網路設備監控管理

南投區域網路中心
唐瑋勵

Outline

- SNMP簡介
- 網路概況監控
  - 網路流量、服務狀態…等
- 網路分析工具
  - 封包收集與分析
- 網路安全
  - 漏洞掃描、入侵偵測

SNMP – 簡易網路管理協定

- Simple Network Management Protocol
  - 用於處理各廠商網路系統之間的管理問題
- 用途
  - 讀取網路設備狀態
    1. 流量、溫度、服務…等(視設備的種類)
  - 控制網路設備
    - 存取設定、網路孔開關…等

SNMP – 簡易網路管理協定

- 由IETF(網路工程工作小組)制定
- 版本
  - SNMPv1: RFC 1155~1157, 1213
    1. 以Community作為是否能存取SNMP Agent的密語
  - SNMPv2: RFC 1441~1452
    1. 效能上的加強、與新式的安全架構
  - SNMPv2c: RFC 1901~1908 (v2 最常用版本)
    1. 延用v1以Community名稱為基礎的安全架構
  - SNMPv3: RFC 3411~3418
    - 提供驗證、隱私、與存取控制等重要功能

SNMP – 簡易網路管理協定

- 核心元件
  - 管理者 Manager
    1. 可以進行網路管理的程式
    2. 可向 Agent 取得資訊與控制設備
  - 代理者 Agent
    1. 預裝在網路設備上的程式
    2. 可獲得本身設備的狀態、並提供給 Manager
  - 管理資料庫 MIB
    - 由許多不同資料所組成的虛擬資料庫
    - 定義各種資料的形態與作用

SNMP – 簡易網路管理協定

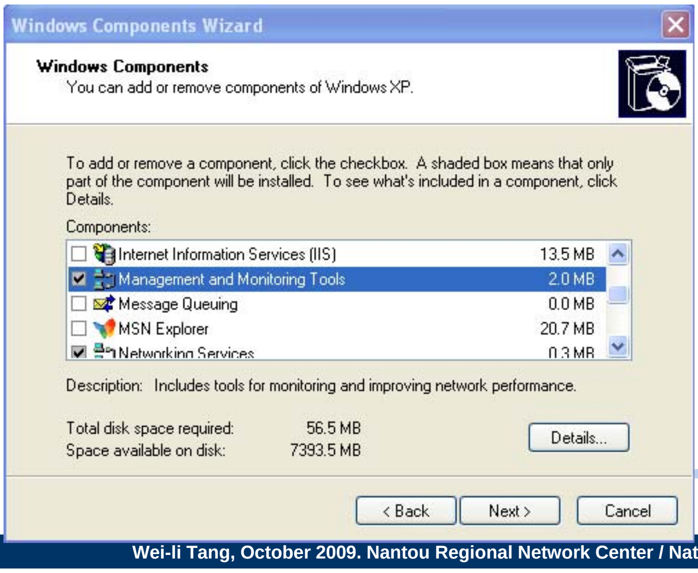
- 哪些設備具有 SNMP Agent?
  - 電腦、伺服器
  - 路由器、交換器(或集線器、IP分享器)
  - 網路印表機
  - 基地台…等

SNMP – 簡易網路管理協定

- 在電腦上安裝SNMP Agent
  - Windows 2000/XP
    1. 控制台 的 新增移除程式
    2. 新增/移除Windows元件
    3. “Management and Monitoring Tools” 細項
    4. 勾選安裝”Simple Network Management Protocol”
  - 啟動 Win2000/XP 的 SNMP Service
    1. 控制台 的 系統管理工具
    2. “服務”
    3. 啟動”SNMP Service”

SNMP – 簡易網路管理協定

- 在電腦上安裝SNMP Agent
  - Windows 2000/XP



Windows Components Wizard

Windows Components

You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

□	Internet Information Services (IIS)	13.5 MB
☑	Management and Monitoring Tools	2.0 MB
□	Message Queuing	0.0 MB
□	MSN Explorer	20.7 MB
☑	Networking Services	0.3 MB

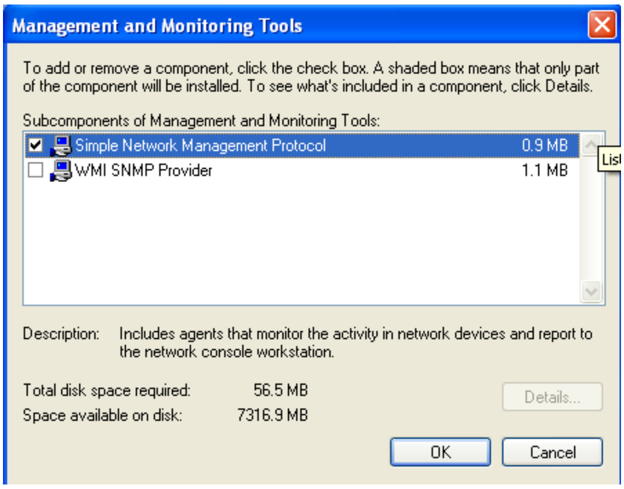
Description: Includes tools for monitoring and improving network performance.

Total disk space required: 56.5 MB

Space available on disk: 7393.5 MB

SNMP – 簡易網路管理協定

- 在電腦上安裝SNMP Agent
  - Windows 2000/XP



Management and Monitoring Tools

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Management and Monitoring Tools:

☑	Simple Network Management Protocol	0.9 MB
☐	WMI SNMP Provider	1.1 MB

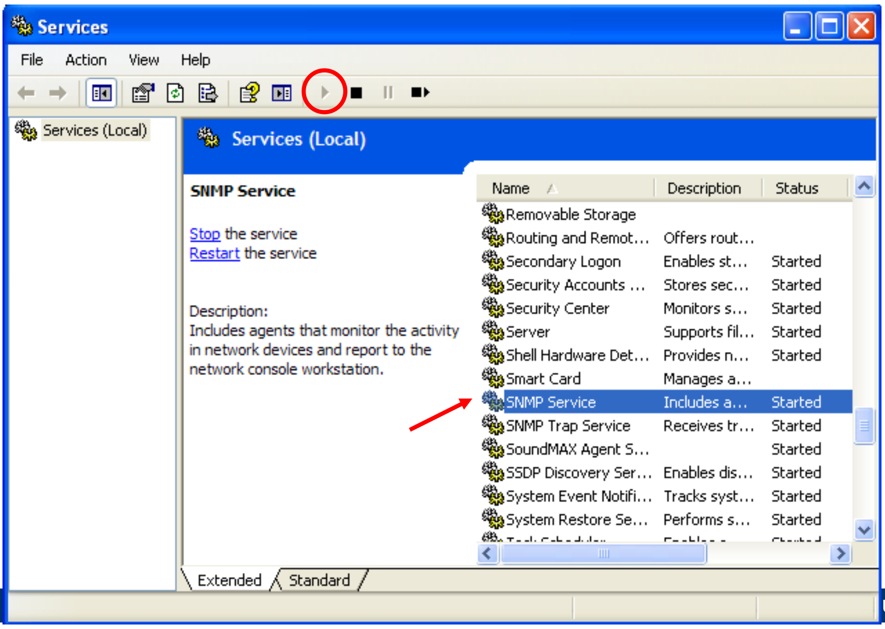
Description: Includes agents that monitor the activity in network devices and report to the network console workstation.

Total disk space required: 56.5 MB

Space available on disk: 7316.9 MB

SNMP – 簡易網路管理協定

- 啟動 Win2000/XP 的 SNMP Service



SNMP Service

Stop the service
Restart the service

Description:
Includes agents that monitor the activity in network devices and report to the network console workstation.

