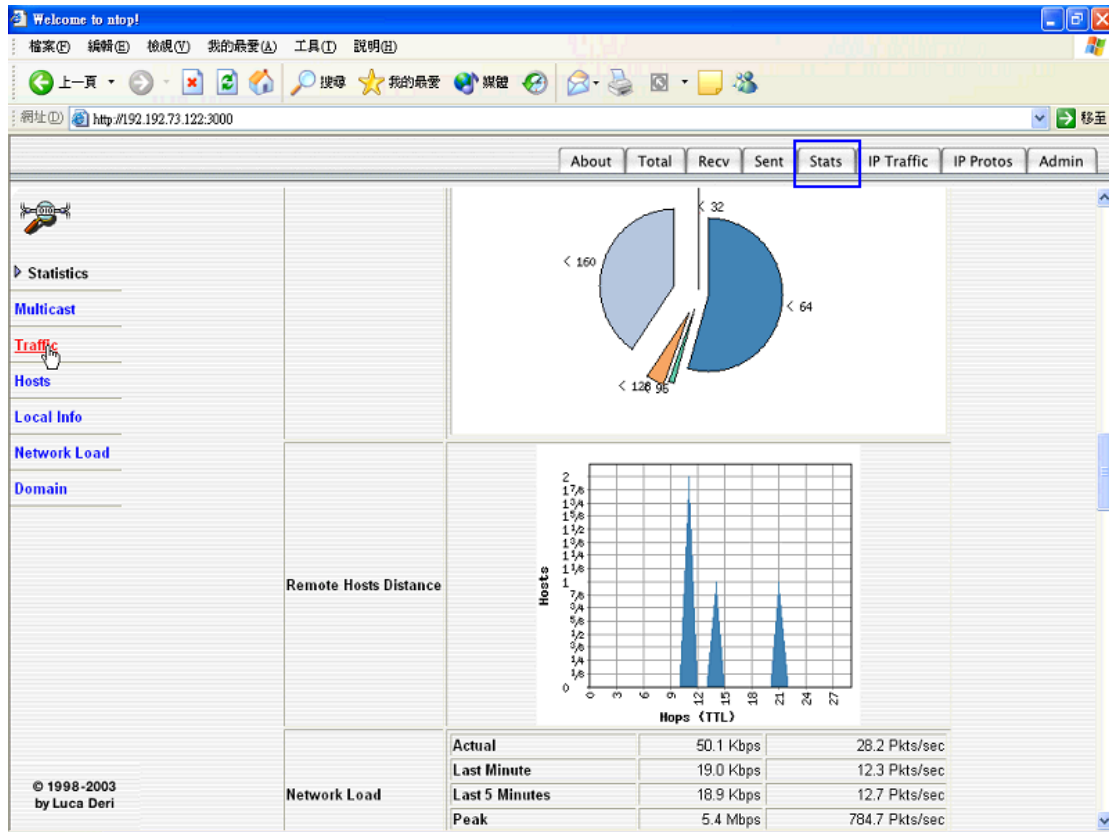
■ 主機活動時間 (Host Activity)

從下圖可以看出主機流量在每個時段傳輸的狀態，依顏色來區分其活動的狀態，紅色表示在這個時間內動作頻繁。



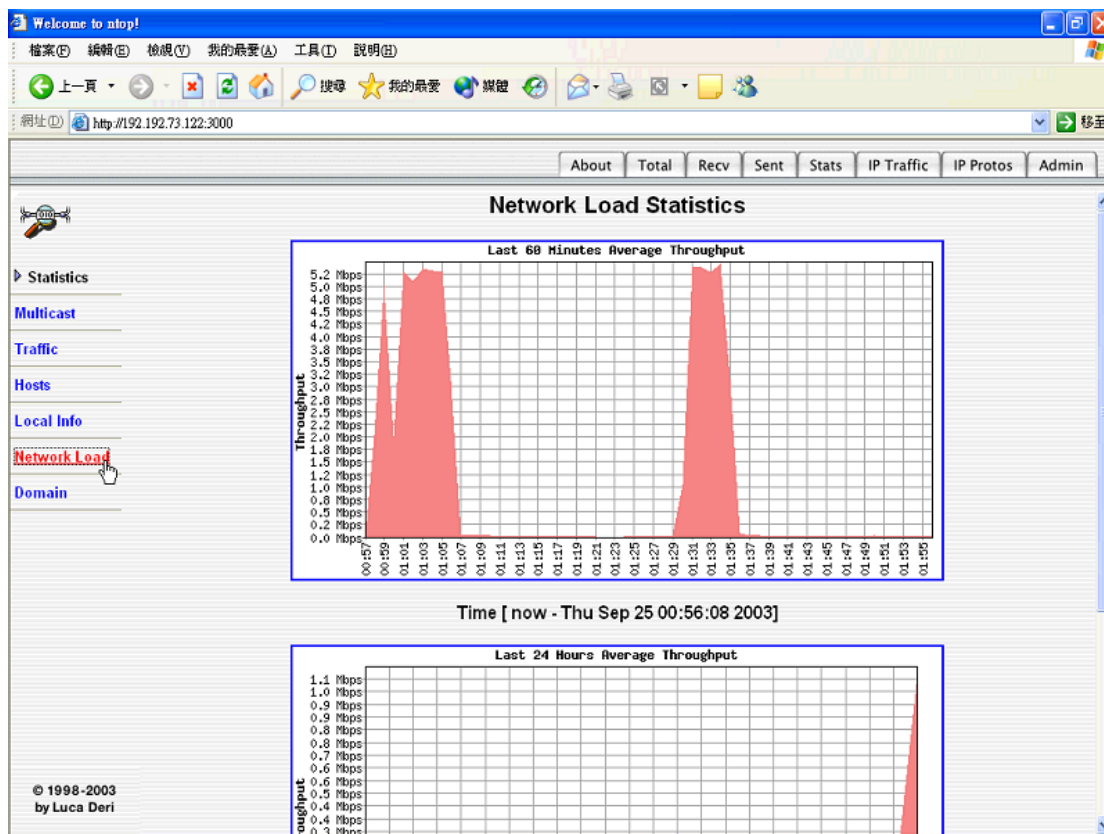
■ 交通狀態

點選【Status】中的『Traffic』，可查看封包的大小數、TTL 反應時間、網路平均負載、協定使用狀況...等。



■ 網路負載



點選【Status】中的『Network Load』，會看到類似 MRTG 的流量統計圖，在第一個圖形中可看出在 00:57~01:07 及 01:29~01:27 這兩個時段是網路流量的尖峰期，也就是在 192.192.73.119 從 ftp.nsysu.edu.tw 下載 ISO 回來時的流量。



