網路品質管理工具
The Dude 簡介

- 報告人：游子興
- Email：davisyou@ntu.edu.tw
- 電話：02-33665008
- 日期：2014/8/21

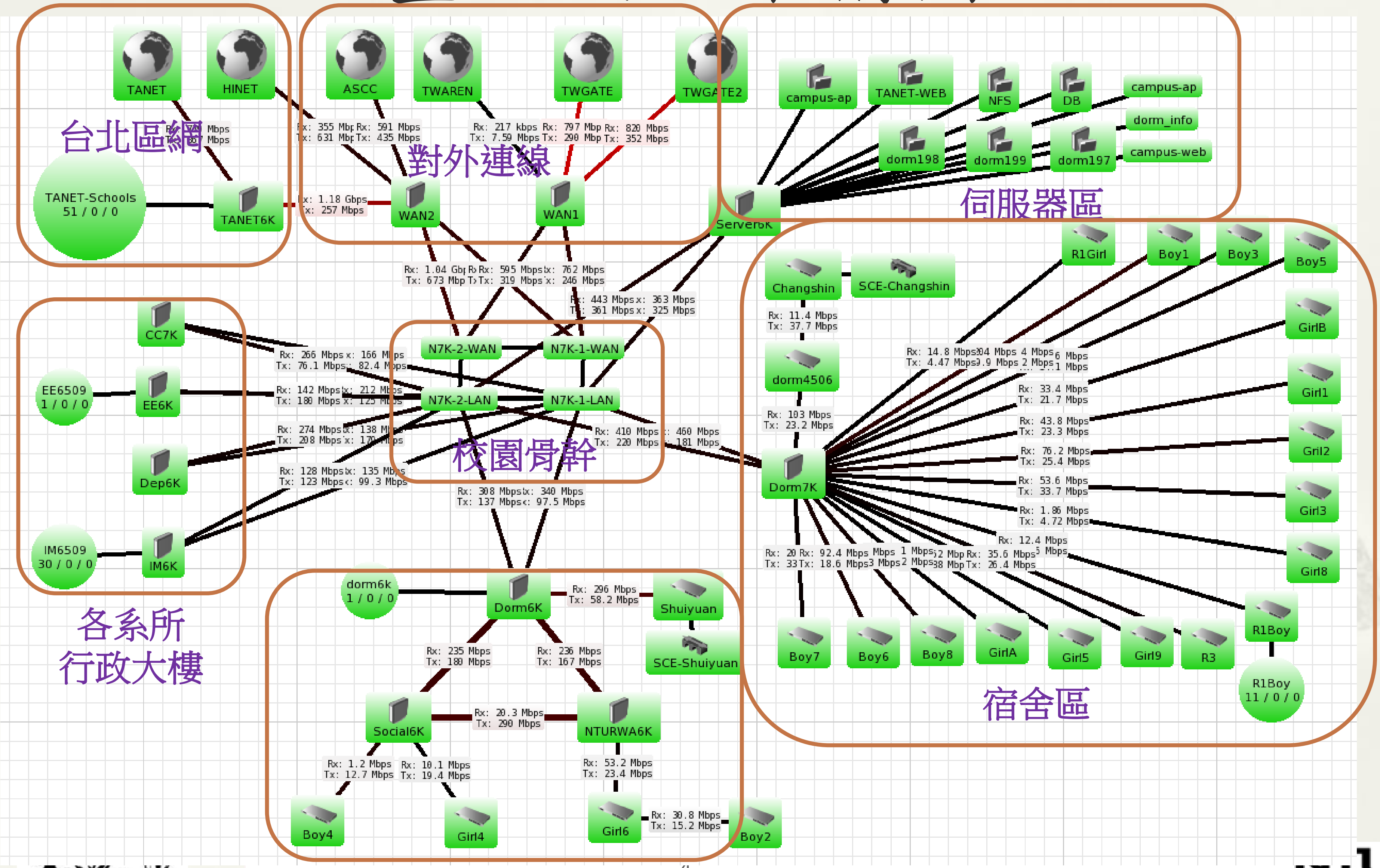
大綱

- The Dude 簡介
- 網路與伺服器服務狀態偵測
- 圖表製作與應用
- 各種服務偵測方法
- SNMP 相關設定
- 異常通知與設定
- 其他設定
- 常用網路查修工具

The Dude 官方網頁

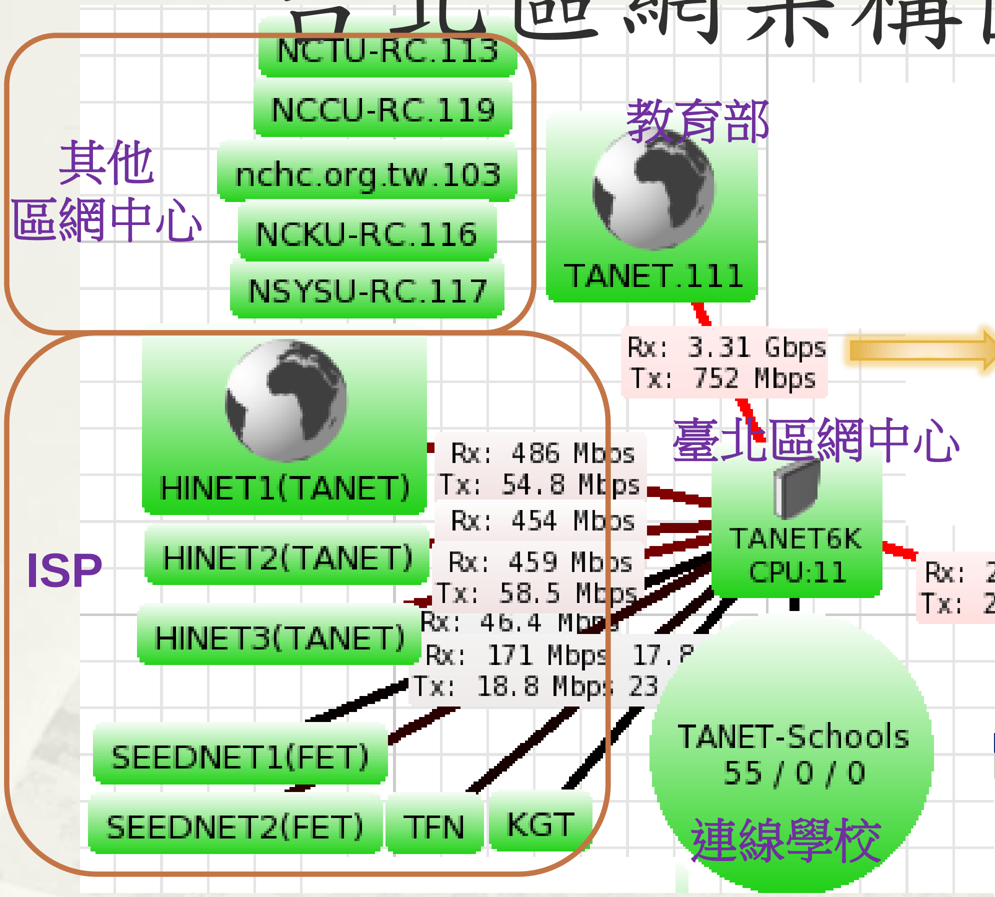
- http://www.mikrotik.com/thedude
- The Dude v4.0beta3
- Freeware、Windows Platform
- Client/Server 架構
- Client
  - 專屬程式
  - Browser

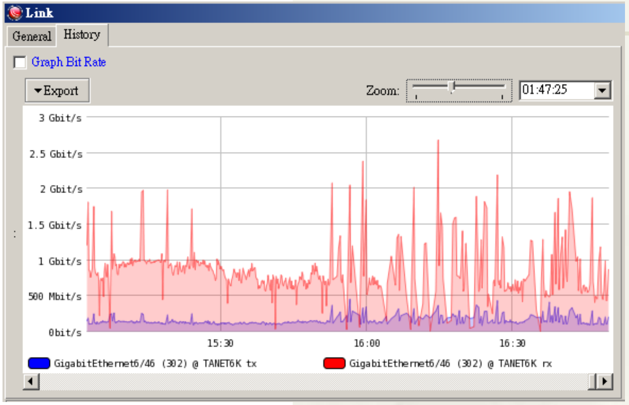
臺大網路架構圖



醫學院、社科院

台北區網架構圖-線路流量



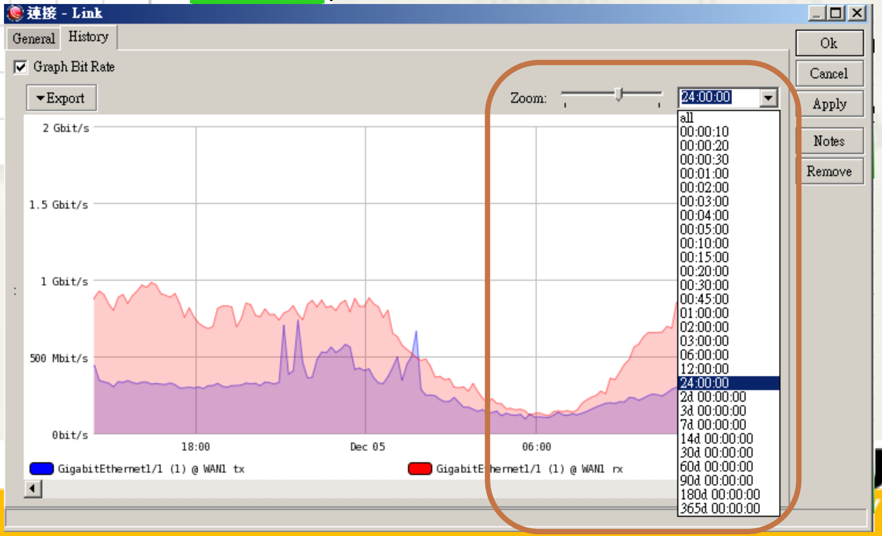


□ Graph Bit Rate

Zoom: 01:47:25

🟦 GigabitEthernet6/46 (302) @ TANET6K tx
🟥 GigabitEthernet6/46 (302) @ TANET6K rx

時間區間:
10秒 ~ 365天



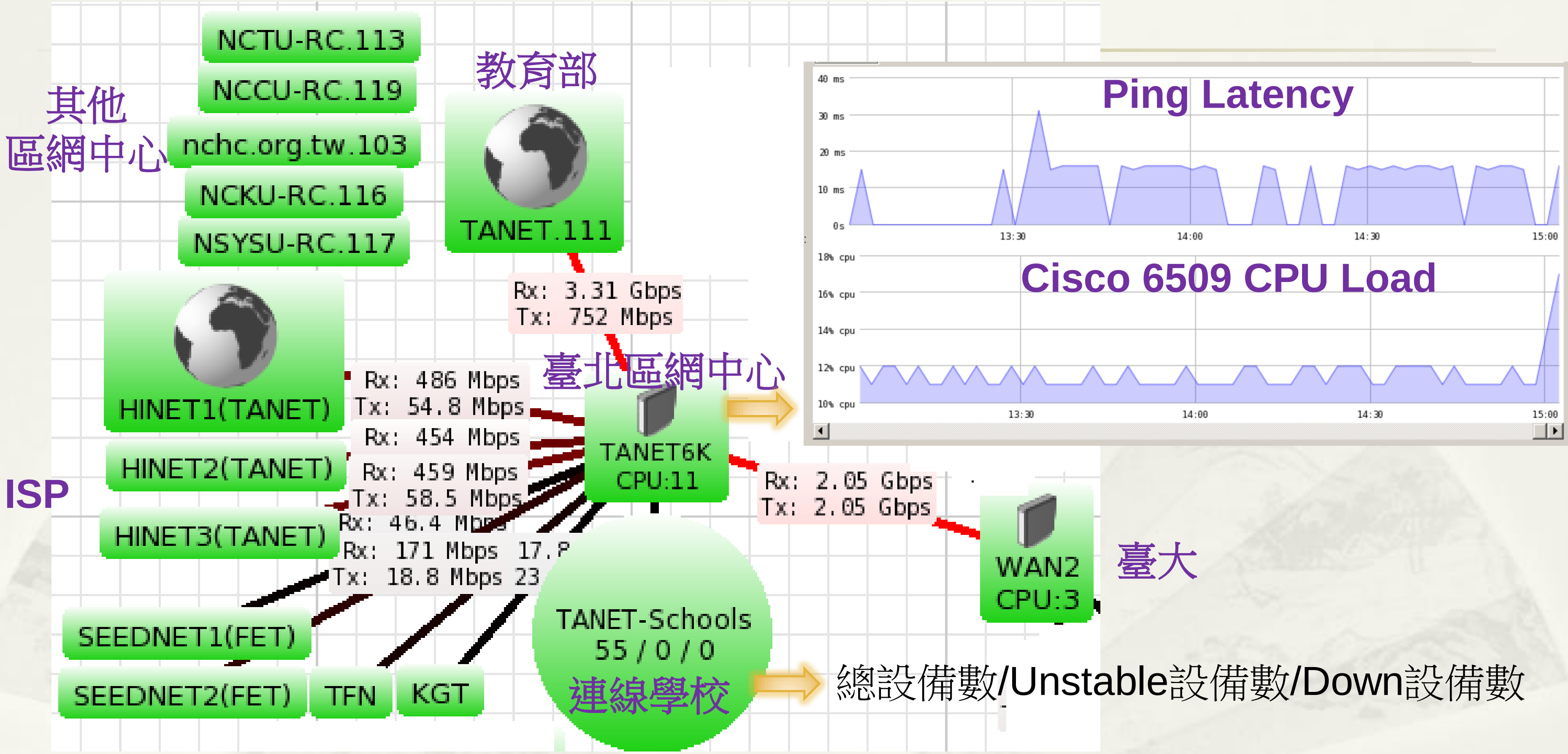
☑ Graph Bit Rate

Zoom: 24:00:00

🟦 GigabitEthernet1/1 (1) @ WAN1 tx
🟥 GigabitEthernet1/1 (1) @ WAN1 rx

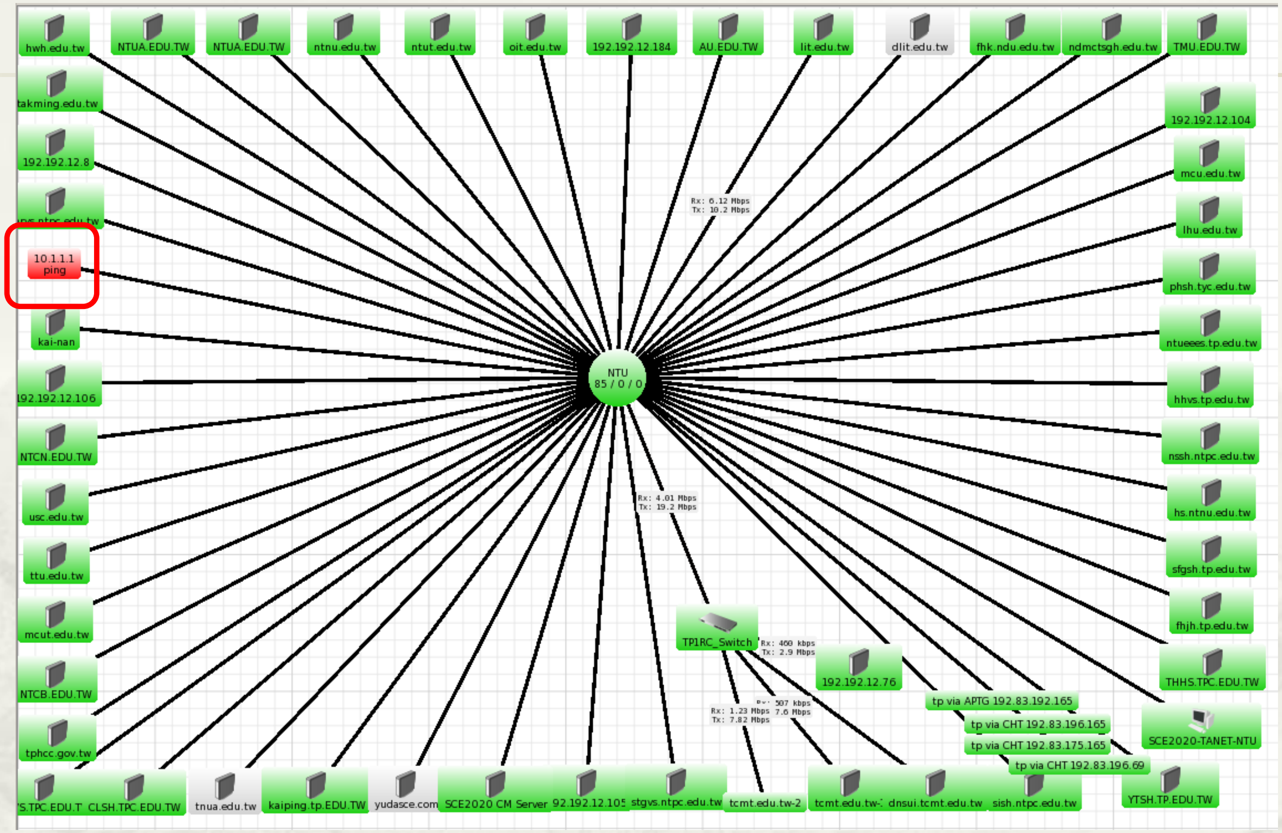
- 線路流量顯示即時
- 流量接近滿載以紅色顯示

台北區網架構圖-Router Status

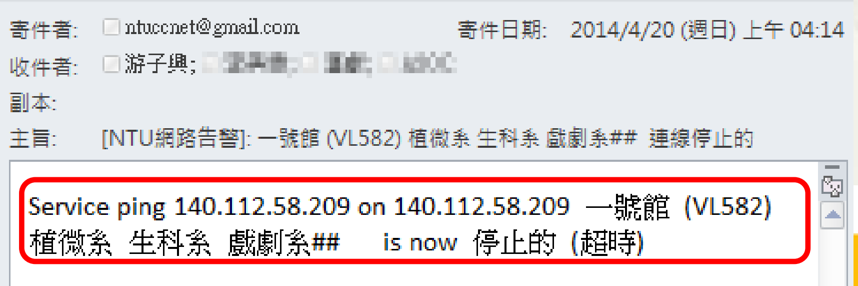


- Router Status即時顯示
- 可 Drill Down 連結不同網路圖

台北區網架構圖- 連線學校



- 線路障礙即時通知 email



寄件者: □ ntuccnet@gmail.com 寄件日期: 2014/4/20 (週日) 上午 04:14

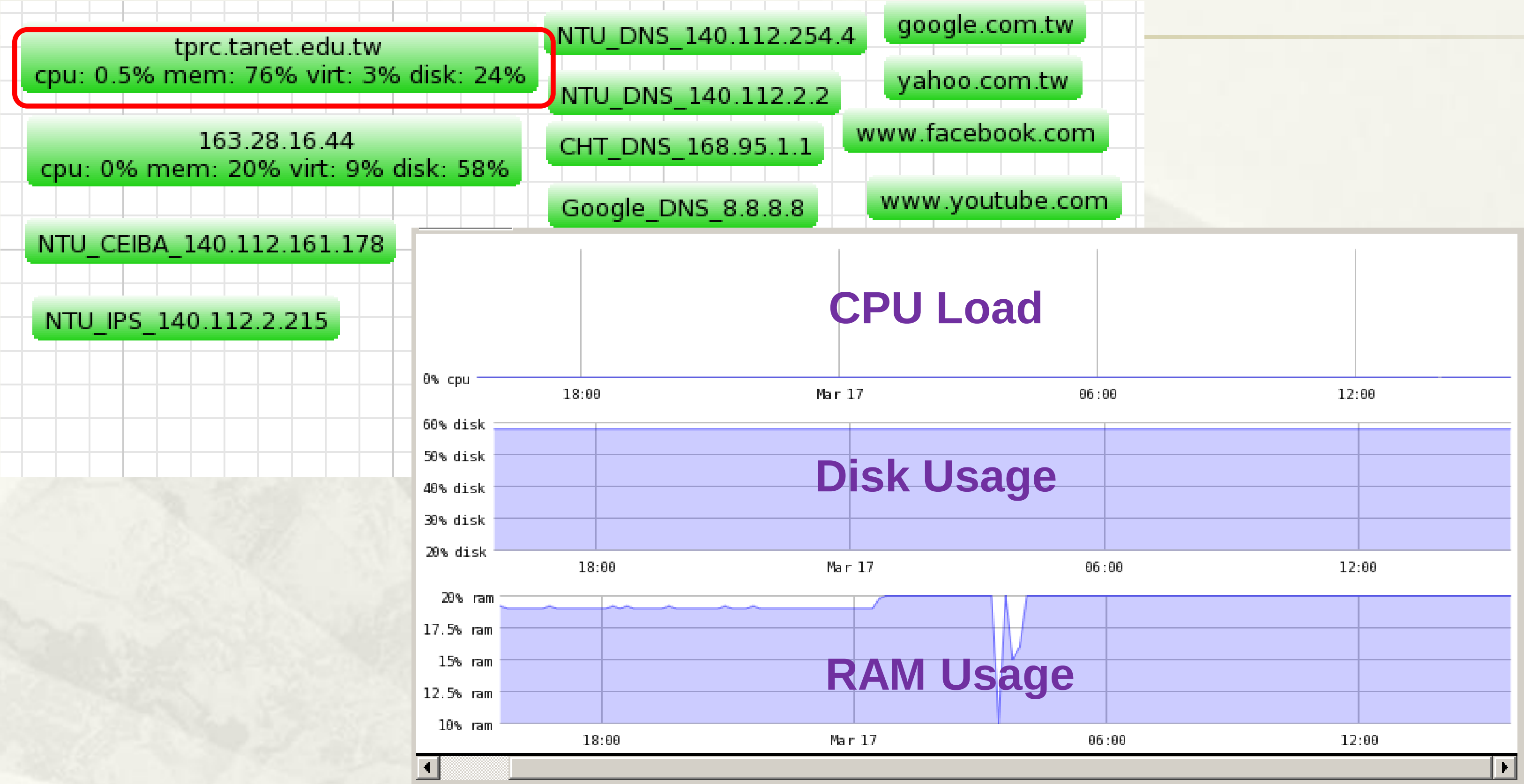
收件者: □ 游子興; [redacted]

副本:

主旨: [NTU網路告警]: 一號館 (VL582) 植微系 生科系 戲劇系## 連線停止的

Service ping 140.112.58.209 on 140.112.58.209 一號館 (VL582)
植微系 生科系 戲劇系## is now 停止的 (超時)

伺服器狀態



tprc.tanet.edu.tw
cpu: 0.5% mem: 76% virt: 3% disk: 24%

163.28.16.44
cpu: 0% mem: 20% virt: 9% disk: 58%

NTU_CEIBA_140.112.161.178

NTU_IPS_140.112.2.215

NTU_DNS_140.112.254.4

NTU_DNS_140.112.2.2

CHT_DNS_168.95.1.1

Google_DNS_8.8.8.8

google.com.tw

yahoo.com.tw

www.facebook.com

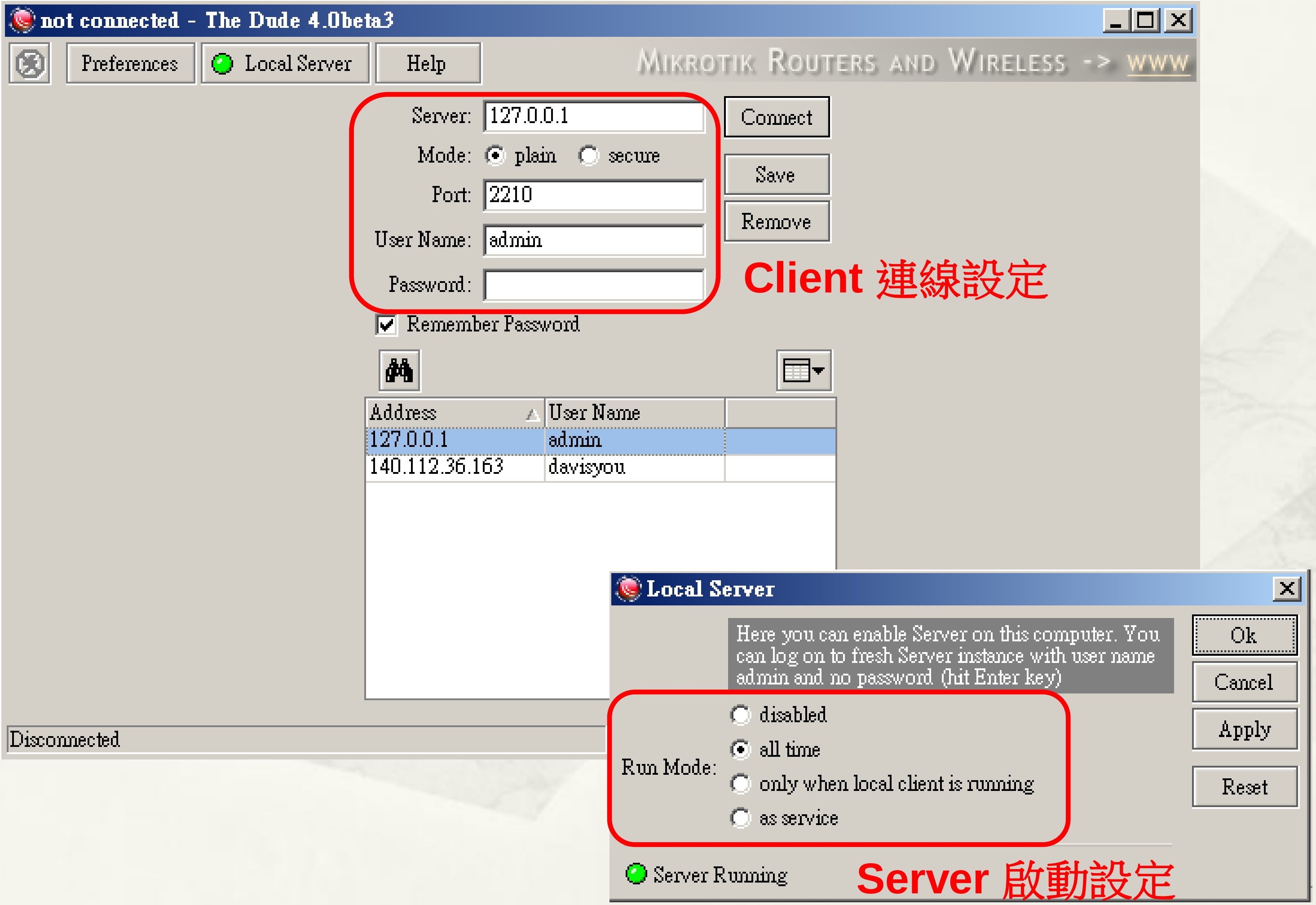
www.youtube.com

- 伺服器狀態即時顯示與歷史記錄
- CPU、記憶體、虛擬記憶體、磁碟空間

Practice 練習

- Browser:
  - 網址 http://140.112.3.82/
  - Login: test
  - Passwd: thedude
- http://www.mikrotik.com/thedude
  - 下載 Dude v4.0beta3 並安裝

Client/Server setup


not connected - The Dude 4.0beta3
Preferences
Local Server
Help
MIKROTIK ROUTERS AND WIRELESS -> WWW
Connect
Save
Remove

Server: 127.0.0.1
Mode: ● plain ○ secure
Port: 2210
User Name: admin
Password:
☑ Remember Password

Client 連線設定

Address	User Name
127.0.0.1	admin
140.112.36.163	davisyou

Disconnected

Here you can enable Server on this computer. You can log on to fresh Server instance with user name admin and no password (hit Enter key)

Run Mode:
○ disabled
● all time
○ only when local client is running
○ as service

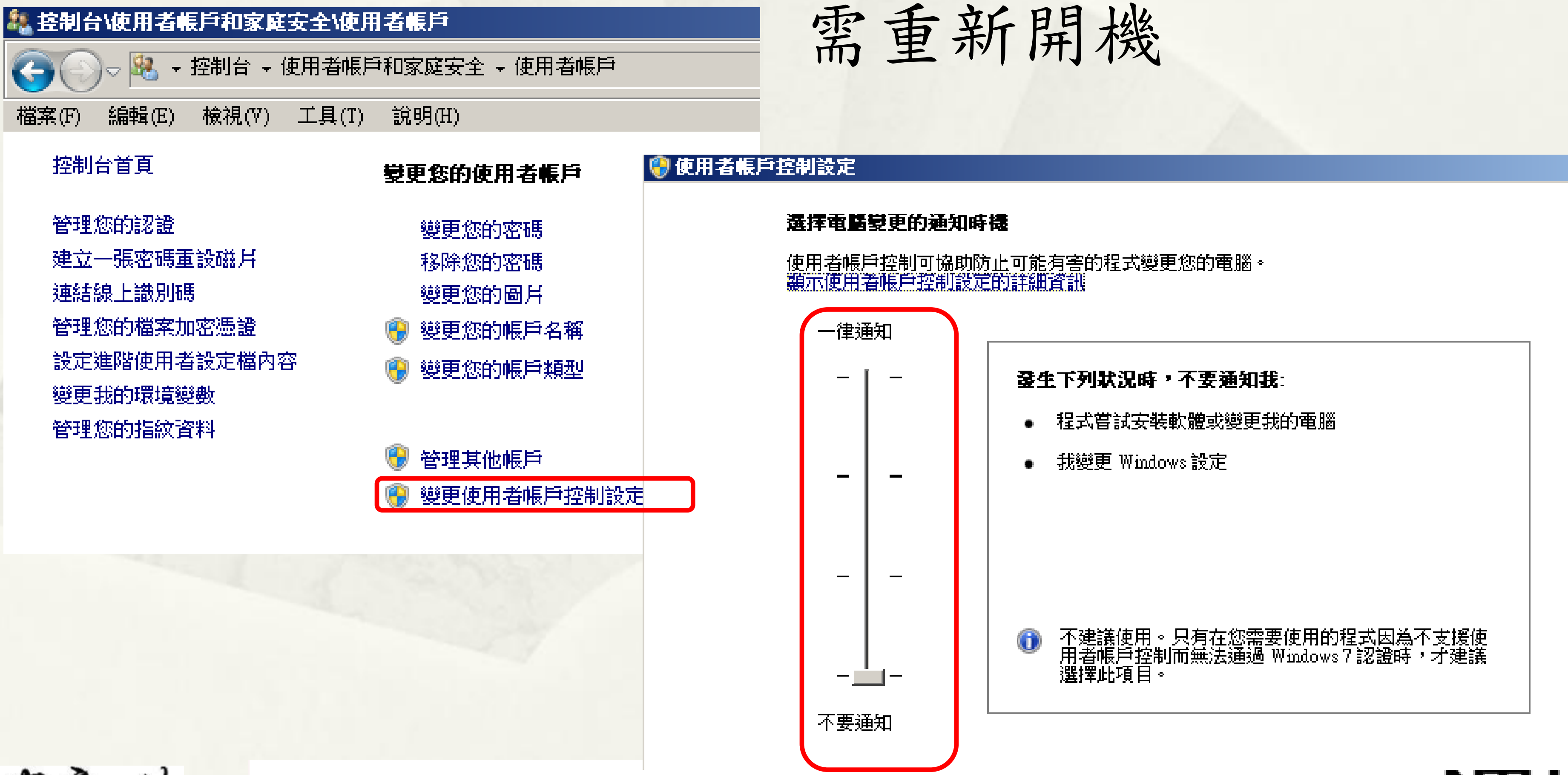
● Server Running

Server 啟動設定

解決 Win7 IP ping failed

- 控制台\使用者帳戶和家庭安全\使用者帳戶

需重新開機



控制台\使用者帳戶和家庭安全\使用者帳戶

控制台 ▸ 使用者帳戶和家庭安全 ▸ 使用者帳戶

檔案(F) 編輯(E) 檢視(V) 工具(T) 說明(H)

控制台首頁

管理您的認證
建立一張密碼重設磁片
連結線上識別碼
管理您的檔案加密憑證
設定進階使用者設定檔內容
變更我的環境變數
管理您的指紋資料

變更您的使用者帳戶

變更您的密碼
移除您的密碼
變更您的圖片
變更您的帳戶名稱
變更您的帳戶類型

管理其他帳戶
變更使用者帳戶控制設定

使用者帳戶控制設定

選擇電腦變更的通知時機

使用者帳戶控制可協助防止可能有害的程式變更您的電腦。
顯示使用者帳戶控制設定的詳細資訊

一律通知

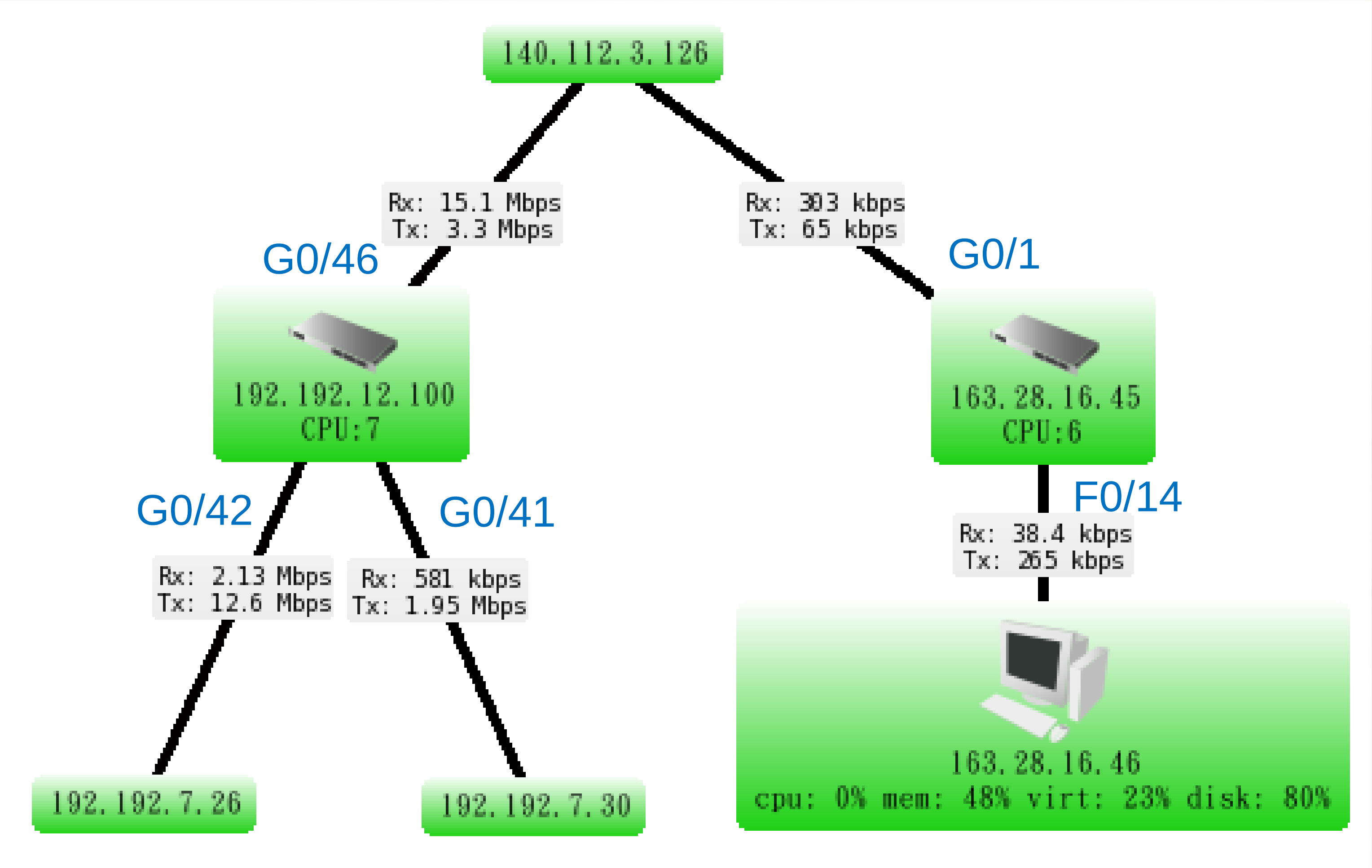
不要通知

發生下列狀況時，不要通知我:

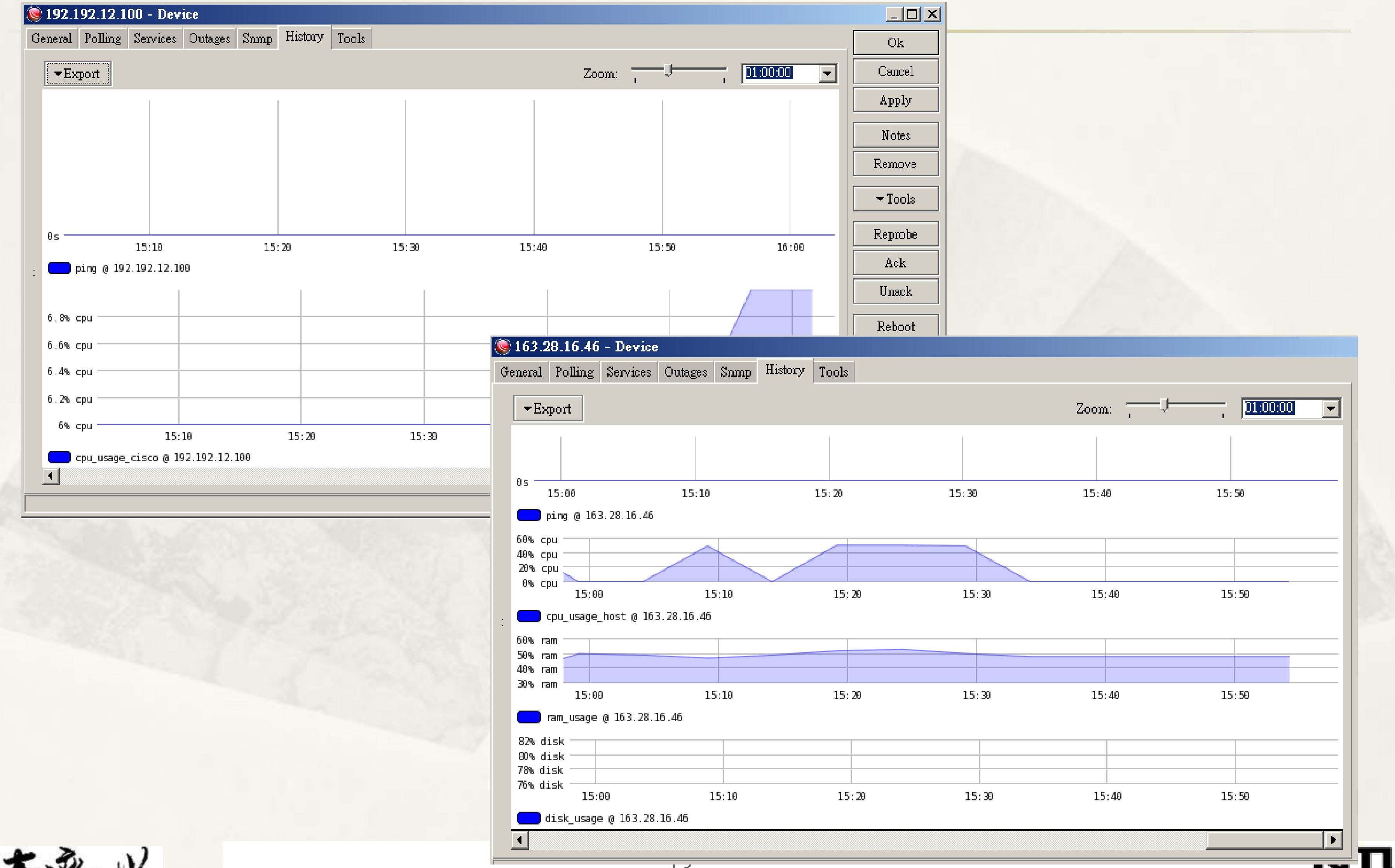
- 程式嘗試安裝軟體或變更我的電腦
- 我變更 Windows 設定

不建議使用。只有在您需要使用的程式因為不支援使用者帳戶控制而無法通過 Windows 7 認證時，才建議選擇此項目。

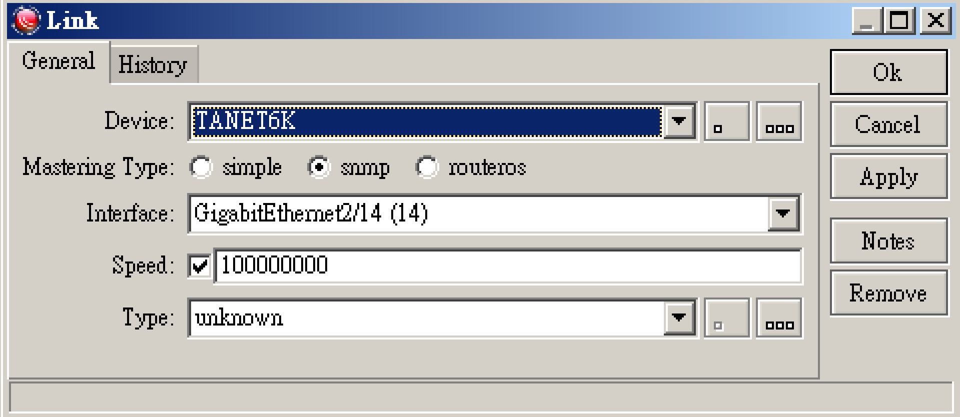
實做 1/2


140.112.3.126
Rx: 15.1 Mbps
Tx: 3.3 Mbps
Rx: 303 kbps
Tx: 65 kbps
G0/46
G0/1
192.192.12.100
CPU:7
163.28.16.45
CPU:6
G0/42
G0/41
F0/14
Rx: 38.4 kbps
Tx: 265 kbps
Rx: 2.13 Mbps
Tx: 12.6 Mbps
Rx: 581 kbps
Tx: 1.95 Mbps
192.192.7.26
192.192.7.30
163.28.16.46
cpu: 0% mem: 48% virt: 23% disk: 80%