Name	Description	Status
Removable Storage		
Routing and Remot…	Offers rout…	
Secondary Logon	Enables st…	Started
Security Accounts …	Stores sec…	Started
Security Center	Monitors s…	Started
Server	Supports fil…	Started
Shell Hardware Det…	Provides n…	Started
Smart Card	Manages a…	
SNMP Service	Includes a…	Started
SNMP Trap Service	Receives tr…	Started
SoundMAX Agent S…		Started
SSDP Discovery Ser…	Enables dis…	Started
System Event Notifi…	Tracks syst…	Started
System Restore Se…	Performs s…	Started
Task Scheduler	Enables a…	Started

SNMP – 簡易網路管理協定

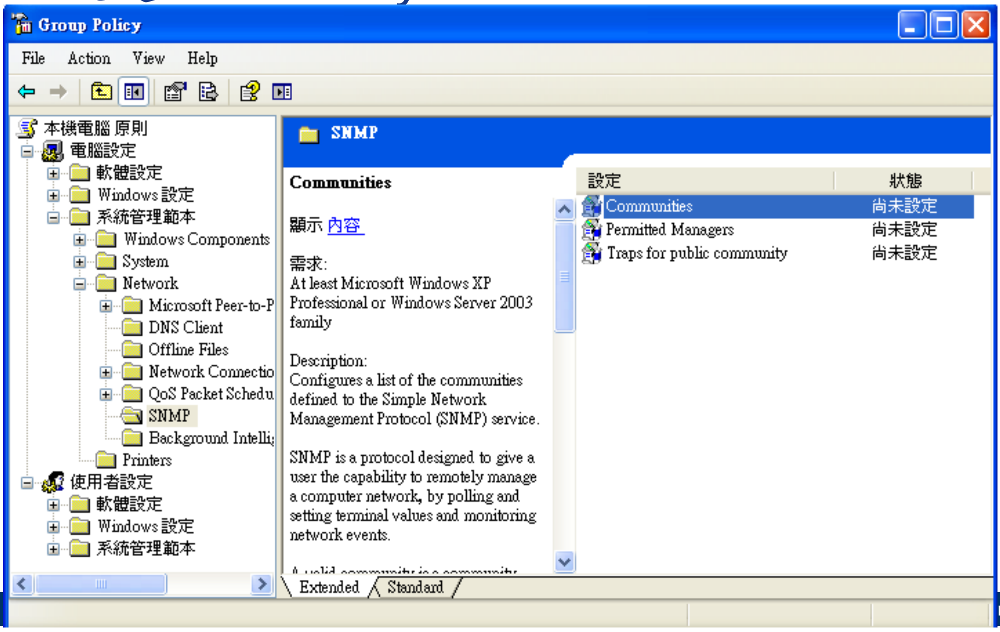
- 在電腦上安裝 SNMP Agent (snmpd)
  - Linux/BSD/UNIX variants
    1. 安裝Net-SNMP套件
    2. http://www.net-snmp.org/
  - Redhat 系列(Fedora, CentOS, RHEL…)
    1. yum install net-snmp
  - Debian/Ubuntu
    - apt-get install snmpd

SNMP – 簡易網路管理協定

- 設定Community
  - Windows XP (不支援 Home 版)
    1. gpedit.msc 群組原則
    2. 電腦設定→系統管理範本→網路→SNMP
    3. 啟用 Communities

SNMP – 簡易網路管理協定

- 設定Community



Communities

顯示 內容

需求:
At least Microsoft Windows XP Professional or Windows Server 2003 family

Description:
Configures a list of the communities defined to the Simple Network Management Protocol (SNMP) service.

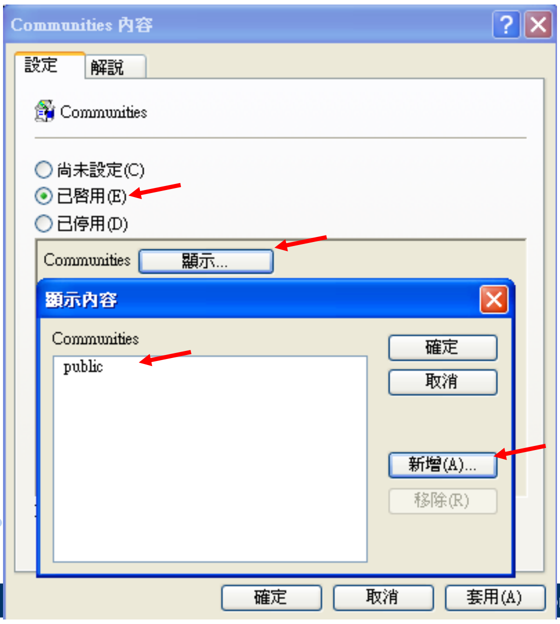
SNMP is a protocol designed to give a user the capability to remotely manage a computer network, by polling and setting terminal values and monitoring network events.

A valid community is a community

設定	狀態
Communities	尚未設定
Permitted Managers	尚未設定
Traps for public community	尚未設定

SNMP – 簡易網路管理協定

- 設定Community



○ 尚未設定(C)
● 已啟用(E)
○ 已停用(D)

Communities

public

SNMP – 簡易網路管理協定

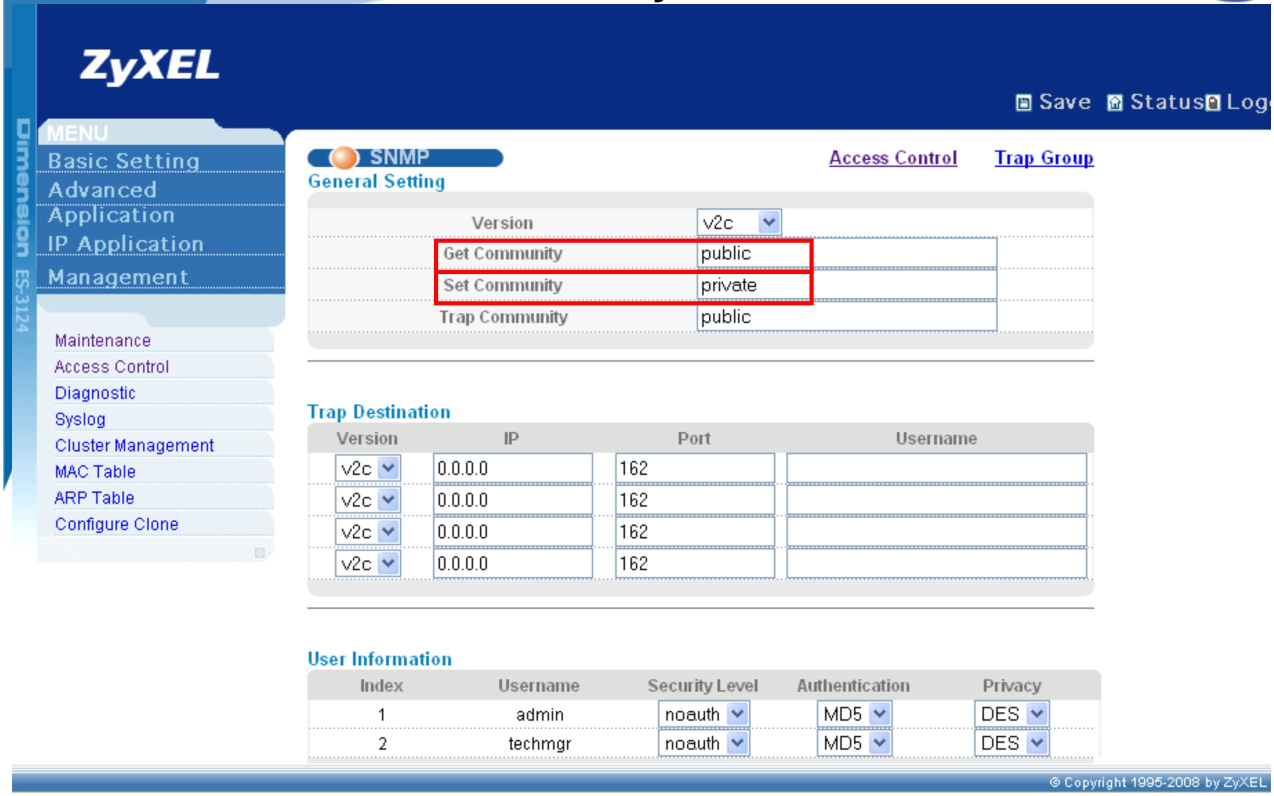
- 設定Community
  - Net-SNMP
    1. 參見 snmpd.conf 的設定方式
  - 其他網路設備
    - 參見設備說明書
    - 通常可透過 Telnet 或網頁管理介面做設定

SNMP – 簡易網路管理協定

- 常見的Communities
  - 唯讀: Get Community (public)
  - 讀寫: Set Community (private)
  - 勿將 Community Name 設為 Public/Private!
    - 預設值容易被猜出

SNMP － 簡易網路管理協定

- 網路設備設定Community示例



General Setting

Version	v2c
Get Community	public
Set Community	private
Trap Community	public

Trap Destination

Version	IP	Port	Username
v2c	0.0.0.0	162	
v2c	0.0.0.0	162	
v2c	0.0.0.0	162	
v2c	0.0.0.0	162	

User Information

Index	Username	Security Level	Authentication	Privacy
1	admin	noauth	MD5	DES
2	techmgr	noauth	MD5	DES