■ 清除流量記錄

首先到【Admin】頁面按下『Reset Stats 』，就會將所有的流量重新歸零統計。

透過 ntop 工具，可以藉此了解校園或是公司內網路流量使用情形，每一台主機佔用頻寬的統計一目了然，而電腦的流量也是完全透明化。

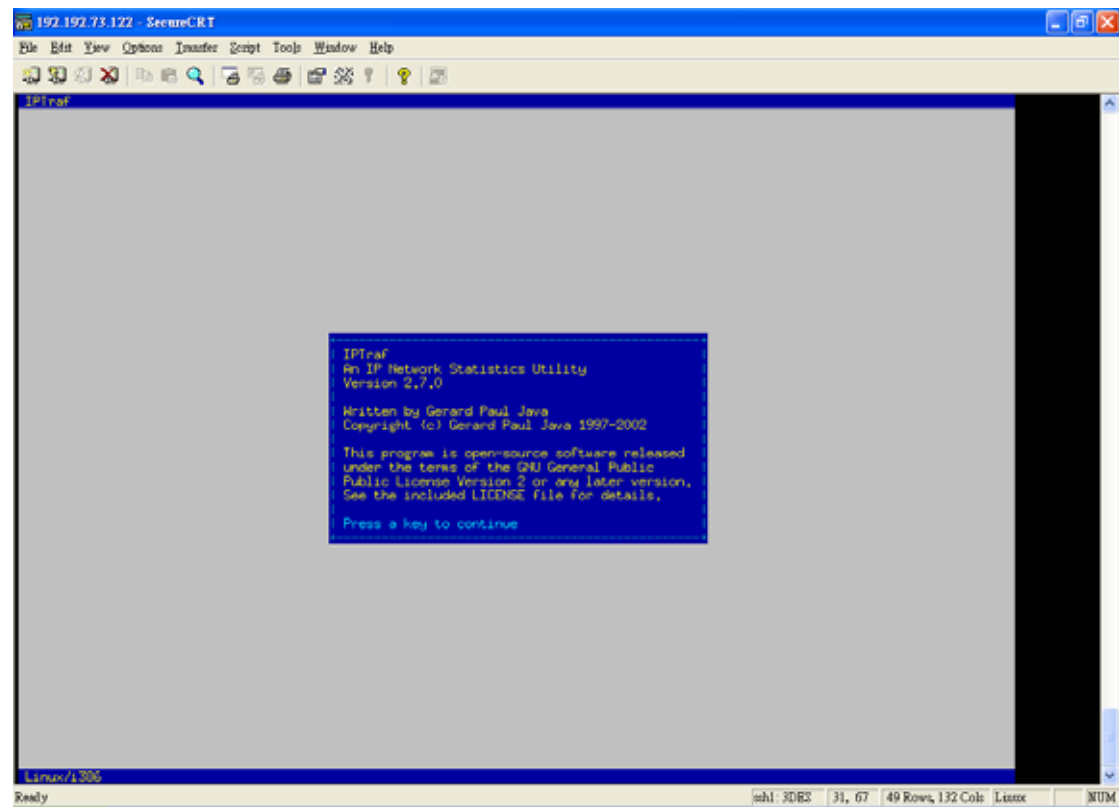
	Client	Server	Data Sent	Data Rcvd	Active Since	Last Seen
IP Protocols	192.192.73.120  :1867	digital.oit.edu.tw:ftp	3.0 KB	3.4 KB	09/25/2003 12:56:42 PM	09/25/2003 01:03:05 PM
Distribution	192.192.73.45:3713	192.192.73.46:microsoft-ds	372	279	09/25/2003 01:03:05 PM	09/25/2003 01:05:58 PM
Usage	192.192.73.13:4335	ee.oit.edu.tw:pop3	88	0	09/25/2003 01:05:58 PM	09/25/2003 01:05:22 PM
Sessions	192.192.72.155:4662	192.192.73.46:135	96	0	09/25/2003 01:05:22 PM	09/25/2003 12:55:04 PM
Routers	192.192.73.120  :1048	baym-gw33.msgr.hotmail.com:http	19.5 KB	19.7 KB	09/25/2003 12:55:04 PM	09/25/2003 01:08:27 PM
ASs	w3-gate.tp1rc.edu.tw:59152	net122.ee.oit.edu.tw:3000	790	84	09/25/2003 01:08:27 PM	
VLANs						

甚至連是在上一個網站看網頁 (http)、下載資料 (ftp) 都會有記錄，例如上圖中的主機 192.192.73.120，就是連到 digital.oit.edu.tw 的 ftp 站，以及使用 baym-gw33.msgr.hotmail.com (http 連線) 在 MSN 上聊天。