實做 2/2


192.192.12.100 - Device
General
Polling
Services
Outages
Snmp
History
Tools
Export
Zoom:
01:00:00
Ok
Cancel
Apply
Notes
Remove
Tools
Reprobe
Ack
Unack
Reboot
0s
15:10
15:20
15:30
15:40
15:50
16:00
ping @ 192.192.12.100
6.8% cpu
6.6% cpu
6.4% cpu
6.2% cpu
6% cpu
15:10
15:20
15:30
cpu_usage_cisco @ 192.192.12.100
163.28.16.46 - Device
General
Polling
Services
Outages
Snmp
History
Tools
Export
Zoom:
01:00:00
0s
15:00
15:10
15:20
15:30
15:40
15:50
ping @ 163.28.16.46
60% cpu
40% cpu
20% cpu
0% cpu
15:00
15:10
15:20
15:30
15:40
15:50
cpu_usage_host @ 163.28.16.46
60% ram
50% ram
40% ram
30% ram
15:00
15:10
15:20
15:30
15:40
15:50
ram_usage @ 163.28.16.46
82% disk
80% disk
78% disk
76% disk
15:00
15:10
15:20
15:30
15:40
15:50
disk_usage @ 163.28.16.46

Link



Link

General | History

Device: TANET6K

Mastering Type: ○ simple ● snmp ○ routeros

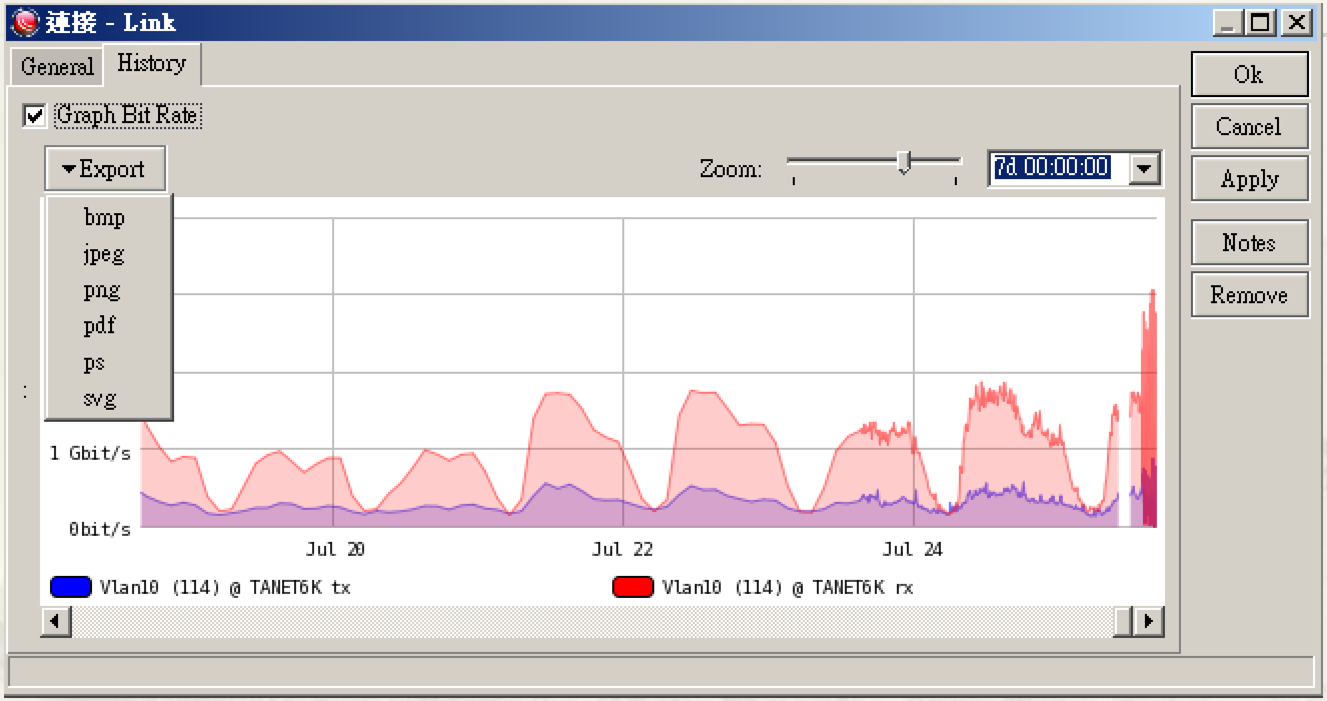
Interface: GigabitEthernet2/14 (14)

Speed: ☑ 100000000

Type: unknown

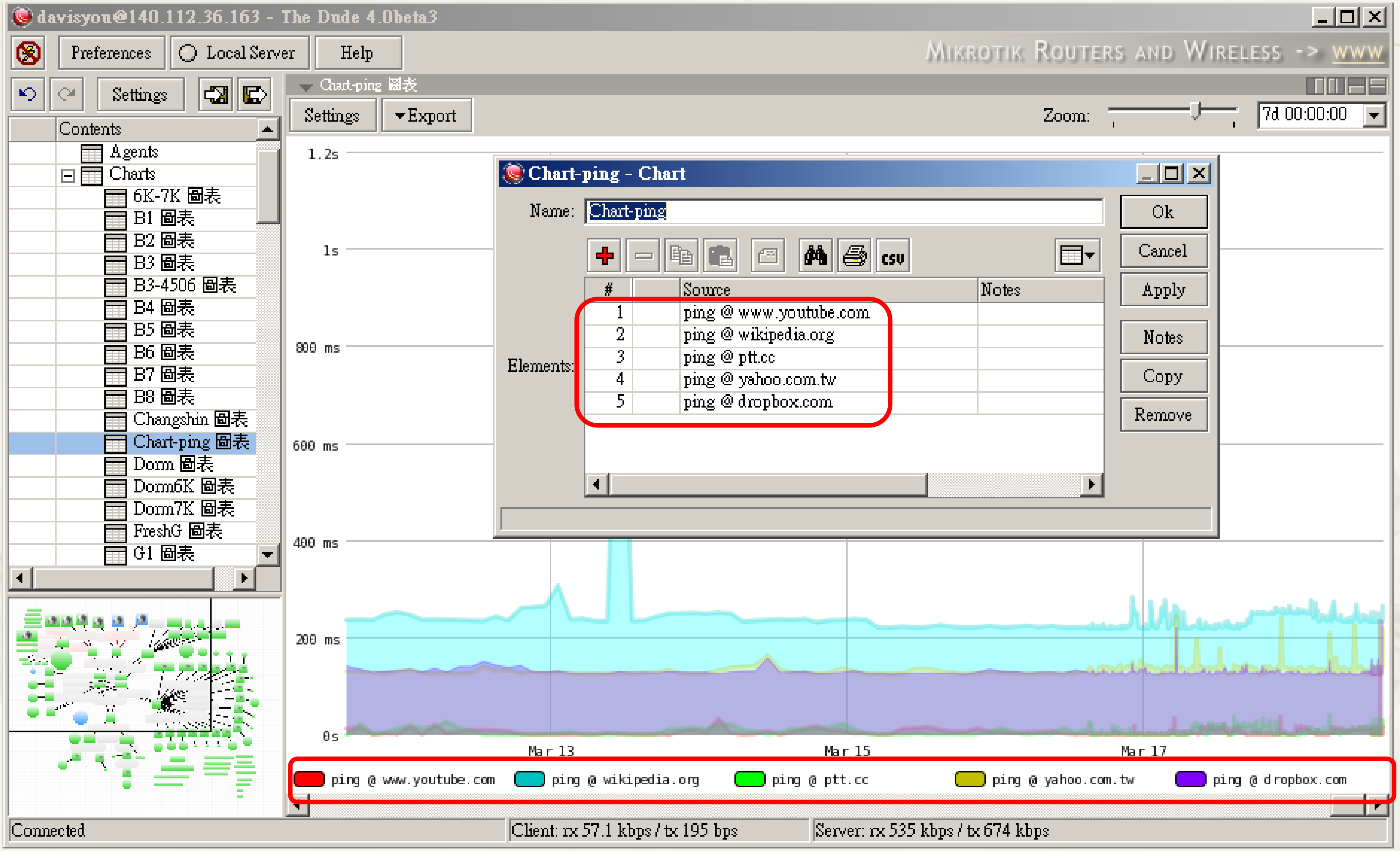
- Device=
- Mastering Type= simple/snmp/routeros
- Speed= -- Maxmum possible speed of link, 決定該線路頻寬是否滿載，若滿載以紅色表示。

Link: Export



- Export: 各種圖檔格式

圖表製作



davisyou@140.112.36.163 - The Dude 4.0beta3

Preferences | ○ Local Server | Help

MIKROTIK ROUTERS AND WIRELESS -> WWW

Settings

Contents
- Agents
- Charts
  - 6K-7K 圖表
  - B1 圖表
  - B2 圖表
  - B3 圖表
  - B3-4506 圖表
  - B4 圖表
  - B5 圖表
  - B6 圖表
  - B7 圖表
  - B8 圖表
  - Changshin 圖表
  - Chart-ping 圖表
  - Dorm 圖表
  - Dorm6K 圖表
  - Dorm7K 圖表
  - FreshG 圖表
  - G1 圖表

Chart-ping 圖表

Settings | ▾Export | Zoom: | 7d 00:00:00

Chart-ping - Chart

Name: Chart-ping

Elements:

#		Source	Notes
1		ping @ www.youtube.com	
2		ping @ wikipedia.org	
3		ping @ ptt.cc	
4		ping @ yahoo.com.tw	
5		ping @ dropbox.com	

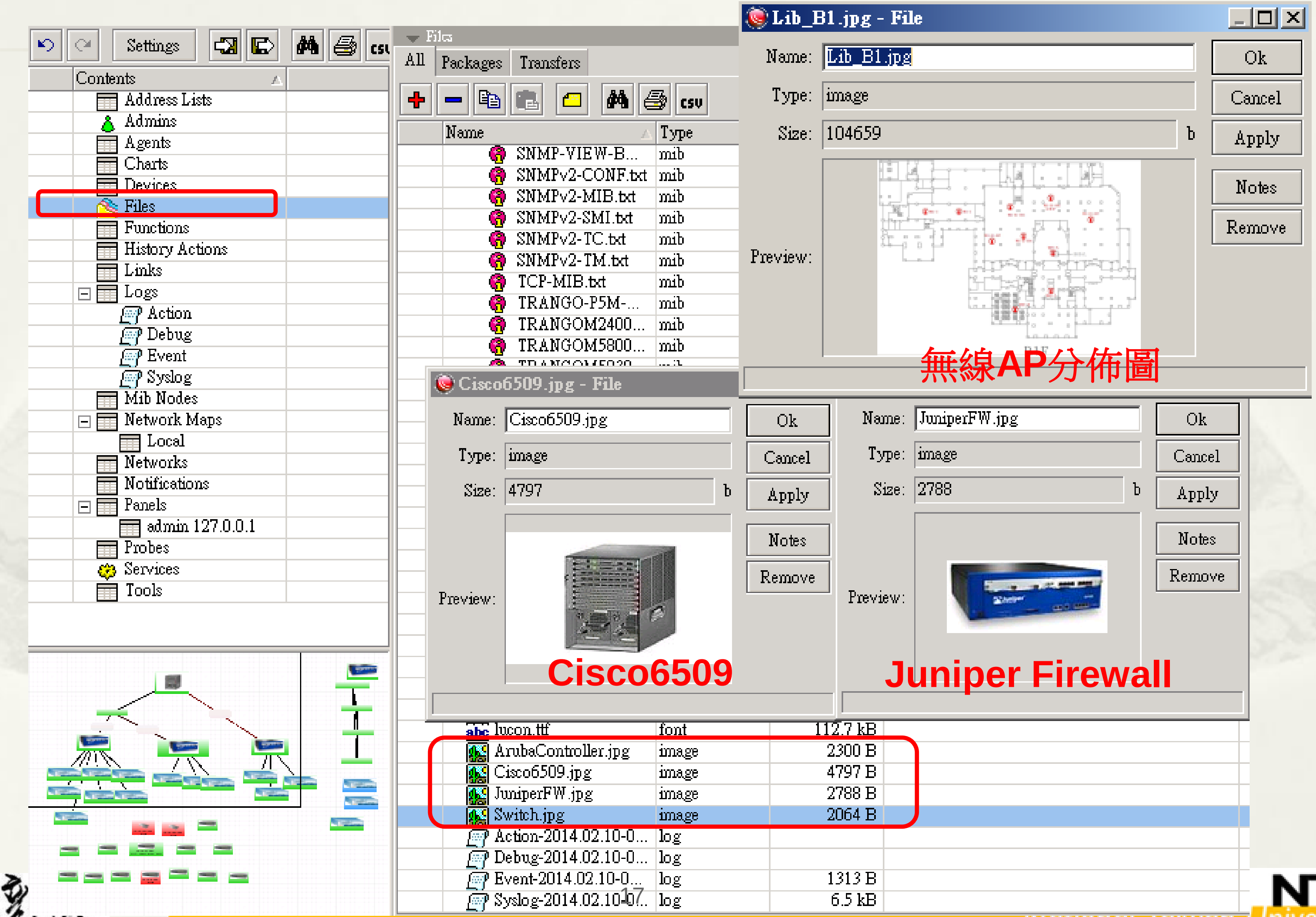
Ok | Cancel | Apply | Notes | Copy | Remove

🟥 ping @ www.youtube.com 🟦 ping @ wikipedia.org 🟩 ping @ ptt.cc 🟨 ping @ yahoo.com.tw 🟪 ping @ dropbox.com

Connected | Client: rx 57.1 kbps / tx 195 bps | Server: rx 535 kbps / tx 674 kbps

- 可自行合併偵測資料製作圖表

Files – 自行上傳圖片



Contents
- Address Lists
- Admins
- Agents
- Charts
- Devices
- Files
- Functions
- History Actions
- Links
- Logs
  - Action
  - Debug
  - Event
  - Syslog
- Mib Nodes
- Network Maps
  - Local
- Networks
- Notifications
- Panels
  - admin 127.0.0.1
- Probes
- Services
- Tools

```
Name                     Type
SNMP-VIEW-B...           mib
SNMPv2-CONF.txt          mib
SNMPv2-MIB.txt           mib
SNMPv2-SMI.txt           mib
SNMPv2-TC.txt            mib
SNMPv2-TM.txt            mib
TCP-MIB.txt              mib
TRANGO-P5M-...           mib
TRANGOM2400...           mib
TRANGOM5800...           mib
lucon.ttf                font      112.7 kB
ArubaController.jpg      image       2300 B
Cisco6509.jpg            image       4797 B
JuniperFW.jpg            image       2788 B
Switch.jpg               image       2064 B
Action-2014.02.10-0...   log
Debug-2014.02.10-0...    log
Event-2014.02.10-...     log         1313 B
Syslog-2014.02.10-0...   log         6.5 kB
```

Lib_B1.jpg - File

Name: Lib_B1.jpg
Type: image
Size: 104659 b
Preview:

無線AP分佈圖

Cisco6509.jpg - File

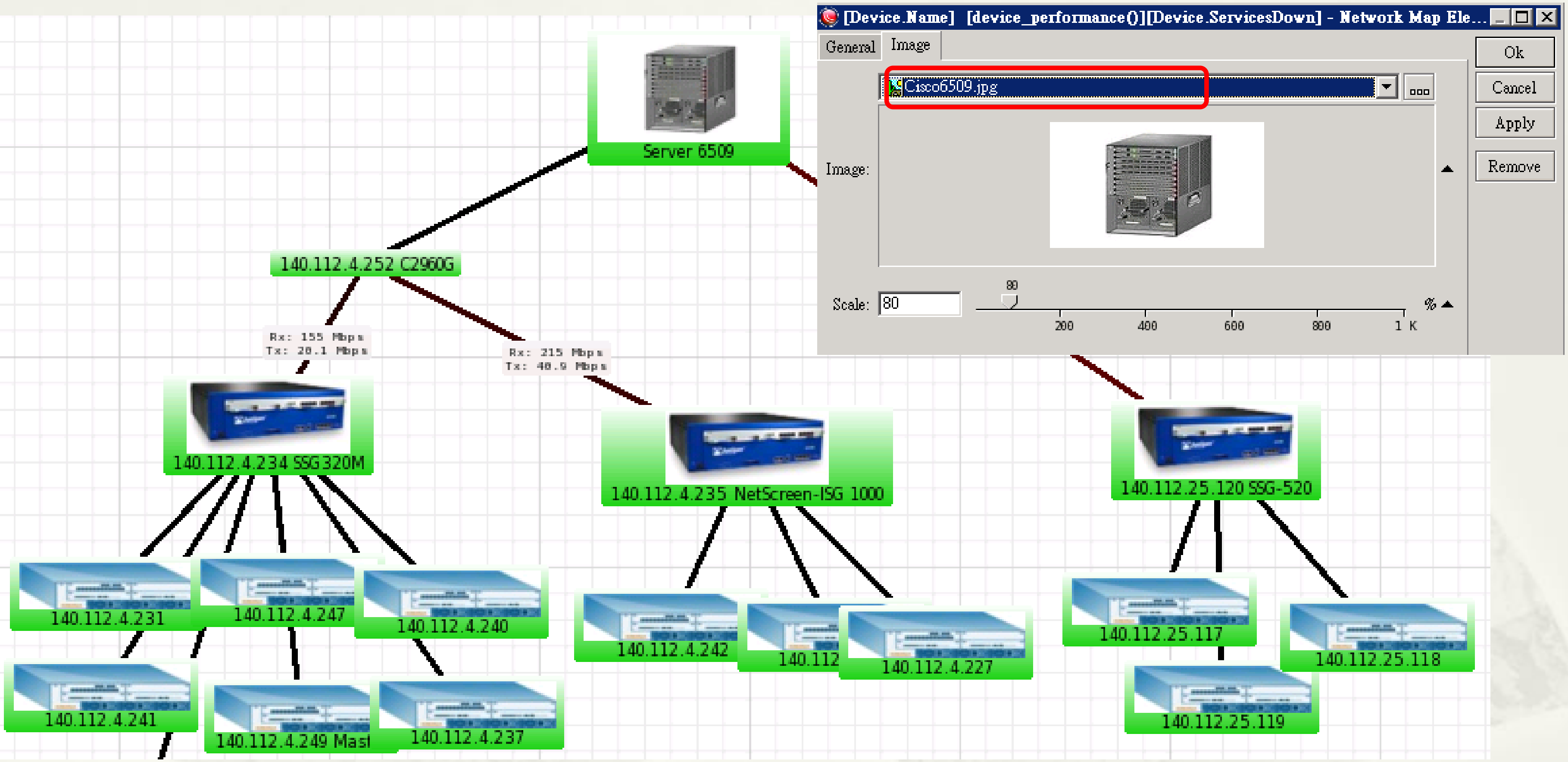
Name: Cisco6509.jpg
Type: image
Size: 4797 b
Preview:

Cisco6509

Name: JuniperFW.jpg
Type: image
Size: 2788 b
Preview:

Juniper Firewall

Device 圖示設定 1/2



[Device.Name] [device_performance()][Device.ServicesDown] - Network Map Ele...

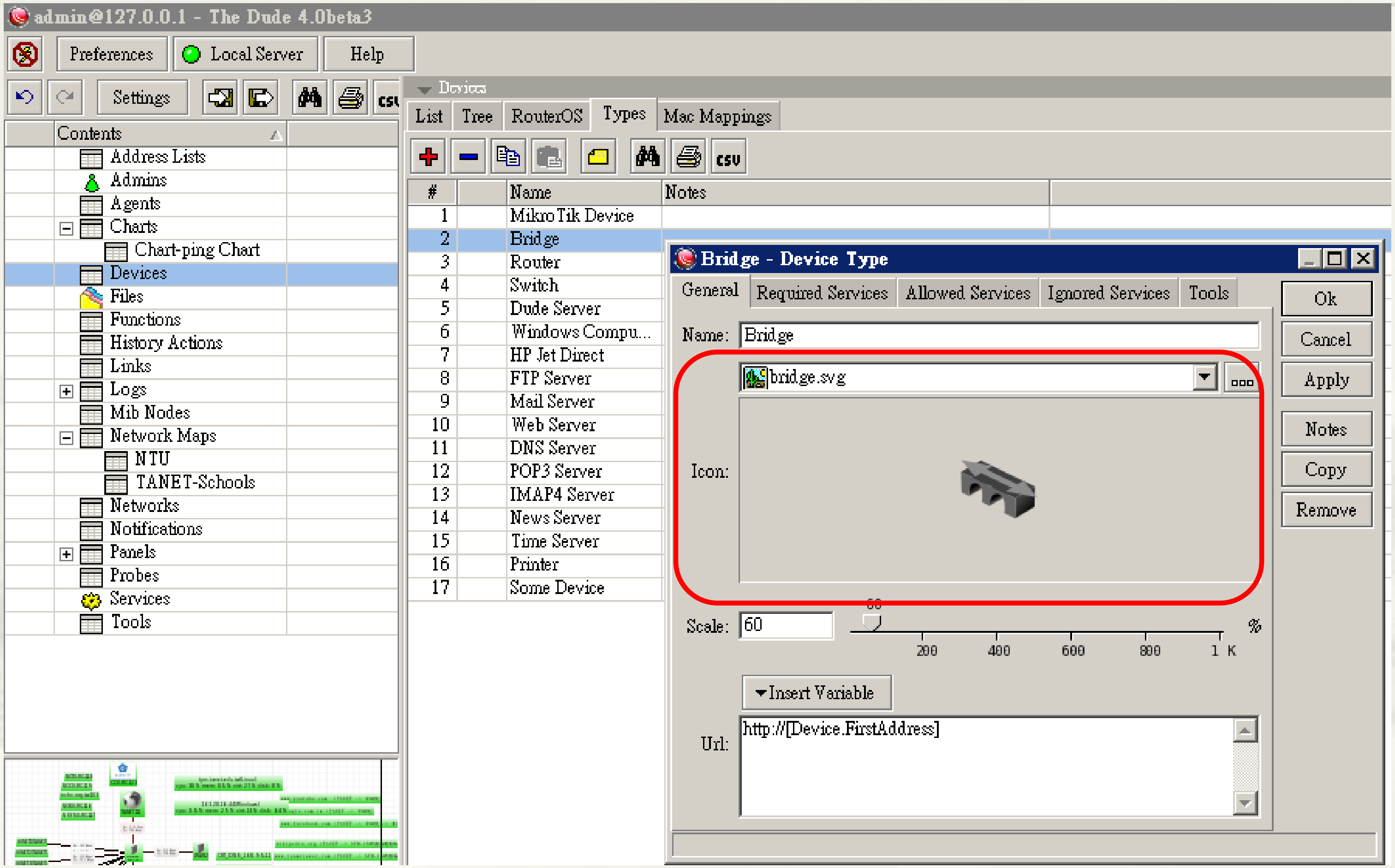
General | Image

Image: Cisco6509.jpg

Scale: 80

- 每個 Device 個別修改

Device 圖示設定 2/2



admin@127.0.0.1 - The Dude 4.0beta3

#	Name	Notes
1	MikroTik Device	
2	Bridge	
3	Router	
4	Switch	
5	Dude Server	
6	Windows Compu...	
7	HP Jet Direct	
8	FTP Server	
9	Mail Server	
10	Web Server	
11	DNS Server	
12	POP3 Server	
13	IMAP4 Server	
14	News Server	
15	Time Server	
16	Printer	
17	Some Device	

Bridge - Device Type

Name: Bridge

Icon: bridge.svg

Scale: 60

Url: http://[Device.FirstAddress]

- 依據 Device Type 批次修改

Network Map – Background 1/2

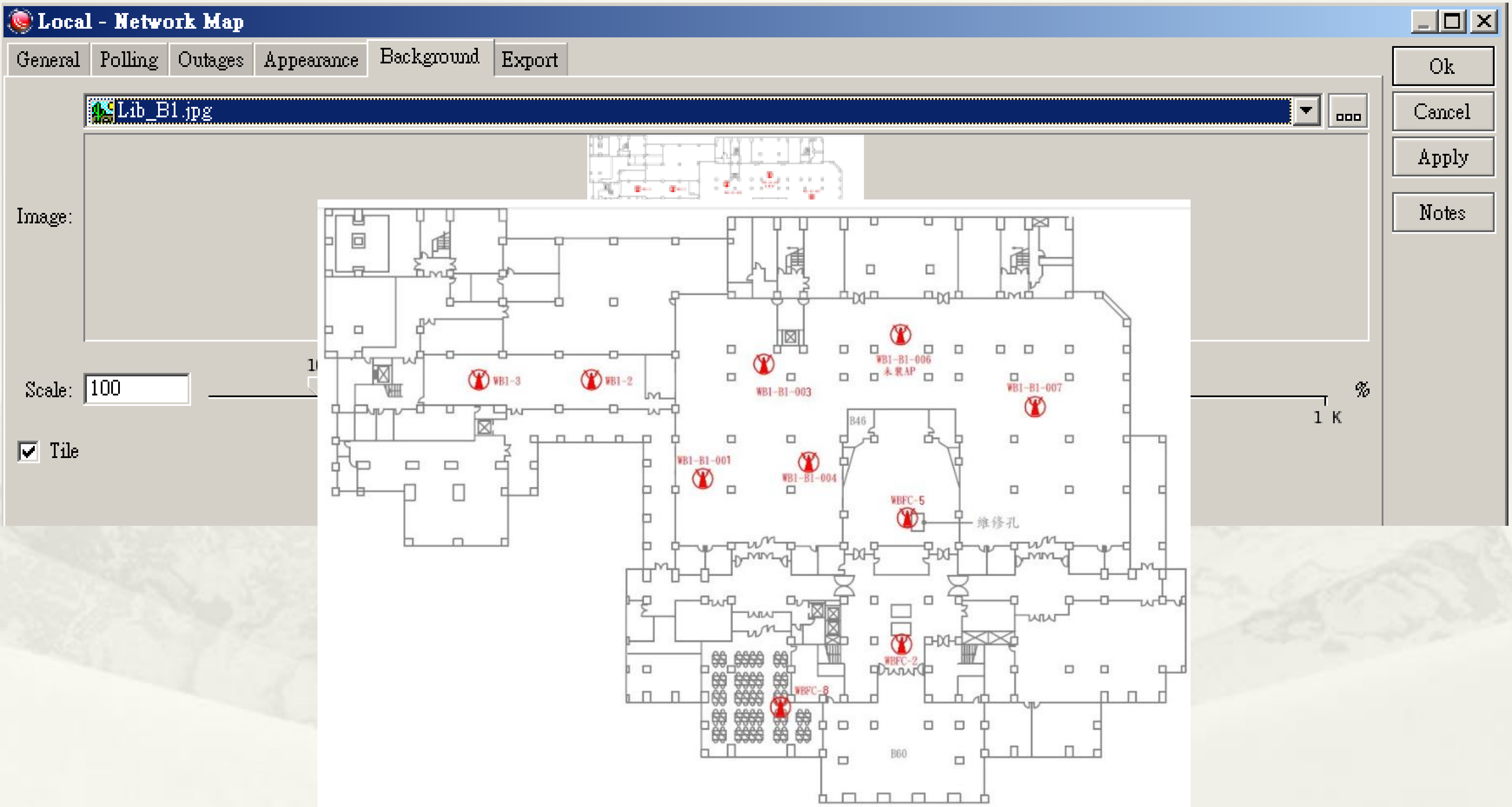


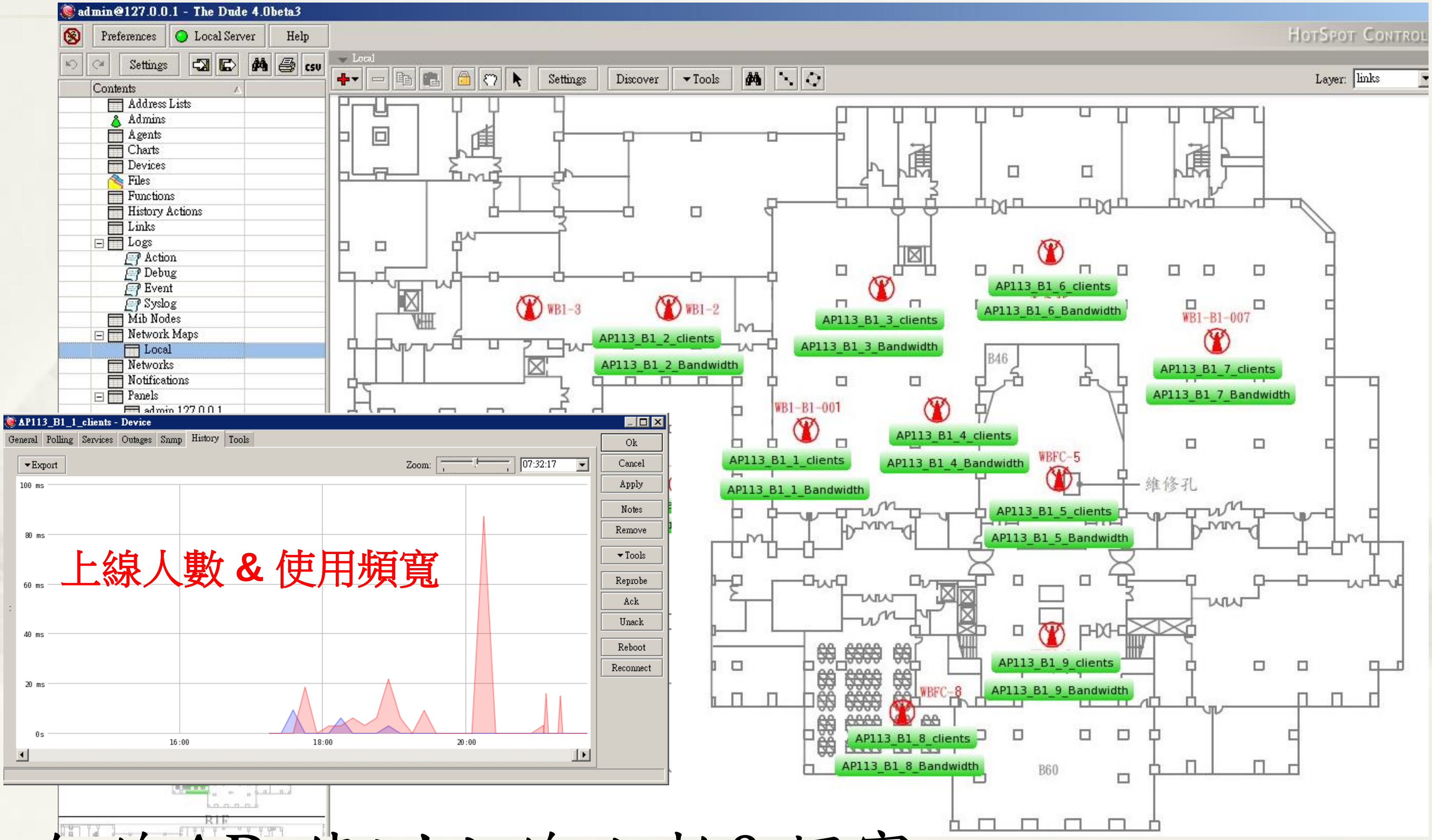
Image: Lib_B1.jpg

Scale: 100

☑ Tile

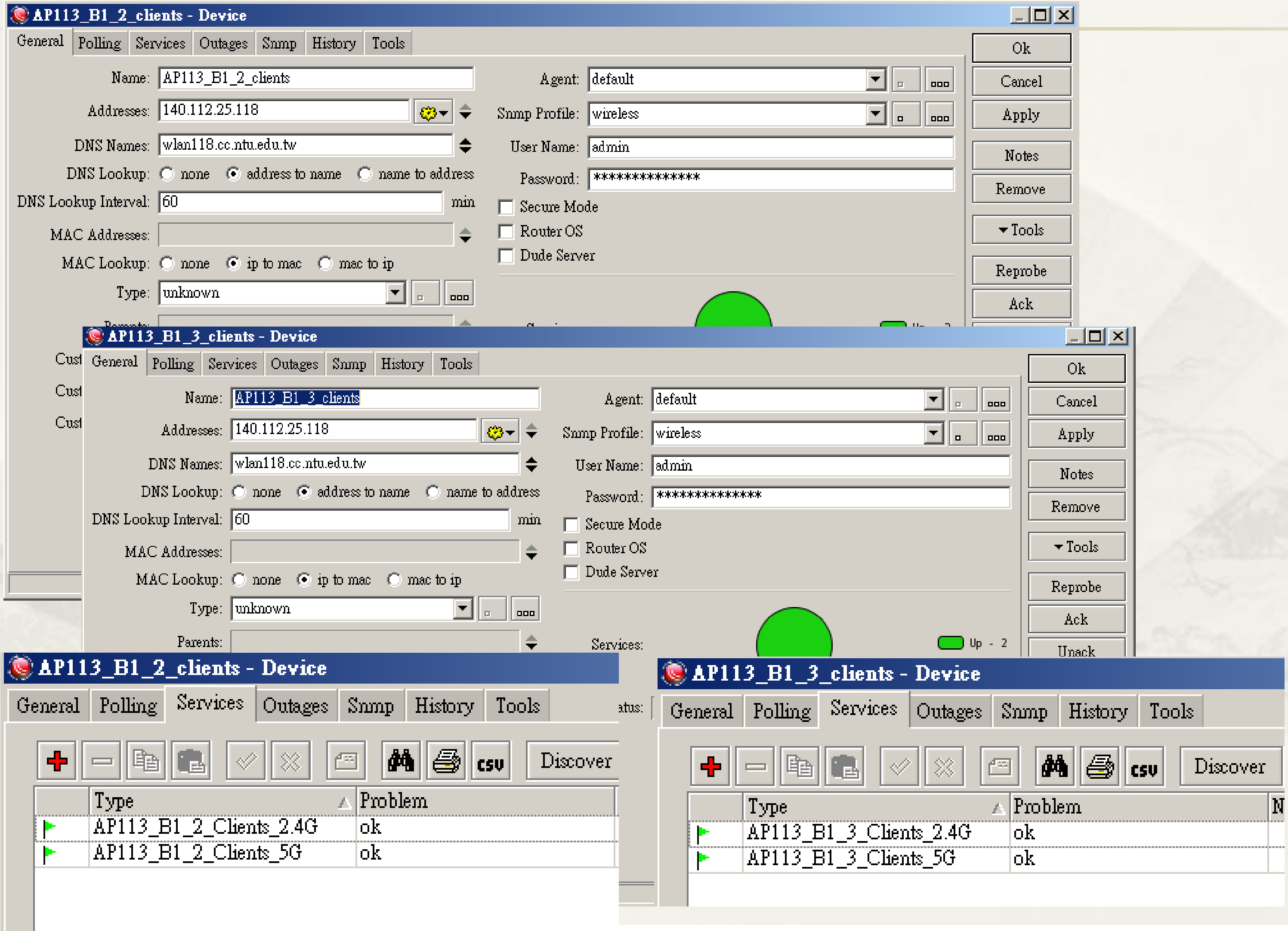
圖書館**B1** 無線**AP**分佈圖

Network Map – Background 2/2



上線人數 & 使用頻寬

- 無線AP-偵測上線人數&頻寬



AP113_B1_2_clients - Device

General | Polling | Services | Outages | Snmp | History | Tools

Name: AP113_B1_2_clients
Addresses: 140.112.25.118
DNS Names: wlan118.cc.ntu.edu.tw
DNS Lookup: ○ none ● address to name ○ name to address
DNS Lookup Interval: 60 min
MAC Addresses:
MAC Lookup: ○ none ● ip to mac ○ mac to ip
Type: unknown

Agent: default
Snmp Profile: wireless
User Name: admin
Password: **************
□ Secure Mode
□ Router OS
□ Dude Server

AP113_B1_3_clients - Device

General | Polling | Services | Outages | Snmp | History | Tools

Name: AP113_B1_3_clients
Addresses: 140.112.25.118
DNS Names: wlan118.cc.ntu.edu.tw
DNS Lookup: ○ none ● address to name ○ name to address
DNS Lookup Interval: 60 min
MAC Addresses:
MAC Lookup: ○ none ● ip to mac ○ mac to ip
Type: unknown
Parents:

Agent: default
Snmp Profile: wireless
User Name: admin
Password: **************
□ Secure Mode
□ Router OS
□ Dude Server
Services: Up - 2