© Copyright 1995-2008 by ZyXEL

SNMP － 簡易網路管理協定

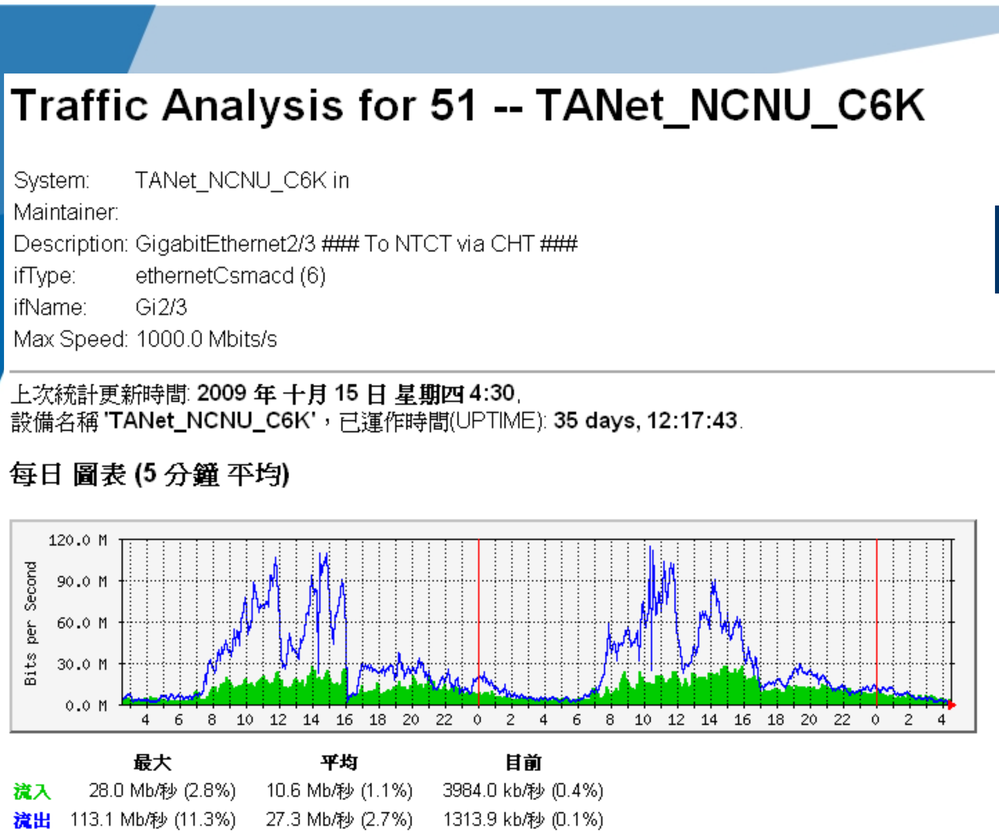
- SNMP Manager
  - 各種網路概況監控工具(如 MRTG…等)
  - snmpwalk (Net-SNMP)
    1. snmpwalk -c <群組名> -v <版本> <IP位址> [OID]
    - 例: snmpwalk -c **public** -v **1 192.168.0.1**
  - **snmpset (Net-SNMP)**
    - 用於設定設備功能之用
  - 註
    - Redhat 須安裝 net-snmp-utils 套件
    - Debian/Ubuntu 須安裝 snmp 套件
    - Windows 可至 Net-SNMP 網站取得 Win32 移植版

網路概況監控

- MRTG
- RRDtool
  - Cacti
  - Ntop
  - Nagios

MRTG

- Multi Router Traffic Grapher
  - 繪製網路流量統計圖表
  - by Tobias Oetiker & Dave Rand (1995)
- 透過SNMP向Agent取得數據
  - 流量累計
  - 電腦狀態
  - 設備溫度
  - 各種需要繪製圖表的應用…等



Traffic Analysis for 51 -- TANet_NCNU_C6K

System:	TANet_NCNU_C6K in
Maintainer:	
Description:	GigabitEthernet2/3 ### To NTCT via CHT ###
ifType:	ethernetCsmacd (6)
ifName:	Gi2/3
Max Speed:	1000.0 Mbits/s

上次統計更新時間: **2009 年 十月 15 日 星期四 4:30**,
設備名稱 **'TANet_NCNU_C6K'**，已運作時間(UPTIME): **35 days, 12:17:43**.

每日 圖表 (5 分鐘 平均)

	最大	**平均**	**目前**
流入	28.0 Mb/秒 (2.8%)	10.6 Mb/秒 (1.1%)	3984.0 kb/秒 (0.4%)
流出	113.1 Mb/秒 (11.3%)	27.3 Mb/秒 (2.7%)	1313.9 kb/秒 (0.1%)

- 例：區網—縣網 (經中華電信)

MRTG

- 安裝方式
  - Linux/BSD/UNIX – 安裝”mrtg”套件
    1. 傳統安裝方式參見 mrtg-unix-guide
       http://www.mrtg.org/doc/mrtg-unix-guide.en.html
  - Windows
    1. 須安裝ActiveState ActivePerl
       http://www.activestate.com/activeperl/downloads/
    2. 取得 MRTG Windows 版程式 (*.zip)
       http://www.mrtg.org/pub/
       目前版本為 mrtg-2.16.2.zip
    3. 參見mrtg-nt-guide (Windows Installation Guide)
       http://www.mrtg.org/doc/mrtg-nt-guide.en.html

MRTG

- 常用程式
  - cfgmaker – 產生 *.cfg 設定檔的程式
  - indexmaker – 產生索引網頁的程式
  - mrtg – 實際繪製圖表與更新數據的程式
    - 一般為每五分鐘執行一次
    - 置於 crontab 執行

MRTG

- 第一步: 產生設定檔
  - 僅適用於路由器、交換器與類似設備
  - 指令

```
cfgmaker --global 'WorkDir: /home/httpd/mrtg'  \
         --global 'Options[_]: bits,growright' \
         --output /home/mrtg/cfg/mrtg.cfg    \
          community@router.abc.xyz
```

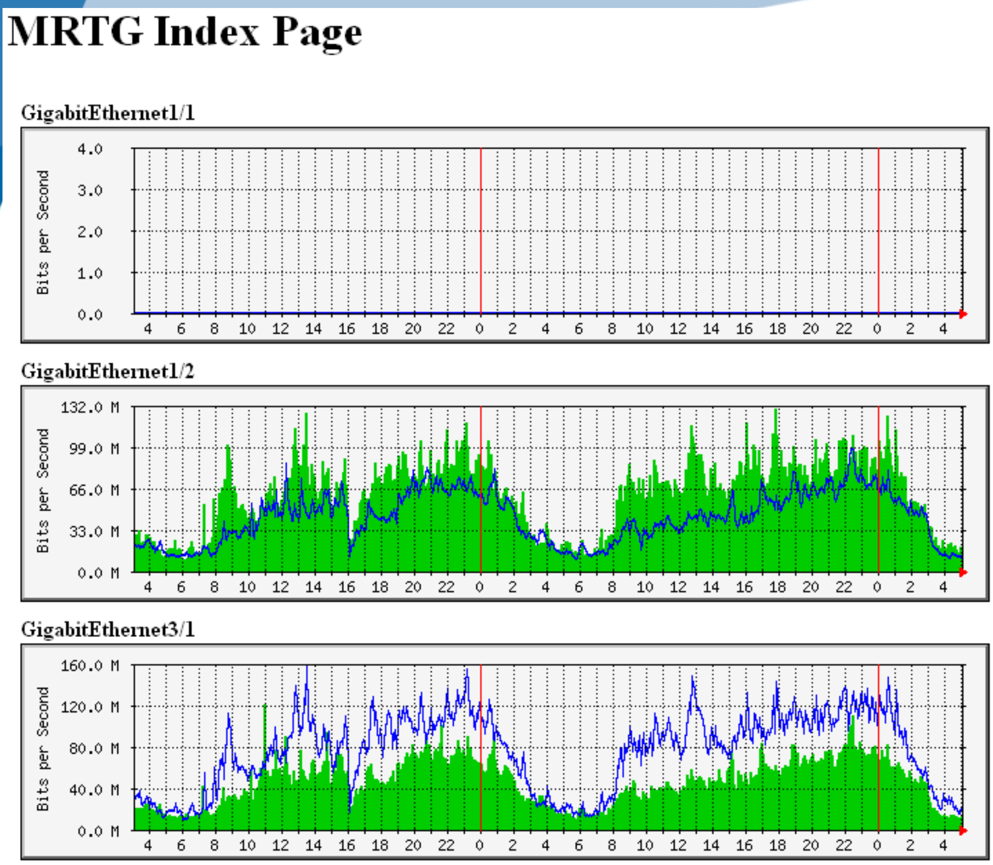
  - 說明
    1. WorkDir: 網頁圖表輸出路徑
    2. Options[_]: 設定全域參數用
    3. output: 設定檔輸出路徑
    4. 目標位址: community@設備位址

MRTG

- 第二步: 執行 MRTG
  - 指令：mrtg <設定檔>
    例
    ```
    mrtg /home/mrtg/cfg/mrtg.cfg
    ```
  - 或是加入 crontab 每五分鐘執行一次
    ```
    */5 * * * *  <mrtg-bin>/mrtg <mrtg-cfg-path>/mrtg.cfg \
                --logging /var/log/mrtg.log
    ```