執行 Iptraf

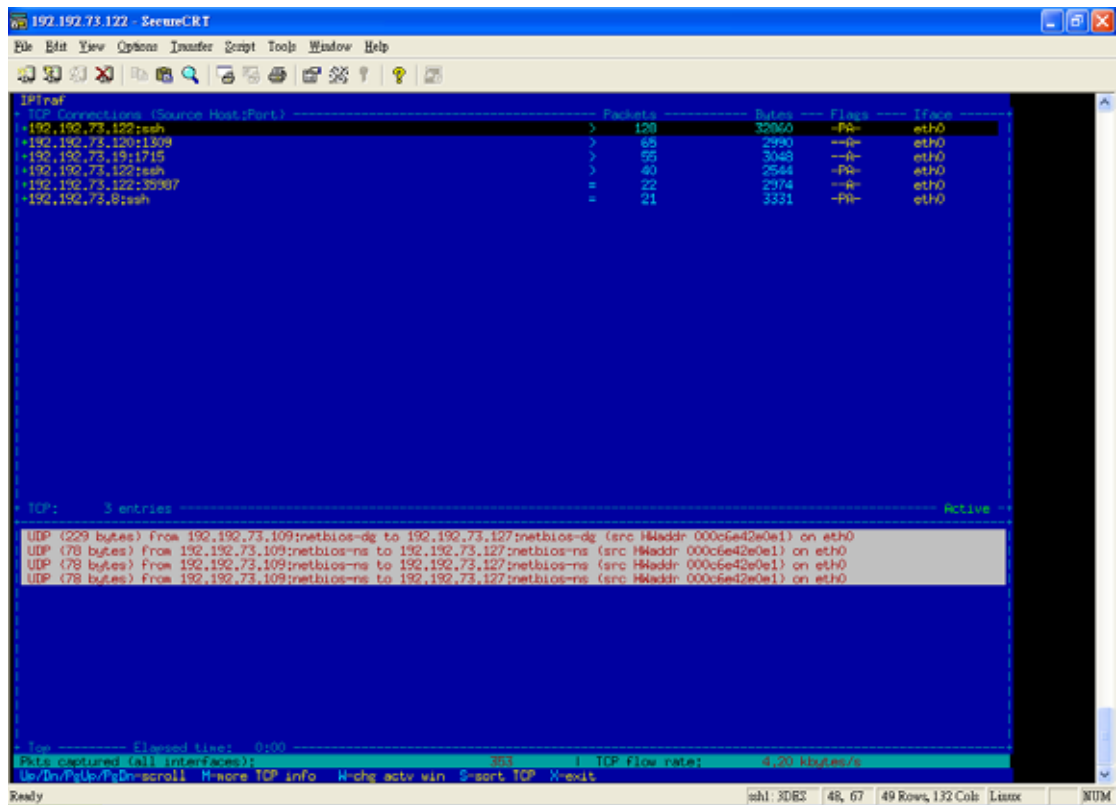
在前一節背景資料的介紹都是在說明如何直接進入該模式來進行監測的動作，其實只要下 iptraf 指令（如下）即可直接進入整個監控的畫面，如下圖所示。

```
[root@net122 ~]# iptraf
```