AP113_B1_2_clients - Device

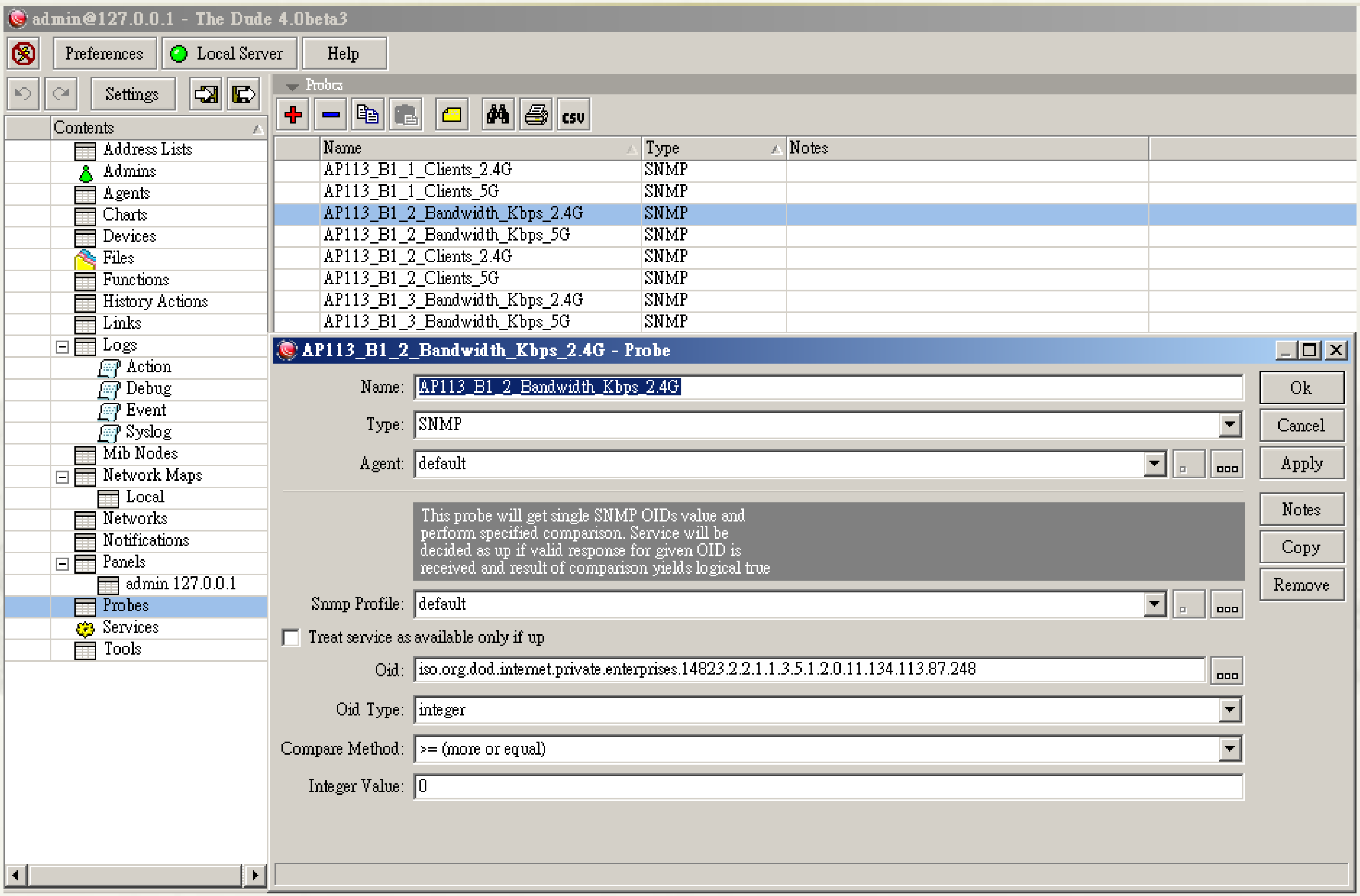
General | Polling | Services | Outages | Snmp | History | Tools

	Type	Problem
▶	AP113_B1_2_Clients_2.4G	ok
▶	AP113_B1_2_Clients_5G	ok

AP113_B1_3_clients - Device

General | Polling | Services | Outages | Snmp | History | Tools

	Type	Problem	N
▶	AP113_B1_3_Clients_2.4G	ok	
▶	AP113_B1_3_Clients_5G	ok	



Name	Type	Notes
AP113_B1_1_Clients_2.4G	SNMP	
AP113_B1_1_Clients_5G	SNMP	
AP113_B1_2_Bandwidth_Kbps_2.4G	SNMP	
AP113_B1_2_Bandwidth_Kbps_5G	SNMP	
AP113_B1_2_Clients_2.4G	SNMP	
AP113_B1_2_Clients_5G	SNMP	
AP113_B1_3_Bandwidth_Kbps_2.4G	SNMP	
AP113_B1_3_Bandwidth_Kbps_5G	SNMP	

AP113_B1_2_Bandwidth_Kbps_2.4G - Probe

Name: AP113_B1_2_Bandwidth_Kbps_2.4G

Type: SNMP

Agent: default

This probe will get single SNMP OIDs value and perform specified comparison. Service will be decided as up if valid response for given OID is received and result of comparison yields logical true

Snmp Profile: default

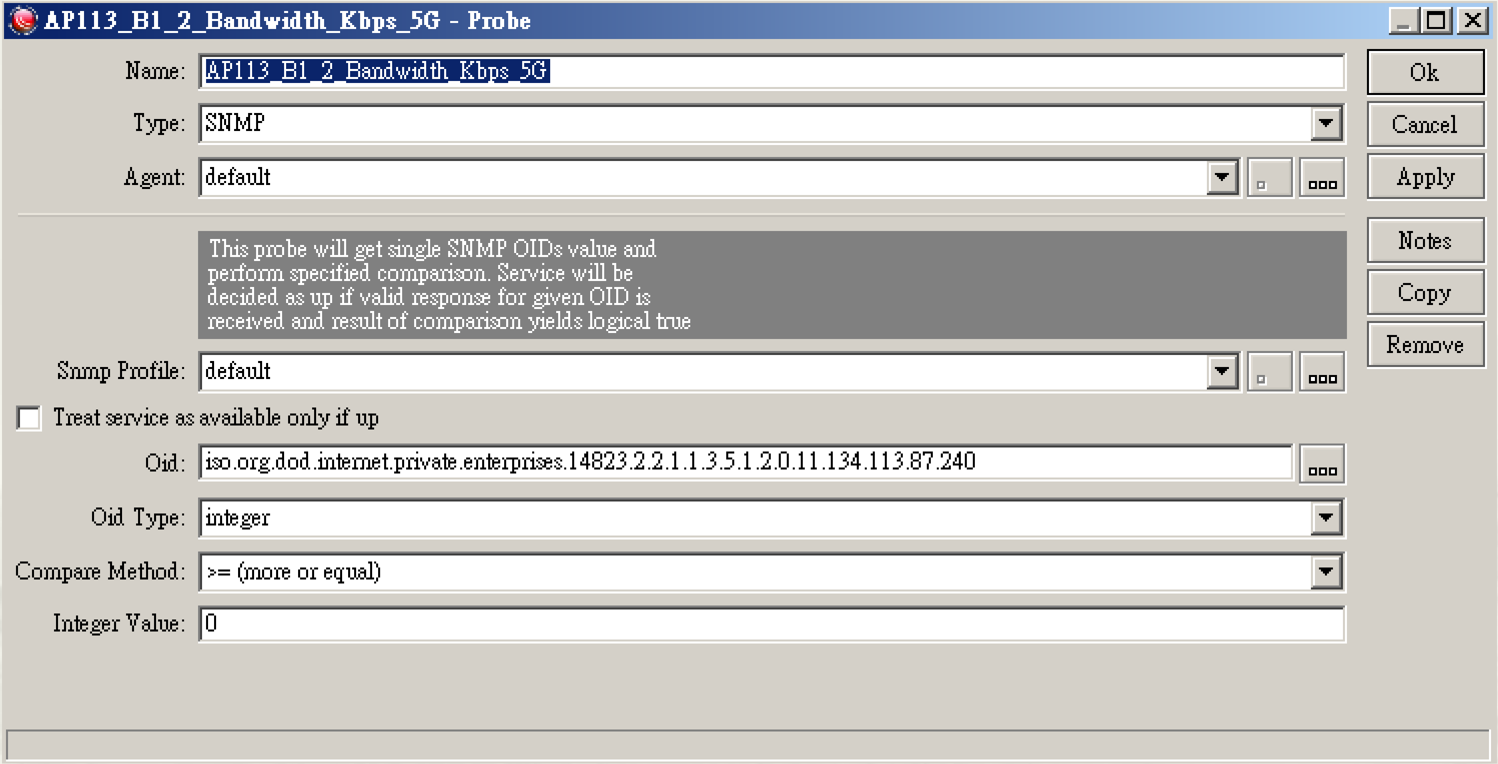
□ Treat service as available only if up

Oid: iso.org.dod.internet.private.enterprises.14823.2.2.1.1.3.5.1.2.0.11.134.113.87.248

Oid Type: integer

Compare Method: >= (more or equal)

Integer Value: 0



AP113_B1_2_Bandwidth_Kbps_5G - Probe

Name: AP113_B1_2_Bandwidth_Kbps_5G

Type: SNMP

Agent: default

This probe will get single SNMP OIDs value and perform specified comparison. Service will be decided as up if valid response for given OID is received and result of comparison yields logical true

Snmp Profile: default

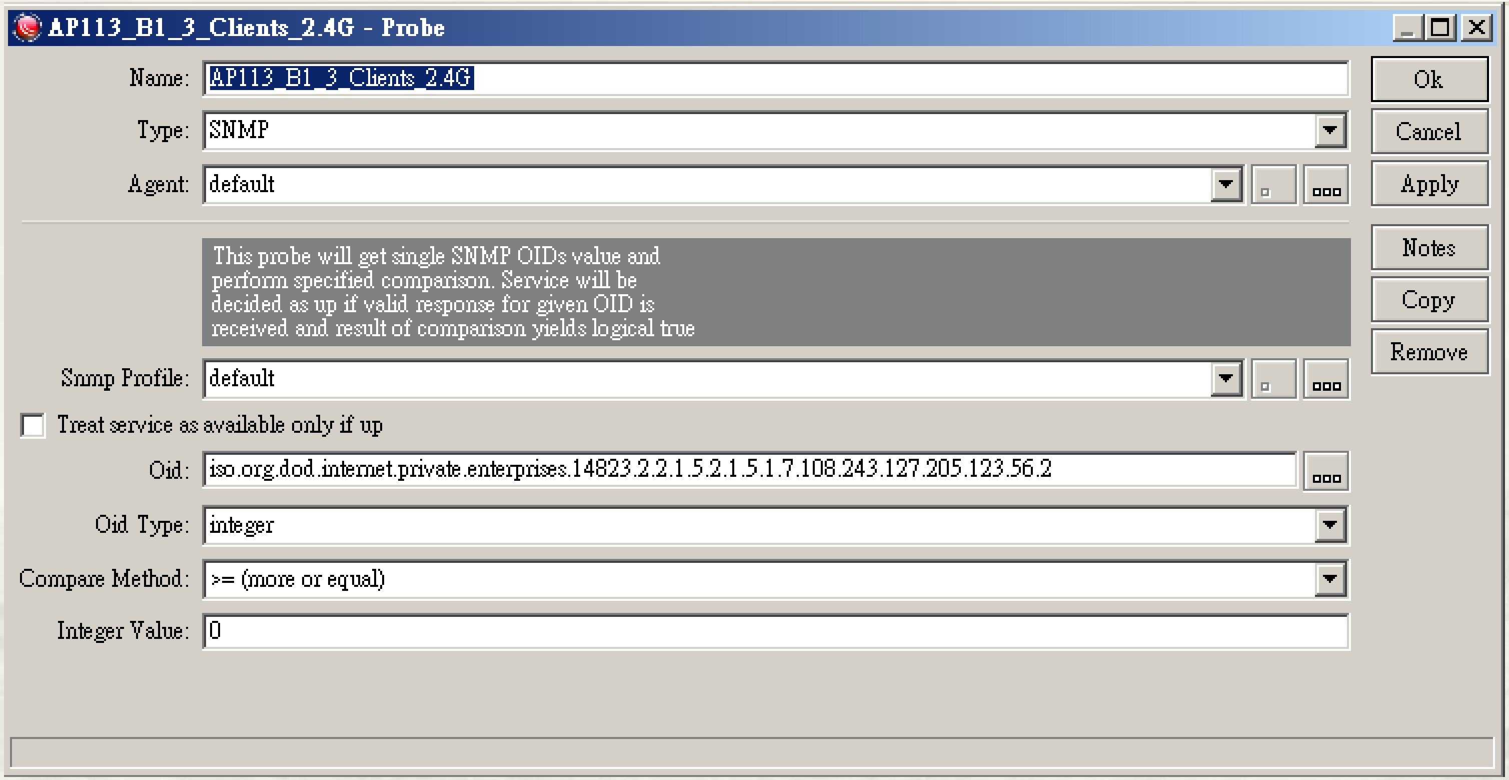
□ Treat service as available only if up

Oid: iso.org.dod.internet.private.enterprises.14823.2.2.1.1.3.5.1.2.0.11.134.113.87.240

Oid Type: integer

Compare Method: >= (more or equal)

Integer Value: 0



Name: AP113_B1_3_Clients_2.4G

Type: SNMP

Agent: default

This probe will get single SNMP OIDs value and perform specified comparison. Service will be decided as up if valid response for given OID is received and result of comparison yields logical true

Snmp Profile: default

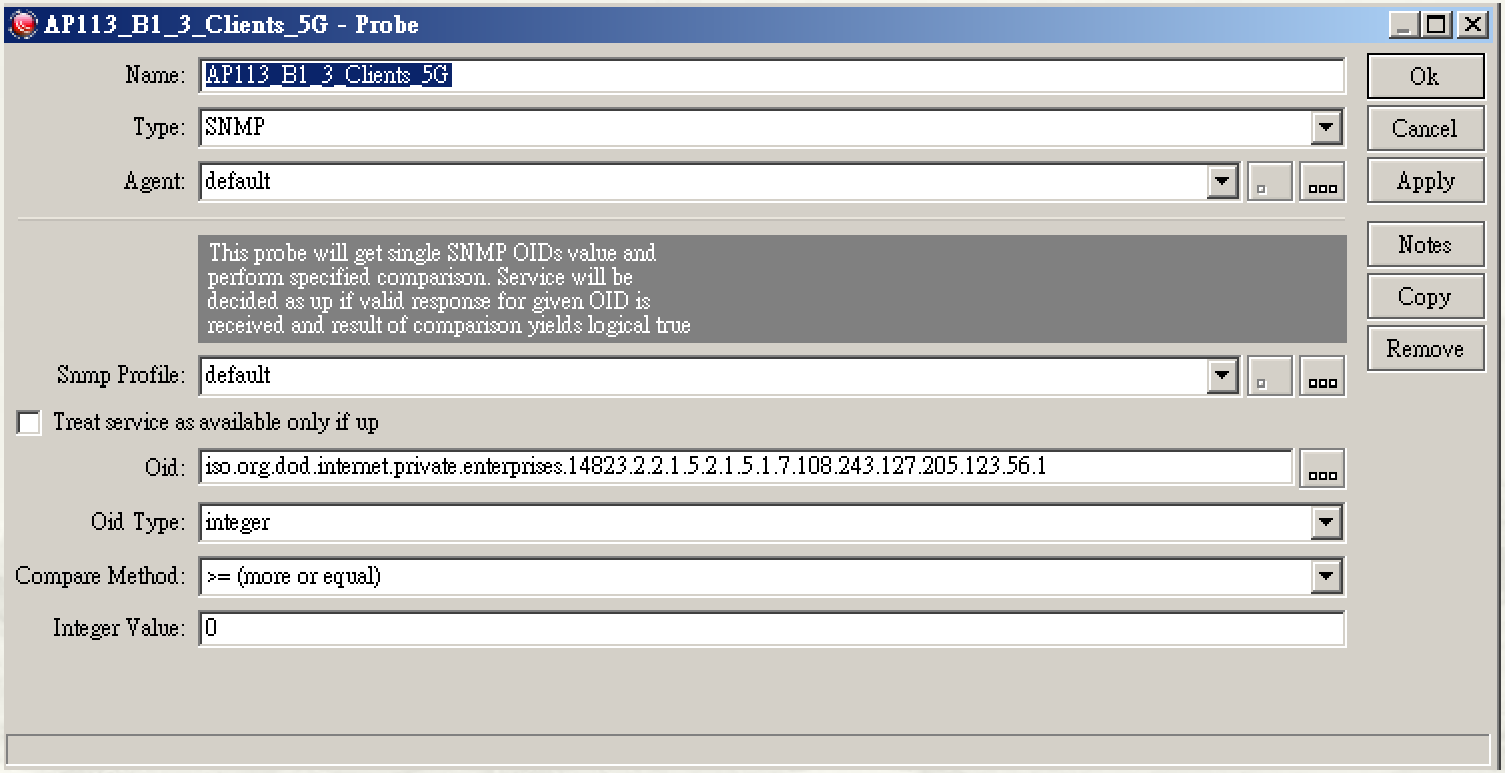
□ Treat service as available only if up

Oid: iso.org.dod.internet.private.enterprises.14823.2.2.1.5.2.1.5.1.7.108.243.127.205.123.56.2

Oid Type: integer

Compare Method: >= (more or equal)

Integer Value: 0



Name: AP113_B1_3_Clients_5G

Type: SNMP

Agent: default

This probe will get single SNMP OIDs value and perform specified comparison. Service will be decided as up if valid response for given OID is received and result of comparison yields logical true

Snmp Profile: default

□ Treat service as available only if up

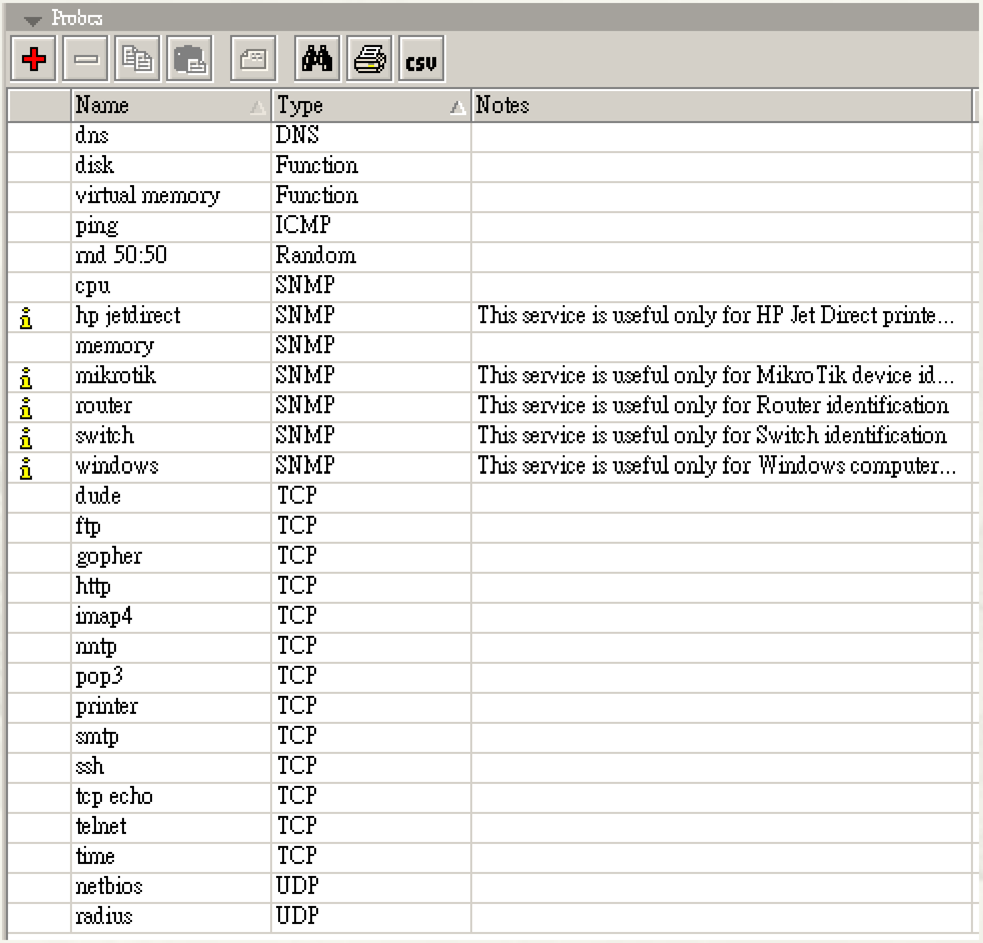
Oid: iso.org.dod.internet.private.enterprises.14823.2.2.1.5.2.1.5.1.7.108.243.127.205.123.56.1

Oid Type: integer

Compare Method: >= (more or equal)

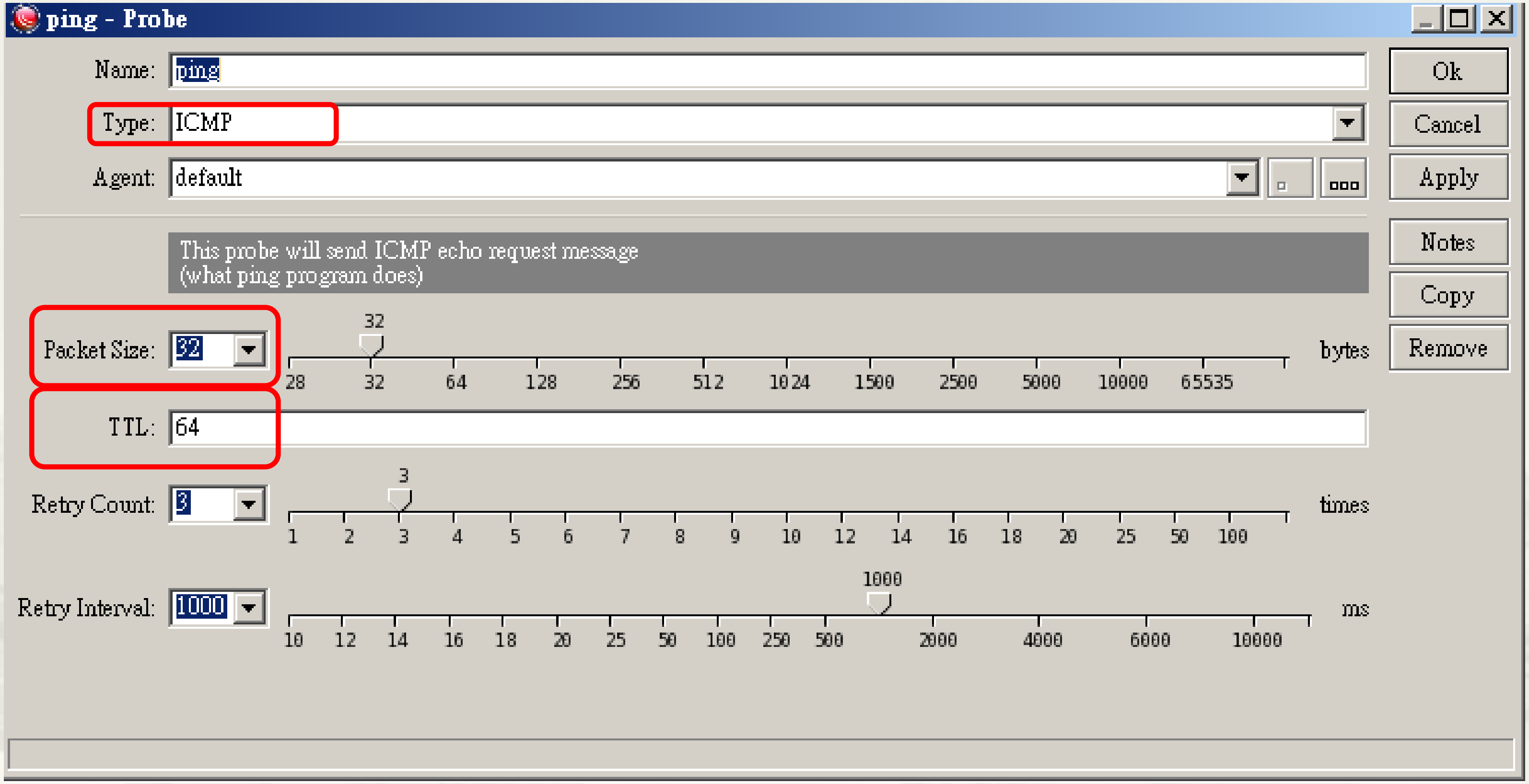
Integer Value: 0

Probe –各種服務偵測



	Name	Type	Notes
	dns	DNS	
	disk	Function	
	virtual memory	Function	
	ping	ICMP	
	rnd 50:50	Random	
	cpu	SNMP	
ℹ	hp jetdirect	SNMP	This service is useful only for HP Jet Direct printe...
	memory	SNMP	
ℹ	mikrotik	SNMP	This service is useful only for MikroTik device id...
ℹ	router	SNMP	This service is useful only for Router identification
ℹ	switch	SNMP	This service is useful only for Switch identification
ℹ	windows	SNMP	This service is useful only for Windows computer...
	dude	TCP	
	ftp	TCP	
	gopher	TCP	
	http	TCP	
	imap4	TCP	
	nntp	TCP	
	pop3	TCP	
	printer	TCP	
	smtp	TCP	
	ssh	TCP	
	tcp echo	TCP	
	telnet	TCP	
	time	TCP	
	netbios	UDP	
	radius	UDP	

Probe – ICMP (Ping)



ping - Probe

Name: ping

Type: ICMP

Agent: default

This probe will send ICMP echo request message
(what ping program does)

Packet Size: 32 bytes

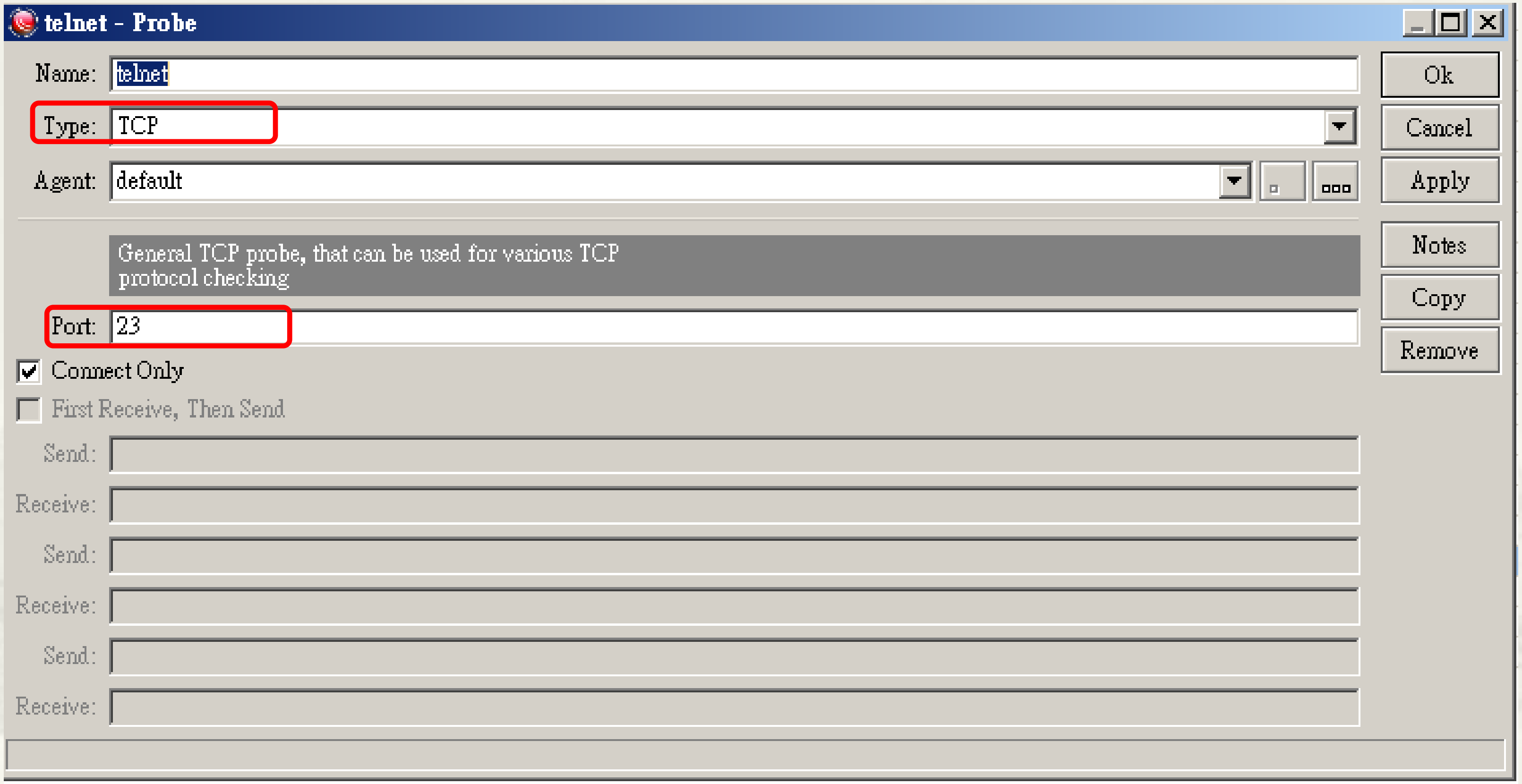
TTL: 64

Retry Count: 3 times

Retry Interval: 1000 ms

- 可自訂 Packet Size、TTL

Probe – TCP (telnet)



Name: telnet

Type: TCP

Agent: default

General TCP probe, that can be used for various TCP protocol checking

Port: 23

☑ Connect Only

□ First Receive, Then Send

Send:

Receive:

Send:

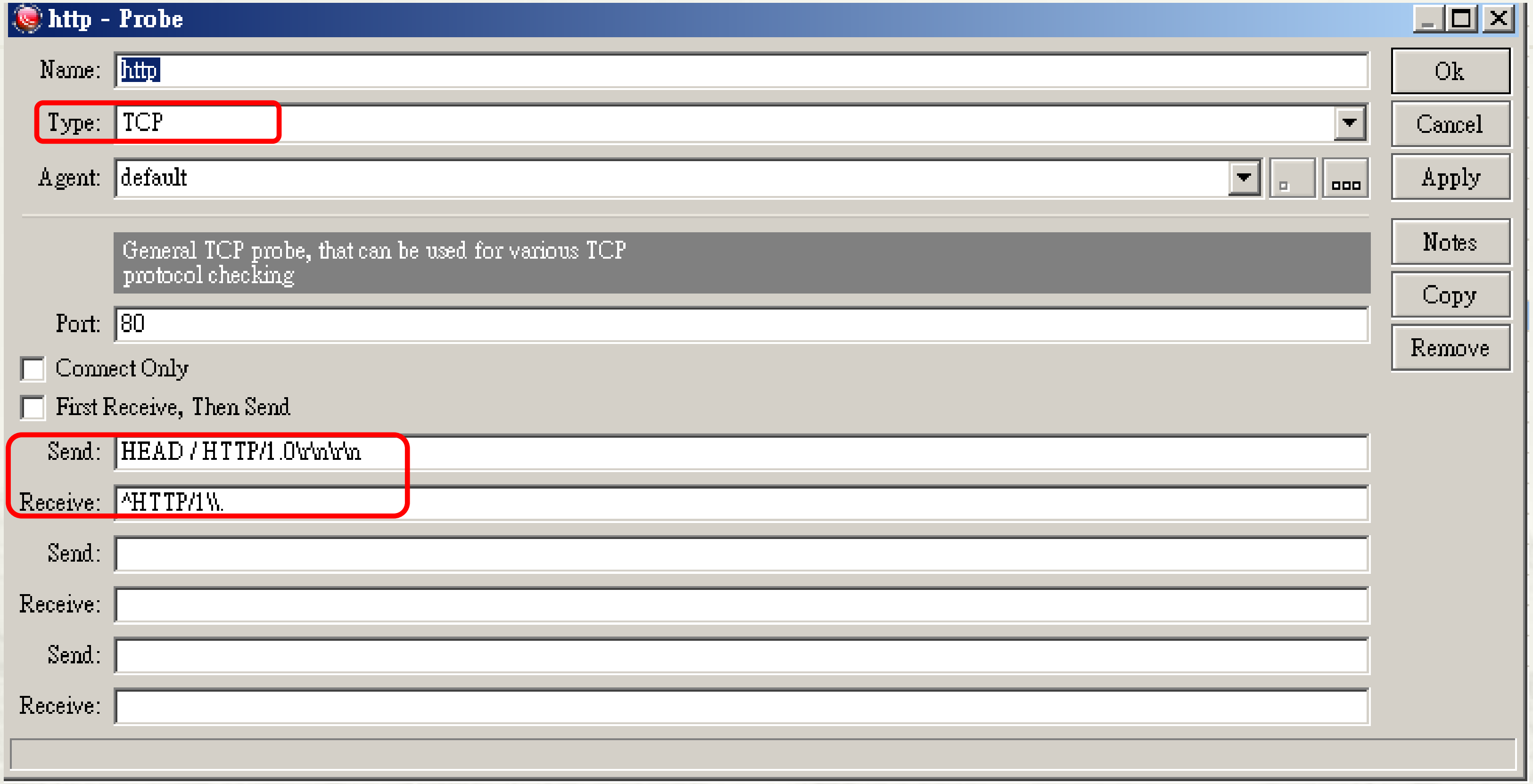
Receive:

Send:

Receive:

- 偵測TCP 特定 port 連線狀況

Probe – TCP (http)



Name: http

Type: TCP

Agent: default

General TCP probe, that can be used for various TCP protocol checking

Port: 80

□ Connect Only

□ First Receive, Then Send

Send: HEAD / HTTP/1.0\r\n\r\n

Receive: ^HTTP/1\\.

Send:

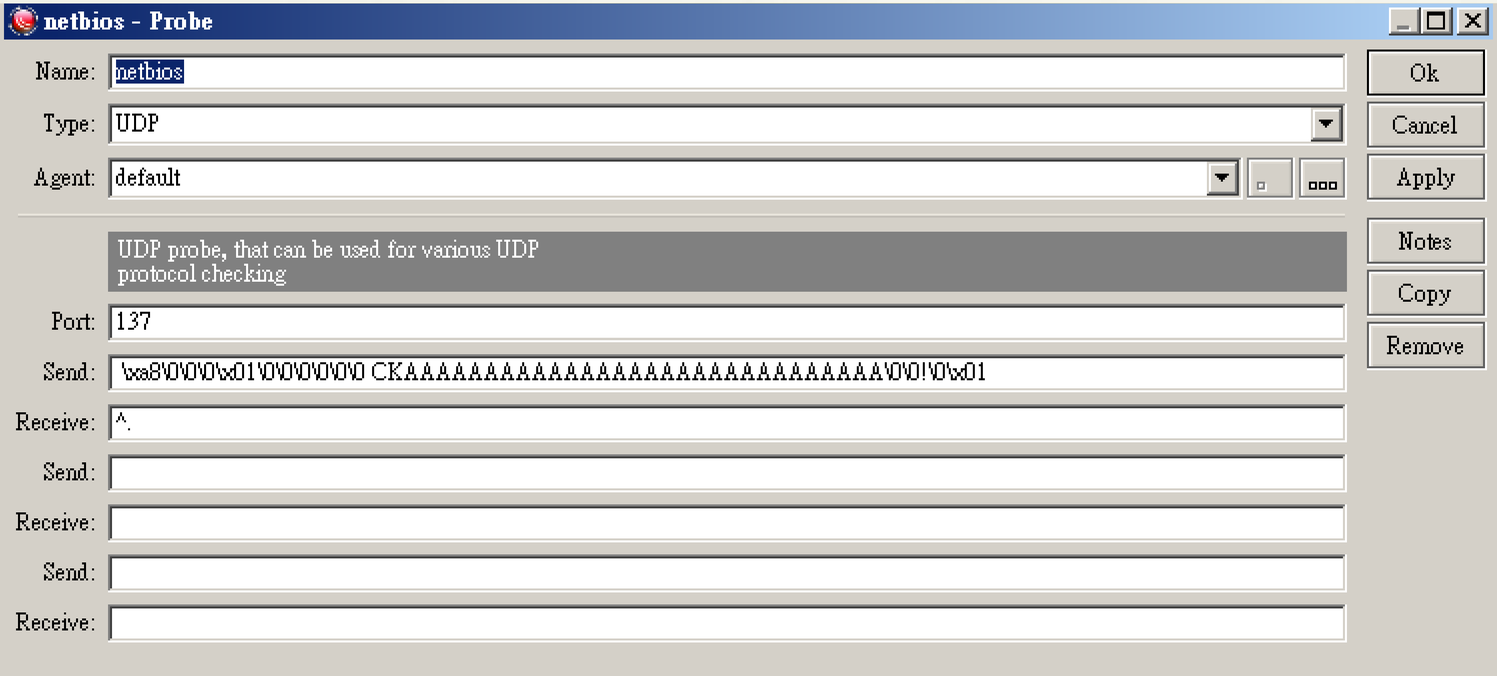
Receive:

Send:

Receive:

- 針對不同服務，可自行定義Send 與預計 Receive 之內容

Probe – UDP (netbios)



Name: netbios

Type: UDP

Agent: default

UDP probe, that can be used for various UDP protocol checking

Port: 137

Send: \xa8\0\0\0\x01\0\0\0\0\0\0 CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\0\0!\0\x01

Receive: ^.