MRTG

- 第三步: 產生索引網頁 (非必要)
  - 指令:
    indexmaker <設定檔> --output <輸出檔名>
    例
    ```
    indexmaker mrtg.cfg --output index.html
    ```



MRTG Index Page

GigabitEthernet1/1

GigabitEthernet1/2

GigabitEthernet3/1

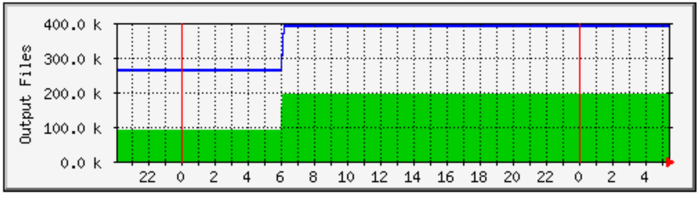
MRTG

- 延伸應用
  - CPU 負載
  - 上線人數
  - 溫溼度
  - 印表機印量…等

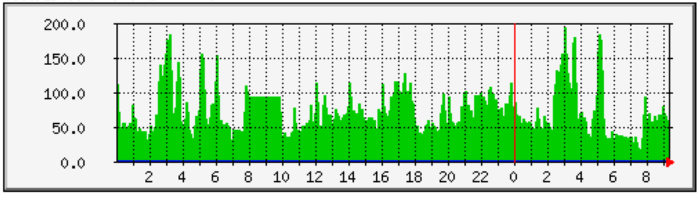
MRTG

- 中山大學檔案伺服器

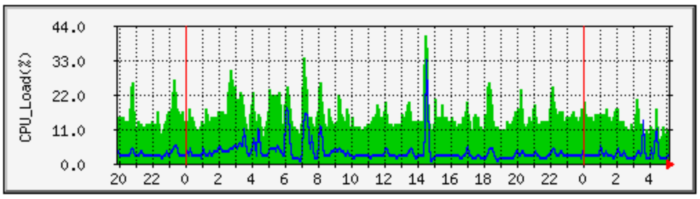
FTP 前日輸出檔案數量 / HTTP 前日輸出檔案數量



系統負荷（乘以100）



CPU Load Ratio

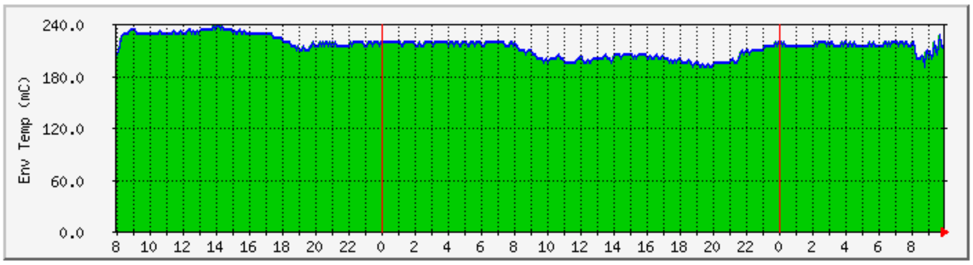


MRTG

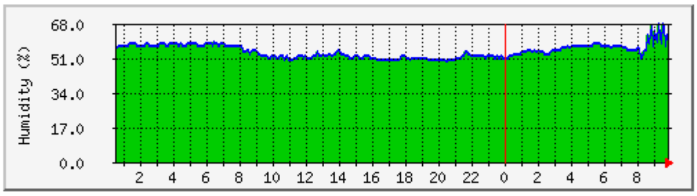
- 暨南大學主機房溫溼度

MRTG Index Page (圖資機房)

機房環境溫度 (單位: 攝氏溫度 X 10)



機房環境溼度



MRTG

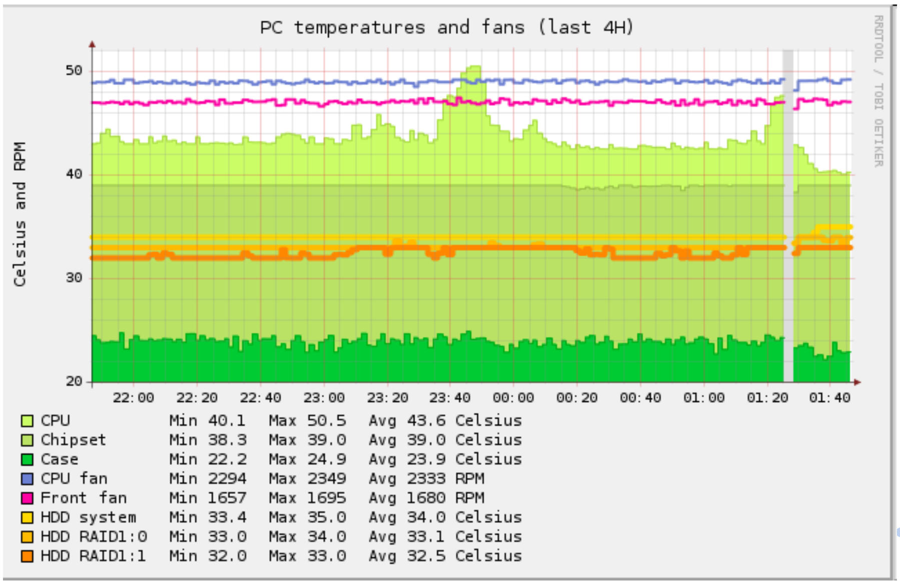
- 其他非網路流量的統計
  - 指定 OID (Target)
  - 載入 MIB 檔案
  - 寫程式
- 參考文件
  - MRTG Third-party Docs
    http://www.mrtg.org/3party.en.html
  - 鳥哥 MRTG 流量偵測法
    http://linux.vbird.org/linux_security/old/04mrtg.php

RRDtool

- Round Robin Database Tool
  - 用於產生 Time-series 圖表 (流量、負載…)
  - 可將多筆資料畫在一張圖上
    1. MRTG只能在一張圖上畫兩筆資料(流入、流出)
  - 網站: http://www.rrdtool.org/
  - 參見RRDtool畫廊
    http://www.rrdtool.org/gallery/

RRDtool

- 電腦溫度與風扇 – by Ciprian Popovici , 2007/10



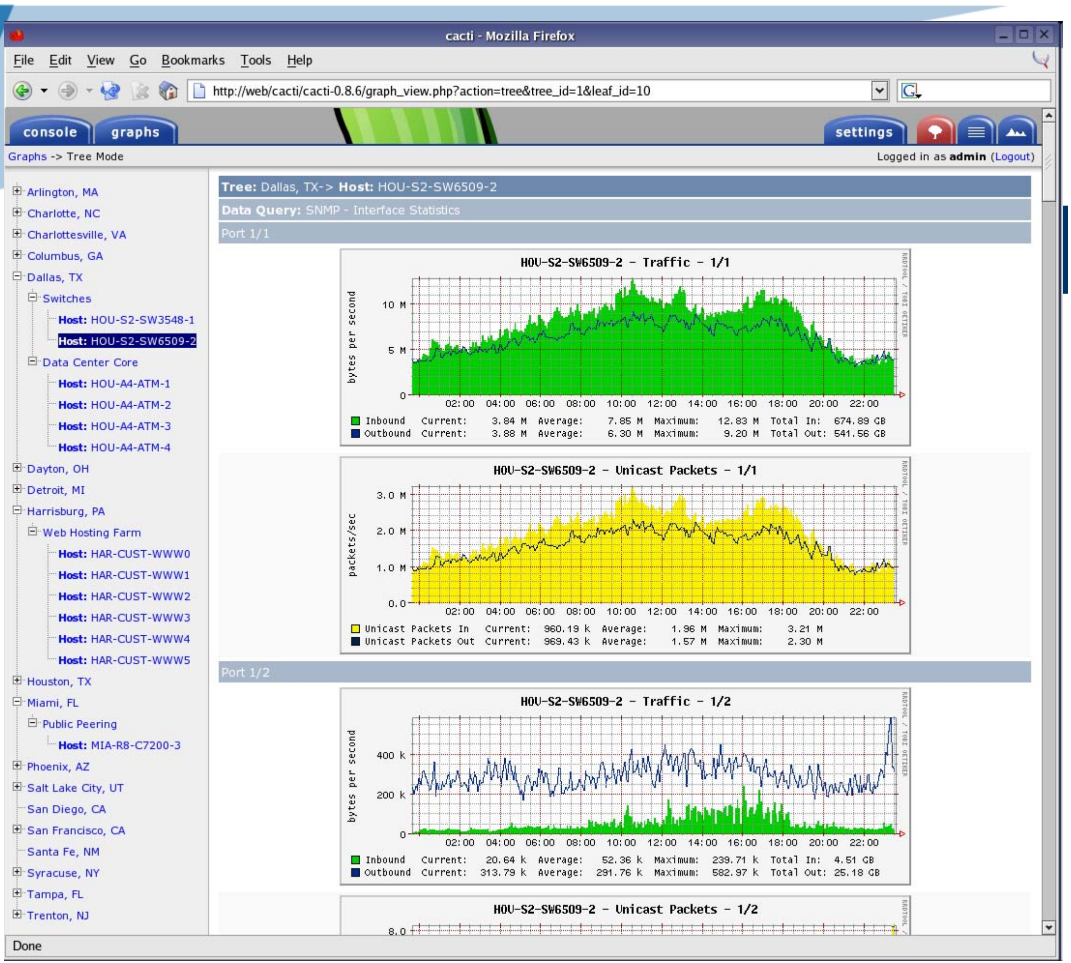
```
🟩 CPU          Min 40.1  Max 50.5  Avg 43.6 Celsius
🟩 Chipset      Min 38.3  Max 39.0  Avg 39.0 Celsius
🟩 Case         Min 22.2  Max 24.9  Avg 23.9 Celsius
🟦 CPU fan      Min 2294  Max 2349  Avg 2333 RPM
🟪 Front fan    Min 1657  Max 1695  Avg 1680 RPM
🟨 HDD system   Min 33.4  Max 35.0  Avg 34.0 Celsius
🟧 HDD RAID1:0  Min 33.0  Max 34.0  Avg 33.1 Celsius
🟧 HDD RAID1:1  Min 32.0  Max 33.0  Avg 32.5 Celsius
```