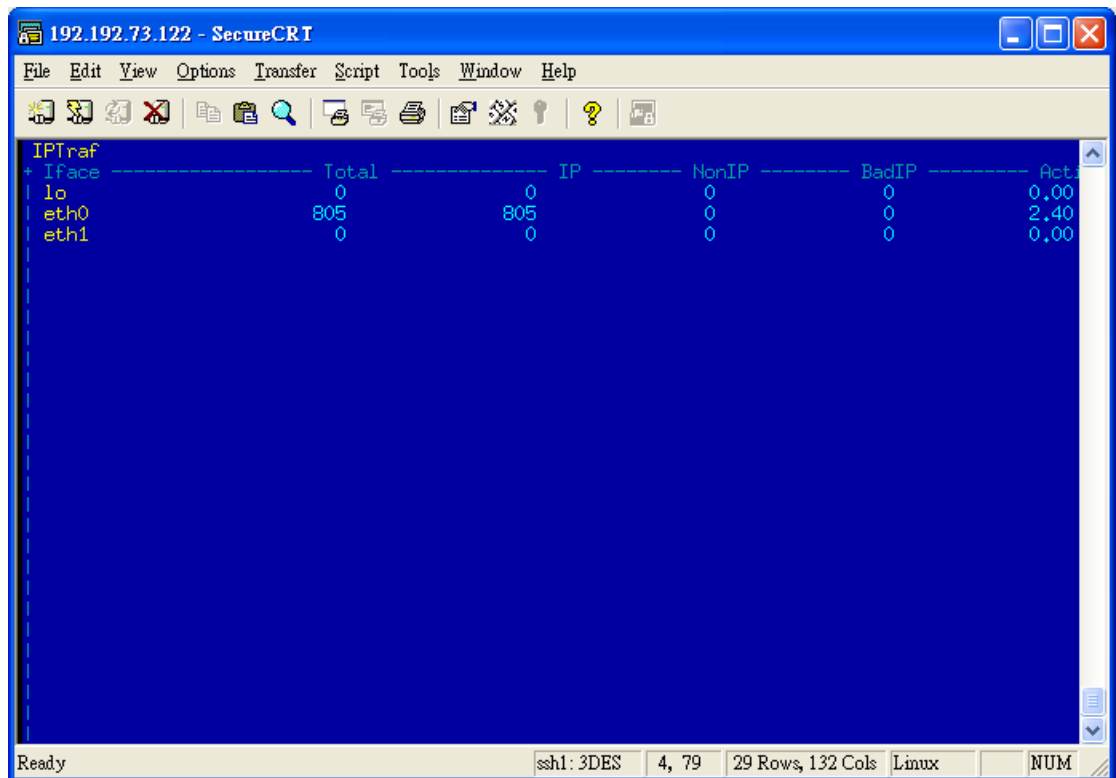


然後再按任何鍵繼續。

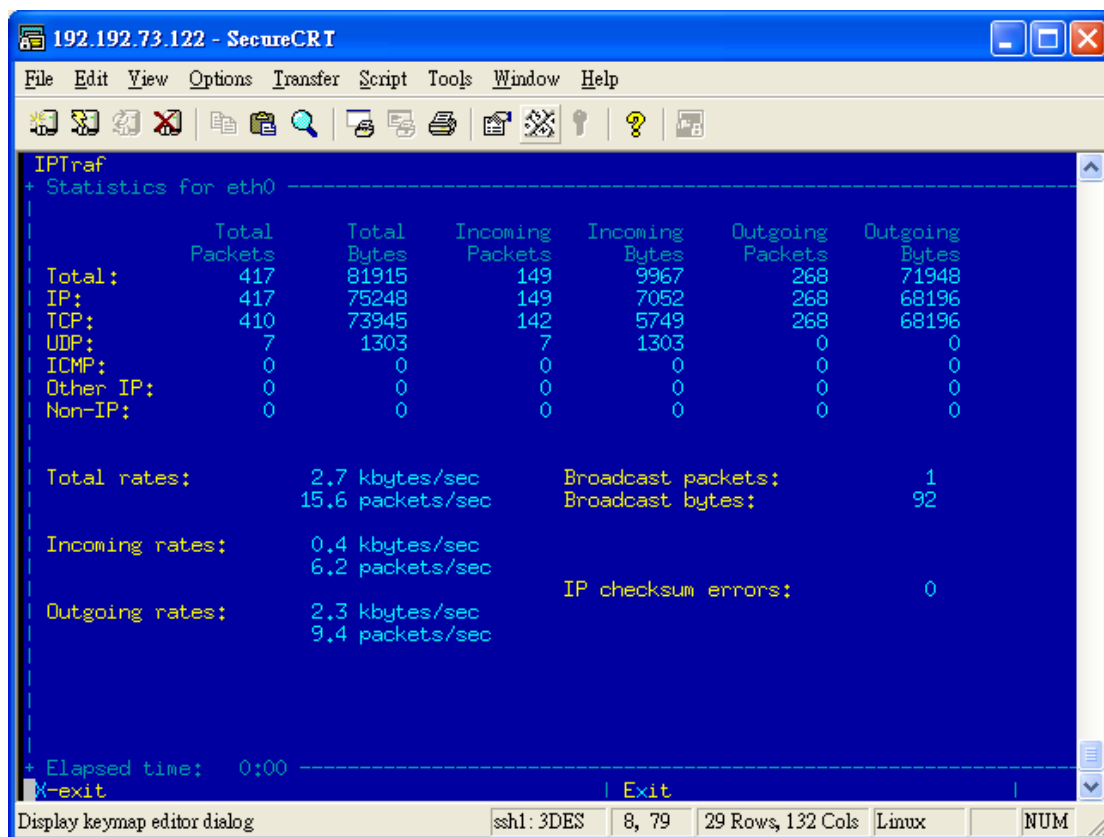
如果要使用監測介面的封包數時，可以使用【IP traffic monitor】模式，然後選擇介面，在此請選擇【All interfaces】，以下是觀測的畫面。



如果要監測簡易的網路卡介流經多少封包時，可以選擇【General interface statistics】，其產生畫面如下圖所示。



如果要監測詳細的網卡介流經多少封包時，可以選擇【Detailed interface statistics】，並選擇一個介面，在此選擇【eth0】，其產生畫面如下圖所示。



```
192.192.73.122 - SecureCRT
File Edit View Options Transfer Script Tools Window Help
IPTraf
+ Statistics for eth0 -----
Total      Total      Incoming  Incoming  Outgoing  Outgoing
Packets    Bytes      Packets   Bytes     Packets   Bytes
Total:     417        81915    149       9967      268       71948
IP:        417        75248    149       7052      268       68196
TCP:       410        73945    142       5749      268       68196
UDP:       7          1303     7         1303      0         0
ICMP:      0          0        0         0         0         0
Other IP:  0          0        0         0         0         0
Non-IP:    0          0        0         0         0         0

Total rates:      2.7 kbytes/sec      Broadcast packets:      1
                  15.6 packets/sec      Broadcast bytes:       92

Incoming rates:  0.4 kbytes/sec
                  6.2 packets/sec

Outgoing rates:  2.3 kbytes/sec
                  9.4 packets/sec

IP checksum errors: 0

+ Elapsed time: 0:00 -----
X-exit | Exit
Display keymap editor dialog  ssh1: 3DES  8, 79  29 Rows, 132 Cols  Linux  NUM
```

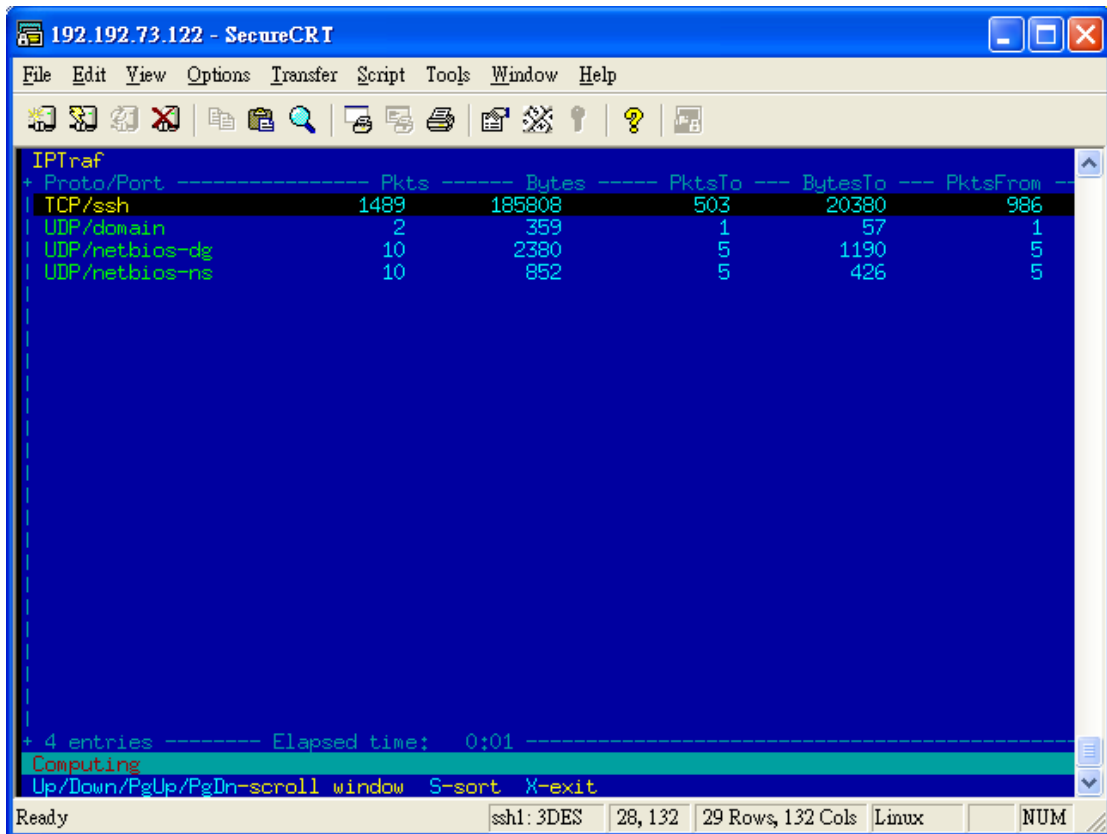
在監測模式中，將所有的封包依照大小來進行分類的動作，在此要選擇選單中的【Statistical breakdowns...】，再選擇【By packet size】，選擇一個介面，其產生畫面如下圖所示。