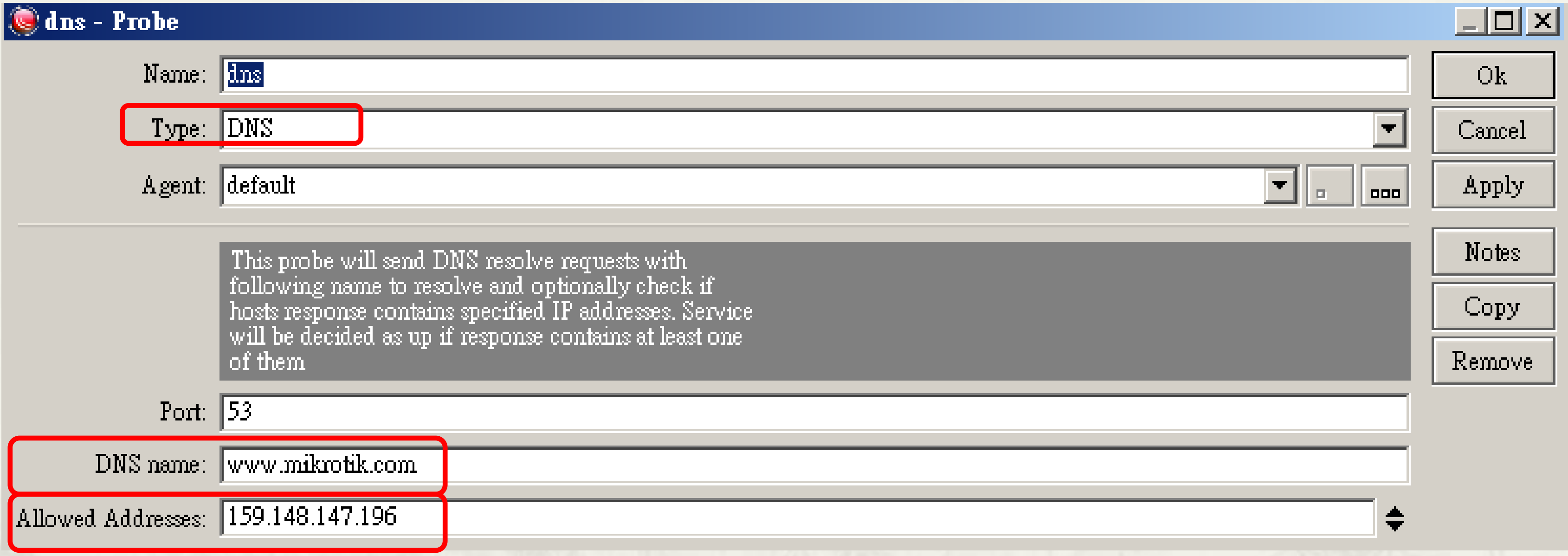
Send:

Receive:

Send:

Receive:

Probe – DNS



dns - Probe

Name: dns

Type: DNS

Agent: default

This probe will send DNS resolve requests with following name to resolve and optionally check if hosts response contains specified IP addresses. Service will be decided as up if response contains at least one of them

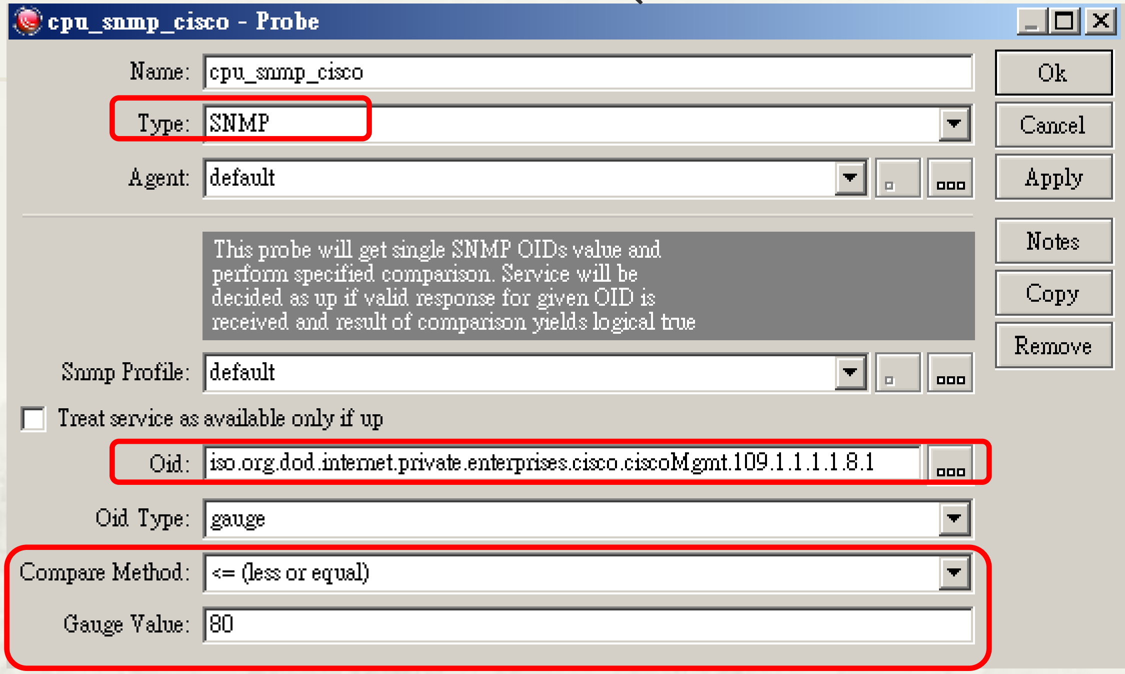
Port: 53

DNS name: www.mikrotik.com

Allowed Addresses: 159.148.147.196

- 自行設定一組 DNS 與預期之正解IP

Probe – SNMP (Cisco CPU load)



cpu_snmp_cisco - Probe

Name: cpu_snmp_cisco

Type: SNMP

Agent: default

This probe will get single SNMP OIDs value and perform specified comparison. Service will be decided as up if valid response for given OID is received and result of comparison yields logical true

Snmp Profile: default

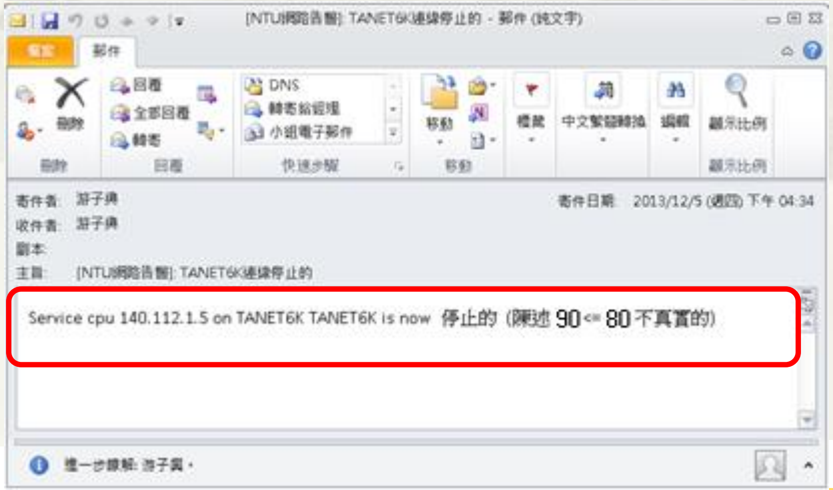
□ Treat service as available only if up

Oid: iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.109.1.1.1.1.8.1

Oid Type: gauge

Compare Method: <= (less or equal)

Gauge Value: 80



[NTU網路告警]: TANET6K連線停止的 - 郵件 (純文字)

寄件者: 游子興

寄件日期: 2013/12/5 (週四) 下午 04:34

收件者: 游子興

副本:

主旨: [NTU網路告警]: TANET6K連線停止的

Service cpu 140.112.1.5 on TANET6K TANET6K is now 停止的 (陳述 90 <= 80 不真實的)

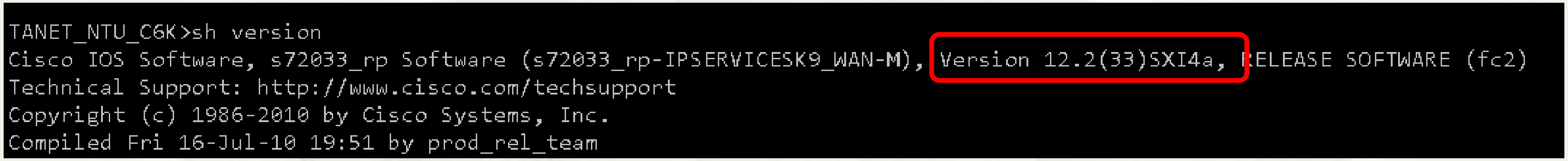
- cpmCPUTotal5minRev.1 (1.3.6.1.4.1.9.9.109.1.1.1.1.8.1)
- 設定SNMP OID與正常回傳範圍
- 若超出範圍表示異常可即時通知

SNMP of Cisco CPU load

- How to Collect CPU Utilization on Cisco IOS Devices Using SNMP
  - http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094a94.shtml
  - cpmCPUTotal5minRev (.1.3.6.1.4.1.9.9.109.1.1.1.1.8):
    - The overall CPU busy percentage in the last five-minute period
- Cisco SNMP Object Navigator
  - http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en
  - Download CISCO-PROCESS-MIB.my
  - Rename to .txt or .mib

Cisco MIB download

- Show version

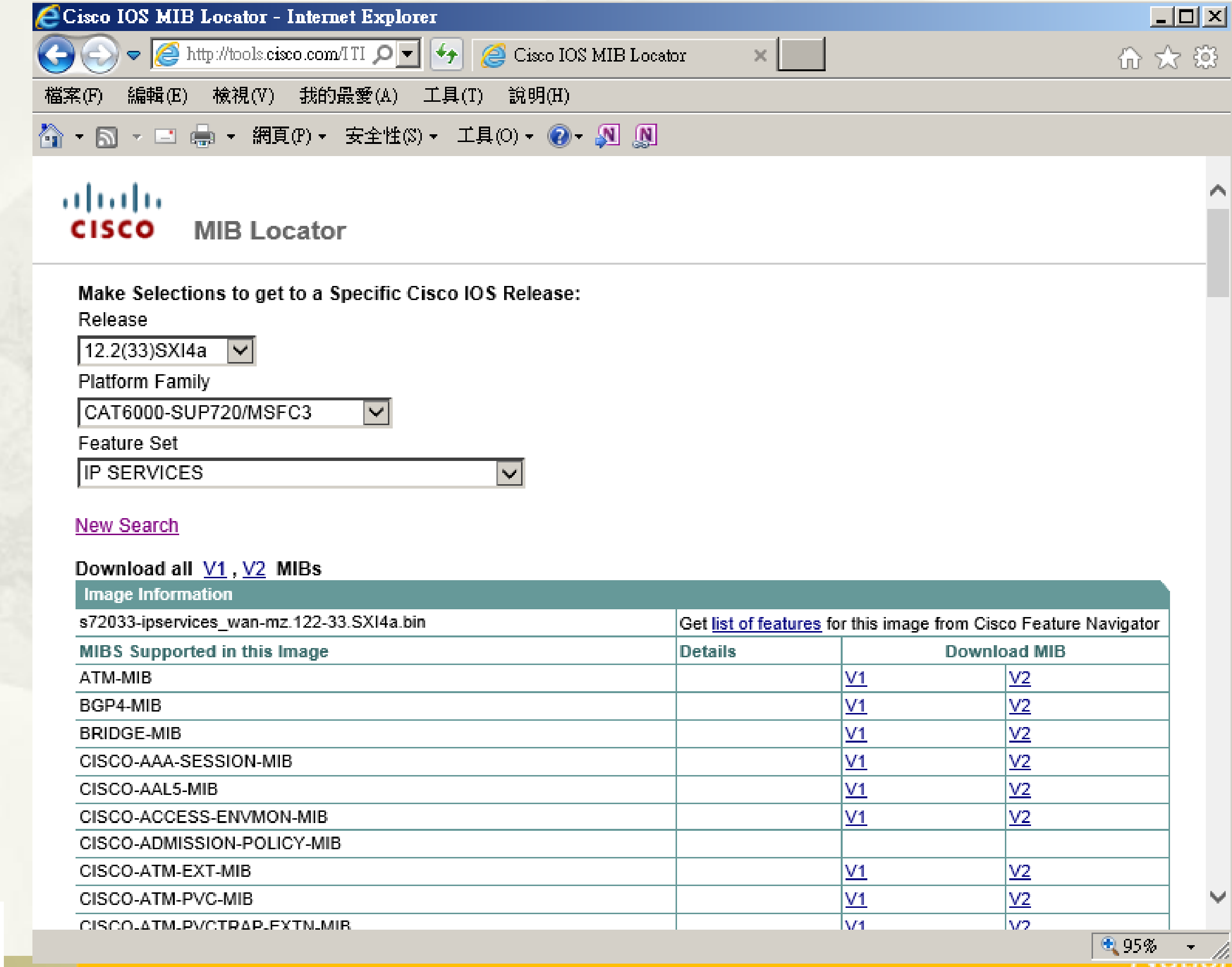


```
TANET_NTU_C6K>sh version
Cisco IOS Software, s72033_rp Software (s72033_rp-IPSERVICESK9_WAN-M), Version 12.2(33)SXI4a, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Fri 16-Jul-10 19:51 by prod_rel_team
```

- Cisco IOS MIB Locator
  - http://tools.cisco.com/ITDIT/MIBS/MainServlet
- MIBs Supported by Product
  - http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Cisco MIB download

- Download CISCO-PROCESS-MIB


Cisco IOS MIB Locator - Internet Explorer
http://tools.cisco.com/ITI
Cisco IOS MIB Locator
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
網頁(P) 安全性(S) 工具(O)
CISCO
95%

MIB Locator

Make Selections to get to a Specific Cisco IOS Release:

Release: 12.2(33)SXI4a

Platform Family: CAT6000-SUP720/MSFC3

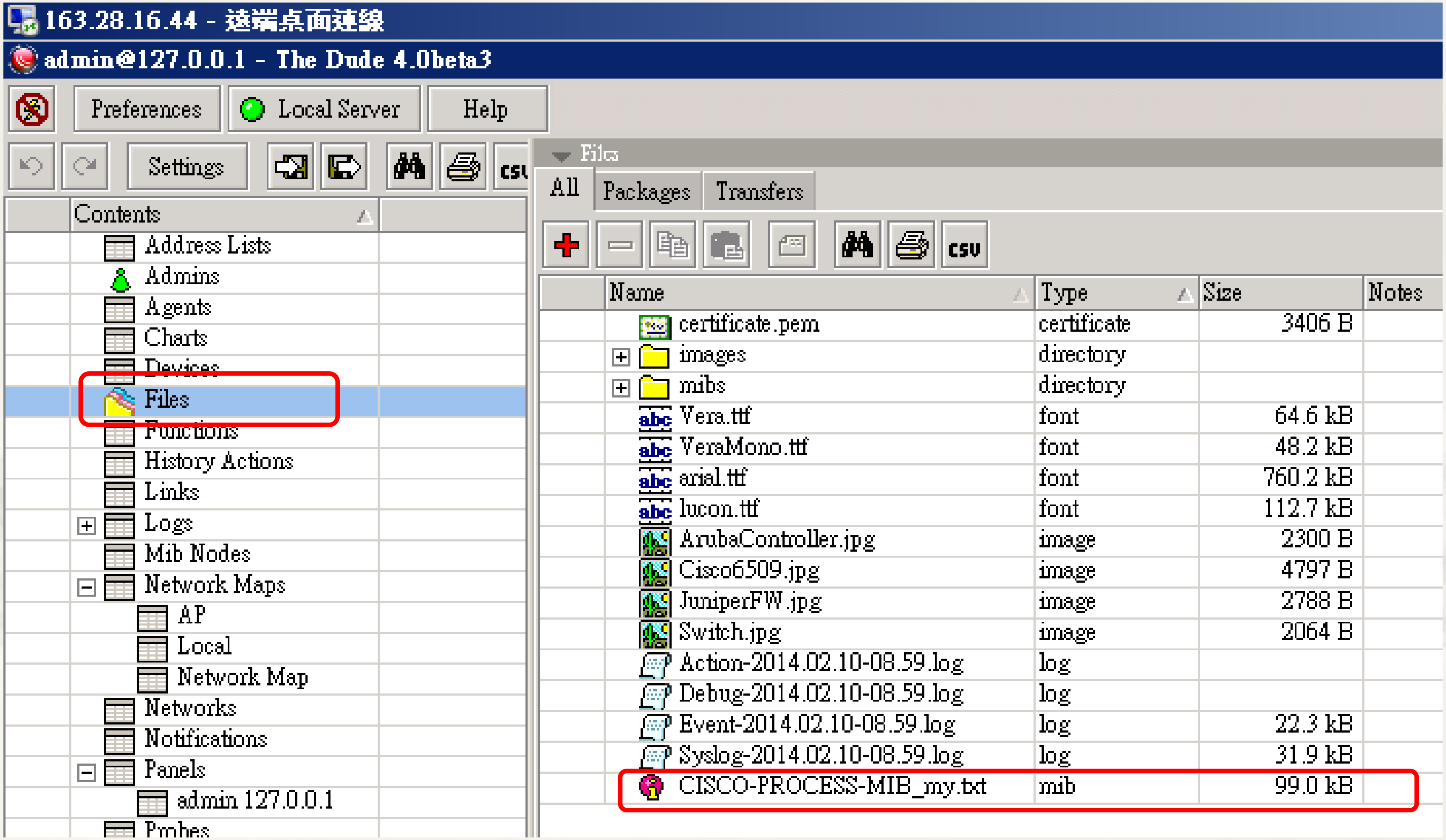
Feature Set: IP SERVICES

New Search

Download all V1 , V2 MIBs

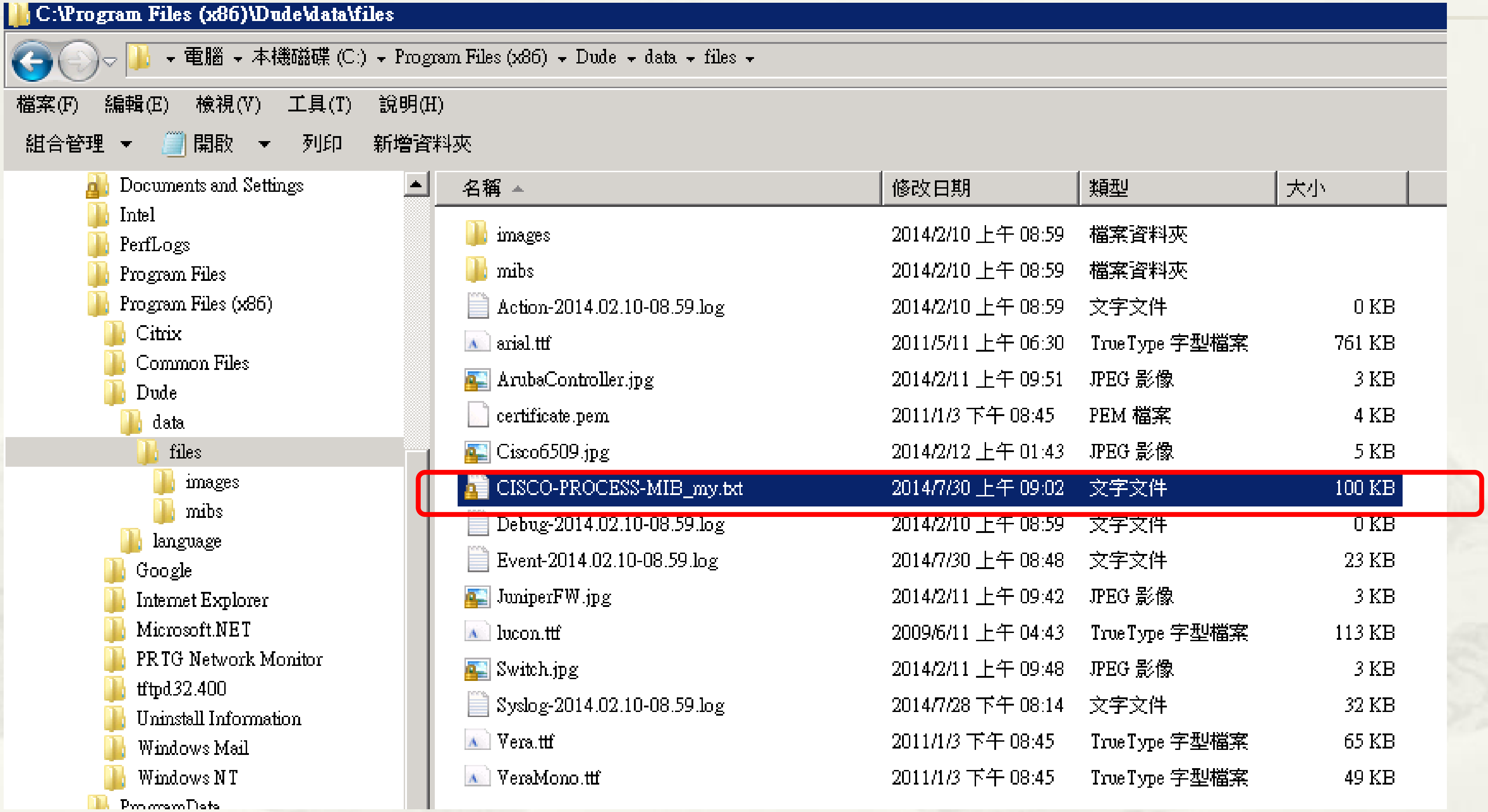
Image Information			
s72033-ipservices_wan-mz.122-33.SXI4a.bin	Get list of features for this image from Cisco Feature Navigator		
MIBS Supported in this Image	Details	Download MIB	
ATM-MIB		V1	V2
BGP4-MIB		V1	V2
BRIDGE-MIB		V1	V2
CISCO-AAA-SESSION-MIB		V1	V2
CISCO-AAL5-MIB		V1	V2
CISCO-ACCESS-ENVMON-MIB		V1	V2
CISCO-ADMISSION-POLICY-MIB			
CISCO-ATM-EXT-MIB		V1	V2
CISCO-ATM-PVC-MIB		V1	V2
CISCO-ATM-PVCTRAP-EXTN-MIB		V1	V2

Files – Upload MIB file (Method1)



Name	Type	Size	Notes
certificate.pem	certificate	3406 B	
images	directory		
mibs	directory		
Vera.ttf	font	64.6 kB	
VeraMono.ttf	font	48.2 kB	
arial.ttf	font	760.2 kB	
lucon.ttf	font	112.7 kB	
ArubaController.jpg	image	2300 B	
Cisco6509.jpg	image	4797 B	
JuniperFW.jpg	image	2788 B	
Switch.jpg	image	2064 B	
Action-2014.02.10-08.59.log	log		
Debug-2014.02.10-08.59.log	log		
Event-2014.02.10-08.59.log	log	22.3 kB	
Syslog-2014.02.10-08.59.log	log	31.9 kB	
CISCO-PROCESS-MIB_my.txt	mib	99.0 kB	

Files – Upload MIB file (Method2)



C:\Program Files (x86)\Dude\data\files

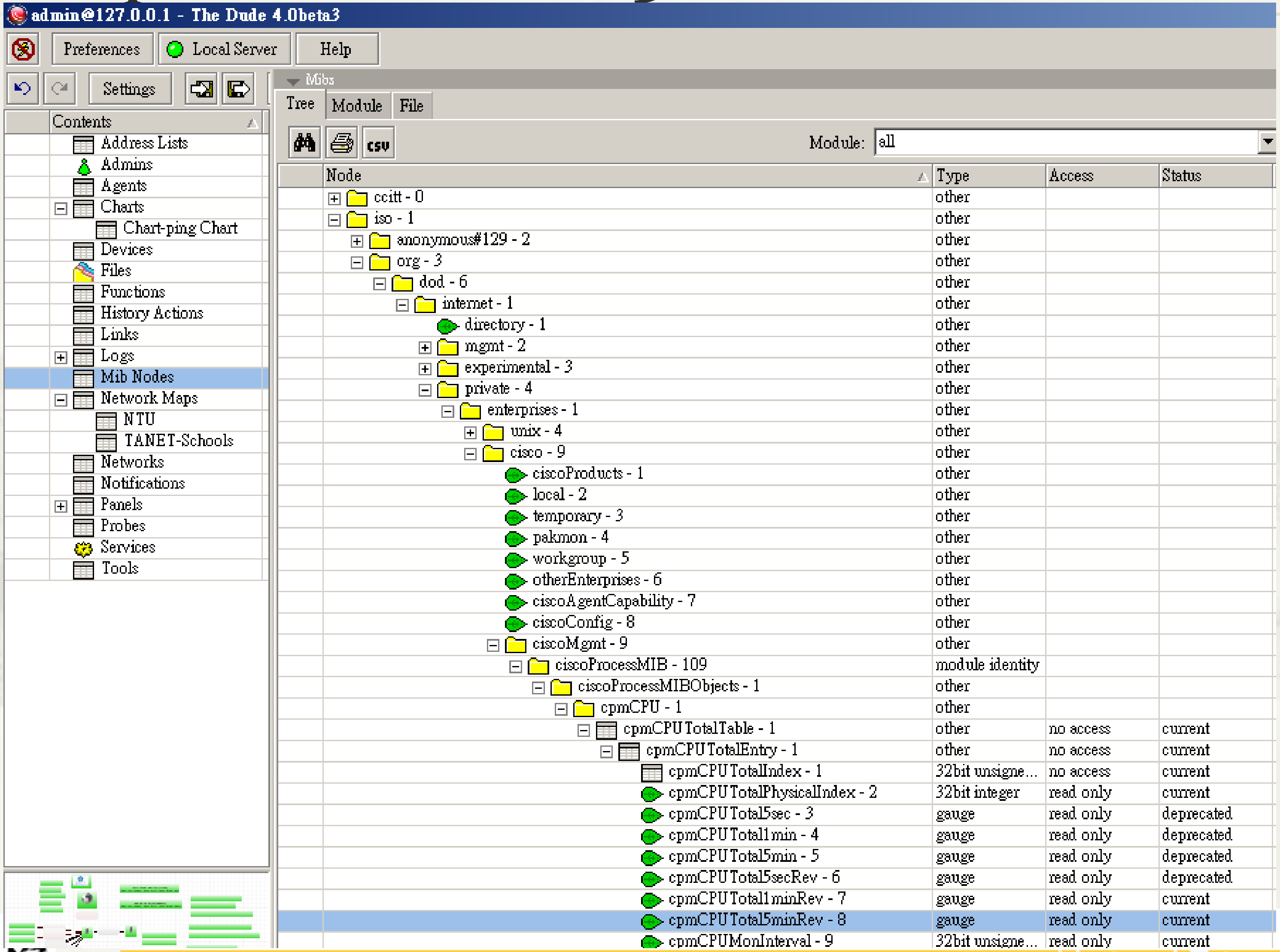
電腦 ▸ 本機磁碟 (C:) ▸ Program Files (x86) ▸ Dude ▸ data ▸ files
檔案(F) 編輯(E) 檢視(V) 工具(T) 說明(H)
組合管理 ▾ 開啟 ▾ 列印 新增資料夾

- Documents and Settings
- Intel
- PerfLogs
- Program Files
- Program Files (x86)
  - Citrix
  - Common Files
  - Dude
    - data
      - files
        - images
        - mibs
      - language
  - Google
  - Internet Explorer
  - Microsoft.NET
  - PRTG Network Monitor
  - tftpd32.400
  - Uninstall Information
  - Windows Mail
  - Windows NT
- ProgramData

名稱	修改日期	類型	大小
images	2014/2/10 上午 08:59	檔案資料夾	
mibs	2014/2/10 上午 08:59	檔案資料夾	
Action-2014.02.10-08.59.log	2014/2/10 上午 08:59	文字文件	0 KB
arial.ttf	2011/5/11 上午 06:30	TrueType 字型檔案	761 KB
ArubaController.jpg	2014/2/11 上午 09:51	JPEG 影像	3 KB
certificate.pem	2011/1/3 下午 08:45	PEM 檔案	4 KB
Cisco6509.jpg	2014/2/12 上午 01:43	JPEG 影像	5 KB
CISCO-PROCESS-MIB_my.txt	2014/7/30 上午 09:02	文字文件	100 KB
Debug-2014.02.10-08.59.log	2014/2/10 上午 08:59	文字文件	0 KB
Event-2014.02.10-08.59.log	2014/7/30 上午 08:48	文字文件	23 KB
JuniperFW.jpg	2014/2/11 上午 09:42	JPEG 影像	3 KB
lucon.ttf	2009/6/11 上午 04:43	TrueType 字型檔案	113 KB
Switch.jpg	2014/2/11 上午 09:48	JPEG 影像	3 KB
Syslog-2014.02.10-08.59.log	2014/7/28 下午 08:14	文字文件	32 KB
Vera.ttf	2011/1/3 下午 08:45	TrueType 字型檔案	65 KB
VeraMono.ttf	2011/1/3 下午 08:45	TrueType 字型檔案	49 KB

- 自行上傳檔案 C:\Program Files (x86)\Dude\data\files

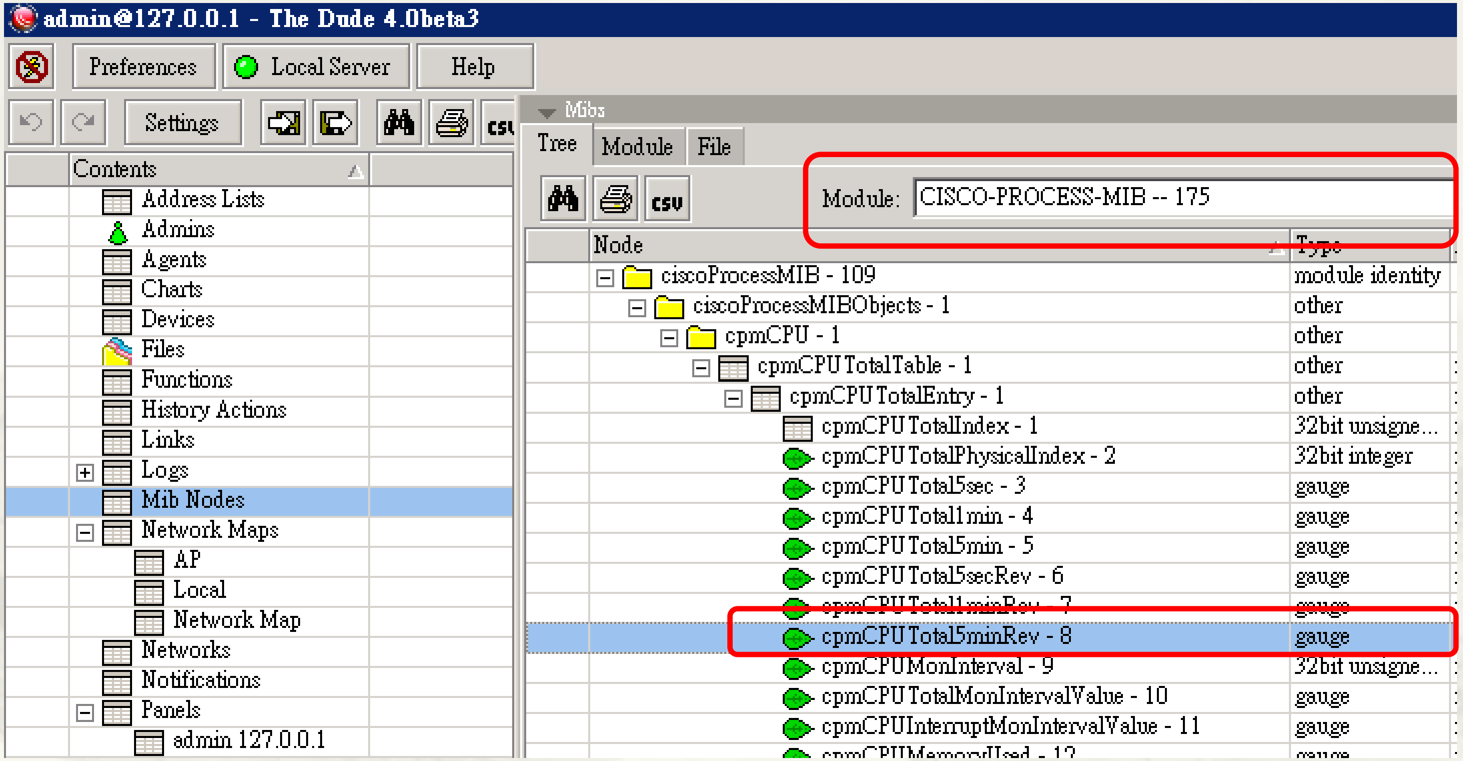
MIB Nodes of cpmCPUTotal5minRev (1/2)



Module: all

Node	Type	Access	Status
ccitt - 0	other		
iso - 1	other		
anonymous#129 - 2	other		
org - 3	other		
dod - 6	other		
internet - 1	other		
directory - 1	other		
mgmt - 2	other		
experimental - 3	other		
private - 4	other		
enterprises - 1	other		
unix - 4	other		
cisco - 9	other		
ciscoProducts - 1	other		
local - 2	other		
temporary - 3	other		
pakmon - 4	other		
workgroup - 5	other		
otherEnterprises - 6	other		
ciscoAgentCapability - 7	other		
ciscoConfig - 8	other		
ciscoMgmt - 9	other		
ciscoProcessMIB - 109	module identity		
ciscoProcessMIBObjects - 1	other		
cpmCPU - 1	other		
cpmCPUTotalTable - 1	other	no access	current
cpmCPUTotalEntry - 1	other	no access	current
cpmCPUTotalIndex - 1	32bit unsigne...	no access	current
cpmCPUTotalPhysicalIndex - 2	32bit integer	read only	current
cpmCPUTotal5sec - 3	gauge	read only	deprecated
cpmCPUTotal1min - 4	gauge	read only	deprecated
cpmCPUTotal5min - 5	gauge	read only	deprecated
cpmCPUTotal5secRev - 6	gauge	read only	deprecated
cpmCPUTotal1minRev - 7	gauge	read only	current
cpmCPUTotal5minRev - 8	gauge	read only	current
cpmCPUMonInterval - 9	32bit unsigne...	read only	current

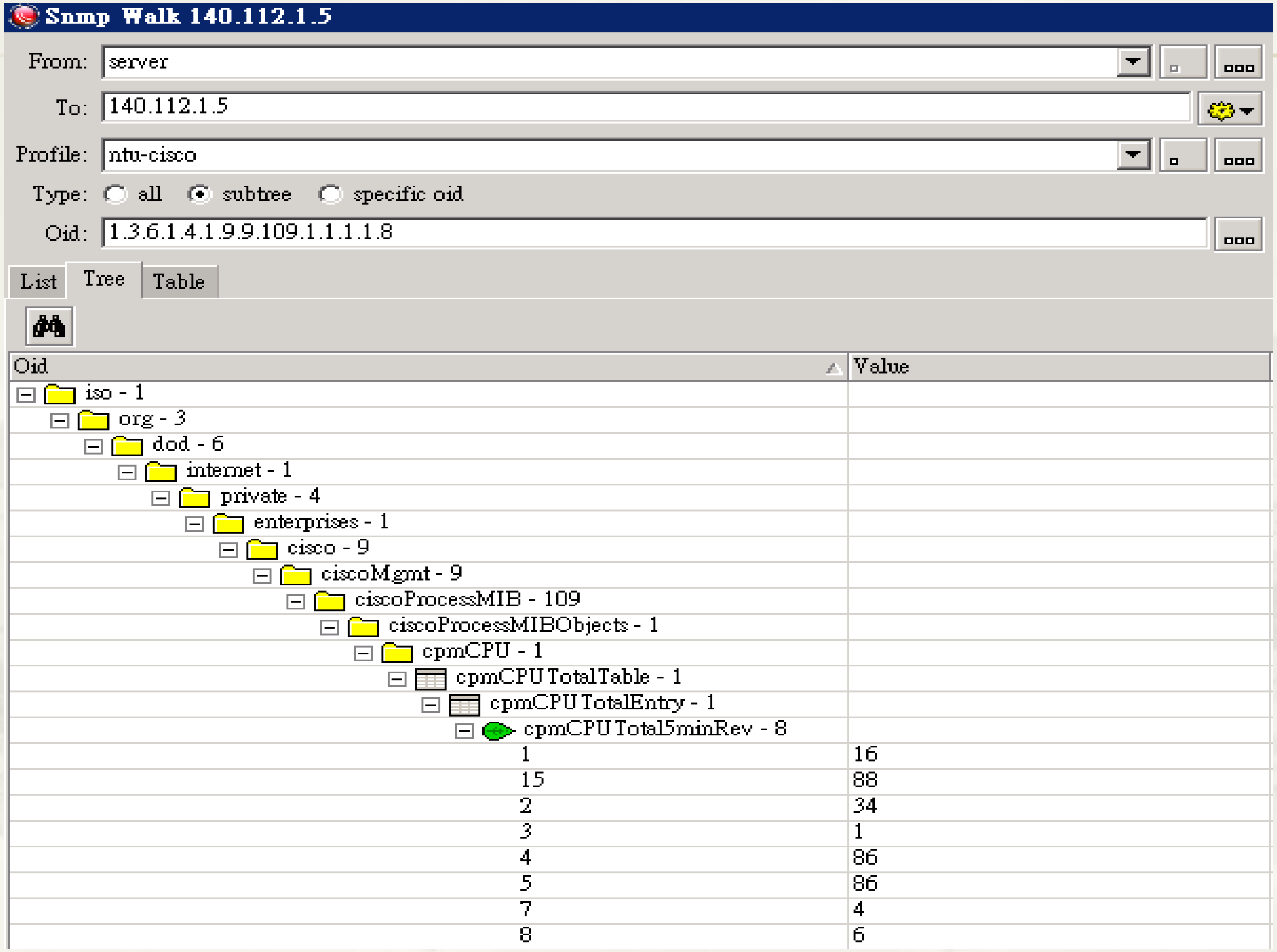
MIB Nodes of cpmCPUTotal5minRev (2/2)



Module: CISCO-PROCESS-MIB -- 175

Node	Type
ciscoProcessMIB - 109	module identity
ciscoProcessMIBObjects - 1	other
cpmCPU - 1	other
cpmCPUTotalTable - 1	other
cpmCPUTotalEntry - 1	other
cpmCPUTotalIndex - 1	32bit unsigne...
cpmCPUTotalPhysicalIndex - 2	32bit integer
cpmCPUTotal5sec - 3	gauge
cpmCPUTotal1min - 4	gauge
cpmCPUTotal5min - 5	gauge
cpmCPUTotal5secRev - 6	gauge
cpmCPUTotal1minRev - 7	gauge
cpmCPUTotal5minRev - 8	gauge
cpmCPUMonInterval - 9	32bit unsigne...
cpmCPUTotalMonIntervalValue - 10	gauge
cpmCPUInterruptMonIntervalValue - 11	gauge
cpmCPUMemoryUsed - 12	gauge

網路查修工具-SnmpWalk



Snmp Walk 140.112.1.5

From: server

To: 140.112.1.5

Profile: ntu-cisco

Type: ○ all ● subtree ○ specific oid

Oid: 1.3.6.1.4.1.9.9.109.1.1.1.1.8

```
Oid                                              Value
⊟ iso - 1
  ⊟ org - 3
    ⊟ dod - 6
      ⊟ internet - 1
        ⊟ private - 4
          ⊟ enterprises - 1
            ⊟ cisco - 9
              ⊟ ciscoMgmt - 9
                ⊟ ciscoProcessMIB - 109
                  ⊟ ciscoProcessMIBObjects - 1
                    ⊟ cpmCPU - 1
                      ⊟ cpmCPUTotalTable - 1
                        ⊟ cpmCPUTotalEntry - 1
                          ⊟ cpmCPUTotal5minRev - 8
                               1                 16
                               15                88
                               2                 34
                               3                 1
                               4                 86
                               5                 86
                               7                 4
                               8                 6
```

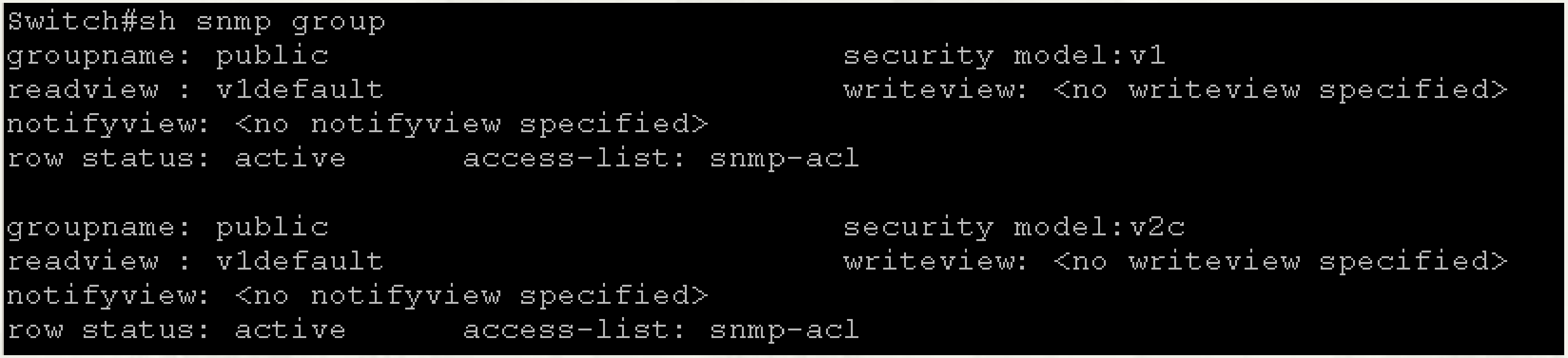
- cpmCPUTotal5minRev (.1.3.6.1.4.1.9.9.109.1.1.1.1.8)

Cisco-SNMP啟用(1/2)

- (config)# snmp-server community public snmp-acl
- (config)# ip access-list standard snmp-acl
- (config-std-nacl)# permit 140.112.0.0 0.0.255.255

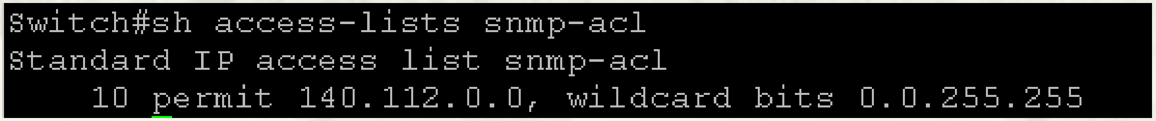
Cisco-SNMP啟用(2/2)