RRDtool

- 採用 RRDtool 的套件
  - Cacti
  - Ntop
  - Nagios

Cacti

- 以 RRDtool 為基礎的繪圖系統
  - 有系統地整理與繪製流量等時間序列圖表
  - 偵測設備服務是否正常
  - 主要透過 SNMP 取得資料
  - 網站: http://www.cacti.net/
  - Cacti中文研究站: http://cacti.xxoo.net/


cacti - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://web/cacti/cacti-0.8.6/graph_view.php?action=tree&tree_id=1&leaf_id=10
console
graphs
settings
Done

Graphs -> Tree Mode

Logged in as **admin** (Logout)

- Arlington, MA
- Charlotte, NC
- Charlottesville, VA
- Columbus, GA
- Dallas, TX
  - Switches
    - **Host:** HOU-S2-SW3548-1
    - **Host:** HOU-S2-SW6509-2
  - Data Center Core
    - **Host:** HOU-A4-ATM-1
    - **Host:** HOU-A4-ATM-2
    - **Host:** HOU-A4-ATM-3
    - **Host:** HOU-A4-ATM-4
- Dayton, OH
- Detroit, MI
- Harrisburg, PA
  - Web Hosting Farm
    - **Host:** HAR-CUST-WWW0
    - **Host:** HAR-CUST-WWW1
    - **Host:** HAR-CUST-WWW2
    - **Host:** HAR-CUST-WWW3
    - **Host:** HAR-CUST-WWW4
    - **Host:** HAR-CUST-WWW5
- Houston, TX
- Miami, FL
  - Public Peering
    - **Host:** MIA-R8-C7200-3
- Phoenix, AZ
- Salt Lake City, UT
- San Diego, CA
- San Francisco, CA
- Santa Fe, NM
- Syracuse, NY
- Tampa, FL
- Trenton, NJ

Tree: Dallas, TX-> **Host:** HOU-S2-SW6509-2

Data Query: SNMP - Interface Statistics

Port 1/1

```
🟩 Inbound   Current:   3.84 M  Average:   7.85 M  Maximum:  12.83 M  Total In:   674.89 GB
🟦 Outbound  Current:   3.88 M  Average:   6.30 M  Maximum:   9.20 M  Total Out:  541.56 GB
```

```
🟨 Unicast Packets In   Current:  960.19 k  Average:   1.96 M  Maximum:   3.21 M
⬛ Unicast Packets Out  Current:  969.43 k  Average:   1.57 M  Maximum:   2.30 M
```

Port 1/2

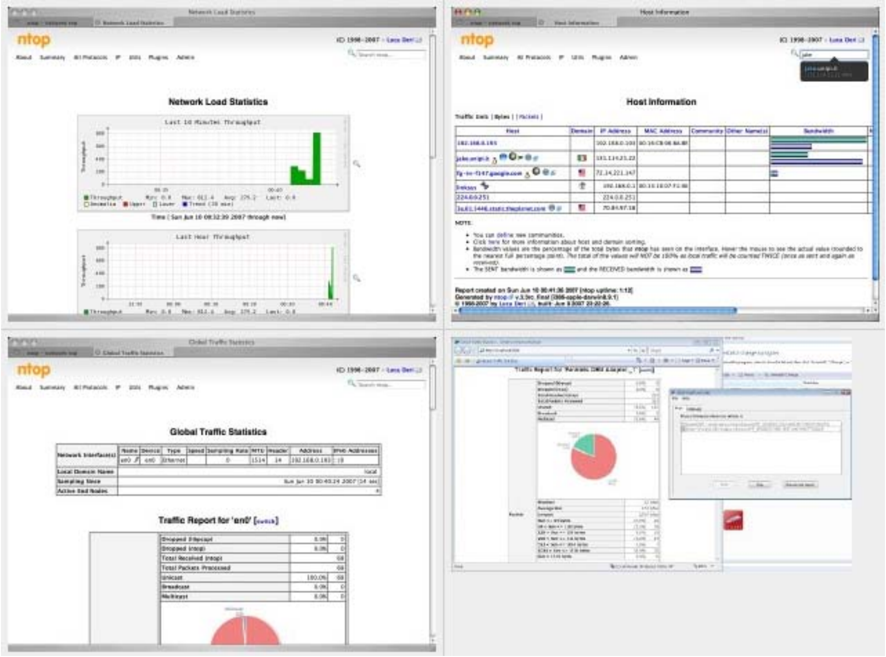
```
🟩 Inbound   Current:  20.64 k  Average:  52.36 k  Maximum:  239.71 k  Total In:   4.51 GB
🟦 Outbound  Current: 313.79 k  Average: 291.76 k  Maximum:  582.97 k  Total Out: 25.18 GB
```

- 來源:
- Wikipedia - Cacti

ntop

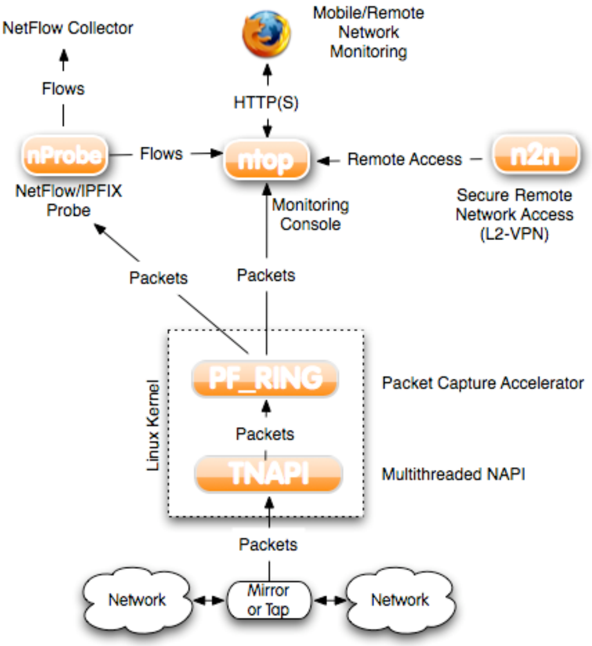
- Network top
  - 網路流量偵測系統
  - 可分析 Layer 7 協定連線 (HTTP, etc.)
- 多樣化的資料來源
  - 直接擷取網卡封包並分析
  - 可接收 Netflow 等外部紀錄
- 網站: http://www.ntop.org/

ntop



- 來源: http://www.ntop.org/overview.html

ntop

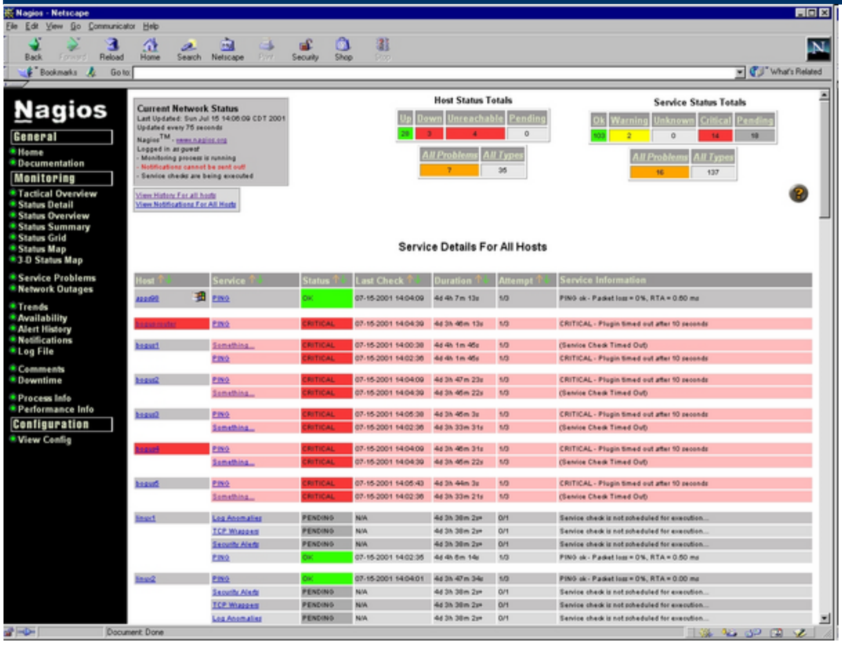


- 來源: http://www.ntop.org/news.html

Nagios

- 開放原始碼網路管理系統(NMS)
  - 監控網路服務如 SMTP, HTTP, SNMP, FTP…
  - 主機資源監控
  - 即時的障礙通報(透過E-Mail或簡訊等)
- 網站: http://www.nagios.org/