The screenshot shows a terminal window titled "192.192.73.122 - SecureCRT". The terminal output is as follows:

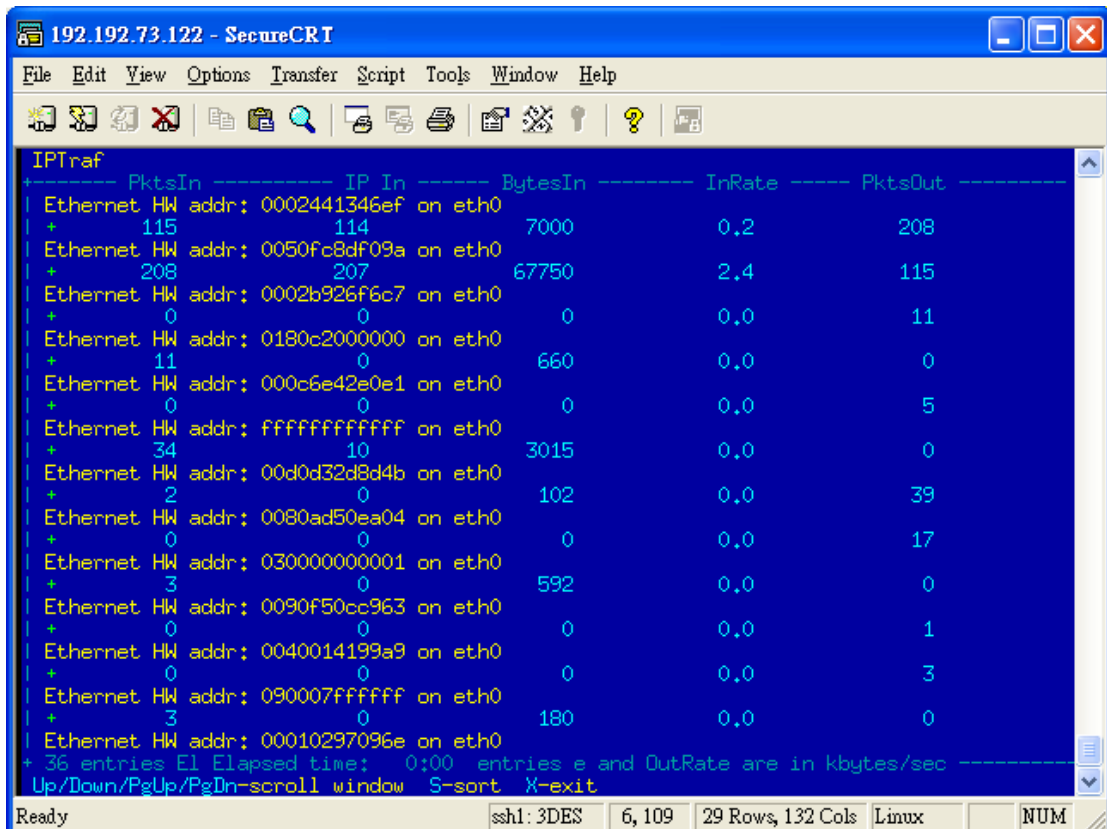
```
IPTraf
+ Packet Distribution by Size -----
|
| Packet size brackets for interface eth0
|
| Packet Size (bytes)      Count      Packet Size (bytes)      Count
| 1 to 75:                 399       751 to 825:              1
| 76 to 150:               673       826 to 900:              0
| 151 to 225:              4         901 to 975:              0
| 226 to 300:              2         976 to 1050:             0
| 301 to 375:              0         1051 to 1125:            0
| 376 to 450:              0         1126 to 1200:            0
| 451 to 525:              0         1201 to 1275:            0
| 526 to 600:              0         1276 to 1350:            0
| 601 to 675:              0         1351 to 1425:            1
| 676 to 750:              0         1426 to 1500+:          3
|
| Interface MTU is 1500 bytes, not counting the data-link header
| Maximum packet size is the MTU plus the data-link header length
| Packet size computations include data-link headers, if any
|
+ Elapsed time: 0:00 -----
X-exit
```

Ready ssh1: 3DES 9, 33 29 Rows, 132 Cols Linux NUM

在監測模式中，將所有的封包依照協定來進行分類的動作，在此要選擇選單中的【Statistical breakdowns...】，再選擇【By TCP/UDP port】，選擇一個介面，其產生畫面如下圖所示。