- sh snmp group



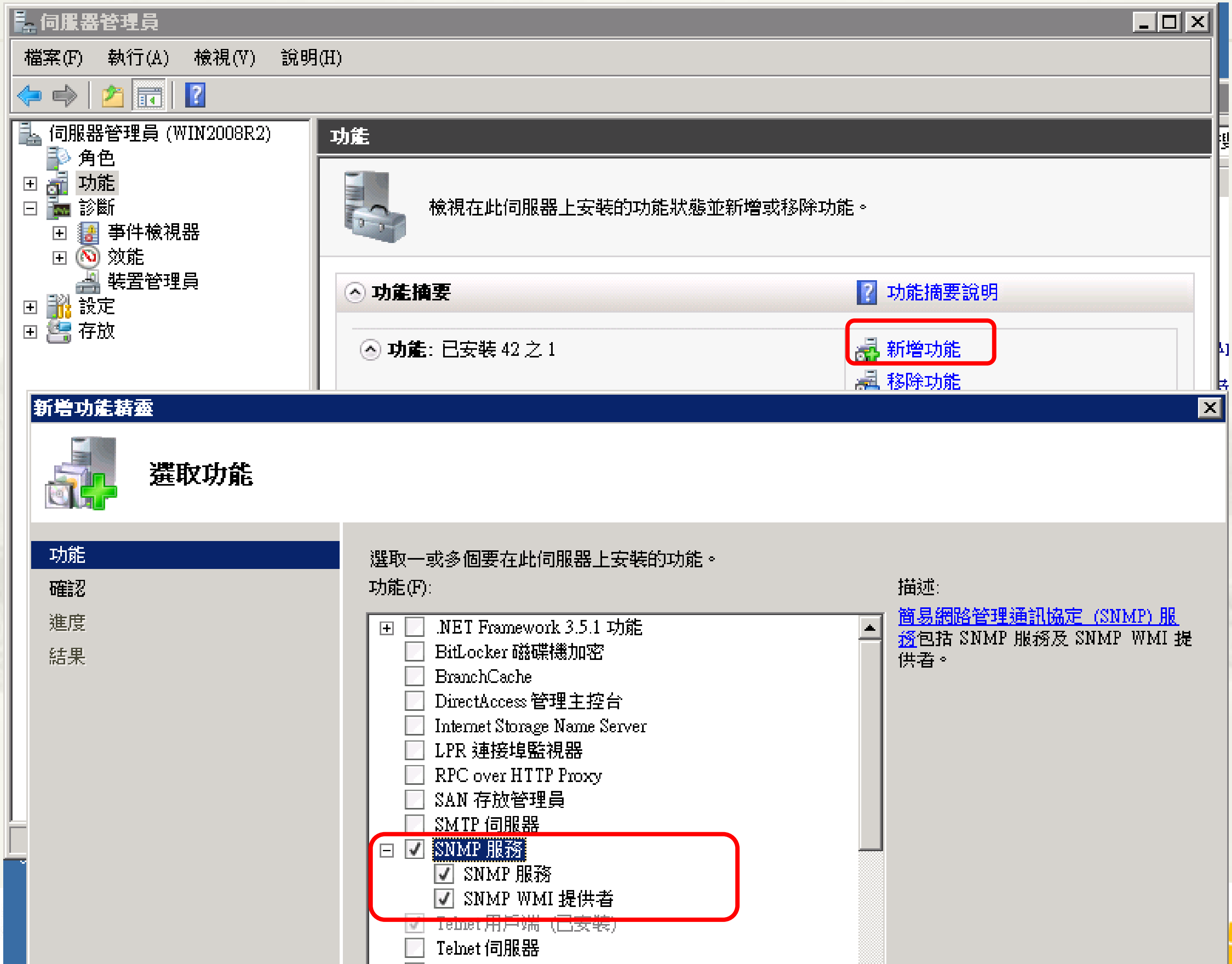
```
Switch#sh snmp group
groupname: public                              security model:v1
readview : v1default                           writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active      access-list: snmp-acl

groupname: public                              security model:v2c
readview : v1default                           writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active      access-list: snmp-acl
```

- sh access-lists snmp-acl



```
Switch#sh access-lists snmp-acl
Standard IP access list snmp-acl
    10 permit 140.112.0.0, wildcard bits 0.0.255.255
```

Windows –SNMP 啟用(1/2)



檢視在此伺服器上安裝的功能狀態並新增或移除功能。

功能: 已安裝 42 之 1

選取一或多個要在此伺服器上安裝的功能。

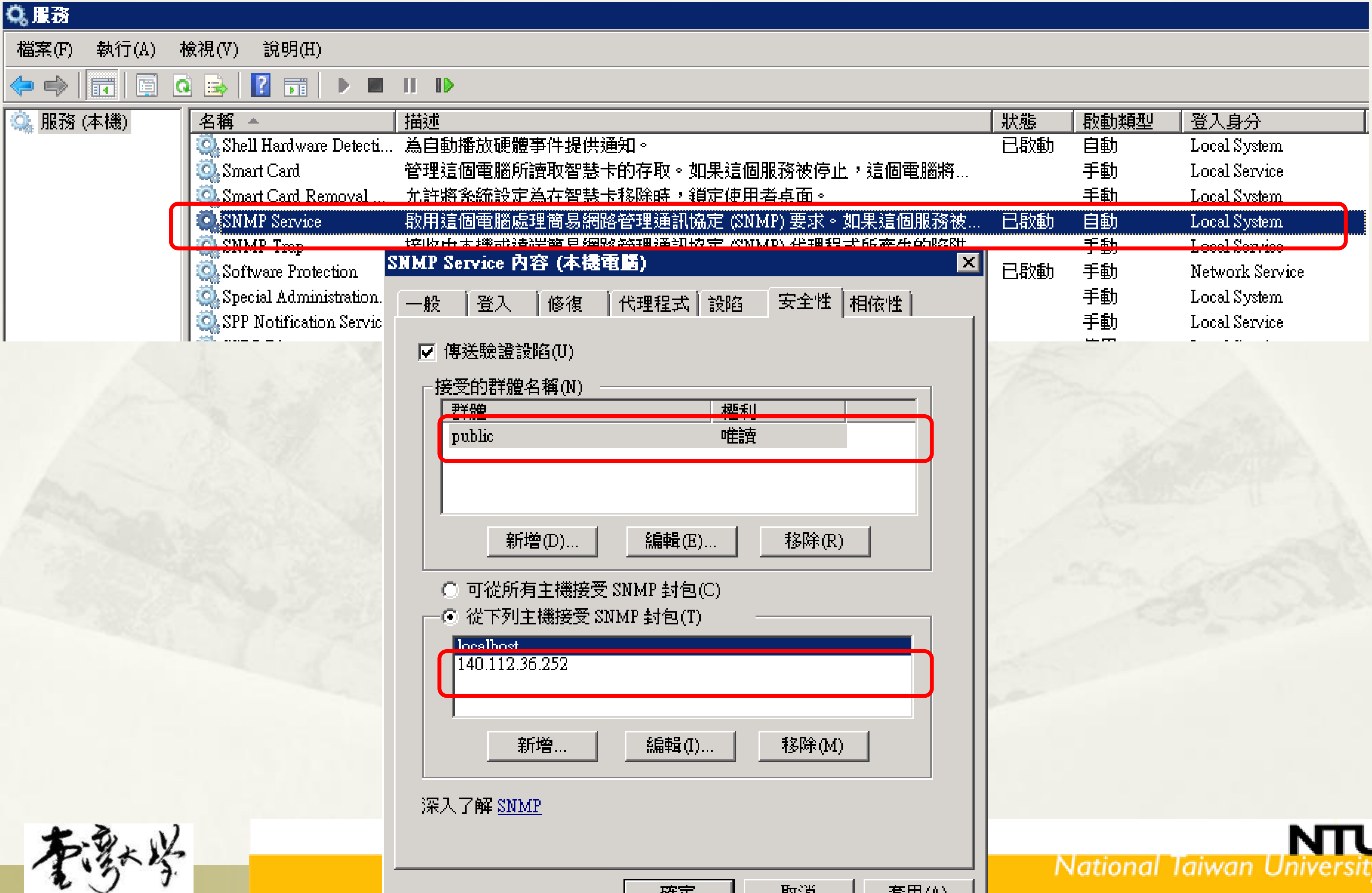
功能(F):

- ⊞ □ .NET Framework 3.5.1 功能
- □ BitLocker 磁碟機加密
- □ BranchCache
- □ DirectAccess 管理主控台
- □ Internet Storage Name Server
- □ LPR 連接埠監視器
- □ RPC over HTTP Proxy
- □ SAN 存放管理員
- □ SMTP 伺服器
- ⊟ ☑ SNMP 服務
  - ☑ SNMP 服務
  - ☑ SNMP WMI 提供者
- ☑ Telnet 用戶端 (已安裝)
- □ Telnet 伺服器

描述:

簡易網路管理通訊協定 (SNMP) 服務包括 SNMP 服務及 SNMP WMI 提供者。

Windows –SNMP 啟用(2/2)



名稱	描述	狀態	啟動類型	登入身分
Shell Hardware Detecti...	為自動播放硬體事件提供通知。	已啟動	自動	Local System
Smart Card	管理這個電腦所讀取智慧卡的存取。如果這個服務被停止，這個電腦將...		手動	Local Service
Smart Card Removal ...	允許將系統設定為在智慧卡移除時，鎖定使用者桌面。		手動	Local System
SNMP Service	啟用這個電腦處理簡易網路管理通訊協定 (SNMP) 要求。如果這個服務被...	已啟動	自動	Local System
SNMP Trap	接收由本機或遠端簡易網路管理通訊協定 (SNMP) 代理程式所產生的陷阱...		手動	Local Service
Software Protection		已啟動	手動	Network Service
Special Administration...			手動	Local System
SPP Notification Servic			手動	Local Service

SNMP Service 內容 (本機電腦)

☑ 傳送驗證設陷(U)

接受的群體名稱(N)

群體	權利
public	唯讀

○ 可從所有主機接受 SNMP 封包(C)

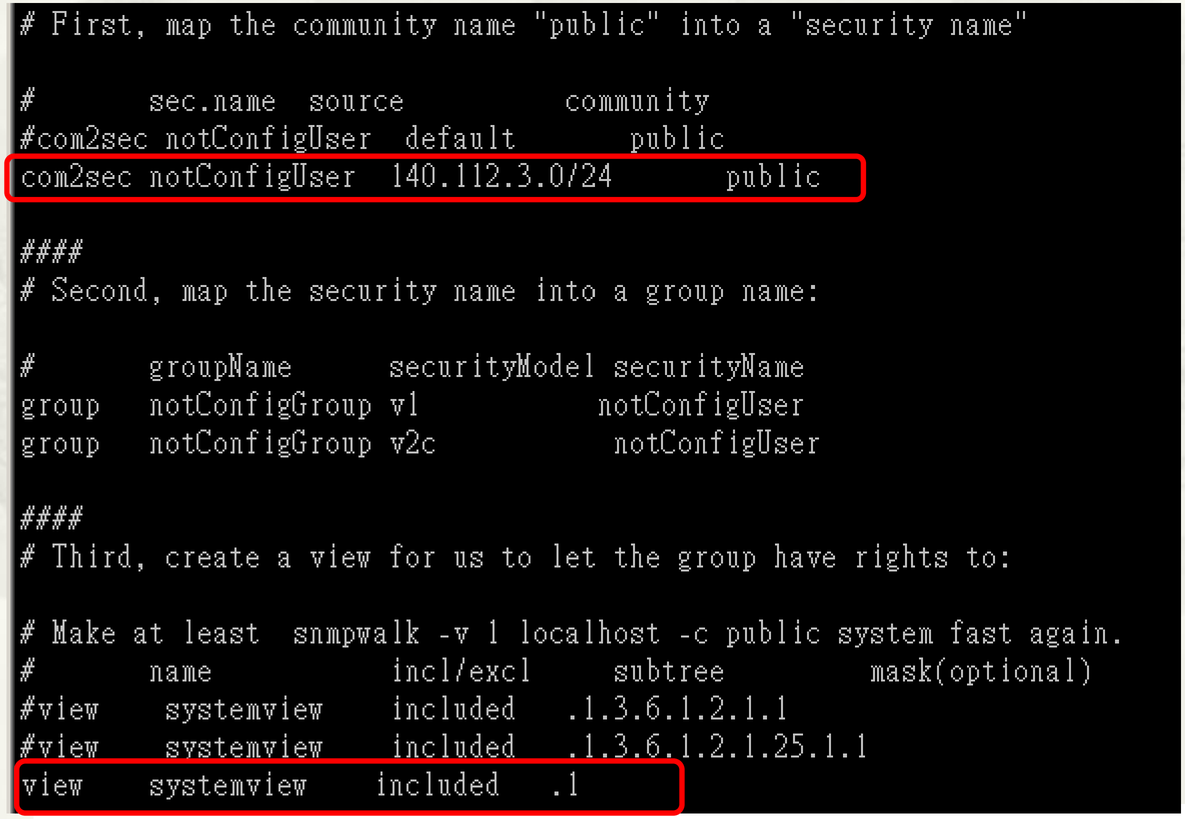
● 從下列主機接受 SNMP 封包(T)

localhost
140.112.36.252

深入了解 SNMP

Linux(CentOS) - SNMP 啟用(1/2)

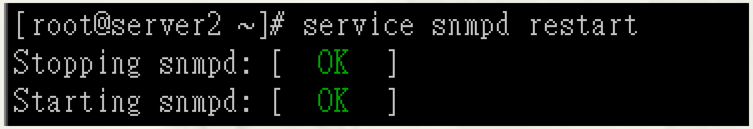
- yum install net-snmp net-snmp-utils
- vi /etc/snmp/snmpd.conf



```
# First, map the community name "public" into a "security name"

#       sec.name  source          community
#com2sec notConfigUser  default       public
com2sec notConfigUser  140.112.3.0/24       public

####
# Second, map the security name into a group name:

#       groupName      securityModel securityName
group   notConfigGroup v1           notConfigUser
group   notConfigGroup v2c           notConfigUser

####
# Third, create a view for us to let the group have rights to:

# Make at least  snmpwalk -v 1 localhost -c public system fast again.
#       name           incl/excl     subtree         mask(optional)
#view    systemview     included   .1.3.6.1.2.1.1
#view    systemview     included   .1.3.6.1.2.1.25.1.1
view    systemview    included   .1
```

Linux(CentOS) - SNMP 啟用(2/2)

- service snmpd restart

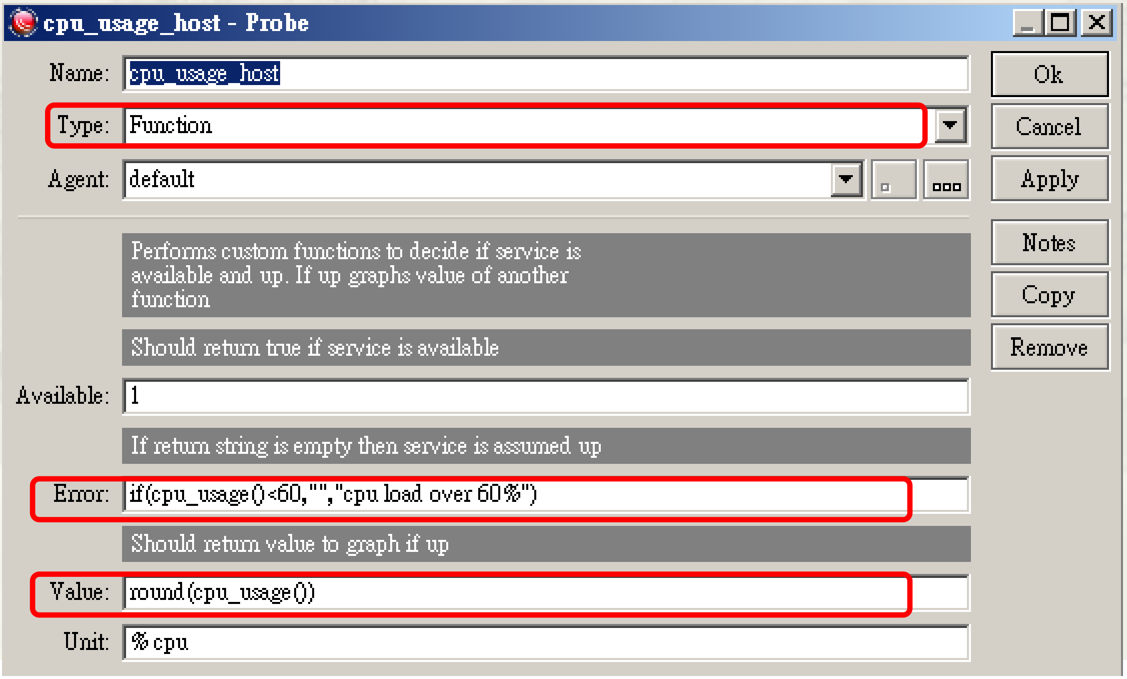


```
[root@server2 ~]# service snmpd restart
Stopping snmpd: [  OK  ]
Starting snmpd: [  OK  ]
```

- Firewall 相關設定
  - UDP port: 161

Probe – Function (Host CPU load)

- 呼叫內建Function()
- 自行定義回傳範圍與異常警示訊息
- Error: if(cpu_usage()<60,"","cpu load over 60%")
- Value: round(cpu_usage())



cpu_usage_host - Probe

Name: cpu_usage_host

Type: Function

Agent: default

Performs custom functions to decide if service is available and up. If up graphs value of another function

Should return true if service is available

Available: 1

If return string is empty then service is assumed up

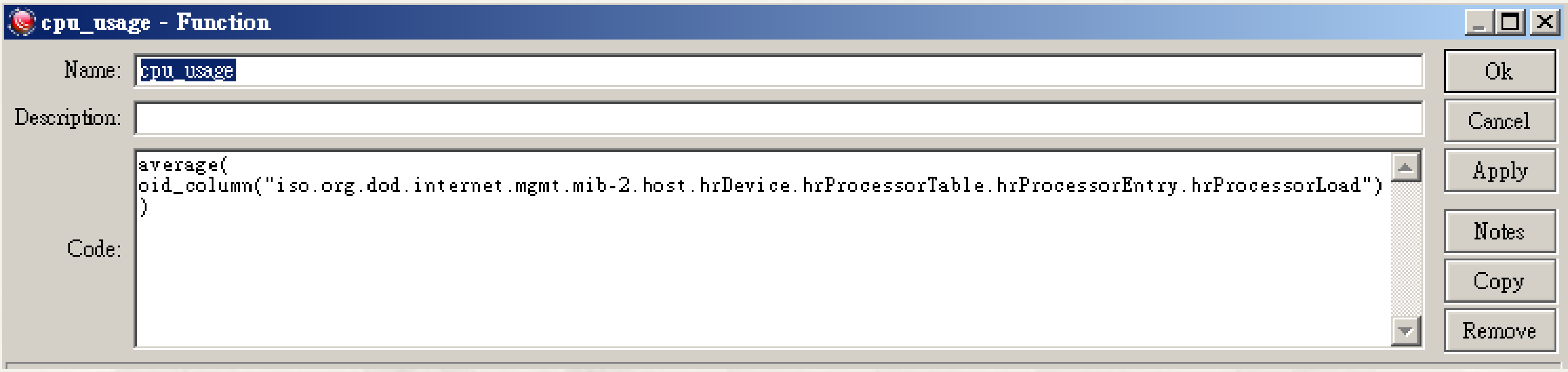
Error: if(cpu_usage()<60,"","cpu load over 60%")

Should return value to graph if up

Value: round(cpu_usage())

Unit: % cpu

Function: cpu_usage



cpu_usage - Function

Name: cpu_usage

Description:

Code:

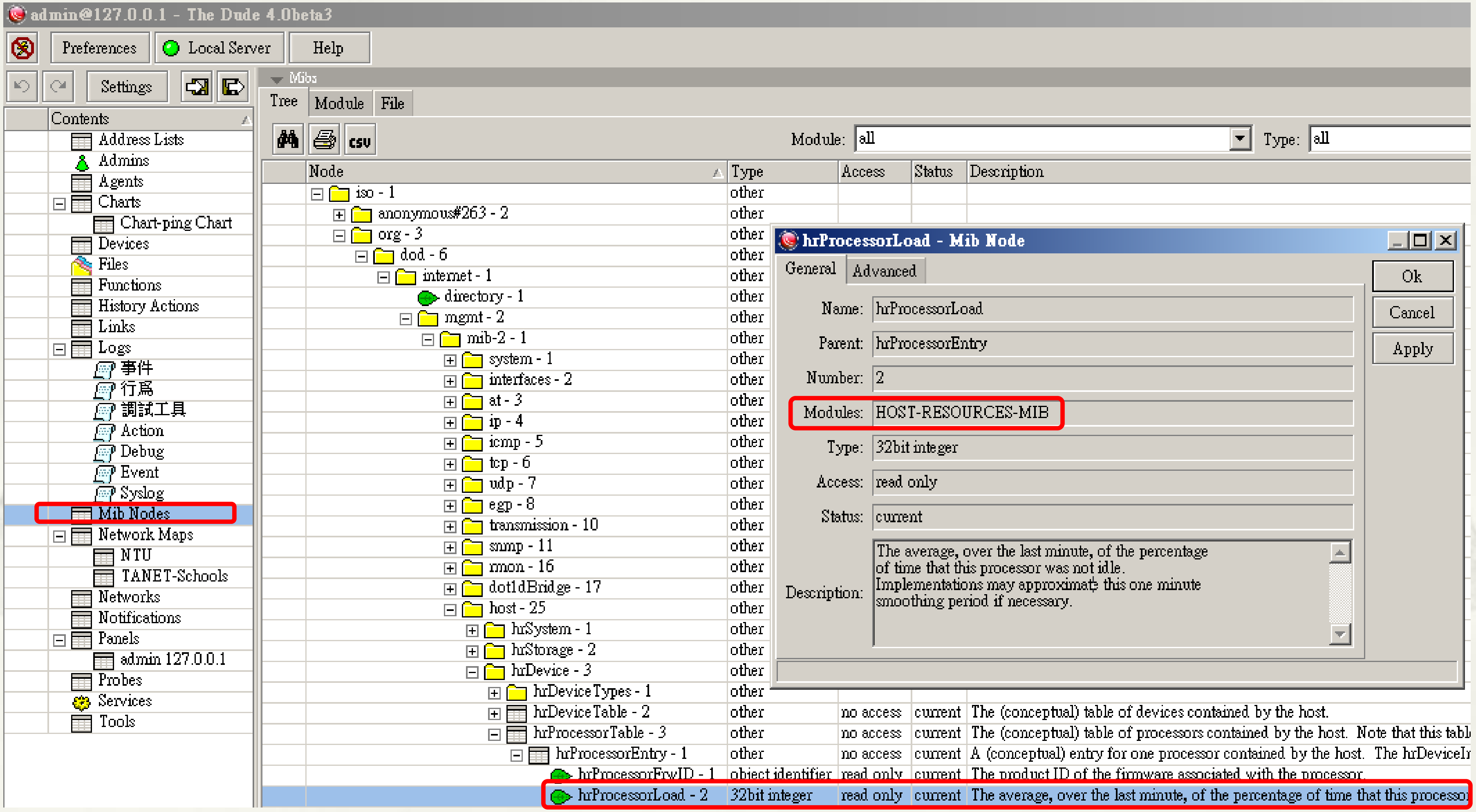
```
average(
oid_column("iso.org.dod.internet.mgmt.mib-2.host.hrDevice.hrProcessorTable.hrProcessorEntry.hrProcessorLoad")
)
```

- average(
- oid_column("iso.org.dod.internet.mgmt.mib-2.host.hrDevice.hrProcessorTable.hrProcessorEntry.hrProcessorLoad")
-)

SNMP of Host Processor Load %

- iso.org.dod.internet.mgmt.mib-2.host.hrDevice.hrProcessorTable.hrProcessorEntry.hrProcessorLoad
- 1.3.6.1.2.1.25.3.3.1.2
  - 1: CPU1 Load
  - 2: CPU2 Load
  - …
- for Linux and Windows, not for Cisco device

MIB Nodes of hrProcessorLoad



Module: all
Type: all

Node	Type	Access	Status	Description
iso - 1	other			
anonymous#263 - 2	other			
org - 3	other			
dod - 6	other			
internet - 1	other			
directory - 1	other			
mgmt - 2	other			
mib-2 - 1	other			
system - 1	other			
interfaces - 2	other			
at - 3	other			
ip - 4	other			
icmp - 5	other			
tcp - 6	other			
udp - 7	other			
egp - 8	other			
transmission - 10	other			
snmp - 11	other			
rmon - 16	other			
dot1dBridge - 17	other			
host - 25	other			
hrSystem - 1	other			
hrStorage - 2	other			
hrDevice - 3	other			
hrDeviceTypes - 1	other			
hrDeviceTable - 2	other	no access	current	The (conceptual) table of devices contained by the host.
hrProcessorTable - 3	other	no access	current	The (conceptual) table of processors contained by the host. Note that this tabl
hrProcessorEntry - 1	other	no access	current	A (conceptual) entry for one processor contained by the host. The hrDeviceIr
hrProcessorFrwID - 1	object identifier	read only	current	The product ID of the firmware associated with the processor.
hrProcessorLoad - 2	32bit integer	read only	current	The average, over the last minute, of the percentage of time that this processo

hrProcessorLoad - Mib Node

Name: hrProcessorLoad

Parent: hrProcessorEntry

Number: 2

Modules: HOST-RESOURCES-MIB

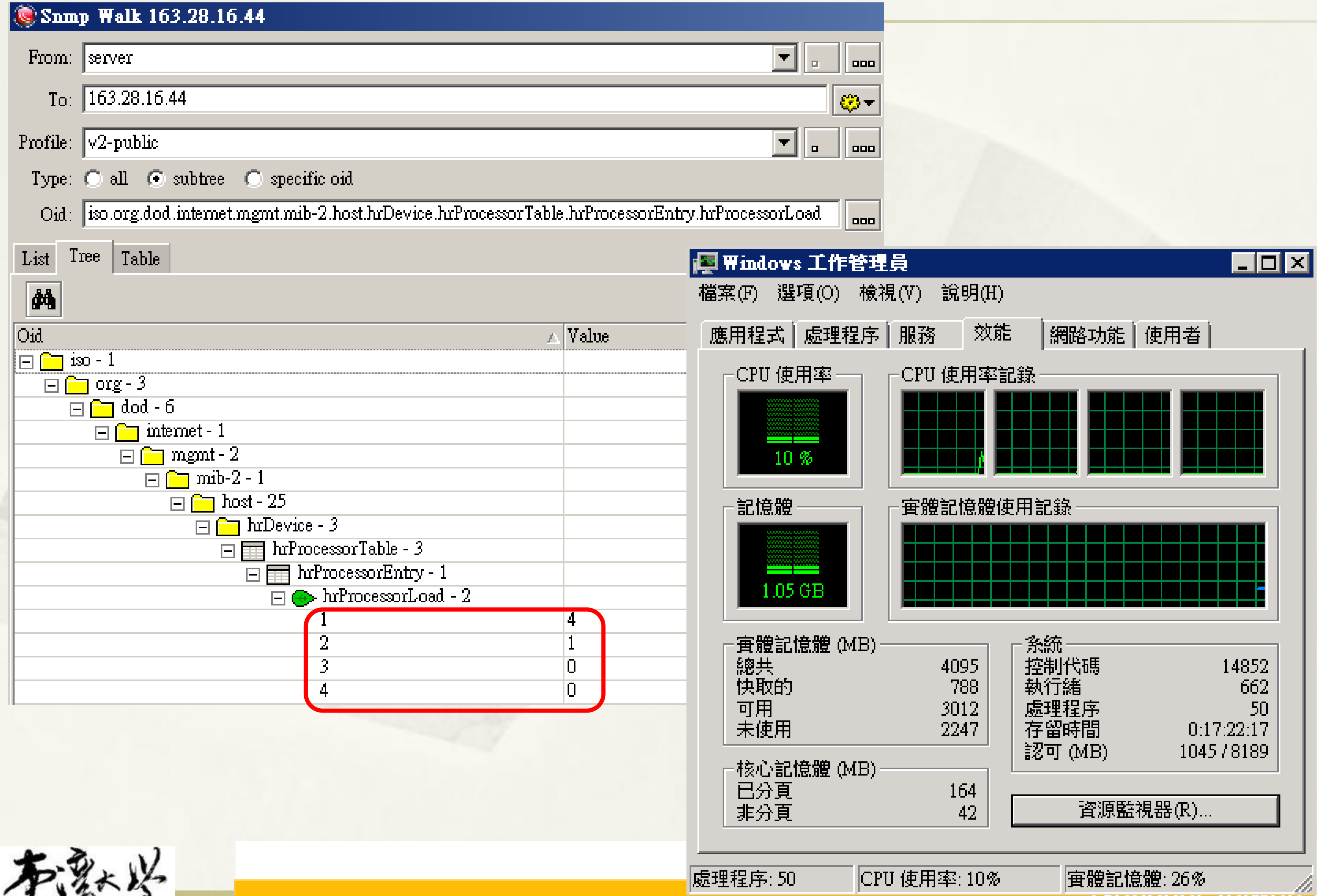
Type: 32bit integer

Access: read only

Status: current

Description: The average, over the last minute, of the percentage of time that this processor was not idle. Implementations may approximate this one minute smoothing period if necessary.

SnmpWalk of hrProcessorLoad



Snmp Walk 163.28.16.44

From: server

To: 163.28.16.44

Profile: v2-public

Type: ○ all ● subtree ○ specific oid

Oid: iso.org.dod.internet.mgmt.mib-2.host.hrDevice.hrProcessorTable.hrProcessorEntry.hrProcessorLoad

```
Oid                                          Value
⊟ iso - 1
  ⊟ org - 3
    ⊟ dod - 6
      ⊟ internet - 1
        ⊟ mgmt - 2
          ⊟ mib-2 - 1
            ⊟ host - 25
              ⊟ hrDevice - 3
                ⊟ hrProcessorTable - 3
                  ⊟ hrProcessorEntry - 1
                    ⊟ hrProcessorLoad - 2
                          1                  4
                          2                  1
                          3                  0
                          4                  0
```

Windows 工作管理員

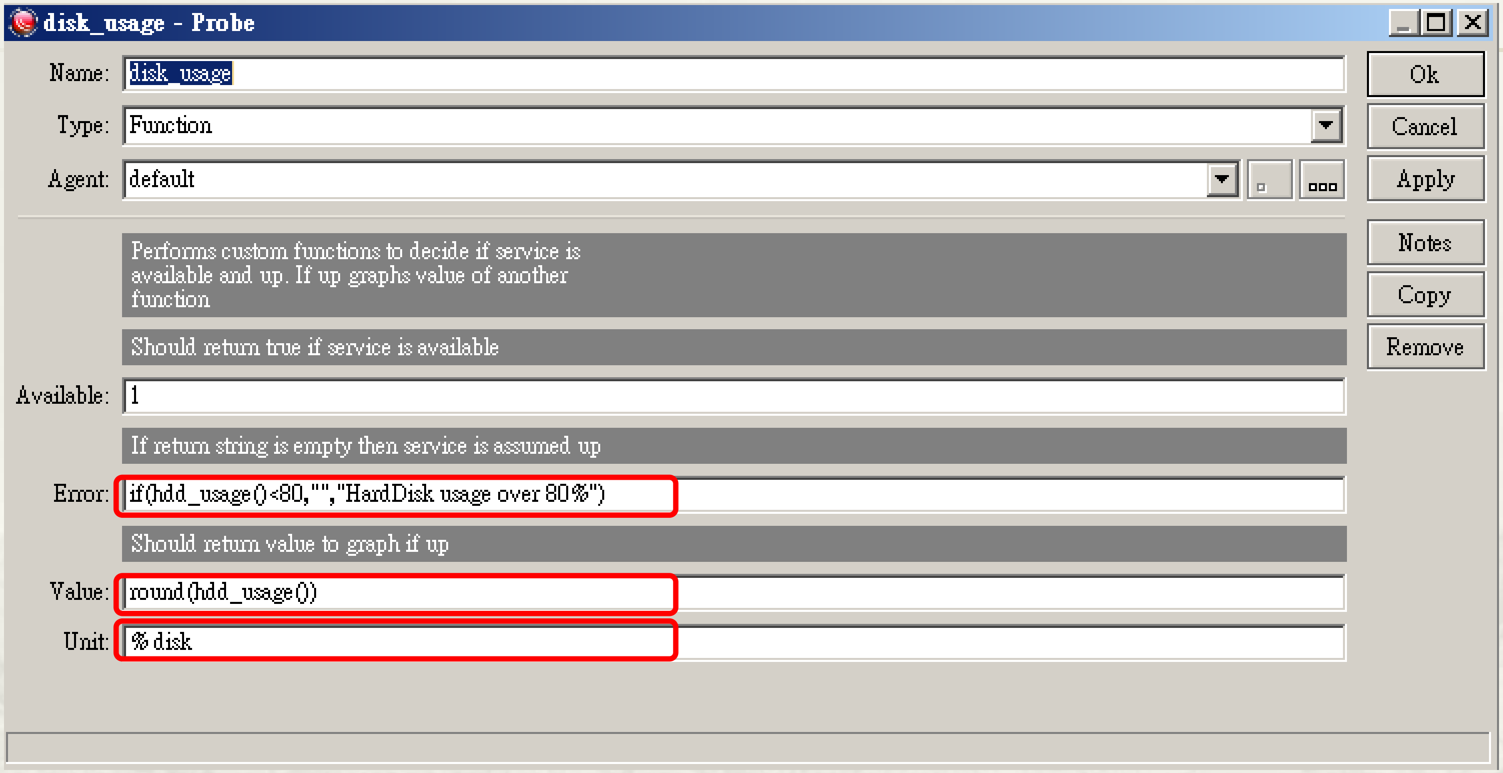
實體記憶體 (MB)	
總共	4095
快取的	788
可用	3012
未使用	2247

核心記憶體 (MB)	
已分頁	164
非分頁	42

系統	
控制代碼	14852
執行緒	662
處理程序	50
存留時間	0:17:22:17
認可 (MB)	1045 / 8189

處理程序: 50 CPU 使用率: 10% 實體記憶體: 26%

Probe – Function (Disk Usage)



Name: disk_usage

Type: Function

Agent: default

Performs custom functions to decide if service is available and up. If up graphs value of another function

Should return true if service is available

Available: 1

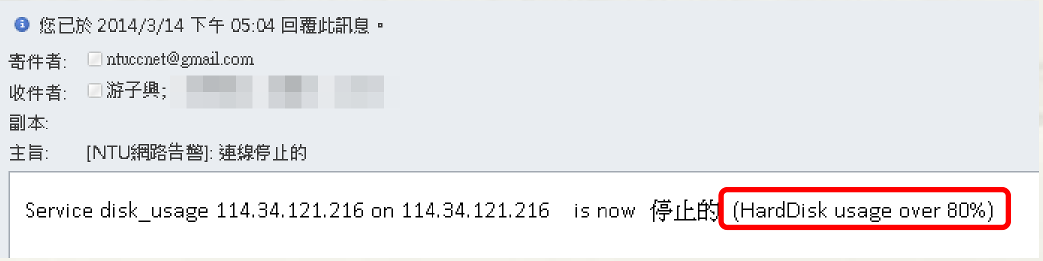
If return string is empty then service is assumed up

Error: if(hdd_usage()<80,"","HardDisk usage over 80%")

Should return value to graph if up

Value: round(hdd_usage())

Unit: % disk



您已於 2014/3/14 下午 05:04 回覆此訊息。

寄件者: ntuccnet@gmail.com

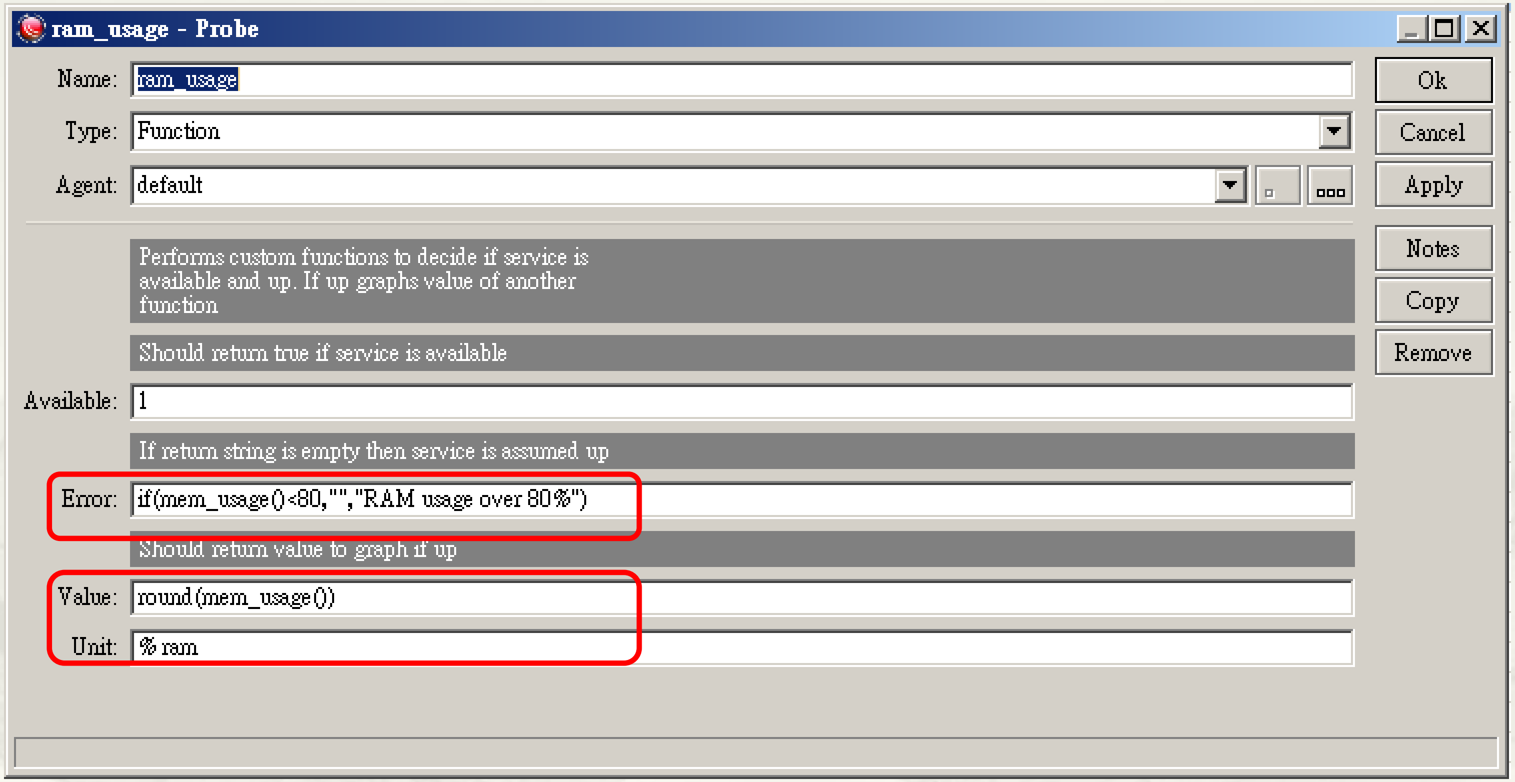
收件者: 游子興; [redacted]

副本:

主旨: [NTU網路告警]: 連線停止的

Service disk_usage 114.34.121.216 on 114.34.121.216 is now 停止的 (HardDisk usage over 80%)

Probe – Function (RAM Usage)



ram_usage - Probe

Name: ram_usage

Type: Function

Agent: default

Performs custom functions to decide if service is available and up. If up graphs value of another function