Nagios



Current Network Status
Last Updated: Sun Jul 15 14:06:09 CDT 2001
Updated every 75 seconds
Nagios™ - www.nagios.org
Logged in as guest
- Monitoring process is running
- Notifications cannot be sent out!
- Service checks are being executed

View History For all hosts
View Notifications For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
28	3	4	0

All Problems	All Types
7	35

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
103	2	0	14	18

All Problems	All Types
16	137

Service Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Service Information
apps98	PING	OK	07-15-2001 14:04:09	4d 4h 7m 13s	1/3	PING ok - Packet loss = 0%, RTA = 0.80 ms
bogusrouter	PING	CRITICAL	07-15-2001 14:04:39	4d 3h 46m 13s	1/3	CRITICAL - Plugin timed out after 10 seconds
bogus1	Something...	CRITICAL	07-15-2001 14:00:38	4d 4h 1m 46s	1/3	(Service Check Timed Out)
	PING	CRITICAL	07-15-2001 14:02:36	4d 4h 1m 46s	1/3	CRITICAL - Plugin timed out after 10 seconds
bogus2	PING	CRITICAL	07-15-2001 14:04:09	4d 3h 47m 23s	1/3	CRITICAL - Plugin timed out after 10 seconds
	Something...	CRITICAL	07-15-2001 14:04:39	4d 3h 46m 22s	1/3	(Service Check Timed Out)
bogus3	PING	CRITICAL	07-15-2001 14:05:38	4d 3h 46m 3s	1/3	CRITICAL - Plugin timed out after 10 seconds
	Something...	CRITICAL	07-15-2001 14:02:36	4d 3h 33m 31s	1/3	(Service Check Timed Out)
bogus4	PING	CRITICAL	07-15-2001 14:04:09	4d 3h 46m 31s	1/3	CRITICAL - Plugin timed out after 10 seconds
	Something...	CRITICAL	07-15-2001 14:04:39	4d 3h 46m 22s	1/3	(Service Check Timed Out)
bogus5	PING	CRITICAL	07-15-2001 14:05:43	4d 3h 44m 3s	1/3	CRITICAL - Plugin timed out after 10 seconds
	Something...	CRITICAL	07-15-2001 14:02:36	4d 3h 33m 21s	1/3	(Service Check Timed Out)
linux1	Log Anomalies	PENDING	N/A	4d 3h 38m 2s	0/1	Service check is not scheduled for execution...
	TCP Wrappers	PENDING	N/A	4d 3h 38m 2s	0/1	Service check is not scheduled for execution...
	Security Alerts	PENDING	N/A	4d 3h 38m 2s	0/1	Service check is not scheduled for execution...
	PING	OK	07-15-2001 14:02:35	4d 4h 6m 14s	1/3	PING ok - Packet loss = 0%, RTA = 0.50 ms
linux2	PING	OK	07-15-2001 14:04:01	4d 3h 47m 34s	1/3	PING ok - Packet loss = 0%, RTA = 0.00 ms
	Security Alerts	PENDING	N/A	4d 3h 38m 2s	0/1	Service check is not scheduled for execution...
	TCP Wrappers	PENDING	N/A	4d 3h 38m 2s	0/1	Service check is not scheduled for execution...
	Log Anomalies	PENDING	N/A	4d 3h 38m 2s	0/1	Service check is not scheduled for execution...

- 來源: Wikipedia - Nagios

封包分析工具

- Wireshark
- tcpdump

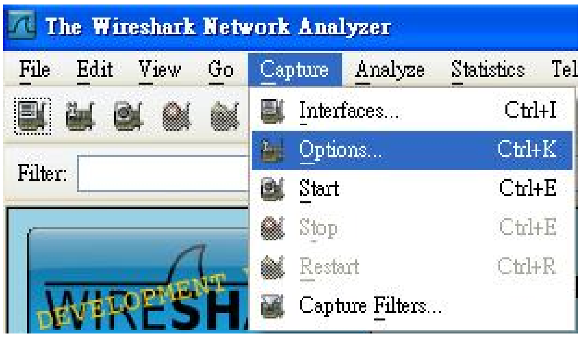
- 來源: Wikipedia - Nagios

Wireshark

- 舊稱 Ethereal
- 網路封包分析軟體
- 廣泛支援 Windows, Linux, BSD 等平台
- 網站: http://www.wireshark.org/

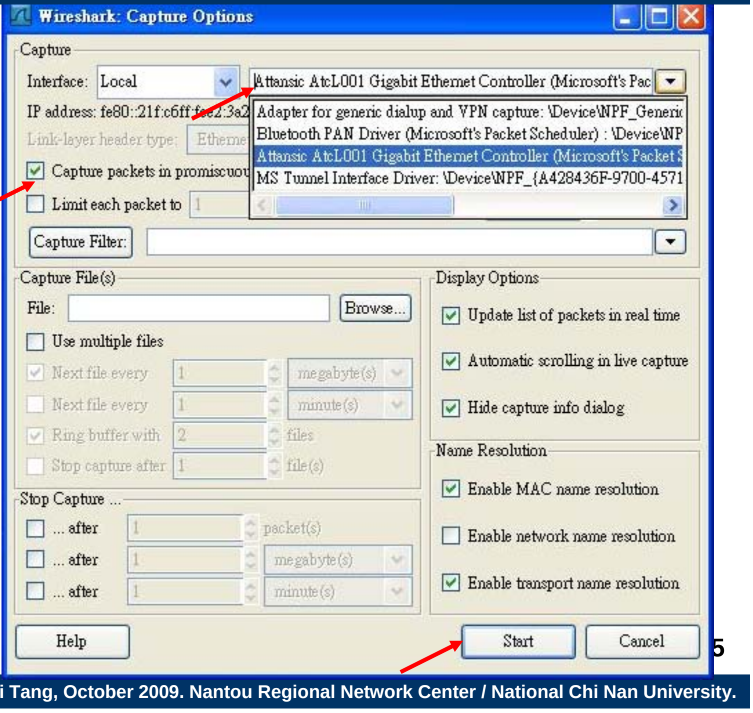
Wireshark

- 網卡監聽步驟
  - 步驟一: Capture - Options



Wireshark

- 網卡監聽步驟
  - 步驟二: 選擇網卡
  - 設定完畢後按Start


Wireshark: Capture Options

Capture

Interface: Local — Attansic AtcL001 Gigabit Ethernet Controller (Microsoft's Pac

IP address: fe80::21f:c6ff:fe62:3a2

Link-layer header type: Etherne

- Adapter for generic dialup and VPN capture: \Device\NPF_Generic
- Bluetooth PAN Driver (Microsoft's Packet Scheduler) : \Device\NP
- Attansic AtcL001 Gigabit Ethernet Controller (Microsoft's Packet S
- MS Tunnel Interface Driver: \Device\NPF_{A428436F-9700-4571

☑ Capture packets in promiscuou

□ Limit each packet to 1

Capture Filter:

Capture File(s)

File: Browse...