若要使用 MAC Address 模式來觀察，請選擇【LAN station monitor】，然後再選擇介面開始觀測即可，其產生畫面如下圖所示。



可以選擇只要觀測某些資訊，在此選擇【Filters...】，進入之後，假設只想看到一個『192.192.73.122』相關的 TCP 資訊，首先必須先建立一個規則後，再將這個規則載入，如下圖所示，點選進入【TCP】，再選擇【Define new filter...】進入以下的畫面後，再將要觀測的 IP 資訊加入。

```
Enter a description for this filter
test
Enter-accept Ctrl+X-cancel
```

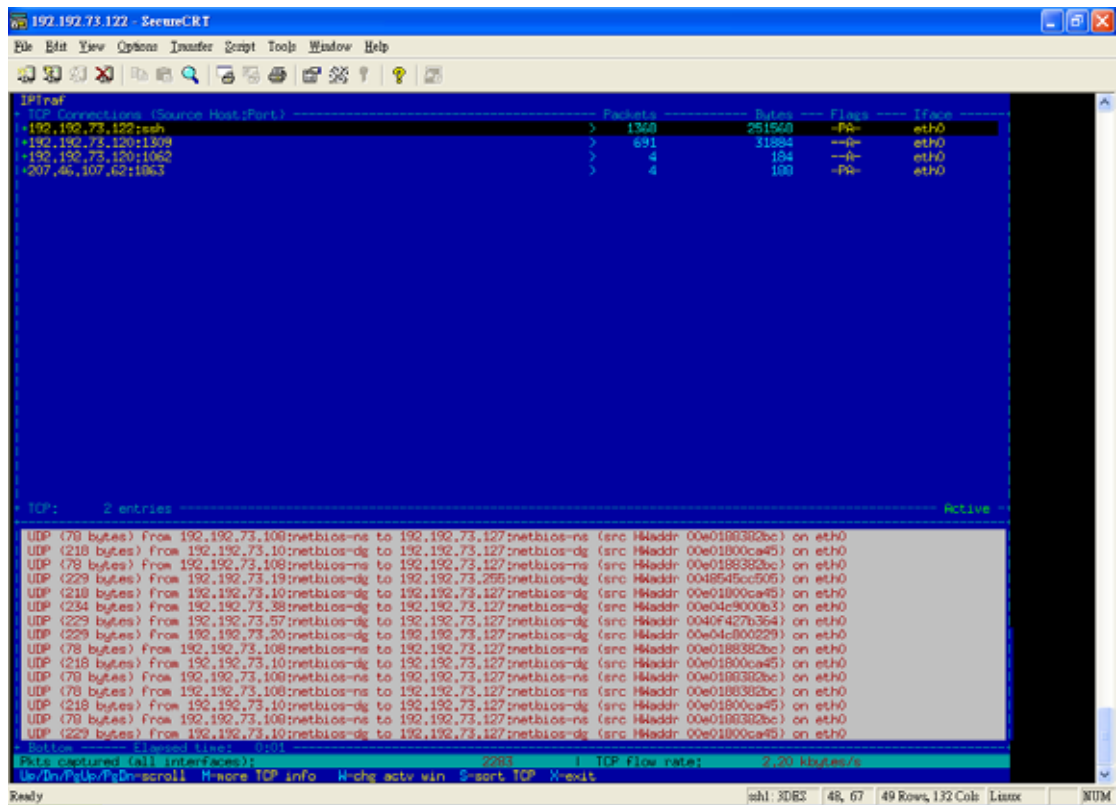
在此使用 test 來為這條規則命名，接著要填入資訊，如下圖所示。

```
----- First ----- Second -----
Host name/IP address: 192.192.73.122 0.0.0.0
Wildcard mask: 255.255.255.128 0.0.0.0
Port: 0
Include/Exclude (I/E): I
Tab-next field Enter-accept Ctrl+X-cancel
```

完成後按下【Enter】儲存即可，按下「CTRL + X」跳出後，在畫面中選擇【Apply filter...】，然後選擇【test】這條規則，如下圖所示。

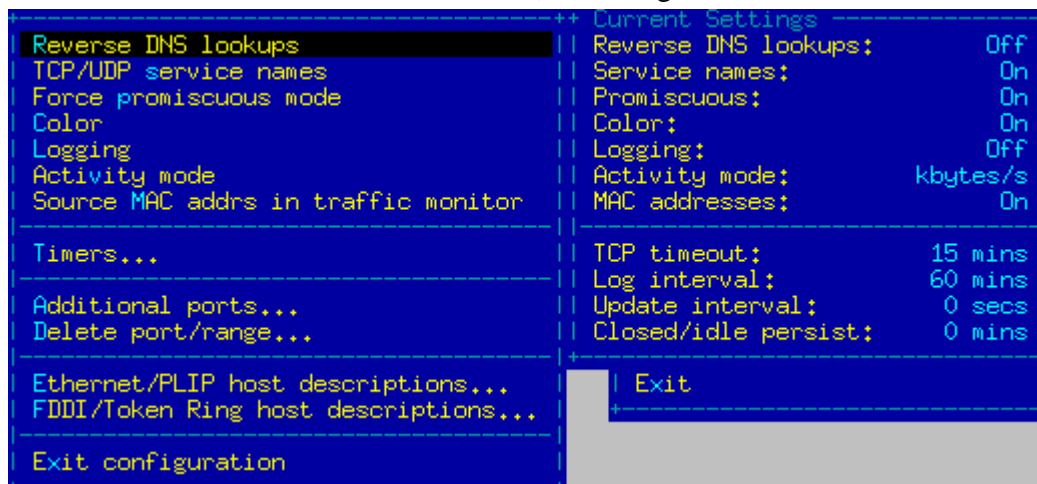
```
+ Select Filter -----
test
```

做到這即完成了。接下來再去測試一次，看看是否所看到的資訊都只和 192.192.73.122 有關。



圖中全部有關 TCP 協定的資訊都只會和 192.192.73.122 相關，而 UDP 的資訊則是沒有限制。

接下來可以進行一些組態的設定，選擇【Configure...】會出現以下的畫面：



其中的【TCP/UDP service names】，是決定是否要顯示 TCP 及 UDP 協定的應用程式的名稱，而【Logging】則是選擇是否要進行記錄，如果已經開啟，在每次進行監測的動作時都會出現決定儲存檔名的對話框，如下圖所示。

```
Logging Enabled
Enter the name of the file to which to write the log.
If you don't specify a path, the log file will
be placed in /var/log/iptraf.
/var/log/iptraf/ip_traffic-1.log
Enter-accept Ctrl+X-cancel (turns logging off)
```