Should return true if service is available

Available: 1

If return string is empty then service is assumed up

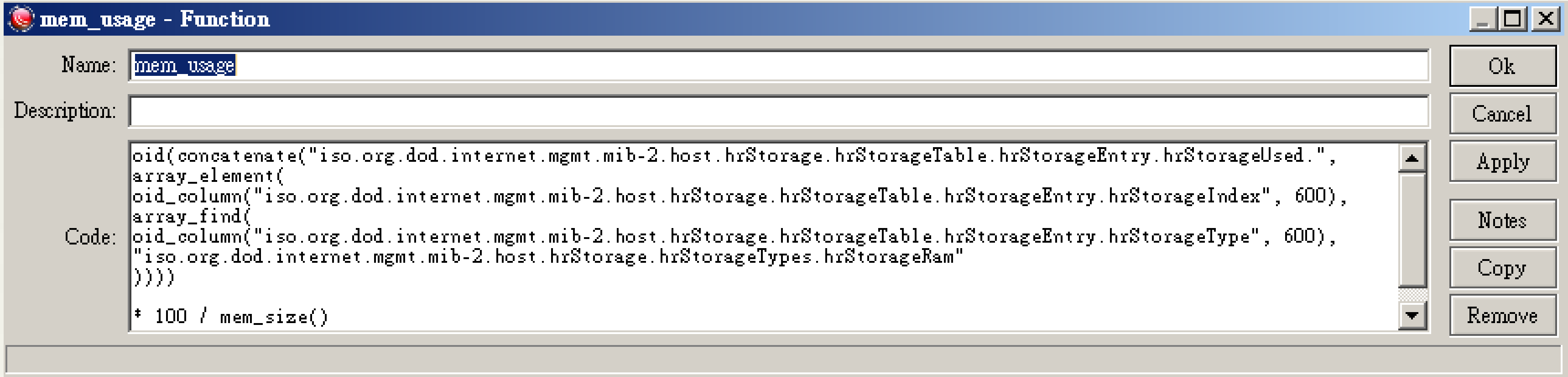
Error: if(mem_usage()<80,"","RAM usage over 80%")

Should return value to graph if up

Value: round(mem_usage())

Unit: % ram

Function: mem_usage



Name: mem_usage

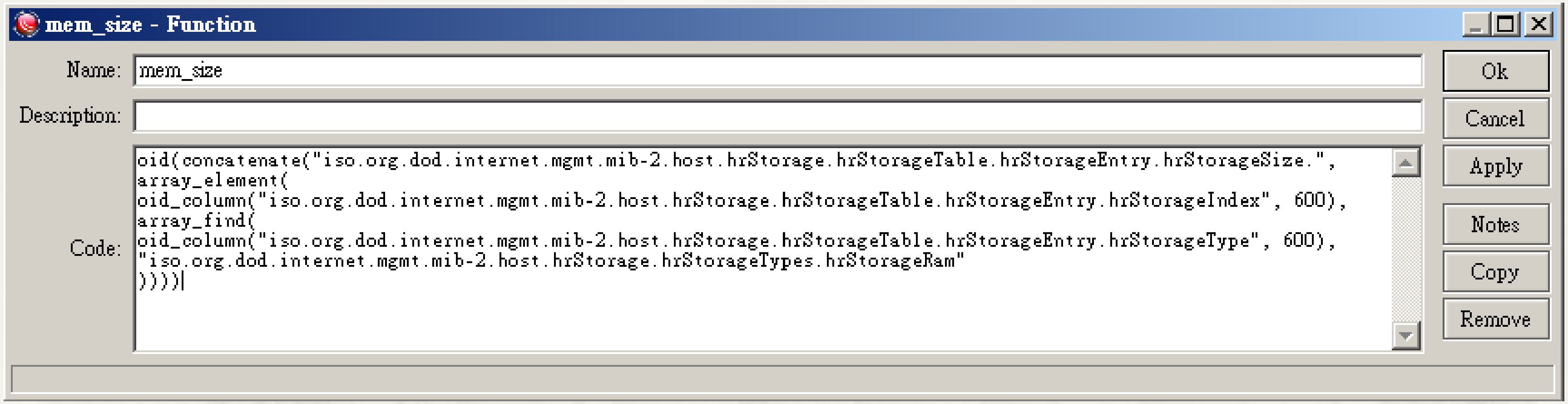
Description:

Code:

```
oid(concatenate("iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageUsed.",
array_element(
oid_column("iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageIndex", 600),
array_find(
oid_column("iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageType", 600),
"iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageRam"
))))

* 100 / mem_size()
```

```
oid(
 concatenate("iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageUsed.",
  array_element(
   oid_column("iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageIndex", 600),
   array_find(
    oid_column("iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageType",600),
     "iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageRam")
   )
  )
 ) * 100 / mem_size()
```

Function: mem_size 1/2



Name: mem_size

Description:

Code:

```
oid(concatenate("iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageSize.",
array_element(
oid_column("iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageIndex", 600),
array_find(
oid_column("iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageType", 600),
"iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageRam"
))))
```

```
oid(
  concatenate("iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageSize.",
    array_element(
      oid_column("iso.org.dod.internet.mgmt.mib- 2.host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageIndex", 600),
      array_find(
        oid_column("iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageType", 600),
        "iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageRam")
      )
  )
)
```

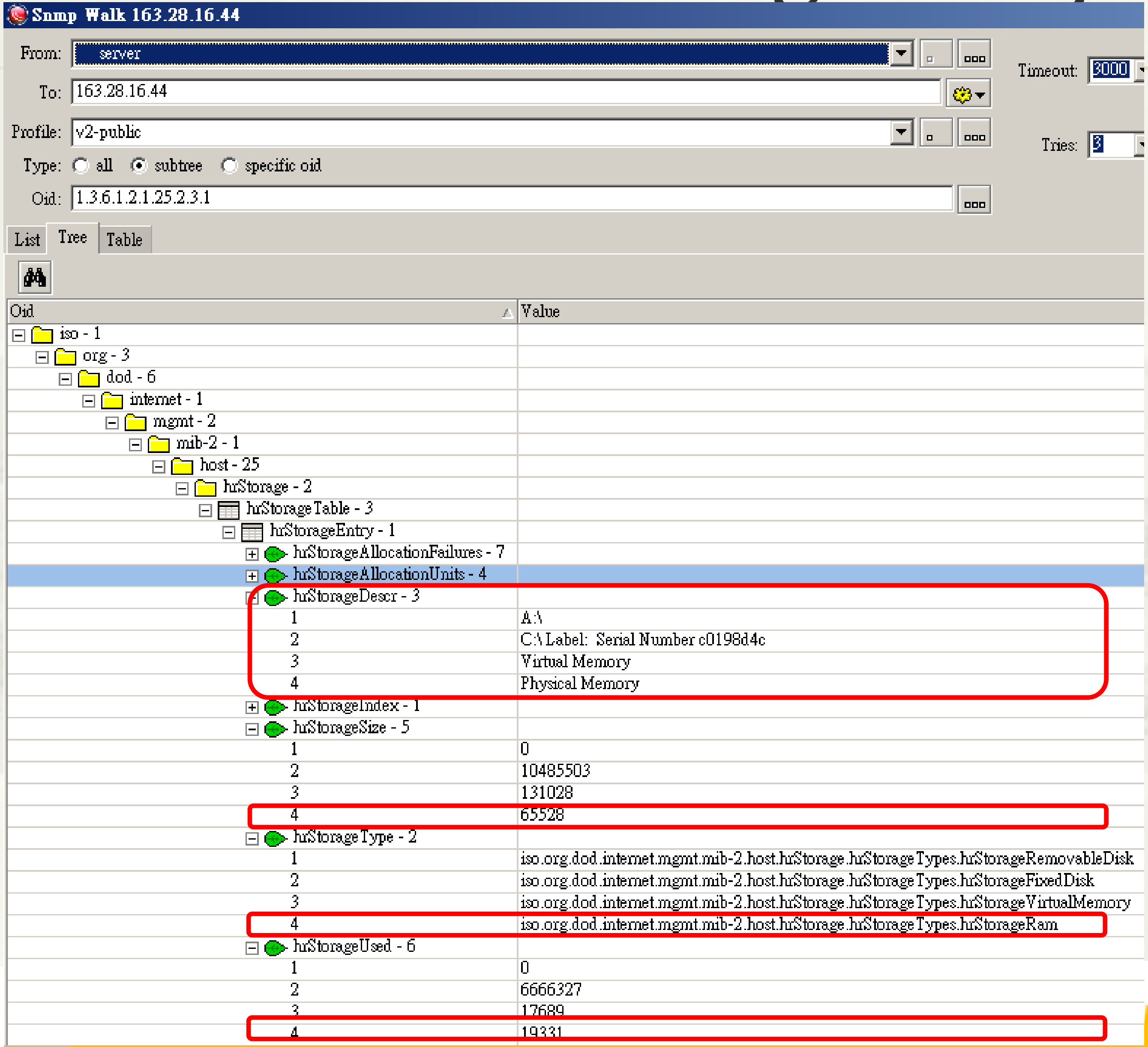
Function: mem_size 2/2

- 1.oid_column("iso……hrStorageEntry.hrStorageType", 600)
  - 使用 snmp walk 搜尋 "iso……hrStorageEntry.hrStorageType"
  - 回傳結果使用 array 存放.
- 2.array_find(array from step1,"iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageRam")
  - 搜尋 array 值中符合 "iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageRam"
  - 回傳 array index 得到 6
- 3.array_element(oid_column("iso……hrStorageEntry.hrStorageIndex", 600),6)
  - 使用 snmp walk 搜尋 "iso……hrStorageEntry.hrStorageIndex" 並回傳 Array 第6個 element 之值
- 4.oid(concatenate("iso……hrStorageEntry.hrStorageSize.",6)
  - 使用 oid("iso……hrStorageEntry.hrStorageSize.6") 查詢結果.

SNMP of Storage/Memory/Virtual Memory

- For Linux/Windows 皆可用
- 1.3.6.1.2.1.25.2.3.1
- iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTable.hrStorageEntry

SNMP of hrStorageEntry



Snmp Walk 163.28.16.44

From: server

To: 163.28.16.44

Profile: v2-public

Type: ○ all ● subtree ○ specific oid

Oid: 1.3.6.1.2.1.25.2.3.1

Timeout: 3000

Tries: 3

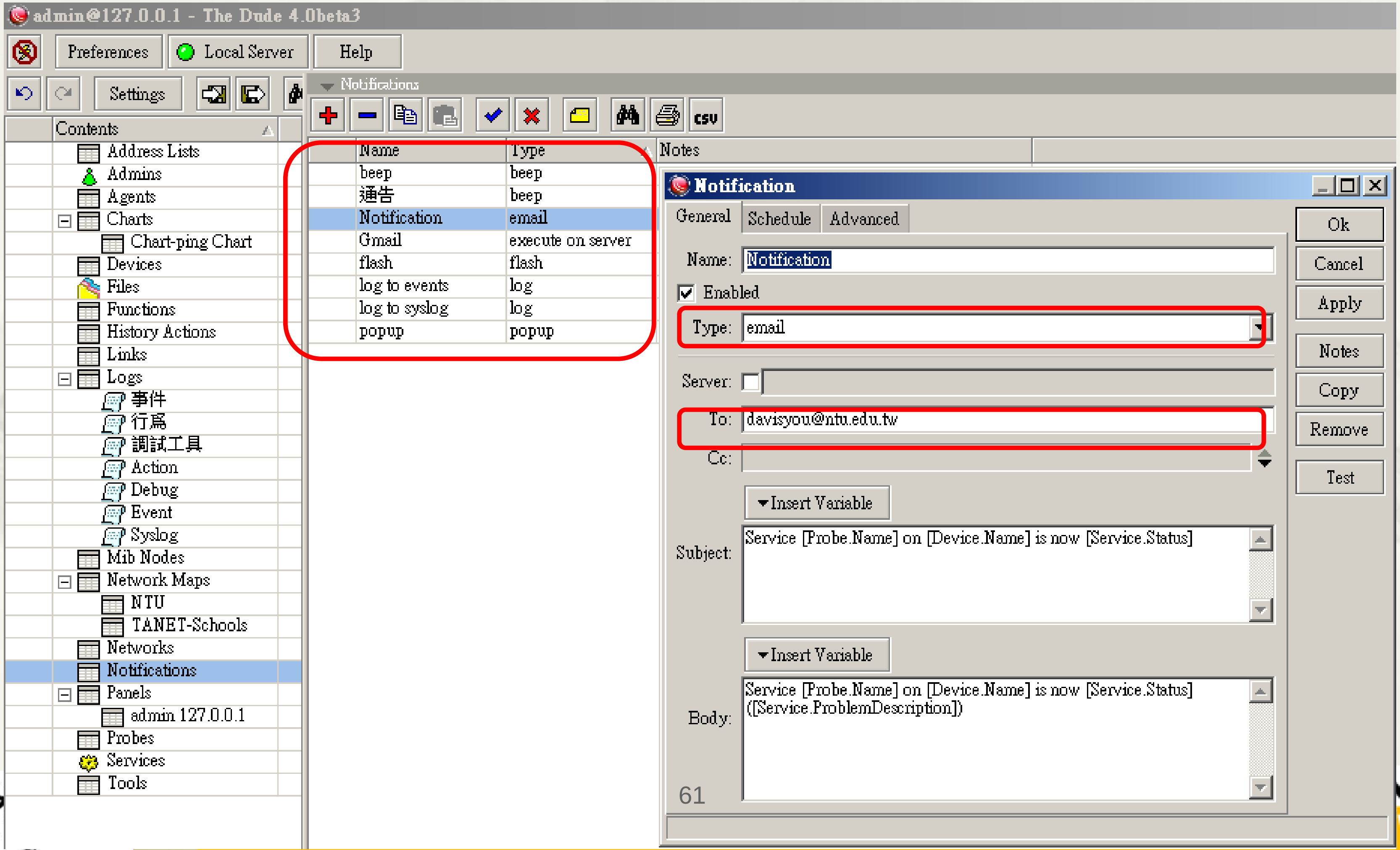
```
Oid                                          Value
⊟ iso - 1
  ⊟ org - 3
    ⊟ dod - 6
      ⊟ internet - 1
        ⊟ mgmt - 2
          ⊟ mib-2 - 1
            ⊟ host - 25
              ⊟ hrStorage - 2
                ⊟ hrStorageTable - 3
                  ⊟ hrStorageEntry - 1
                    ⊞ hrStorageAllocationFailures - 7
                    ⊞ hrStorageAllocationUnits - 4
                    ⊟ hrStorageDescr - 3
                        1                    A:\
                        2                    C:\ Label:  Serial Number c0198d4c
                        3                    Virtual Memory
                        4                    Physical Memory
                    ⊞ hrStorageIndex - 1
                    ⊟ hrStorageSize - 5
                        1                    0
                        2                    10485503
                        3                    131028
                        4                    65528
                    ⊟ hrStorageType - 2
                        1                    iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageRemovableDisk
                        2                    iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk
                        3                    iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageVirtualMemory
                        4                    iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageRam
                    ⊟ hrStorageUsed - 6
                        1                    0
                        2                    6666327
                        3                    17689
                        4                    19331
```

Functions Reference

- average(array)
  - calculates and returns average value of given array
- array_element(array,index)
  - return array element with given index.
- array_find(array,criteria)
  - return array index from element that match criteria.
- concatenate(string1,string2,..)
  - concatenates two or more strings.
- round(number)
  - return number rounded to nearest integer.
- oid(oid)
  - returns value of given snmp OID
- oid_column(oid)
  - returns array of values using snmpwalk with given base OID.“
  - Ex. oid_column("oid_column("iso.org.dod.internet.mgmt.mib-2.host.hrDevice.hrProcessorTable.hrProcessorEntry.hrProcessorLoad")")

異常通知方式 – email 1/2

- 使用標準 SMTP 發送 email



Name	Type	Notes
beep	beep	
通告	beep	
Notification	email	
Gmail	execute on server	
flash	flash	
log to events	log	
log to syslog	log	
popup	popup	

Name: Notification

☑ Enabled

Type: email

Server: □

To: davisyou@ntu.edu.tw

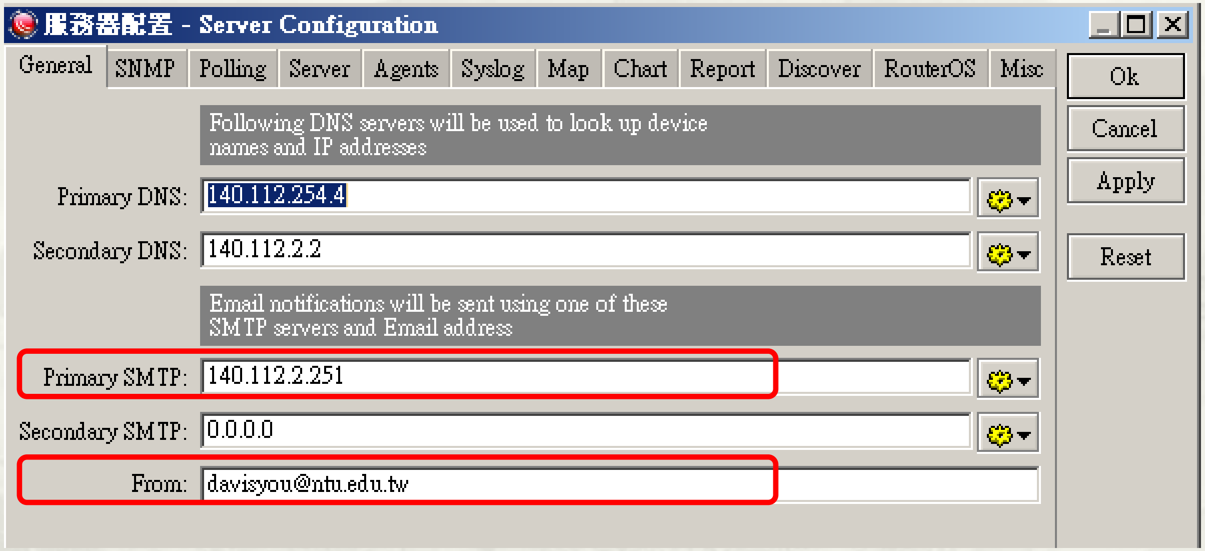
Cc:

Subject: Service [Probe.Name] on [Device.Name] is now [Service.Status]

Body: Service [Probe.Name] on [Device.Name] is now [Service.Status]
([Service.ProblemDescription])

異常通知方式 – email 2/2

- SMTP Server Setup



服務器配置 - Server Configuration

Following DNS servers will be used to look up device names and IP addresses

Primary DNS: 140.112.254.4

Secondary DNS: 140.112.2.2

Email notifications will be sent using one of these SMTP servers and Email address

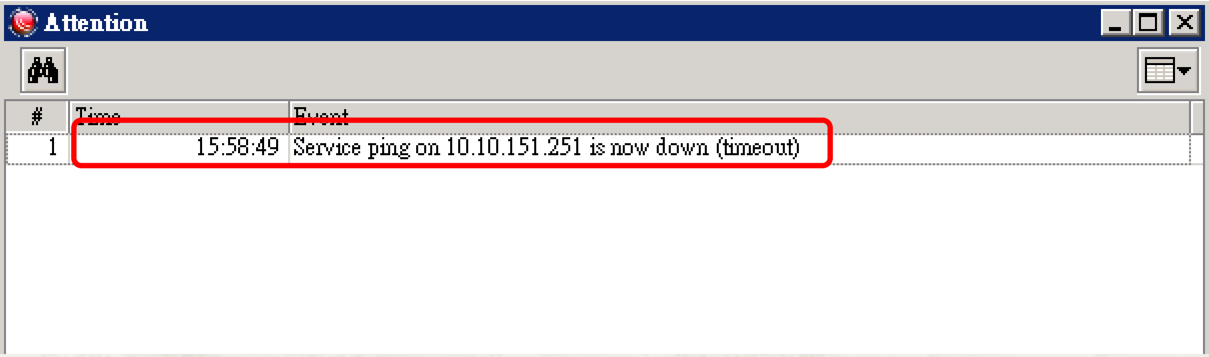
Primary SMTP: 140.112.2.251

Secondary SMTP: 0.0.0.0

From: davisyou@ntu.edu.tw

異常通知方式-- Popup

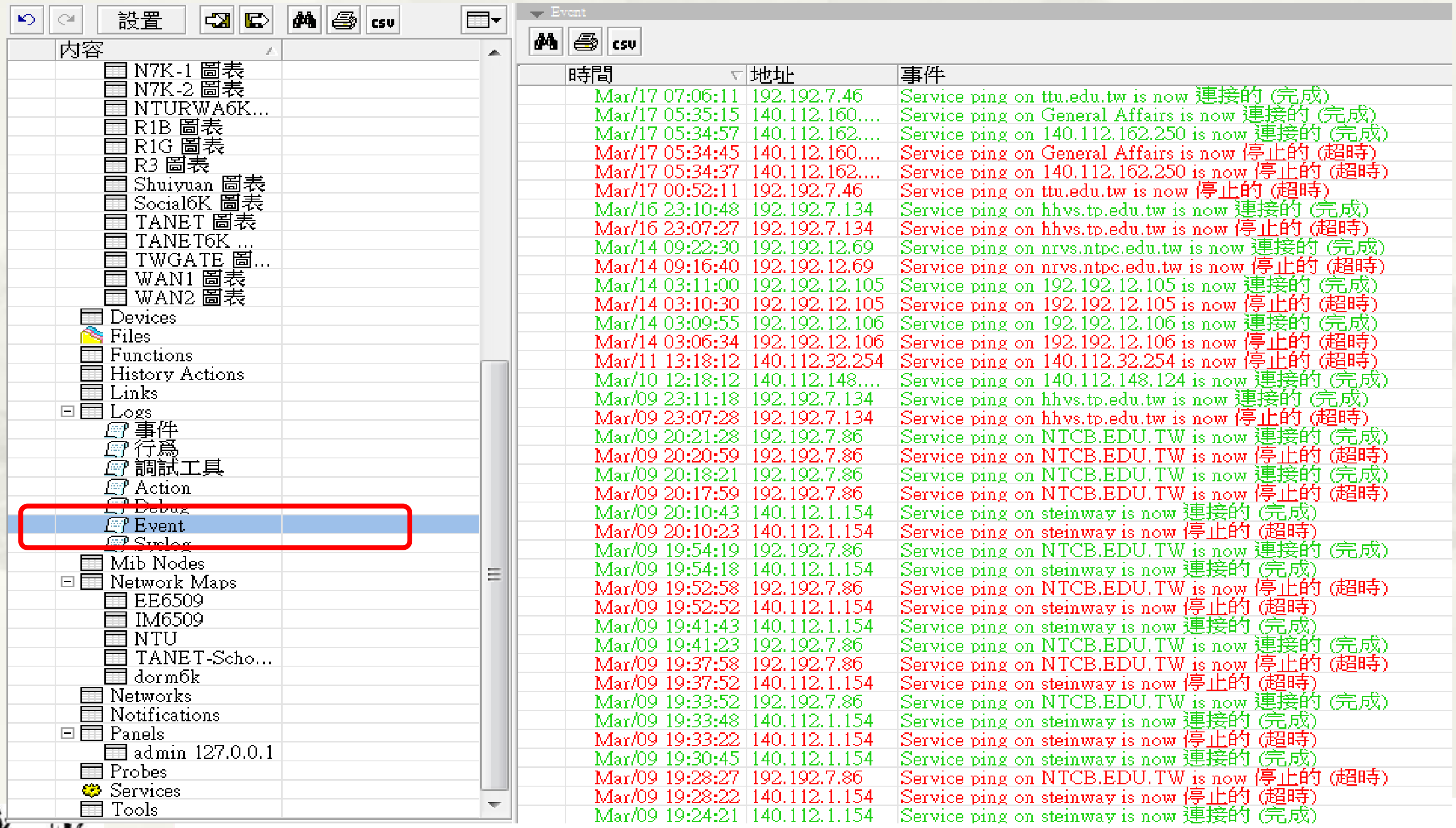
- 在 Client 電腦彈出警示視窗



#	Time	Event
1	15:58:49	Service ping on 10.10.151.251 is now down (timeout)

異常通知方式– log to events

- Event: 記錄異常事件

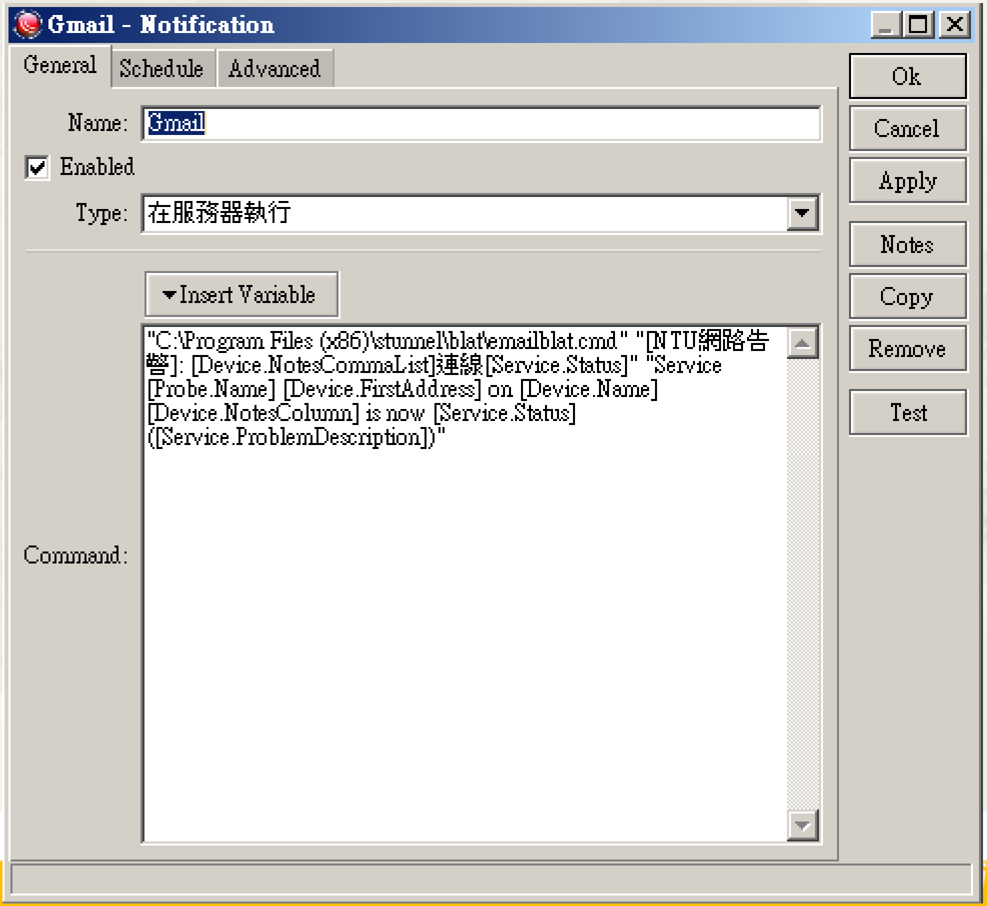


- N7K-1 圖表
- N7K-2 圖表
- NTURWA6K...
- R1B 圖表
- R1G 圖表
- R3 圖表
- Shuiyuan 圖表
- Social6K 圖表
- TANET 圖表
- TANET6K ...
- TWGATE 圖...
- WAN1 圖表
- WAN2 圖表
- Devices
- Files
- Functions
- History Actions
- Links
- Logs
  - 事件
  - 行爲
  - 調試工具
  - Action
  - Debug
  - Event
  - Syslog
- Mib Nodes
- Network Maps
  - EE6509
  - IM6509
  - NTU
  - TANET-Scho...
  - dorm6k
- Networks
- Notifications
- Panels
  - admin 127.0.0.1
- Probes
- Services
- Tools

時間	地址	事件
Mar/17 07:06:11	192.192.7.46	Service ping on ttu.edu.tw is now 連接的 (完成)
Mar/17 05:35:15	140.112.160....	Service ping on General Affairs is now 連接的 (完成)
Mar/17 05:34:57	140.112.162....	Service ping on 140.112.162.250 is now 連接的 (完成)
Mar/17 05:34:45	140.112.160....	Service ping on General Affairs is now 停止的 (超時)
Mar/17 05:34:37	140.112.162....	Service ping on 140.112.162.250 is now 停止的 (超時)
Mar/17 00:52:11	192.192.7.46	Service ping on ttu.edu.tw is now 停止的 (超時)
Mar/16 23:10:48	192.192.7.134	Service ping on hhvs.tp.edu.tw is now 連接的 (完成)
Mar/16 23:07:27	192.192.7.134	Service ping on hhvs.tp.edu.tw is now 停止的 (超時)
Mar/14 09:22:30	192.192.12.69	Service ping on nrvs.ntpc.edu.tw is now 連接的 (完成)
Mar/14 09:16:40	192.192.12.69	Service ping on nrvs.ntpc.edu.tw is now 停止的 (超時)
Mar/14 03:11:00	192.192.12.105	Service ping on 192.192.12.105 is now 連接的 (完成)
Mar/14 03:10:30	192.192.12.105	Service ping on 192.192.12.105 is now 停止的 (超時)
Mar/14 03:09:55	192.192.12.106	Service ping on 192.192.12.106 is now 連接的 (完成)
Mar/14 03:06:34	192.192.12.106	Service ping on 192.192.12.106 is now 停止的 (超時)
Mar/11 13:18:12	140.112.32.254	Service ping on 140.112.32.254 is now 停止的 (超時)
Mar/10 12:18:12	140.112.148....	Service ping on 140.112.148.124 is now 連接的 (完成)
Mar/09 23:11:18	192.192.7.134	Service ping on hhvs.tp.edu.tw is now 連接的 (完成)
Mar/09 23:07:28	192.192.7.134	Service ping on hhvs.tp.edu.tw is now 停止的 (超時)
Mar/09 20:21:28	192.192.7.86	Service ping on NTCB.EDU.TW is now 連接的 (完成)
Mar/09 20:20:59	192.192.7.86	Service ping on NTCB.EDU.TW is now 停止的 (超時)
Mar/09 20:18:21	192.192.7.86	Service ping on NTCB.EDU.TW is now 連接的 (完成)
Mar/09 20:17:59	192.192.7.86	Service ping on NTCB.EDU.TW is now 停止的 (超時)
Mar/09 20:10:43	140.112.1.154	Service ping on steinway is now 連接的 (完成)
Mar/09 20:10:23	140.112.1.154	Service ping on steinway is now 停止的 (超時)
Mar/09 19:54:19	192.192.7.86	Service ping on NTCB.EDU.TW is now 連接的 (完成)
Mar/09 19:54:18	140.112.1.154	Service ping on steinway is now 連接的 (完成)
Mar/09 19:52:58	192.192.7.86	Service ping on NTCB.EDU.TW is now 停止的 (超時)
Mar/09 19:52:52	140.112.1.154	Service ping on steinway is now 停止的 (超時)
Mar/09 19:41:43	140.112.1.154	Service ping on steinway is now 連接的 (完成)
Mar/09 19:41:23	192.192.7.86	Service ping on NTCB.EDU.TW is now 連接的 (完成)
Mar/09 19:37:58	192.192.7.86	Service ping on NTCB.EDU.TW is now 停止的 (超時)
Mar/09 19:37:52	140.112.1.154	Service ping on steinway is now 停止的 (超時)
Mar/09 19:33:52	192.192.7.86	Service ping on NTCB.EDU.TW is now 連接的 (完成)
Mar/09 19:33:48	140.112.1.154	Service ping on steinway is now 連接的 (完成)
Mar/09 19:33:22	140.112.1.154	Service ping on steinway is now 停止的 (超時)
Mar/09 19:30:45	140.112.1.154	Service ping on steinway is now 連接的 (完成)
Mar/09 19:28:27	192.192.7.86	Service ping on NTCB.EDU.TW is now 停止的 (超時)
Mar/09 19:28:22	140.112.1.154	Service ping on steinway is now 停止的 (超時)
Mar/09 19:24:21	140.112.1.154	Service ping on steinway is now 連接的 (完成)

異常通知方式 – execute on server

- 在Server 端執行特定程式
  - 使用Gmail 發送 email
  - 簡訊發送



Gmail - Notification

Name: Gmail

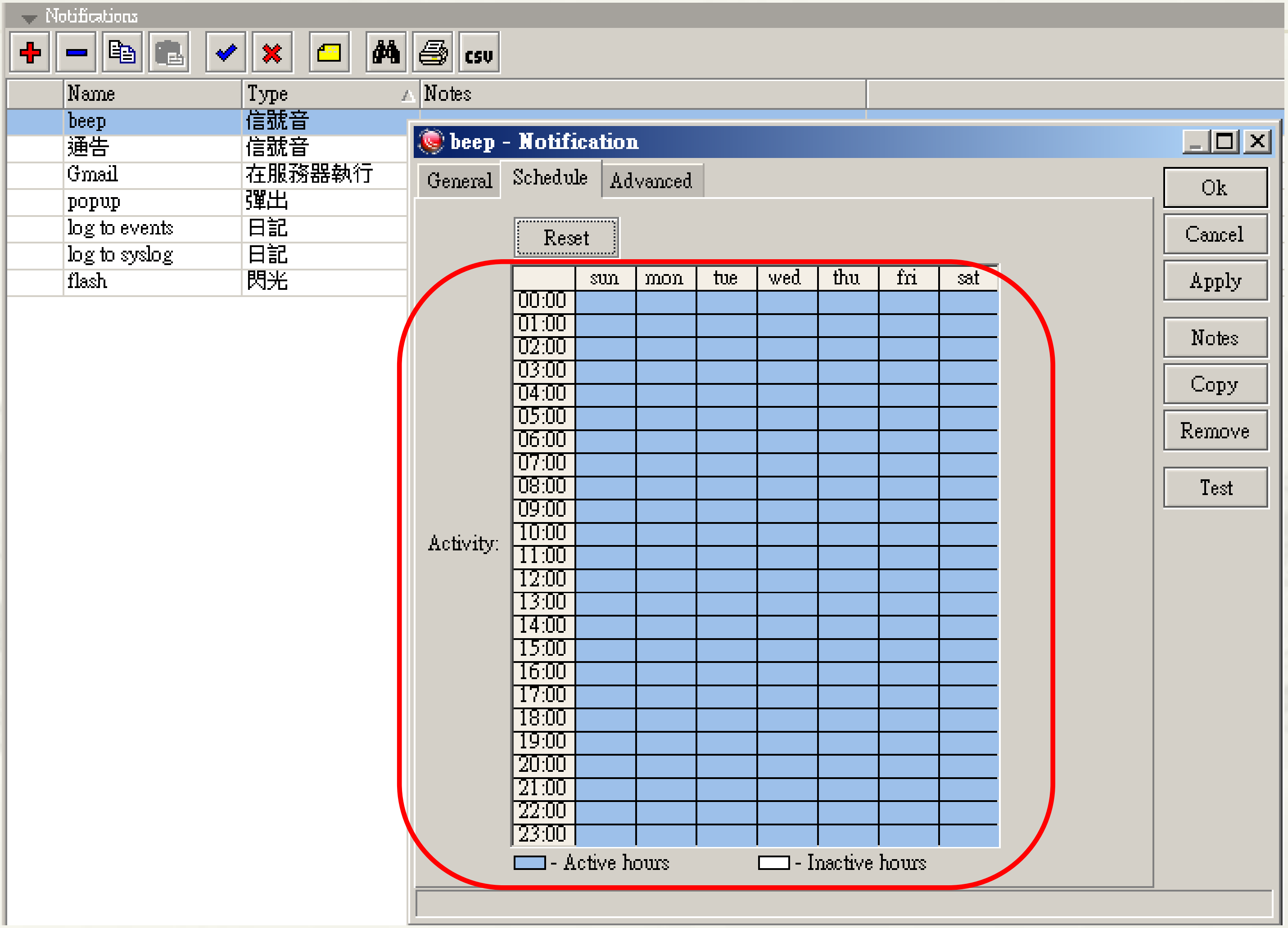
☑ Enabled

Type: 在服務器執行

Command:

```
"C:\Program Files (x86)\stunnel\blat\emailblat.cmd" "[NTU網路告警]: [Device.NotesCommaList]連線[Service.Status]" "Service [Probe.Name] [Device.FirstAddress] on [Device.Name] [Device.NotesColumn] is now [Service.Status] ([Service.ProblemDescription])"
```

異常通知警訊—有效時段



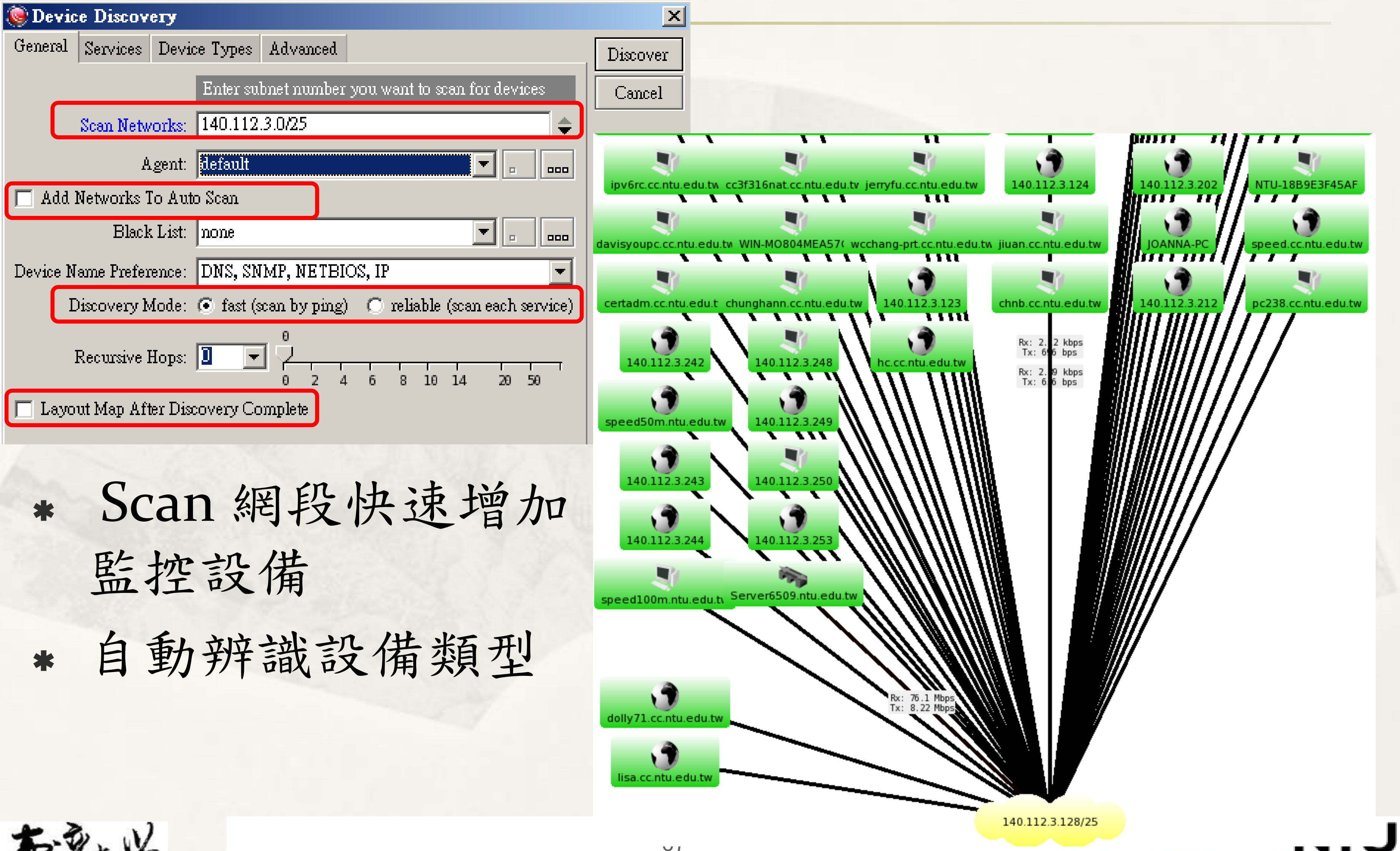
Name	Type	Notes
beep	信號音	
通告	信號音	
Gmail	在服務器執行	
popup	彈出	
log to events	日記	
log to syslog	日記	
flash	閃光	

Activity:

	sun	mon	tue	wed	thu	fri	sat
00:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
01:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
02:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
03:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
04:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
05:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
06:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
07:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
08:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
09:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
10:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
11:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
12:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
13:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
14:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
15:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
16:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
17:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
18:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
19:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
20:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
21:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
22:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
23:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦

🟦 - Active hours ⬜ - Inactive hours

Discovery 1/2



Device Discovery

Enter subnet number you want to scan for devices

Scan Networks: 140.112.3.0/25

Agent: default

☐ Add Networks To Auto Scan

Black List: none

Device Name Preference: DNS, SNMP, NETBIOS, IP

Discovery Mode: ● fast (scan by ping) ○ reliable (scan each service)

Recursive Hops: 0

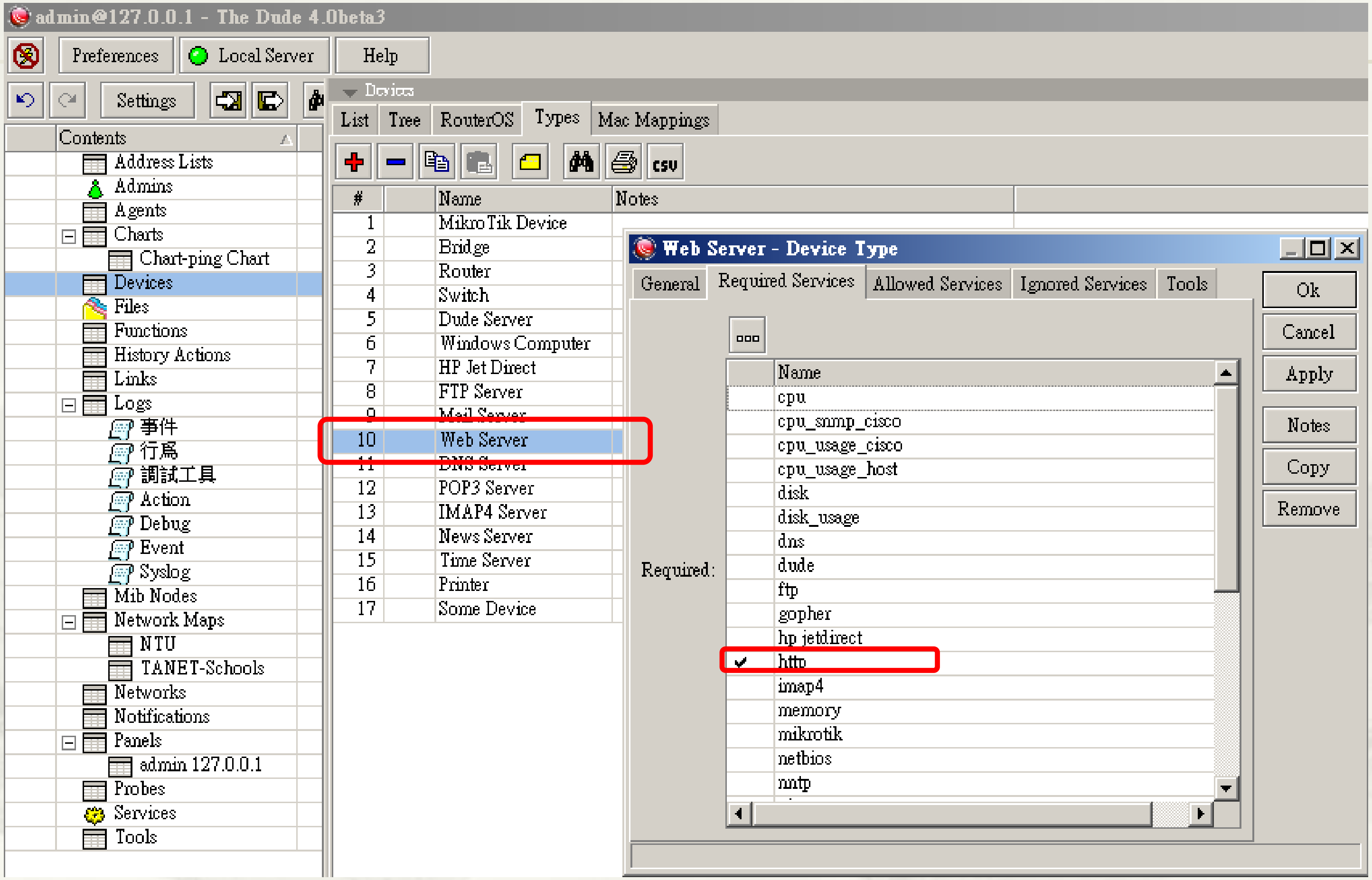
☐ Layout Map After Discovery Complete

- Scan 網段快速增加監控設備
- 自動辨識設備類型

Discovery 2/2

- Add networks to auto scan:
  - It will keep updating the map when new devices appear even after the initial scan is finished.
- Discovery mode
  - Fast(scan by ping) -- devices can respond to ping will be added, and then their services will be proofed.
  - Reliable(scan each service) -- the Dude will look for the specified services even in the devices that couldn't be pinged.
- Layout Map After discovery complete:
  - It will attempt to draw a logical map layout. Especially useful if discovering by more than 1 hop.