□ Use multiple files

☑ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

☑ Ring buffer with 2 files

□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

Name Resolution

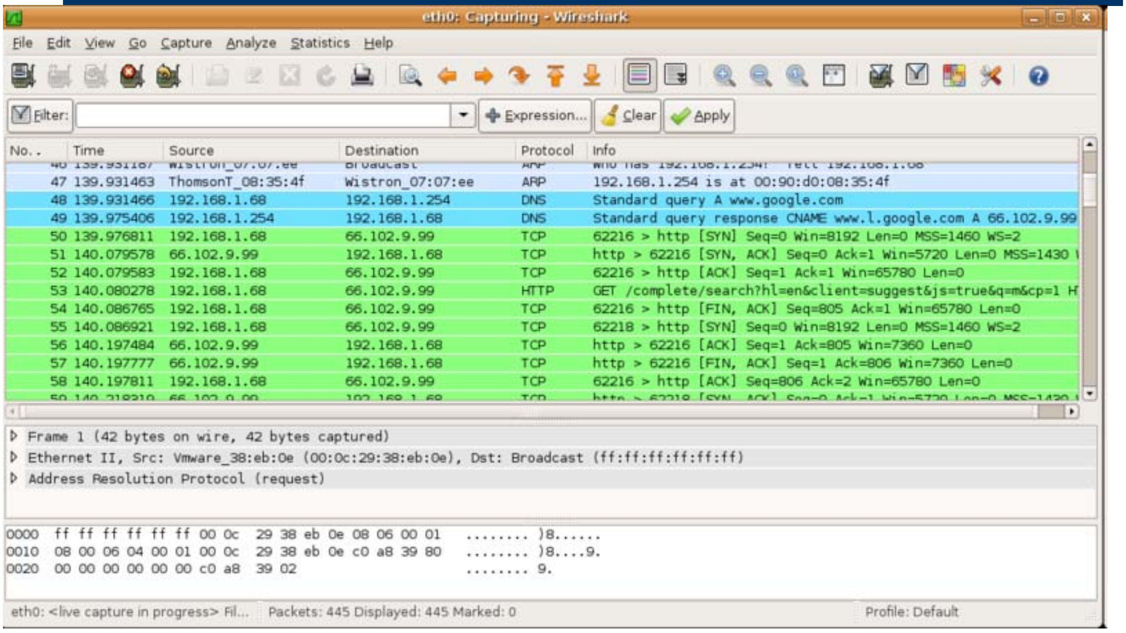
☑ Enable MAC name resolution

□ Enable network name resolution

☑ Enable transport name resolution

註：監聽無線網卡
　請取消 promiscuous mode

Wireshark


eth0: Capturing - Wireshark

```
No. .  Time        Source              Destination         Protocol  Info
    46 139.931187  Wistron_07:07:ee    Broadcast           ARP       Who has 192.168.1.254?  Tell 192.168.1.68
    47 139.931463  ThomsonT_08:35:4f   Wistron_07:07:ee    ARP       192.168.1.254 is at 00:90:d0:08:35:4f
    48 139.931466  192.168.1.68        192.168.1.254       DNS       Standard query A www.google.com
    49 139.975406  192.168.1.254       192.168.1.68        DNS       Standard query response CNAME www.l.google.com A 66.102.9.99
    50 139.976811  192.168.1.68        66.102.9.99         TCP       62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
    51 140.079578  66.102.9.99         192.168.1.68        TCP       http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 W
    52 140.079583  192.168.1.68        66.102.9.99         TCP       62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
    53 140.080278  192.168.1.68        66.102.9.99         HTTP      GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
    54 140.086765  192.168.1.68        66.102.9.99         TCP       62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
    55 140.086921  192.168.1.68        66.102.9.99         TCP       62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
    56 140.197484  66.102.9.99         192.168.1.68        TCP       http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
    57 140.197777  66.102.9.99         192.168.1.68        TCP       http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
    58 140.197811  192.168.1.68        66.102.9.99         TCP       62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
    59 140.218319  66.102.9.99         192.168.1.68        TCP       http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 W
```

```
▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.
```

eth0: <live capture in progress> Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default

- 來源: Wikipedia – Wireshark on Ubuntu

tcpdump

- 封包擷取工具
  - 適合在純文字模式下使用
  - 獲擷取的封包可存為檔案供 Wireshark 分析
- 指令: tcpdump
  - 例: tcpdump -i eth0 ‘src or dst host 192.168.0.1’
    指擷取經由 eth0 網卡、來源或目的為IP位址 192.168.0.1 的封包

網路安全

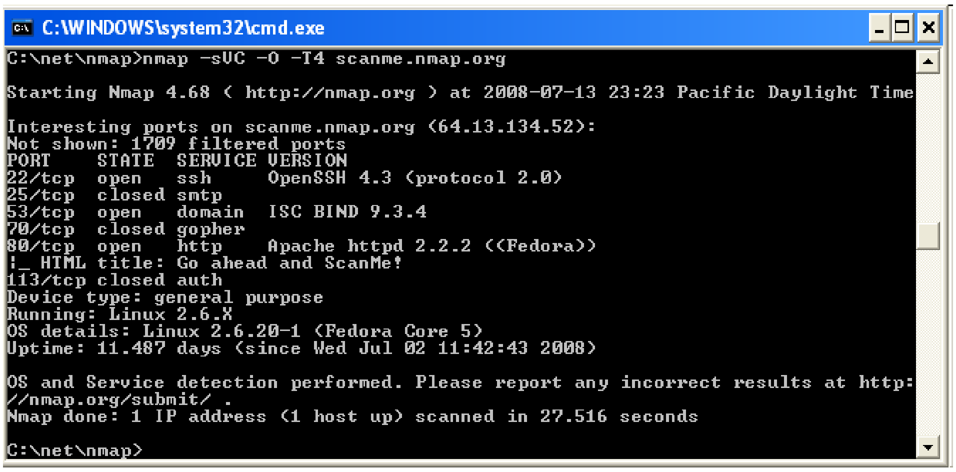
- Nmap
- Angry IP Scanner (ipscan.exe)
- Nessus

Nmap

- 網路安全掃瞄器
  - Port Scanning
- 純文字指令:
  - nmap <IP位址/網域名稱>
- http://www.nmap.org/

Nmap

- 測試：
  - nmap -sVC -O -T4 scanme.nmap.org

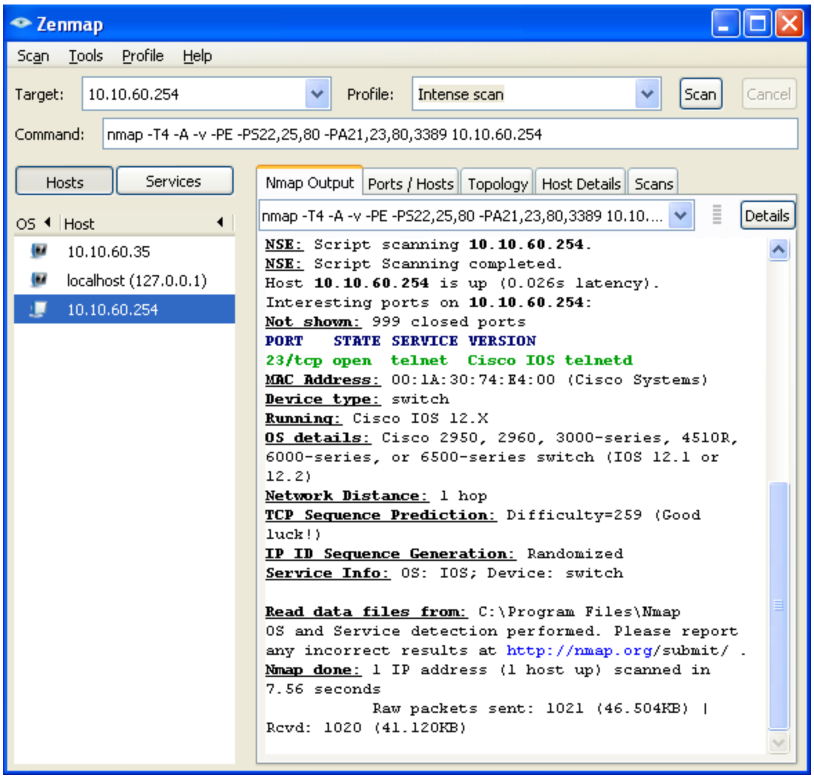


```
C:\net\nmap>nmap -sVC -O -T4 scanme.nmap.org

Starting Nmap 4.68 ( http://nmap.org ) at 2008-07-13 23:23 Pacific Daylight Time

Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 1709 filtered ports
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 4.3 (protocol 2.0)
25/tcp   closed smtp
53/tcp   open   domain  ISC BIND 9.3.4
70/tcp   closed gopher
80/tcp   open   http    Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Go ahead and ScanMe!
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 11.487 days (since Wed Jul 02 11:42:43 2008)

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.516 seconds

C:\net\nmap>
```