其中的功能如下：

- **【Activity mode】**：決定該以『kbytes/s』模式還是『kbits/s』的模式顯示。
- **【Timers...】**：決定 Iptraf 的運作時間。
- **【Additional ports...】** 及 **【Delete port/range...】**：則是增加或者是刪除高於 1024 port 號的狀態。

以上為 Iptraf 的用法，基本上 Iptraf 是一個不錯的網路監控的軟體，能夠讓網路管理人員簡單的了解目前網路的流量及連線狀態，雖然比起其他商用軟體還是遜色不少，但已經夠用了。

Sniffit 軟體的取得與安裝

首先要先取得 sniffit 的原始碼，可以到 Freshmeat 網站 (<http://freshmeat.net/>)，或者是直接連到 <http://reptile.rug.ac.be/~coder/sniffit/sniffit.html> 來下載。

下載完畢後，將 sniffit 上傳至主機中，並將程式碼解壓縮，指令如下所示：

```
[root@net122 root]# wget
http://reptile.rug.ac.be/~coder/sniffit/files/sniffit.0.3.7.beta.tar.gz
[root@net122 root]# tar zxvf sniffit.0.3.7.beta.tar.gz
```

解壓縮之後會看到 sniffit.0.3.7.beta 這個目錄，進到這個目錄後，建議將所有的文件檔都先仔細的看一遍，以了解軟體的安裝過程和 sniffit 的使用方法。

首先，先下如下的指令來編譯 sniffit：

```
[root@net122 sniffit.0.3.7.beta]# ./configure
```

修改 sn_structs.h 這個檔案，並找到下面這一行：

```
_32_bit short source_port, destination_port;
```

將 short 刪除，然後存檔離開，修改為：

```
32_bit source_port, destination_port;
```

接下來執行 make 指令：

```
[root@net122 sniffit.0.3.7.beta]#make
```

如果會產生 sniffit 這個可以執行的指令，即代表編譯成功。接下來要學習使用 sniffit 這個程式。

- -v：顯示此軟體的版本。
- -t <IP nr/name>：執行 sniffit 去竊聽封包的機器的 IP。
- -i：使用視窗介面，顯示有哪些機器正在你的網域中。
- -c <File>：使用文件來執刪 sniffit，如何撰寫這份文件，稍後會介紹。
- -F <device>：強制 sniffit 去使用網路磁碟機。
- -n：顯示出假的封包，就像是使用 ARP、RARP 或是其他不是 IP 的封包也會顯示出來。

接下來的指令是指在使用【-i】選項時無法一起使用的參數。

- -d：將所竊聽到的封包顯示於螢幕上，使用的單位是位元及 16 進位法。
- -a：和前一項相同，只是輸出改用 ASCII。
- -A <char>：當監聽的封包內容有不認識的字元時，將由<char>代替。
- -P protocol：定義所要監聽的協定，預設值是 TCP，可以使用的選項有 IP、TCP、ICMP、UDP 等，當然也可以將它們結合在一起。
- -p <port>：定義所要監聽的 port 號，預設是 0，也就是全部。
- -l：設定所要監聽的封包大小，預設值是 300bytes，可以自行設定。

接下來要進行竊聽的動作，以下是部分的範例。

範例一：

```
./sniffit -p 21 -t 61.62.103.105
```

說明：對連線至 61.62.103.105 的 ftp port 進行監聽。

接下來看記錄檔的內容：

```
[root@net122 sniffit.0.3.7.beta]# less 192.192.73.122.35989-61.62.103.105.21
```

```
USER linul
```

```
PASS 123456
```

```
SYST
```

由於沒有加密的作用，所以會有明碼的密碼。

範例二：

```
./sniffit -p 22 -l 1000-t 61.62.103.105
```

說明：對連線至 61.62.103.105 的 ssh port 進行監聽，設封包大小為 1000bytes。

接下來看記錄檔的內容：

```
[root@net122 sniffit.0.3.7.beta]# less 192.192.73.122.35990-61.62.103.105.22
"192.192.73.122.35990-61.62.103.105.22" may be a binary file.  See it anyway?
SSH-2.0-OpenSSH_3.5p1
^@^@^B^\      ^T?藤 | z)羶
      ^A?G@^@^@=diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
^@^@^@^@Ossh-rsa,ssh-dss^@^@^@f
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndae
l-cbc@lysator.liu.se^@^@^@faes128-cbc,3des-cbc,blo
wfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se^@
^@^@U hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd1
60@openssh.com,hmac-sha1-96,hmac-md5-
```