Device Type



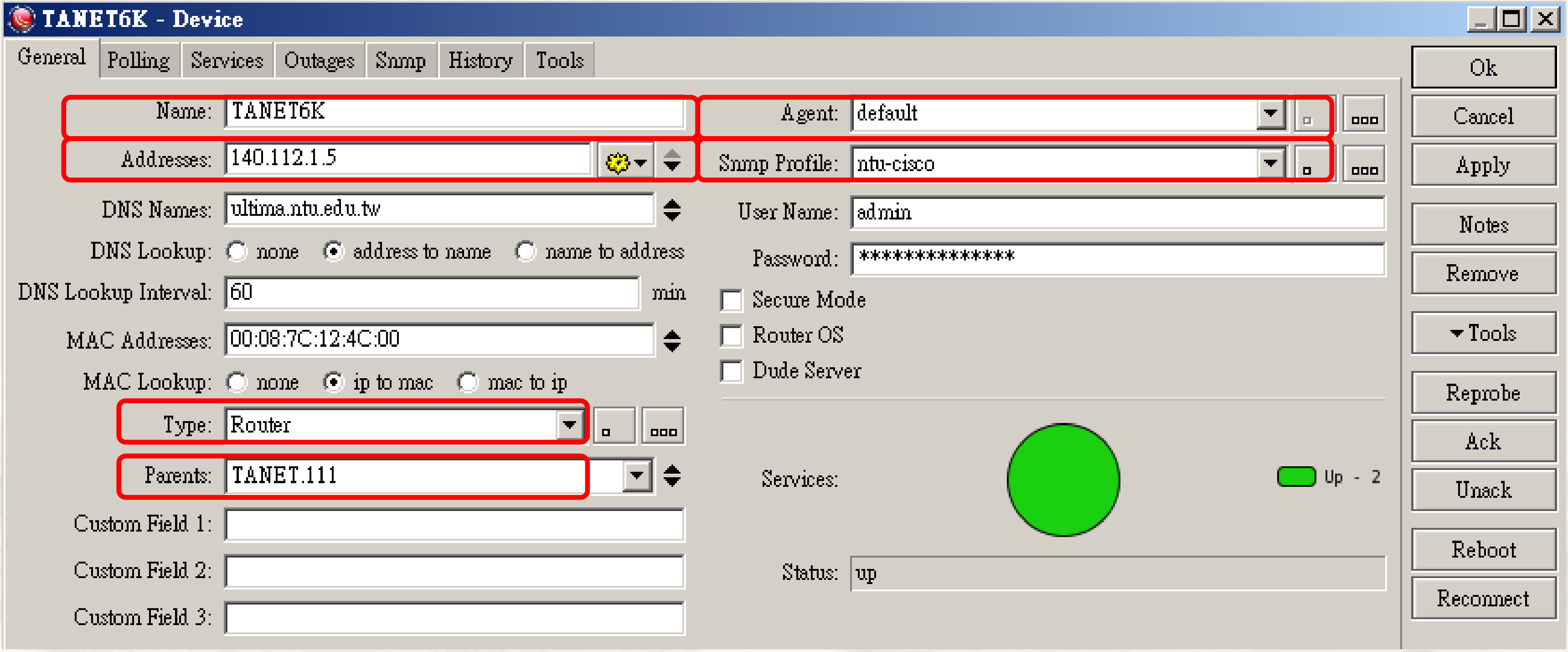
#	Name	Notes
1	MikroTik Device	
2	Bridge	
3	Router	
4	Switch	
5	Dude Server	
6	Windows Computer	
7	HP Jet Direct	
8	FTP Server	
9	Mail Server	
10	Web Server	
11	DNS Server	
12	POP3 Server	
13	IMAP4 Server	
14	News Server	
15	Time Server	
16	Printer	
17	Some Device	

Required:

	Name
	cpu
	cpu_snmp_cisco
	cpu_usage_cisco
	cpu_usage_host
	disk
	disk_usage
	dns
	dude
	ftp
	gopher
	hp jetdirect
✓	http
	imap4
	memory
	mikrotik
	netbios
	nntp

- Required Services: 由此決定 Discovery時, Devices Type 為何.
- Allowed Services: Discovery時, 自動被加入之 Services

Device 設定



TANET6K - Device

Name: TANET6K

Addresses: 140.112.1.5

DNS Names: ultima.ntu.edu.tw

DNS Lookup: ○ none ● address to name ○ name to address

DNS Lookup Interval: 60 min

MAC Addresses: 00:08:7C:12:4C:00

MAC Lookup: ○ none ● ip to mac ○ mac to ip

Type: Router

Parents: TANET.111

Custom Field 1:

Custom Field 2:

Custom Field 3:

Agent: default

Snmp Profile: ntu-cisco

User Name: admin

Password: **************

□ Secure Mode

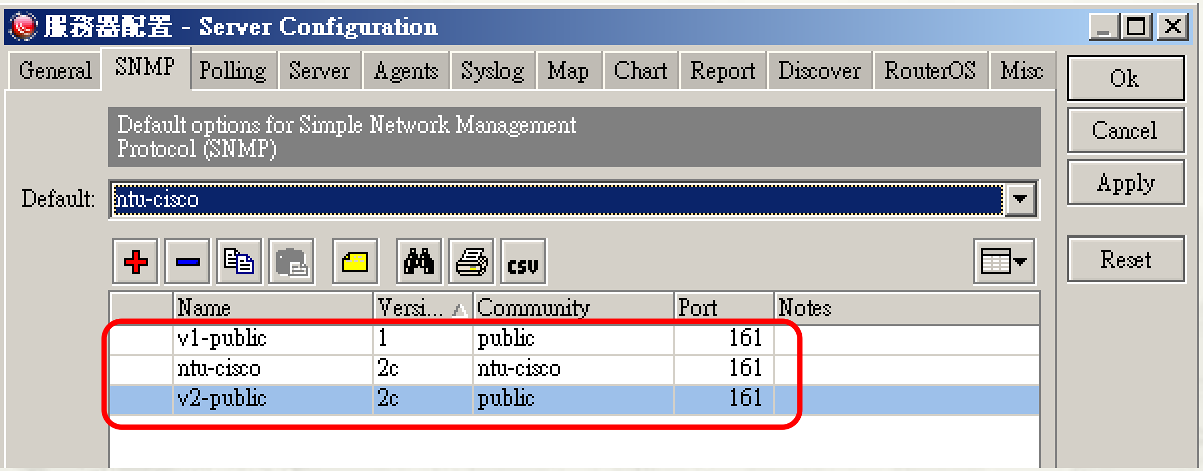
□ Router OS

□ Dude Server

Services: 🟩 Up - 2

Status: up

SNMP Profile Setup

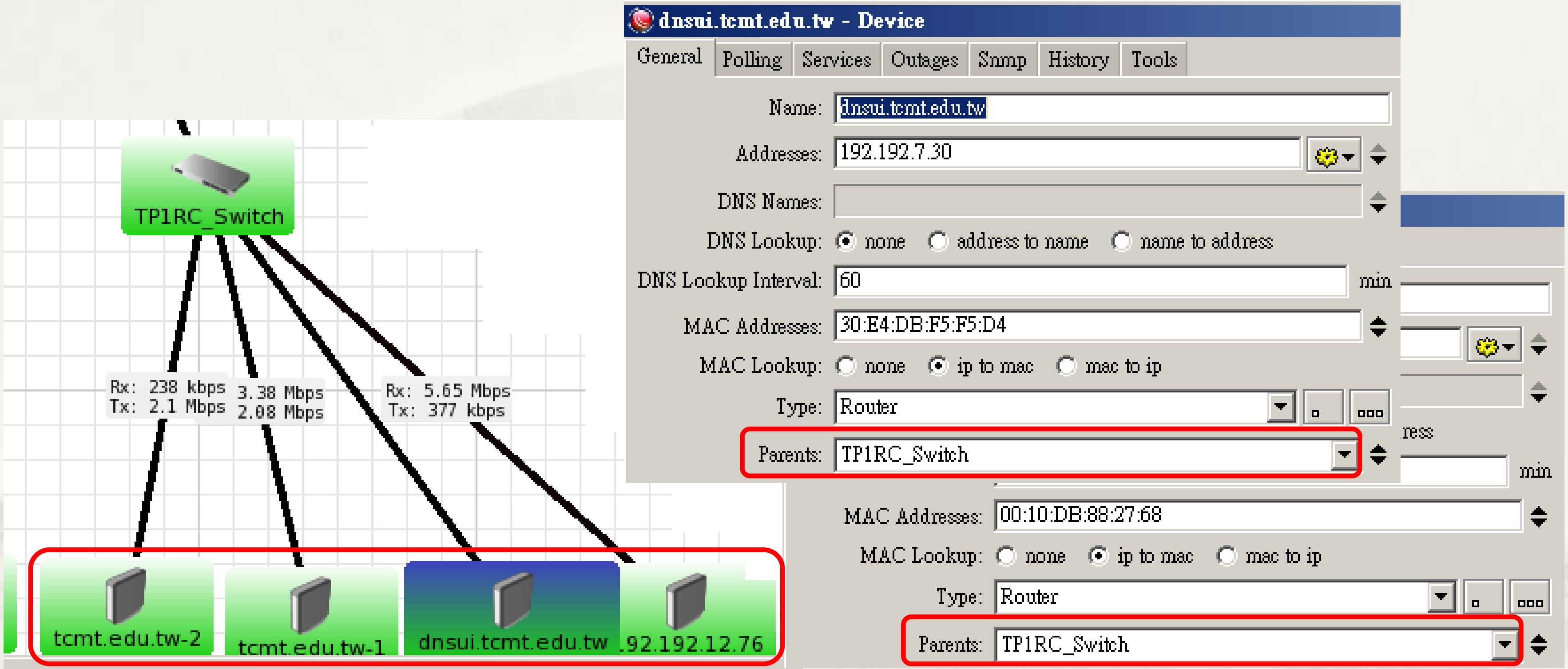


Default options for Simple Network Management Protocol (SNMP)

Default: ntu-cisco

Name	Versi...	Community	Port	Notes
v1-public	1	public	161	
ntu-cisco	2c	ntu-cisco	161	
v2-public	2c	public	161	

Parents of Device



dnsui.tcmt.edu.tw - Device

General | Polling | Services | Outages | Snmp | History | Tools

Name: dnsui.tcmt.edu.tw

Addresses: 192.192.7.30

DNS Names:

DNS Lookup: ● none ○ address to name ○ name to address

DNS Lookup Interval: 60 min

MAC Addresses: 30:E4:DB:F5:F5:D4

MAC Lookup: ○ none ● ip to mac ○ mac to ip

Type: Router

Parents: TP1RC_Switch

MAC Addresses: 00:10:DB:88:27:68

MAC Lookup: ○ none ● ip to mac ○ mac to ip

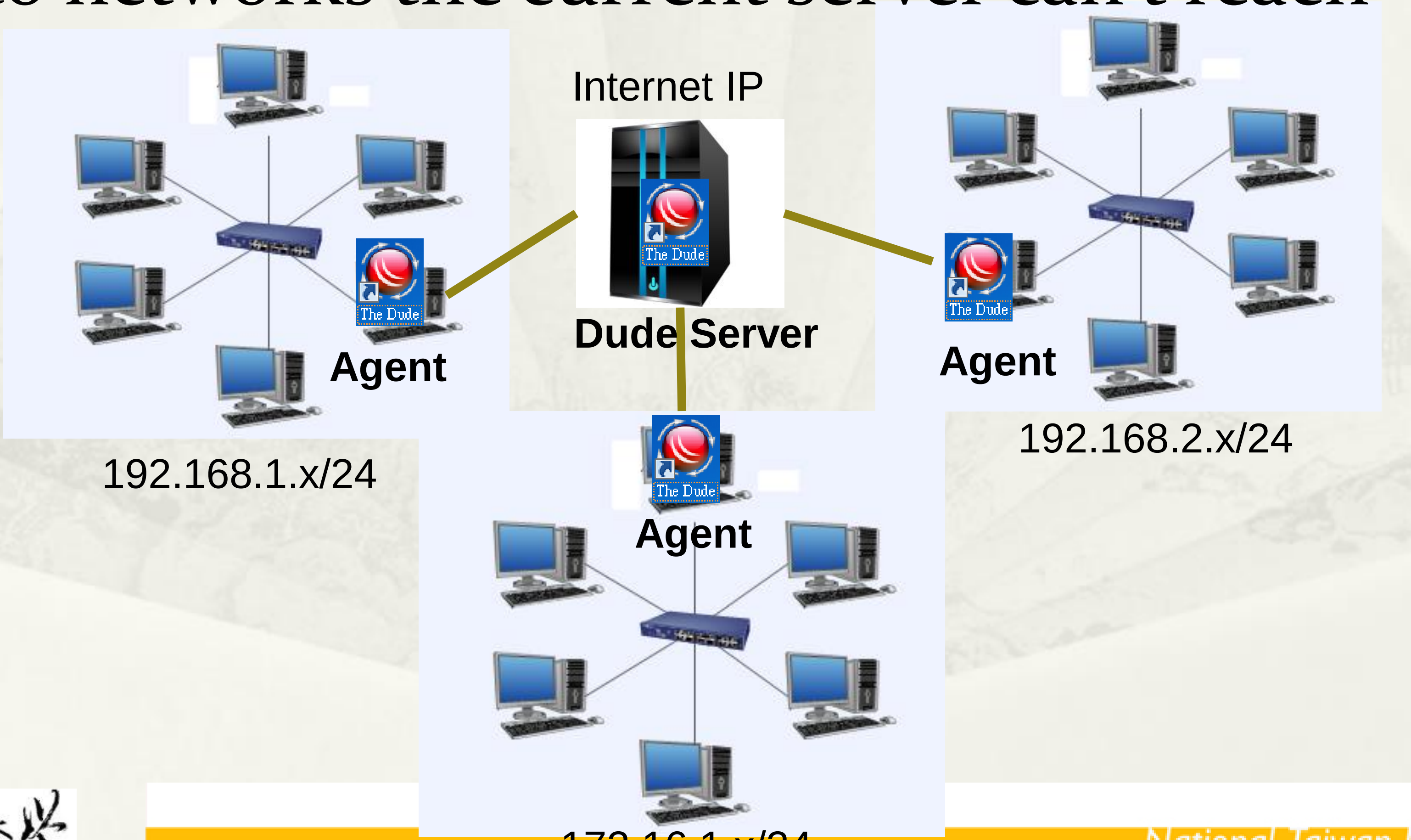
Type: Router

Parents: TP1RC_Switch

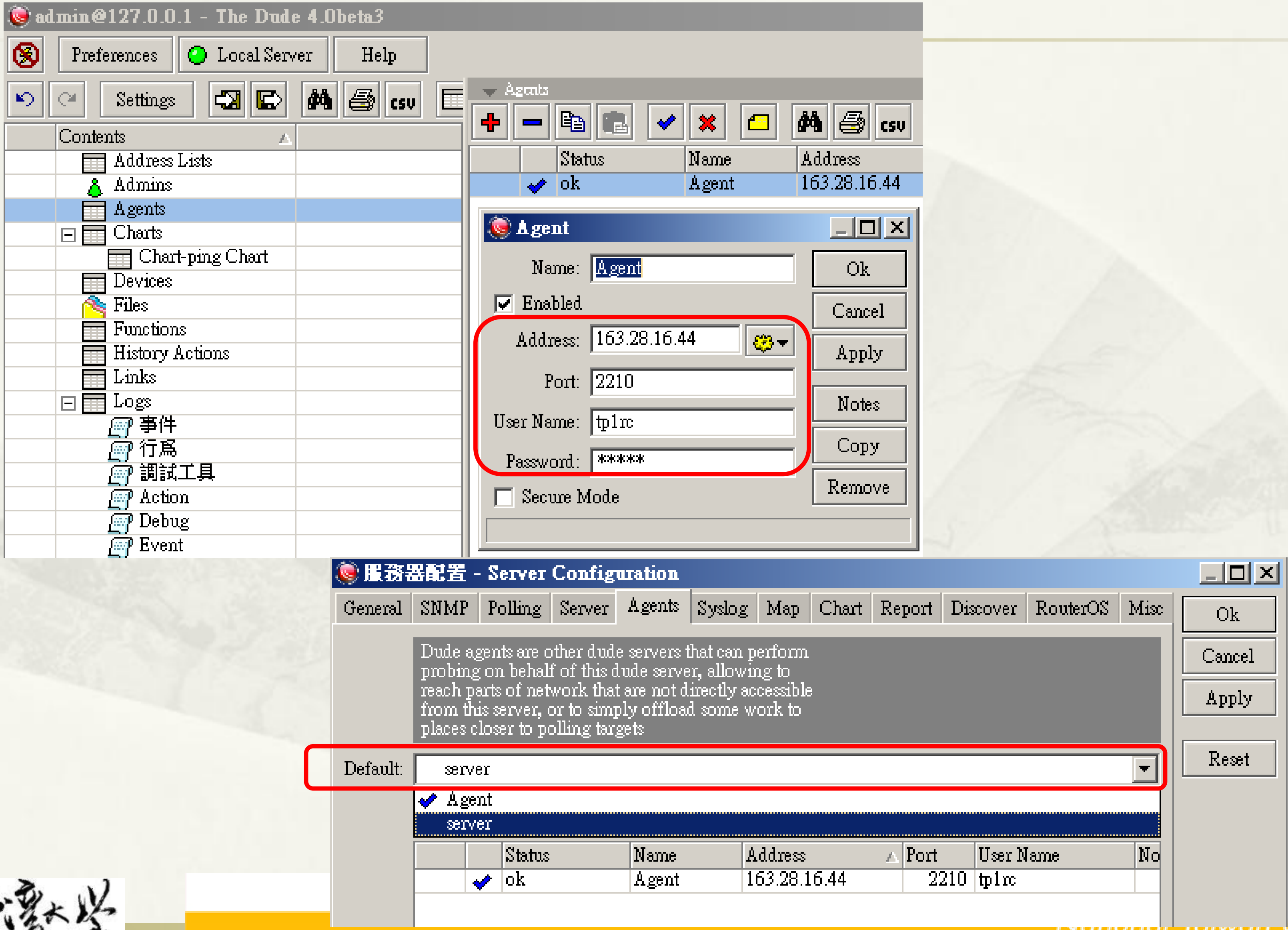
- Parents: Which device is the hierarchical parent of this one, builds reachability dependencies to avoid multiple notifications in case parent device fails (in which case child devices are also unreachable)

Agent Concept

- Agent: Other Dude servers that have acess to networks the current server can't reach



Agents setup



	Status	Name	Address
✓	ok	Agent	163.28.16.44

Name: Agent

☑ Enabled

Address: 163.28.16.44

Port: 2210

User Name: tp1rc

Password: *****

□ Secure Mode

Dude agents are other dude servers that can perform probing on behalf of this dude server, allowing to reach parts of network that are not directly accessible from this server, or to simply offload some work to places closer to polling targets

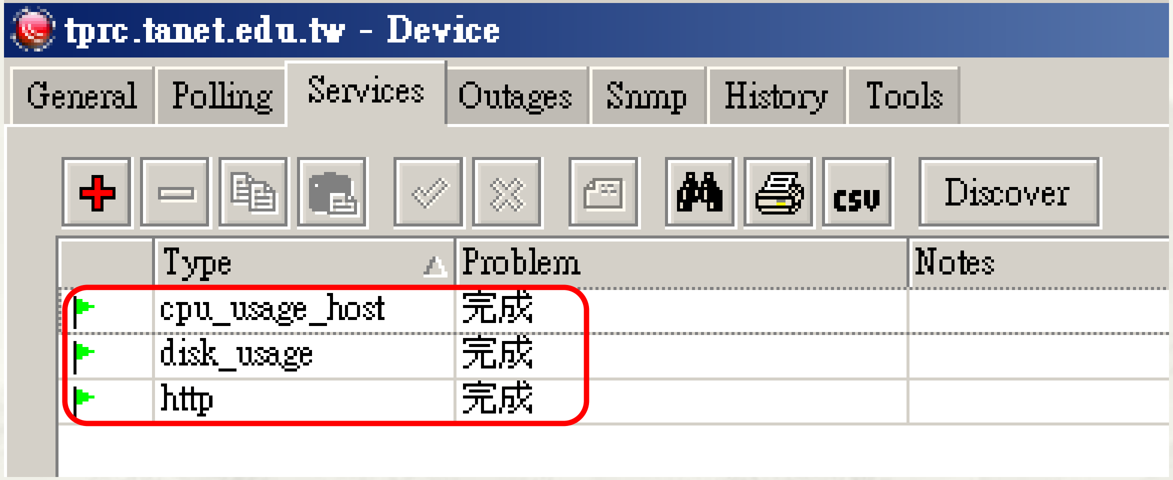
Default: server

✓ Agent

server

	Status	Name	Address	Port	User Name	No
✓	ok	Agent	163.28.16.44	2210	tp1rc	

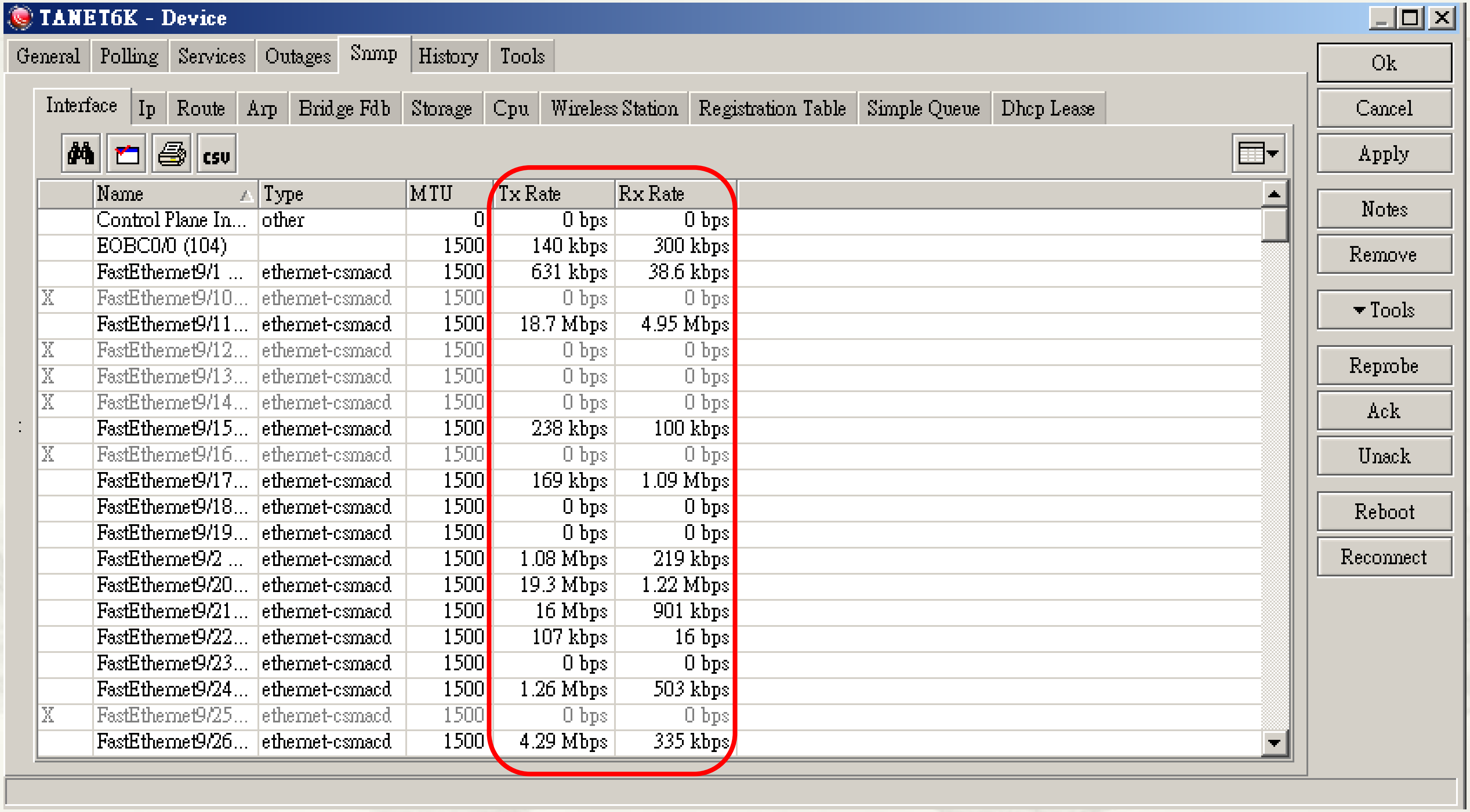
Device 設定 - Services



	Type	Problem	Notes
	cpu_usage_host	完成	
	disk_usage	完成	
	http	完成	

- 同時設定多種偵測方式

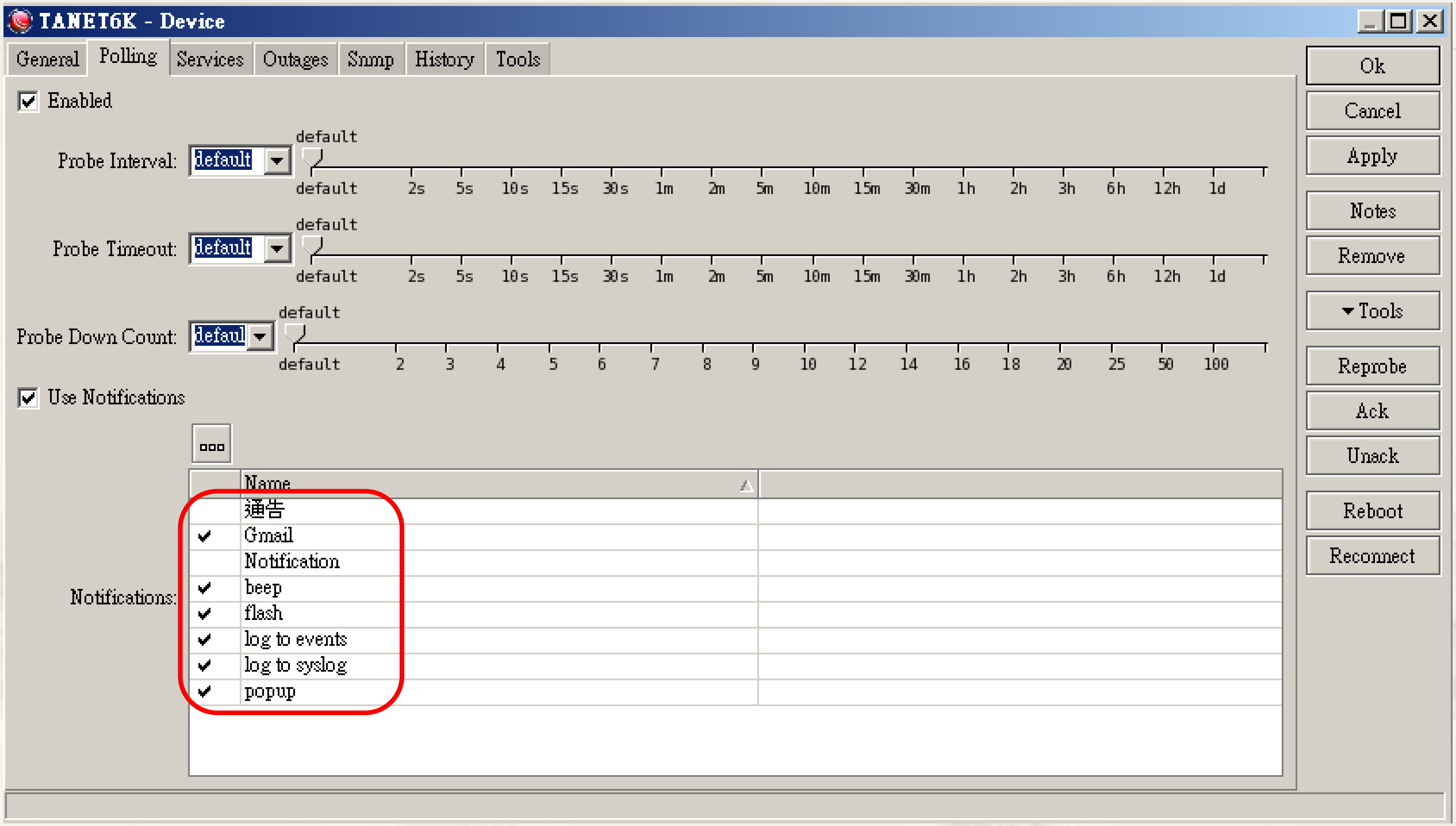
Device 設定-Snmp



	Name	Type	MTU	Tx Rate	Rx Rate
	Control Plane In...	other	0	0 bps	0 bps
	EOBC0/0 (104)		1500	140 kbps	300 kbps
	FastEthernet9/1 ...	ethernet-csmacd	1500	631 kbps	38.6 kbps
X	FastEthernet9/10...	ethernet-csmacd	1500	0 bps	0 bps
	FastEthernet9/11...	ethernet-csmacd	1500	18.7 Mbps	4.95 Mbps
X	FastEthernet9/12...	ethernet-csmacd	1500	0 bps	0 bps
X	FastEthernet9/13...	ethernet-csmacd	1500	0 bps	0 bps
X	FastEthernet9/14...	ethernet-csmacd	1500	0 bps	0 bps
	FastEthernet9/15...	ethernet-csmacd	1500	238 kbps	100 kbps
X	FastEthernet9/16...	ethernet-csmacd	1500	0 bps	0 bps
	FastEthernet9/17...	ethernet-csmacd	1500	169 kbps	1.09 Mbps
	FastEthernet9/18...	ethernet-csmacd	1500	0 bps	0 bps
	FastEthernet9/19...	ethernet-csmacd	1500	0 bps	0 bps
	FastEthernet9/2 ...	ethernet-csmacd	1500	1.08 Mbps	219 kbps
	FastEthernet9/20...	ethernet-csmacd	1500	19.3 Mbps	1.22 Mbps
	FastEthernet9/21...	ethernet-csmacd	1500	16 Mbps	901 kbps
	FastEthernet9/22...	ethernet-csmacd	1500	107 kbps	16 bps
	FastEthernet9/23...	ethernet-csmacd	1500	0 bps	0 bps
	FastEthernet9/24...	ethernet-csmacd	1500	1.26 Mbps	503 kbps
X	FastEthernet9/25...	ethernet-csmacd	1500	0 bps	0 bps
	FastEthernet9/26...	ethernet-csmacd	1500	4.29 Mbps	335 kbps

- 顯示 SNMP 相關資訊: Interface 即時流量

Device 設定--Notification


TANET6K - Device

General
Polling
Services
Outages
Snmp
History
Tools
Ok
Cancel
Apply
Notes
Remove
Tools
Reprobe
Ack
Unack
Reboot
Reconnect
default
default 2s 5s 10s 15s 30s 1m 2m 5m 10m 15m 30m 1h 2h 3h 6h 12h 1d
default
default 2s 5s 10s 15s 30s 1m 2m 5m 10m 15m 30m 1h 2h 3h 6h 12h 1d
default
default 2 3 4 5 6 7 8 9 10 12 14 16 18 20 25 50 100
ooo

☑ Enabled

Probe Interval: default

Probe Timeout: default

Probe Down Count: defaul

☑ Use Notifications

Notifications:

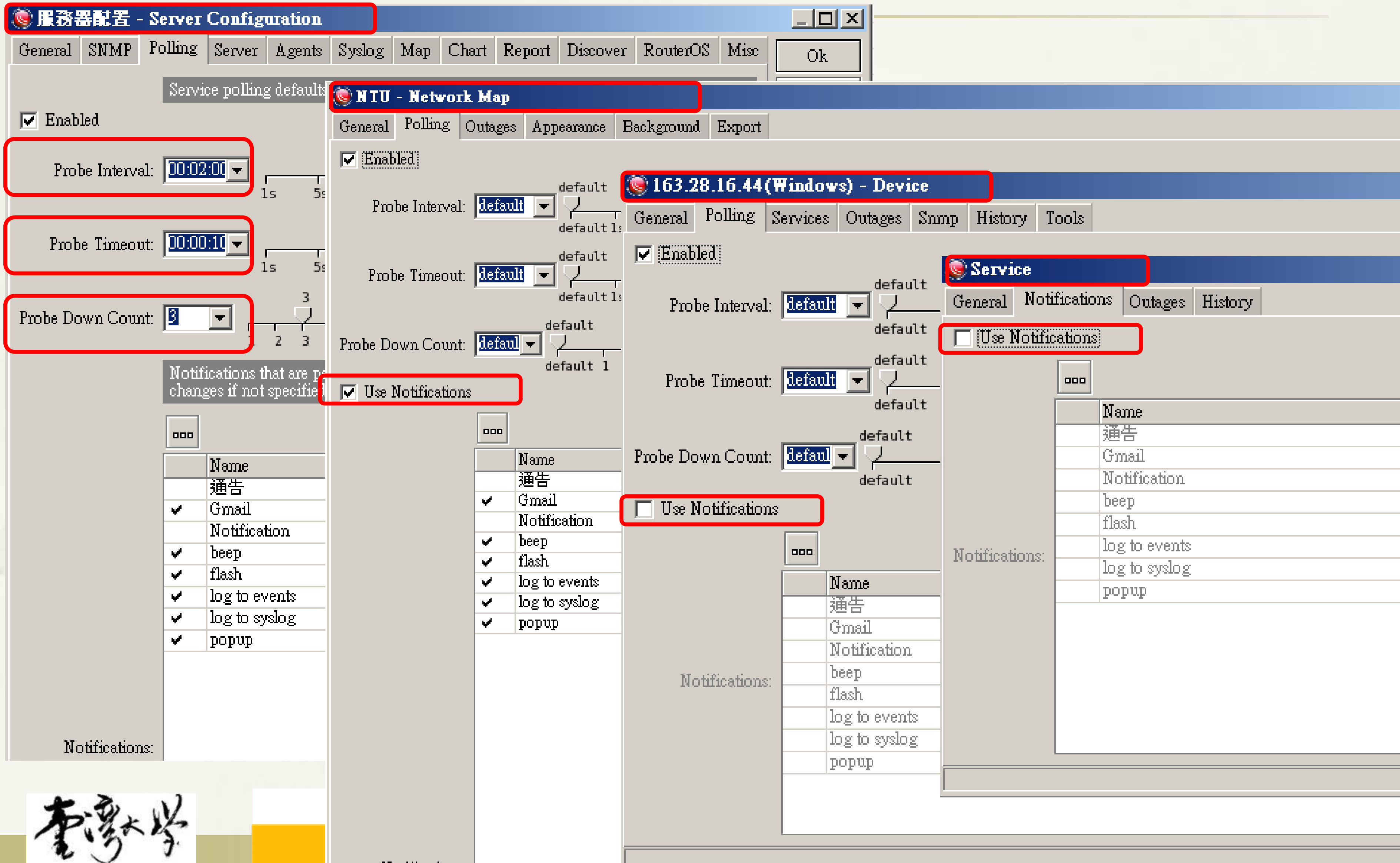
	Name
	通告
✓	Gmail
	Notification
✓	beep
✓	flash
✓	log to events
✓	log to syslog
✓	popup

- 異常發生通知方式

Polling/Notification Setup Level 1/2

- Level: 越下層優先權越高
  - Server Configuration
  - Network Map
  - Node
  - Service
- 若無勾選 Use Notifications, 則以上一層之設定為準.
- 若勾選 Use Notifications, 則必須選擇特定之 Notifications, 若無勾選則視同無 Notifications.
- Polling 之概念相同.