- 來源: http://nmap.org/book/inst-windows.html

Zenmap － Nmap GUI Frontend

- 註: (Windows版) 已同捆於Nmap安裝程式



Target: 10.10.60.254

Profile: Intense scan

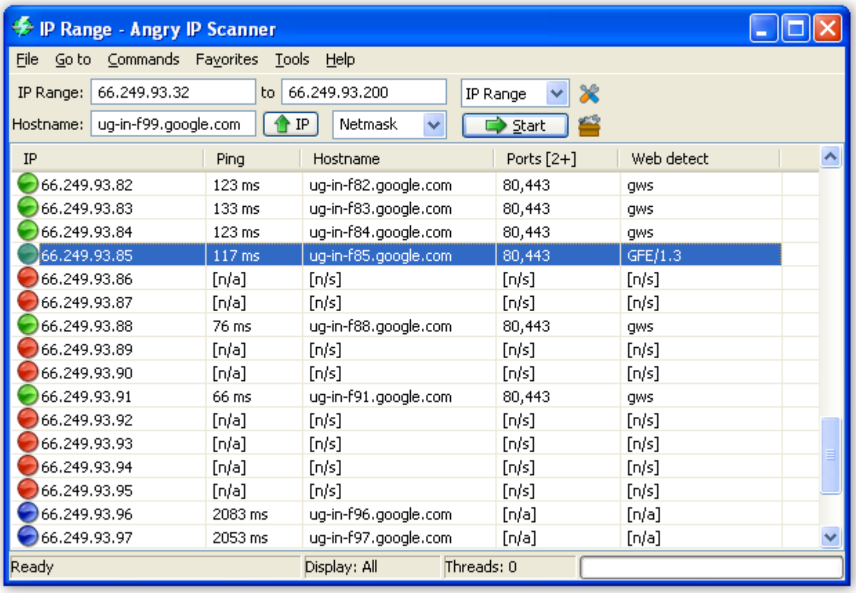
Command: nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 10.10.60.254

```
nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 10.10....
NSE: Script scanning 10.10.60.254.
NSE: Script Scanning completed.
Host 10.10.60.254 is up (0.026s latency).
Interesting ports on 10.10.60.254:
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Cisco IOS telnetd
MAC Address: 00:1A:30:74:E4:00 (Cisco Systems)
Device type: switch
Running: Cisco IOS 12.X
OS details: Cisco 2950, 2960, 3000-series, 4510R,
6000-series, or 6500-series switch (IOS 12.1 or
12.2)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good
luck!)
IP ID Sequence Generation: Randomized
Service Info: OS: IOS; Device: switch

Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report
any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in
7.56 seconds
           Raw packets sent: 1021 (46.504KB) |
Rcvd: 1020 (41.120KB)
```

Angry IP Scanner

- ipscan.exe
  - 輕量級 Scanner, 檔案大小<1M!
  - 掃描特定IP位址或網段是否有設備存在
    1. 可指定協定與 Port number
  - 網站: http://www.angryip.org/

Angry IP Scanner



IP Range: 66.249.93.32 to 66.249.93.200 IP Range

Hostname: ug-in-f99.google.com Netmask

IP	Ping	Hostname	Ports [2+]	Web detect
🟢 66.249.93.82	123 ms	ug-in-f82.google.com	80,443	gws
🟢 66.249.93.83	133 ms	ug-in-f83.google.com	80,443	gws
🟢 66.249.93.84	123 ms	ug-in-f84.google.com	80,443	gws
🟢 66.249.93.85	117 ms	ug-in-f85.google.com	80,443	GFE/1.3
🔴 66.249.93.86	[n/a]	[n/s]	[n/s]	[n/s]
🔴 66.249.93.87	[n/a]	[n/s]	[n/s]	[n/s]
🟢 66.249.93.88	76 ms	ug-in-f88.google.com	80,443	gws
🔴 66.249.93.89	[n/a]	[n/s]	[n/s]	[n/s]
🔴 66.249.93.90	[n/a]	[n/s]	[n/s]	[n/s]
🟢 66.249.93.91	66 ms	ug-in-f91.google.com	80,443	gws
🔴 66.249.93.92	[n/a]	[n/s]	[n/s]	[n/s]
🔴 66.249.93.93	[n/a]	[n/s]	[n/s]	[n/s]
🔴 66.249.93.94	[n/a]	[n/s]	[n/s]	[n/s]
🔴 66.249.93.95	[n/a]	[n/s]	[n/s]	[n/s]
🔵 66.249.93.96	2083 ms	ug-in-f96.google.com	[n/a]	[n/a]
🔵 66.249.93.97	2053 ms	ug-in-f97.google.com	[n/a]	[n/a]

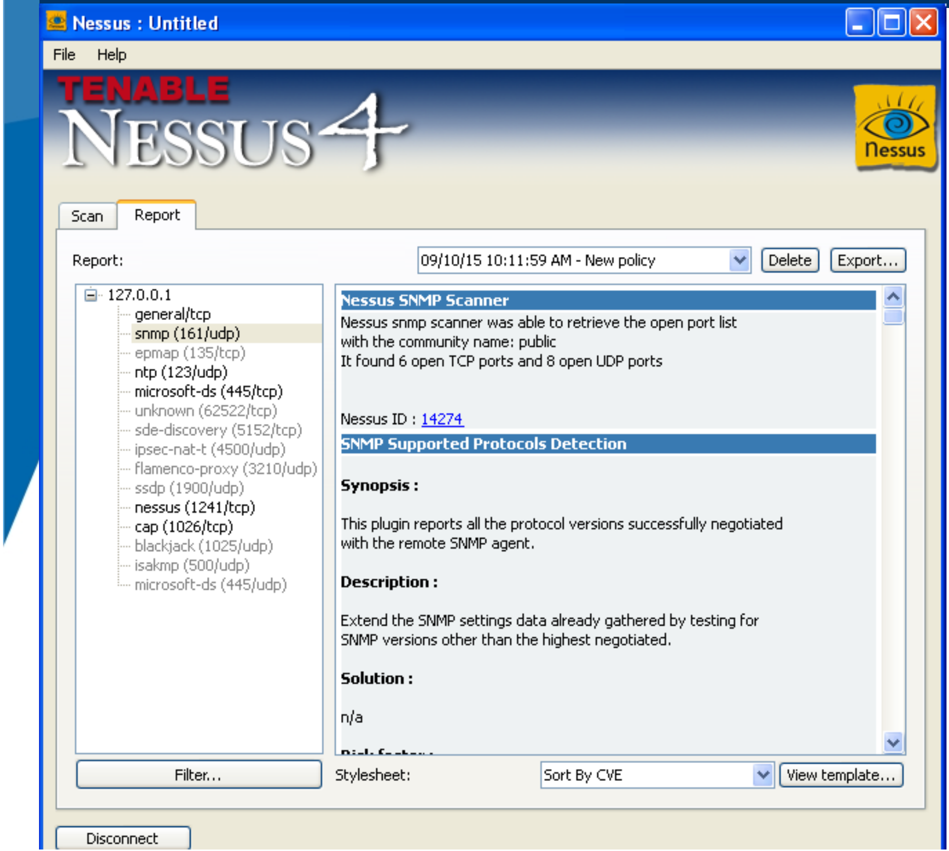
Ready Display: All Threads: 0

- 來源: http://www.angryip.org/w/Screenshots

Nessus

- 弱點掃描系統
  - 漏洞偵測
  - 敏感資料偵測
  - 特徵掃描
- Client/Server架構
  - 以 Client 控制、由 Server 進行測試
- 商業軟體
  - 家用免費更新特徵碼(需上網註冊)
- 網站: http://www.nessus.org/

Nessus



Report: 09/10/15 10:11:59 AM - New policy

- 127.0.0.1
  - general/tcp
  - snmp (161/udp)
  - epmap (135/tcp)
  - ntp (123/udp)
  - microsoft-ds (445/tcp)
  - unknown (62522/tcp)
  - sde-discovery (5152/tcp)
  - ipsec-nat-t (4500/udp)
  - flamenco-proxy (3210/udp)
  - ssdp (1900/udp)
  - nessus (1241/tcp)
  - cap (1026/tcp)
  - blackjack (1025/udp)
  - isakmp (500/udp)
  - microsoft-ds (445/udp)

Nessus SNMP Scanner

Nessus snmp scanner was able to retrieve the open port list
with the community name: public
It found 6 open TCP ports and 8 open UDP ports

Nessus ID : 14274

SNMP Supported Protocols Detection

Synopsis :

This plugin reports all the protocol versions successfully negotiated
with the remote SNMP agent.

Description :

Extend the SNMP settings data already gathered by testing for
SNMP versions other than the highest negotiated.

Solution :

n/a

Stylesheet: Sort By CVE

其他網路安全系統

- Snort
  - 網路入侵防止與偵測系統(IDS/IPS)
  - http://www.snort.org/
- Honeypots
  - 攻擊誘捕系統
  - http://www.honeypots.net/

延伸閱讀

- 蔡一郎、邱敏乘 "Linux 網管技術—流量統計與效能監控" 上奇, 民95
- 蔣大偉 譯 "SNMP 網管實務 (Essential SNMP, 2/e)", 歐萊禮, 民96

謝謝

敬請來信指導

alextwl@ms11.voip.edu.tw

98年10月22日