因為 ssh 有進行加密，所以此檔會變成亂碼。

範例三：

```
./sniffit -p 21 -d -t 61.62.103.105
```

說明：將連線至 61.62.103.105 的 ftp port 的封包顯示在螢幕上。

當進行連線時，畫面上會出現如下的狀態，即表示目前有連線在進行。

```
[root@net122 sniffit.0.3.7.beta]# ./sniffit -p 21 -d -t 61.62.103.105
Supported Network device found. (eth0)
Sniffit.0.3.7 Beta is up and running... (61.62.103.105)

Packet ID (from_IP,port-to_IP,port): 192.192.73.122.35991-61.62.103.105.21
45 00 00 3C 8E 78 40 00 40 06 FD 61 C0 C0 49 7A 3D 3E 67 69 8C 97 00 15 02 9E
E8 C8 00 00 00 00 A0 02 16 D0 A2 B8 00 00 02 04 05 B4 04 02 08 0A 00 D9 66 B0
00 00 00 00 01 03 03 00

Packet ID (from_IP,port-to_IP,port): 192.192.73.122.35991-61.62.103.105.21
45 00 00 34 8E 79 40 00 40 06 FD 68 C0 C0 49 7A 3D 3E 67 69 8C 97 00 15 02 9E
E8 C9 43 74 79 FE 80 10 16 D0 00 32 00 00 01 01 08 0A 00 D9 66 B4 00 09 13 BC

Packet ID (from_IP,port-to_IP,port): 192.192.73.122.35991-61.62.103.105.21
45 10 00 34 8E 7A 40 00 40 06 FD 57 C0 C0 49 7A 3D 3E 67 69 8C 97 00 15 02 9E
E8 C9 43 74 7A 38 80 10 16 D0 FF 79 00 00 01 01 08 0A 00 D9 66 F3 00 09 13 FB
```

先前提到 sniffit 可以用文件來執行，在此將介紹如何使用描述檔，指令如下：

```
./sifferit -c 文件檔
```


檔案的內容如下：

```
select from host 192.192.73.2
```

```
select to host 192.192.73.120
```

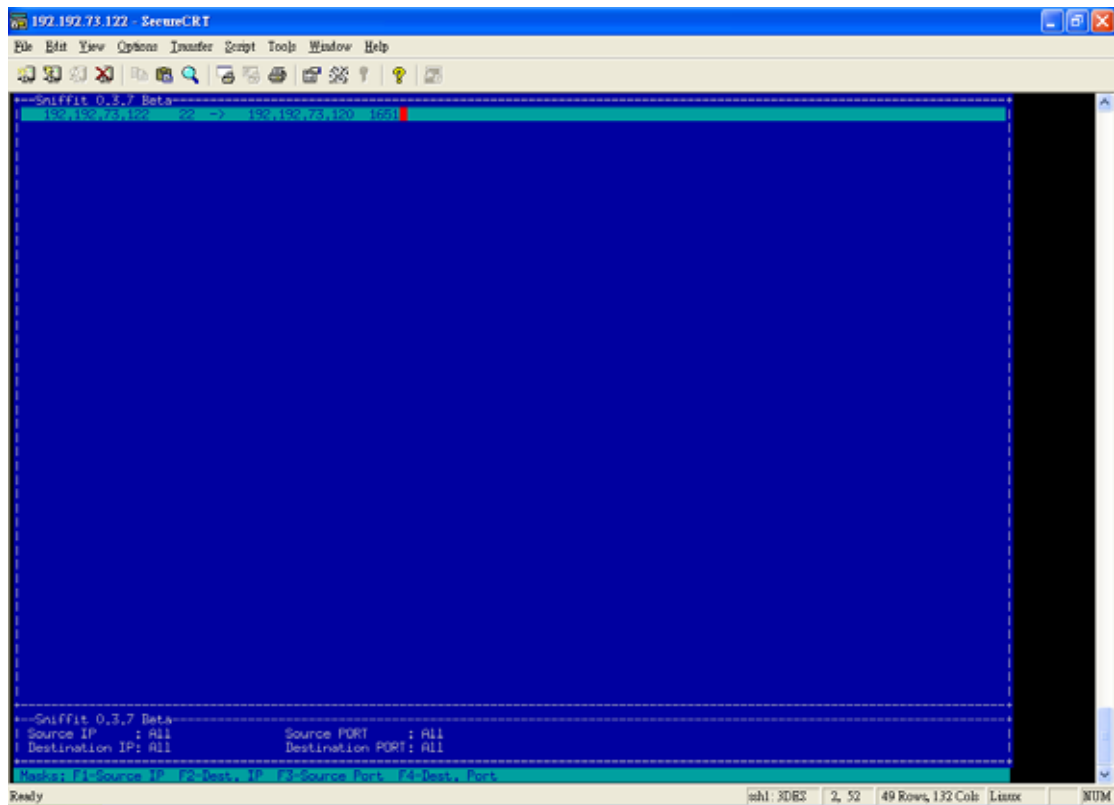
```
select both port 22
```

以上是表示將從 192.192.73.2 送往 192.192.73.120 的 22 port 封包給紀錄下來，要特別注意的是，在此只記錄 192.192.73.2 至 192.192.73.120 的 port22 的封包，詳細的設定請閱讀 README.FIRST 文件。

視窗環境

只要執行 `sniffit -i` 就可以進入視窗模式，指令如下，而畫面如下所示。

```
[root@net122 sniffit.0.3.7.beta]# ./sniffit -i
```



從這個視窗就可以看到所有區域網路內的機器的 IP、使用了哪些 port 號，而視窗中有一些指令，如下列所示：

- q: 離開這個視窗畫面，結束程式。
- r: 清除畫面，並且重新顯示正在連線的機器。
- n: 會產生一個新的小畫面，是有關於 TCP、IP、ICMP、UDP 等協定流量。

- g: 產生封包。
- F1: 改變來源網域的 IP 位置，預設是 ALL。
- F2: 改變目的網域的 IP 位置，預設是 ALL。
- F3: 改變來源機器的 port 號，預設是 ALL。
- F4: 改變目的機器的 port 號，預設是 ALL。

5.問題與討論

1. 如何利用 ntop 來增加系統的安全性？
2. 參考第 24 個實驗，將 ntop 的服務埠號 (3000,3001) 限定於特定網段可以取得。
3. 比較 ntop 和 MRTG 的差異。
4. 如何將 Iptraf 的資料寫入檔案中？
5. 如何將 Snffit 的資料寫入檔案中？
6. 還有哪些即時流量分析軟體？