Polling/Notification Setup Level 2/2



服務器配置 - Server Configuration

General | SNMP | Polling | Server | Agents | Syslog | Map | Chart | Report | Discover | RouterOS | Misc

Ok

Service polling defaults

☑ Enabled

Probe Interval: 00:02:00

Probe Timeout: 00:00:10

Probe Down Count: 3

Notifications that are p
changes if not specifie

Notifications:

	Name
	通告
✓	Gmail
	Notification
✓	beep
✓	flash
✓	log to events
✓	log to syslog
✓	popup

NTU - Network Map

General | Polling | Outages | Appearance | Background | Export

☑ Enabled

Probe Interval: default

Probe Timeout: default

Probe Down Count: defaul

☑ Use Notifications

	Name
	通告
✓	Gmail
	Notification
✓	beep
✓	flash
✓	log to events
✓	log to syslog
✓	popup

163.28.16.44(Windows) - Device

General | Polling | Services | Outages | Snmp | History | Tools

☑ Enabled

Probe Interval: default

Probe Timeout: default

Probe Down Count: defaul

□ Use Notifications

Notifications:

	Name
	通告
	Gmail
	Notification
	beep
	flash
	log to events
	log to syslog
	popup

Service

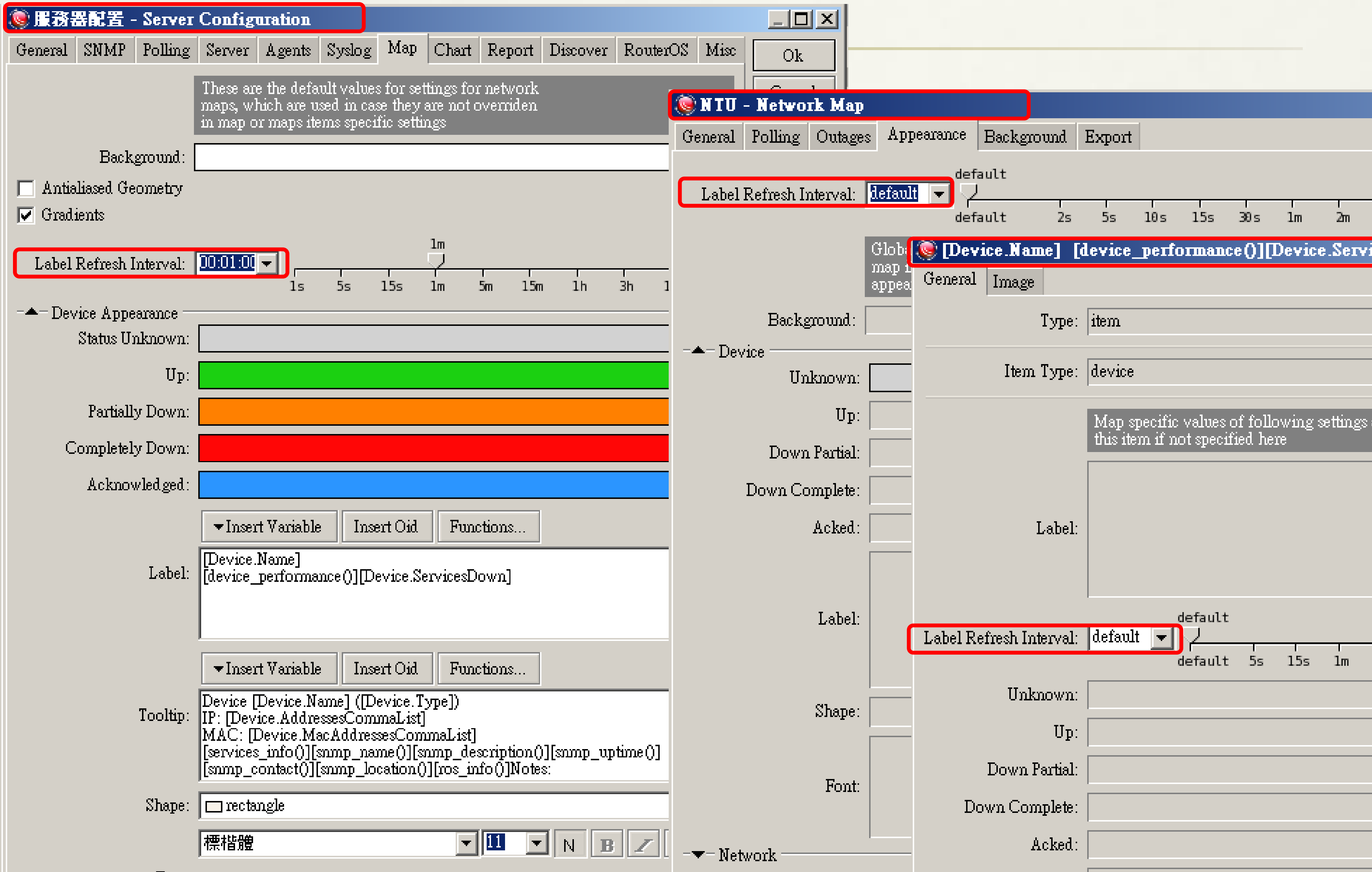
General | Notifications | Outages | History

□ Use Notifications

Notifications:

	Name
	通告
	Gmail
	Notification
	beep
	flash
	log to events
	log to syslog
	popup

Appearance Setup Level



These are the default values for settings for network maps, which are used in case they are not overriden in map or maps items specific settings

Background:

□ Antialiased Geometry

☑ Gradients

Label Refresh Interval: 00:01:00

Device Appearance

Status Unknown:

Up: 🟩

Partially Down: 🟧

Completely Down: 🟥

Acknowledged: 🟦

Label: [Device.Name]
[device_performance()][Device.ServicesDown]

Tooltip: Device [Device.Name] ([Device.Type])
IP: [Device.AddressesCommaList]
MAC: [Device.MacAddressesCommaList]
[services_info()][snmp_name()][snmp_description()][snmp_uptime()]
[snmp_contact()][snmp_location()][ros_info()]Notes:

Shape: rectangle

標楷體 11

Label Refresh Interval: default

Background:

Device

Unknown:

Up:

Down Partial:

Down Complete:

Acked:

Label:

Shape:

Font:

Network

Type: item

Item Type: device

Map specific values of following settings this item if not specified here

Label:

Label Refresh Interval: default

Unknown:

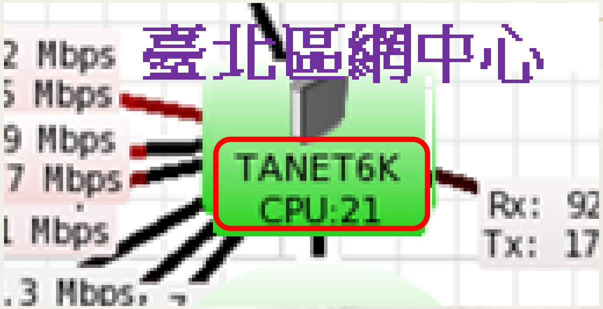
Up:

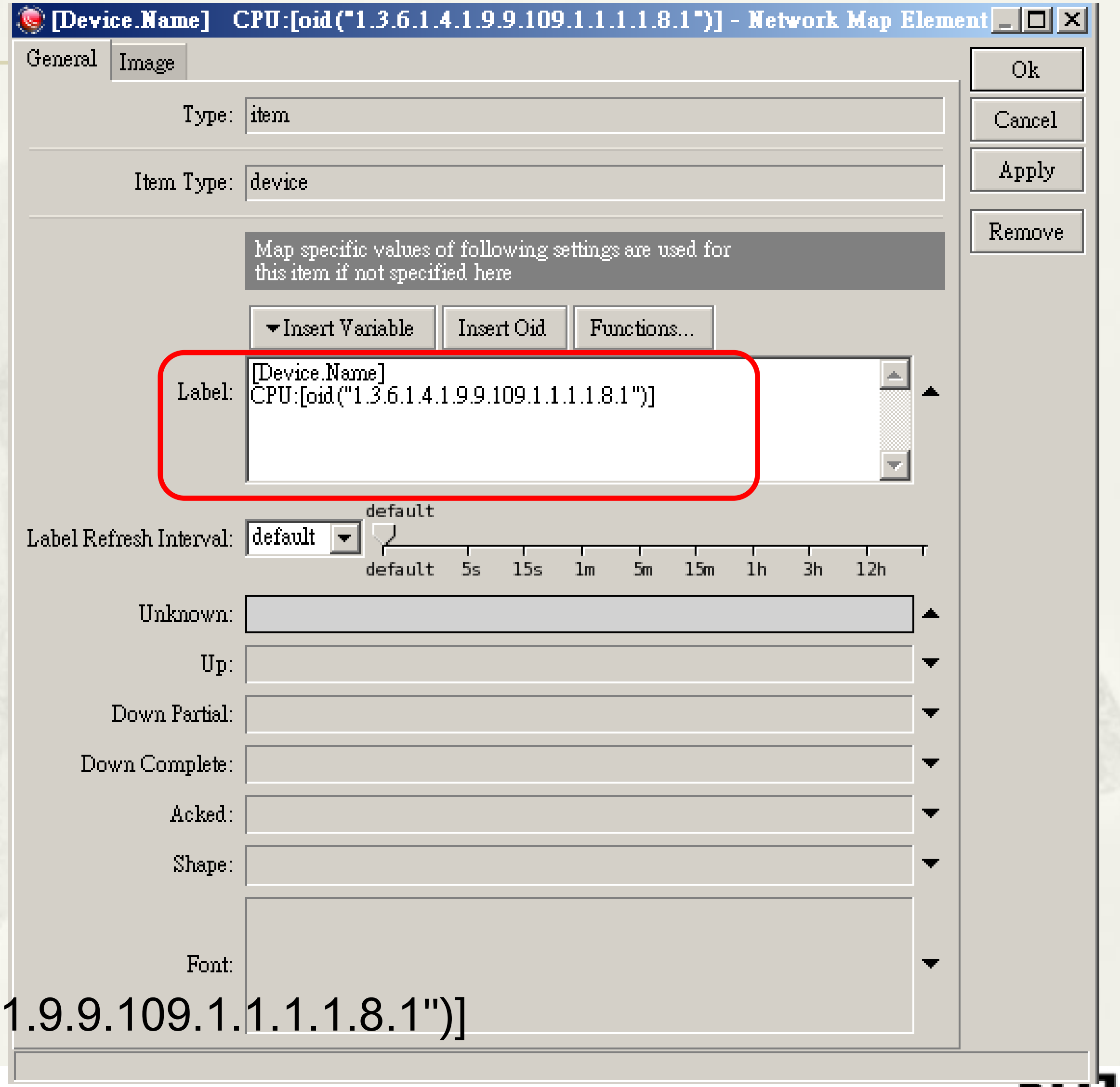
Down Partial:

Down Complete:

Acked:

Appearance–顯示Cisco CPU Load




[Device.Name] CPU:[oid("1.3.6.1.4.1.9.9.109.1.1.1.1.8.1")] - Network Map Element

Type: item

Item Type: device

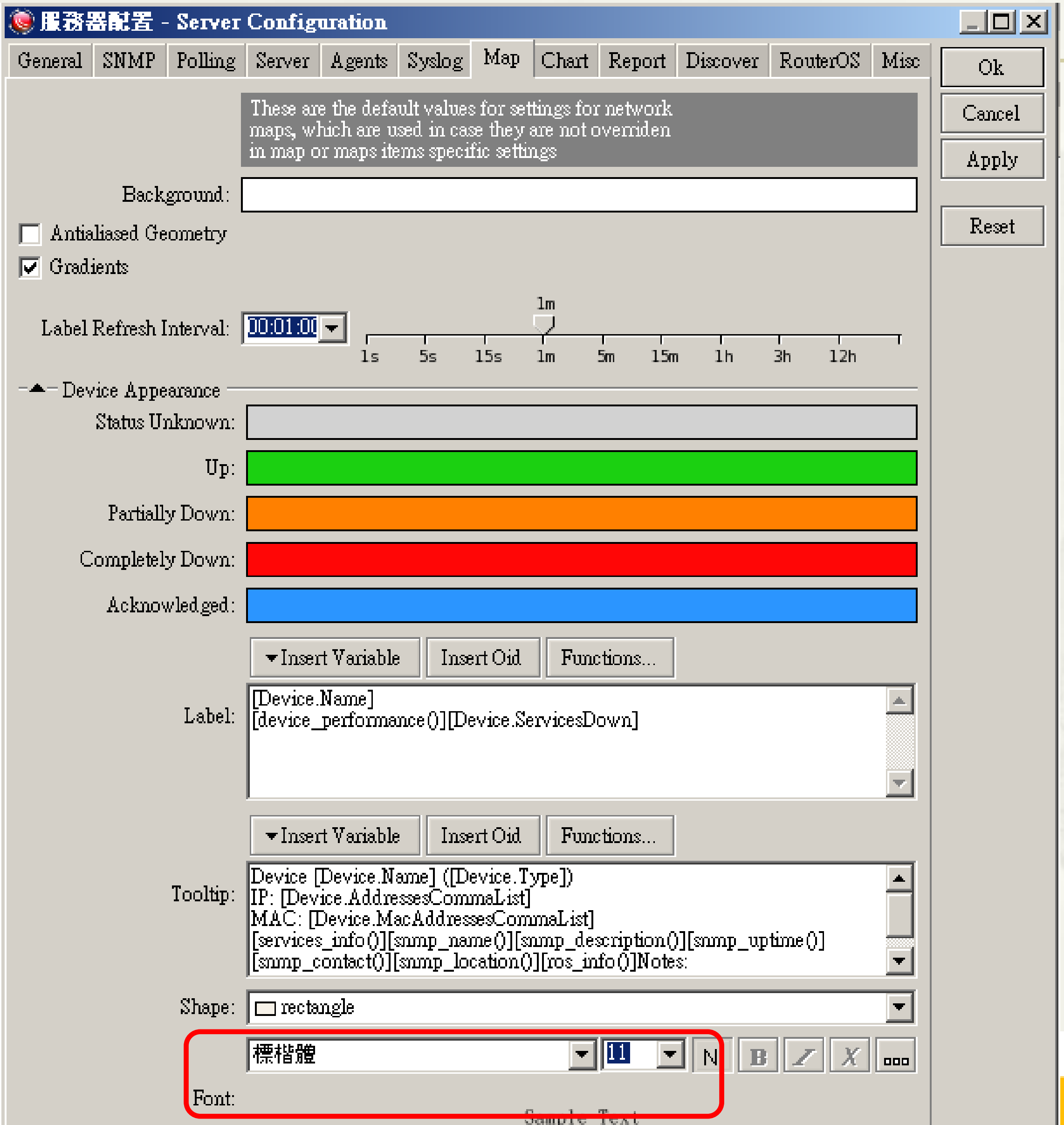
Map specific values of following settings are used for this item if not specified here

Label: [Device.Name]
CPU:[oid("1.3.6.1.4.1.9.9.109.1.1.1.1.8.1")]

Label Refresh Interval: default

[Device.Name]
CPU:[oid(“1.3.6.1.4.1.9.9.109.1.1.1.1.8.1")]

Appearance - 中文亂碼解決



These are the default values for settings for network maps, which are used in case they are not overriden in map or maps items specific settings

Background:

□ Antialiased Geometry

☑ Gradients

Label Refresh Interval: 00:01:00

Device Appearance

Status Unknown:

Up: 🟩

Partially Down: 🟧

Completely Down: 🟥

Acknowledged: 🟦

Label: [Device.Name]
[device_performance()][Device.ServicesDown]

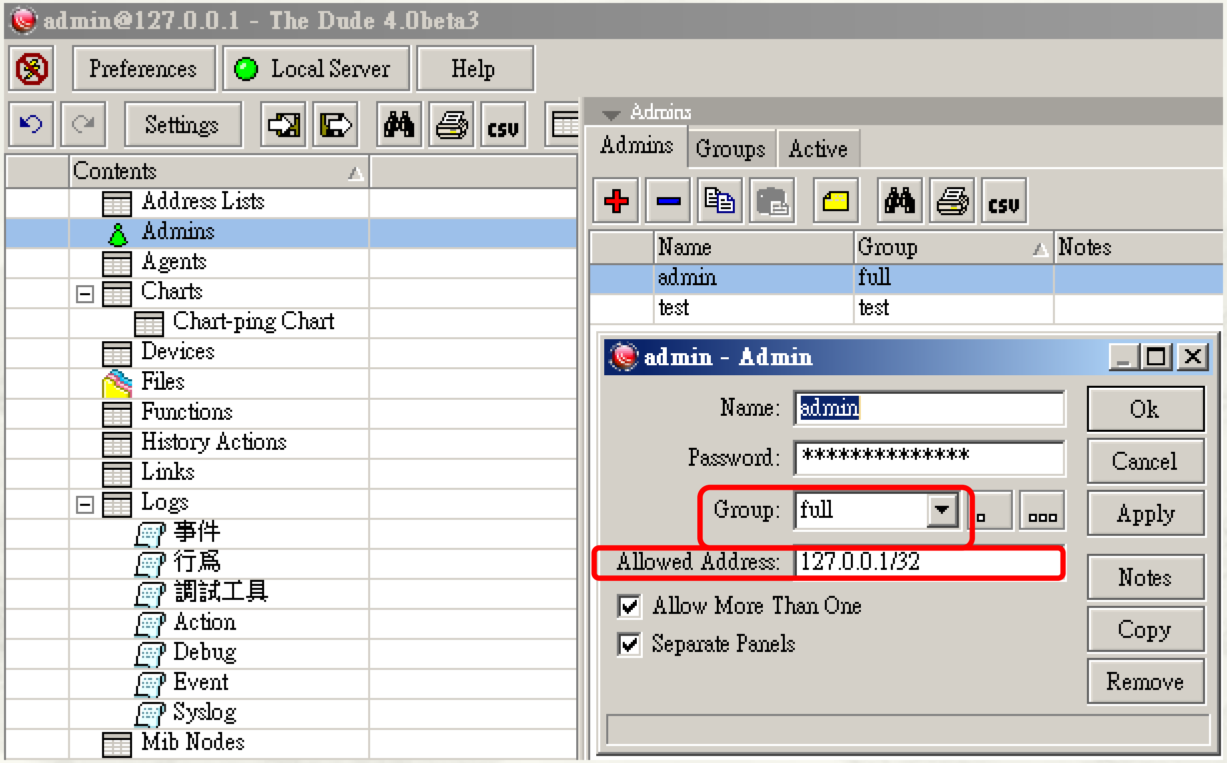
Tooltip: Device [Device.Name] ([Device.Type])
IP: [Device.AddressesCommaList]
MAC: [Device.MacAddressesCommaList]
[services_info()][snmp_name()][snmp_description()][snmp_uptime()]
[snmp_contact()][snmp_location()][ros_info()]Notes:

Shape: rectangle

Font: 標楷體 11

- 增加標楷體
- Copy C:\Windows\Fonts\kaiu.ttf to C:\Program Files (x86)\Dude\data\files

Admins: login user



admin@127.0.0.1 - The Dude 4.0beta3

Name	Group	Notes
admin	full	
test	test	

admin - Admin

Name: admin

Password: **************

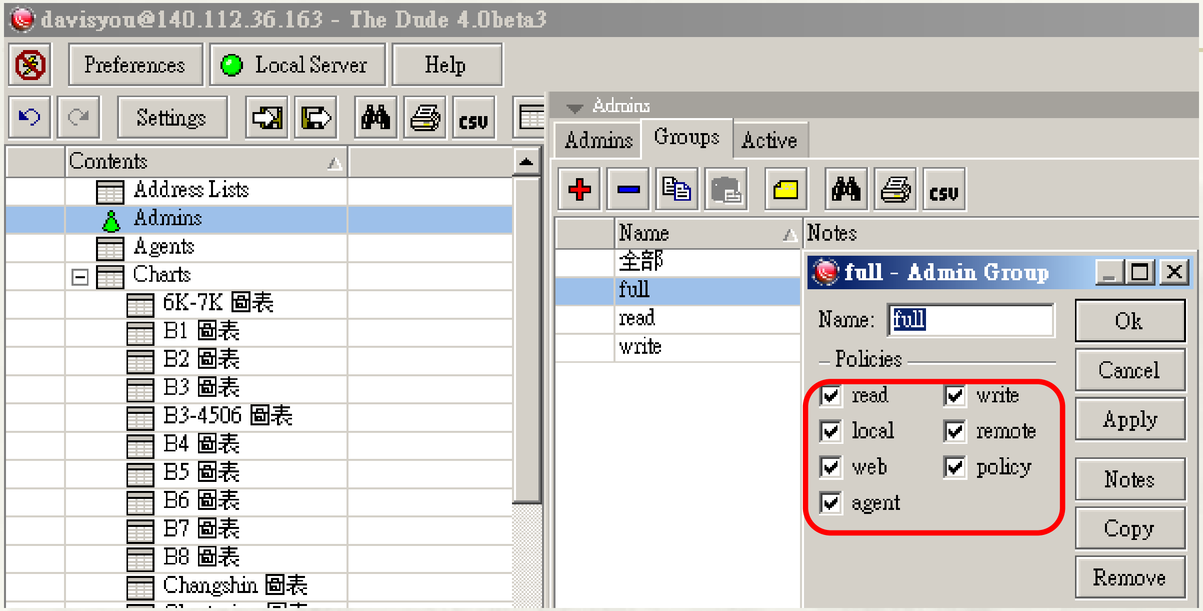
Group: full

Allowed Address: 127.0.0.1/32

☑ Allow More Than One

☑ Separate Panels

Admins: Groups



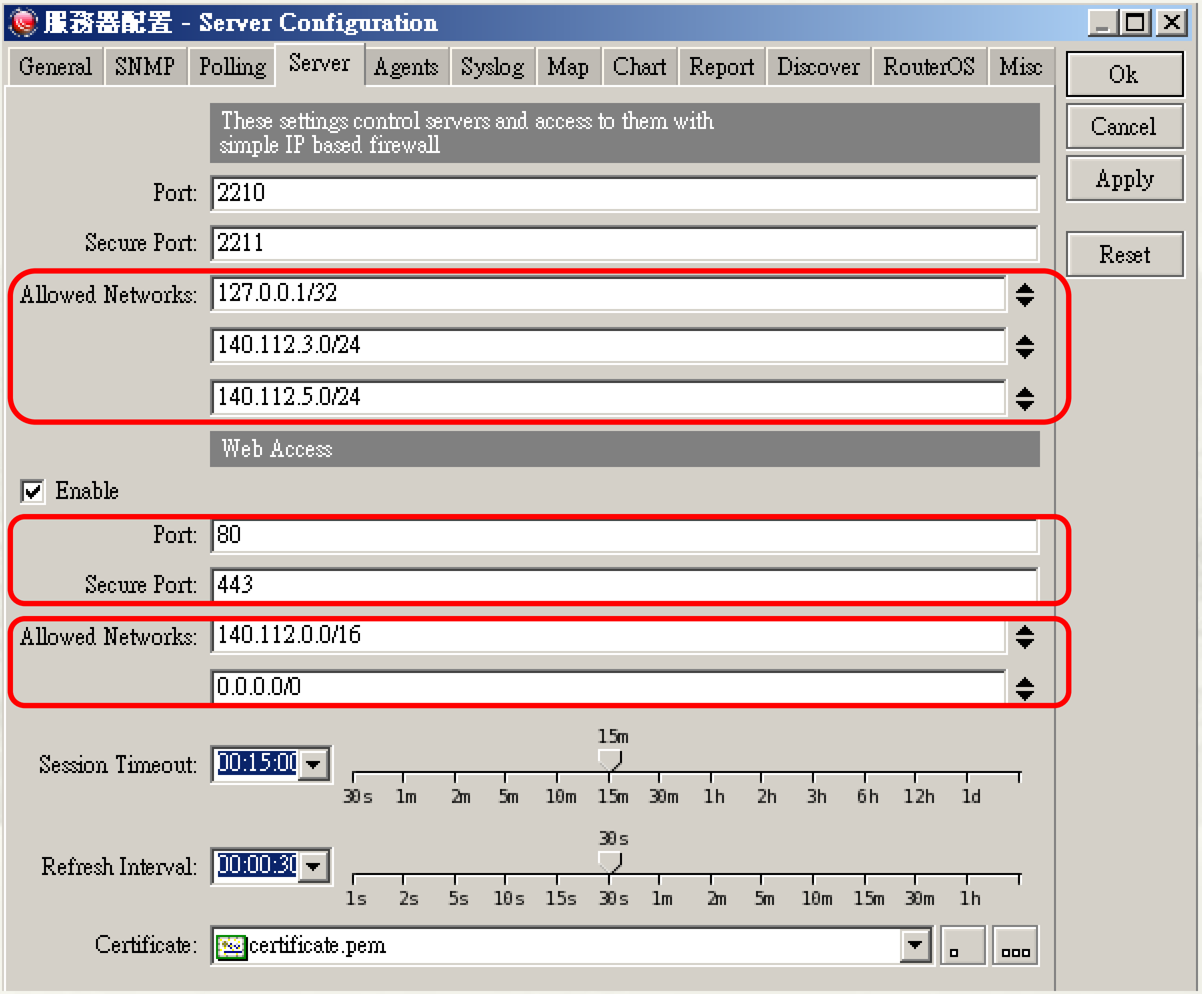
Name: full

Policies

- ☑ read
- ☑ write
- ☑ local
- ☑ remote
- ☑ web
- ☑ policy
- ☑ agent

- Read - can't change settings, only view them .
- Write - can't become Full user or connect as an agent (has no policy and agent rights)
- Local - connect to local server.
- Remote - connect to remote servers by specifying an address.
- Web - access to Web service
- Policy - changing of users and groups.
- Agent - connecting to remote dude as an Agent.

Server - Allowed Networks



These settings control servers and access to them with simple IP based firewall

Port: 2210

Secure Port: 2211

Allowed Networks: 127.0.0.1/32

140.112.3.0/24

140.112.5.0/24

Web Access

☑ Enable

Port: 80

Secure Port: 443

Allowed Networks: 140.112.0.0/16

0.0.0.0/0

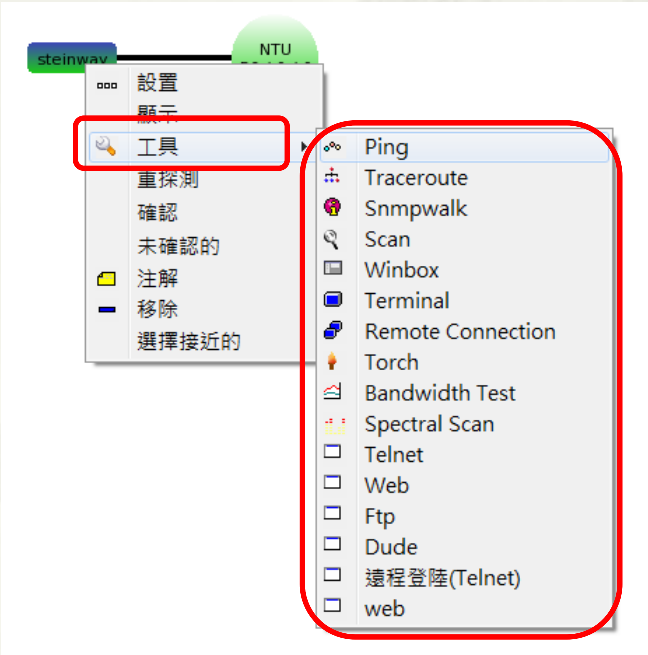
Session Timeout: 00:15:00

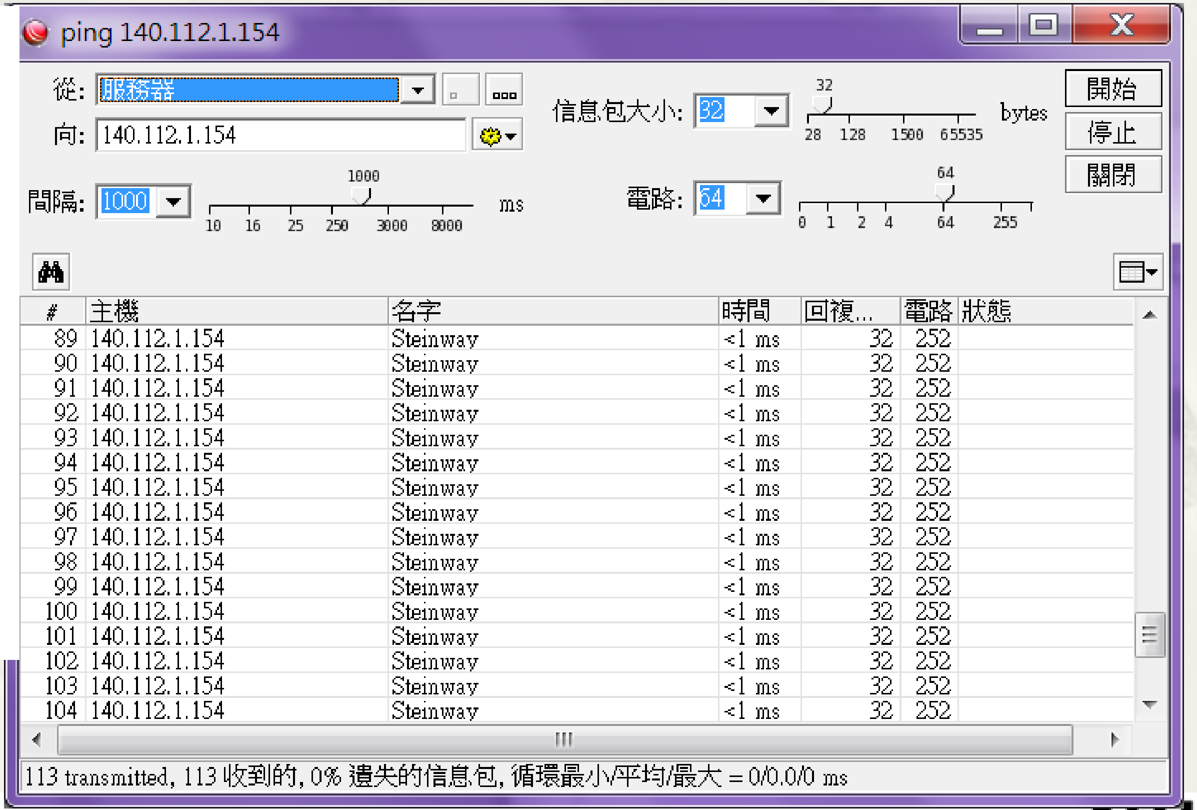
Refresh Interval: 00:00:30

Certificate: certificate.pem

常用網路查修工具

- 常用工具檢測網路狀況
  - Ping、Traceroute





ping 140.112.1.154

從: 服務器

向: 140.112.1.154

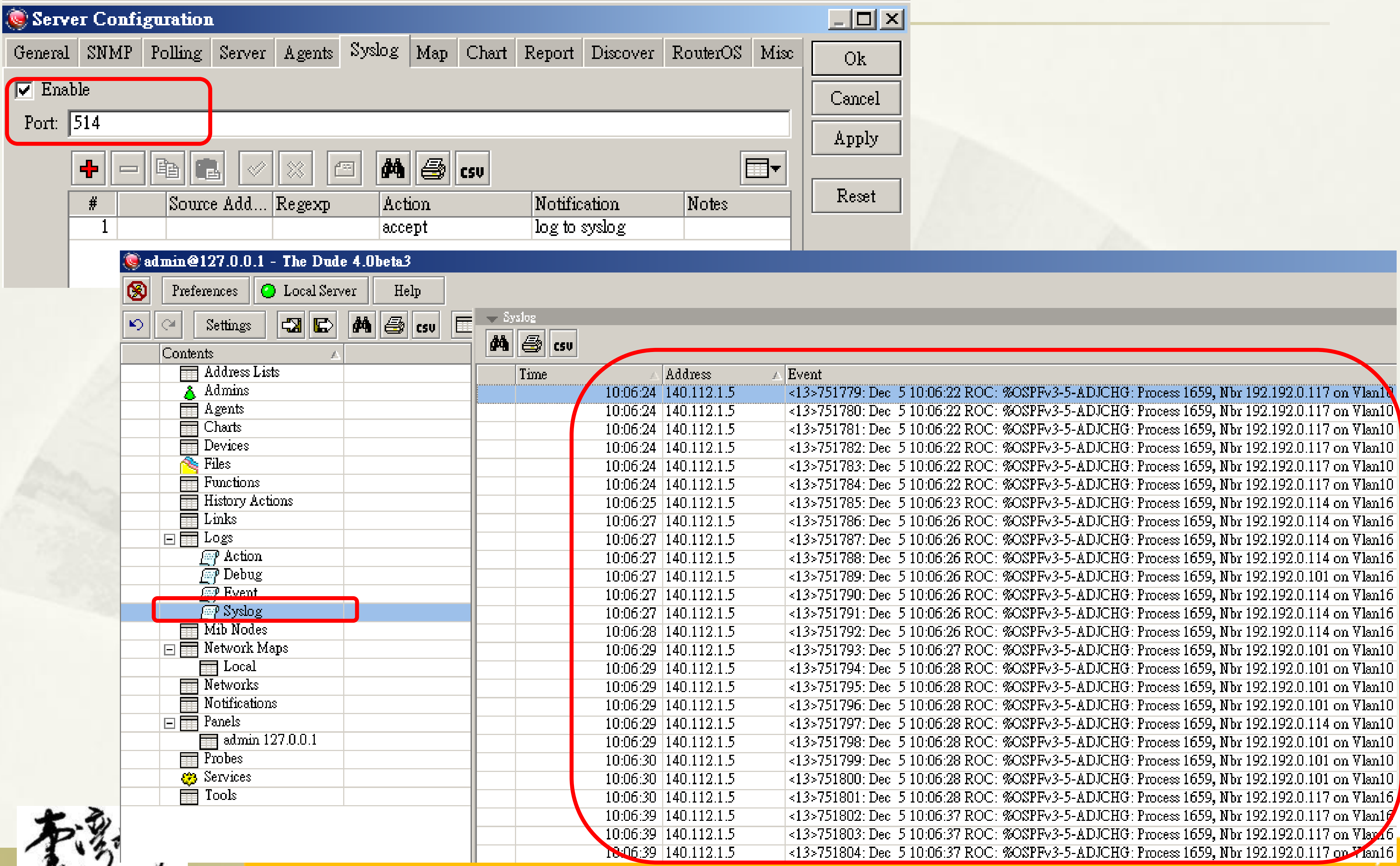
信息包大小: 32 bytes

間隔: 1000 ms

電路: 64

```
#    主機           名字       時間   回複... 電路 狀態
 89  140.112.1.154  Steinway   <1 ms    32   252
 90  140.112.1.154  Steinway   <1 ms    32   252
 91  140.112.1.154  Steinway   <1 ms    32   252
 92  140.112.1.154  Steinway   <1 ms    32   252
 93  140.112.1.154  Steinway   <1 ms    32   252
 94  140.112.1.154  Steinway   <1 ms    32   252
 95  140.112.1.154  Steinway   <1 ms    32   252
 96  140.112.1.154  Steinway   <1 ms    32   252
 97  140.112.1.154  Steinway   <1 ms    32   252
 98  140.112.1.154  Steinway   <1 ms    32   252
 99  140.112.1.154  Steinway   <1 ms    32   252
100  140.112.1.154  Steinway   <1 ms    32   252
101  140.112.1.154  Steinway   <1 ms    32   252
102  140.112.1.154  Steinway   <1 ms    32   252
103  140.112.1.154  Steinway   <1 ms    32   252
104  140.112.1.154  Steinway   <1 ms    32   252
113 transmitted, 113 收到的, 0% 遺失的信息包, 循環最小/平均/最大 = 0/0.0/0 ms
```

Syslog Server



☑ Enable

Port: 514

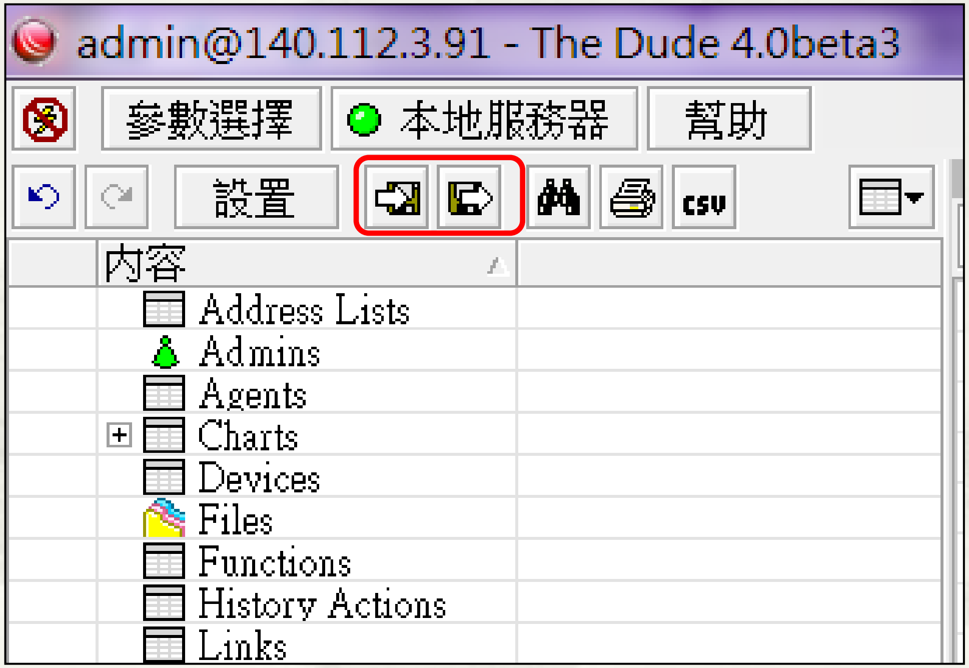
#		Source Add...	Regexp	Action	Notification	Notes
1				accept	log to syslog	

- Address Lists
- Admins
- Agents
- Charts
- Devices
- Files
- Functions
- History Actions
- Links
- Logs
  - Action
  - Debug
  - Event
  - Syslog
- Mib Nodes
- Network Maps
  - Local
- Networks
- Notifications
- Panels
  - admin 127.0.0.1
- Probes
- Services
- Tools

Time	Address	Event
10:06:24	140.112.1.5	<13>751779: Dec 5 10:06:22 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.117 on Vlan10
10:06:24	140.112.1.5	<13>751780: Dec 5 10:06:22 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.117 on Vlan10
10:06:24	140.112.1.5	<13>751781: Dec 5 10:06:22 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.117 on Vlan10
10:06:24	140.112.1.5	<13>751782: Dec 5 10:06:22 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.117 on Vlan10
10:06:24	140.112.1.5	<13>751783: Dec 5 10:06:22 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.117 on Vlan10
10:06:24	140.112.1.5	<13>751784: Dec 5 10:06:22 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.117 on Vlan10
10:06:25	140.112.1.5	<13>751785: Dec 5 10:06:23 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.114 on Vlan16
10:06:27	140.112.1.5	<13>751786: Dec 5 10:06:26 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.114 on Vlan16
10:06:27	140.112.1.5	<13>751787: Dec 5 10:06:26 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.114 on Vlan16
10:06:27	140.112.1.5	<13>751788: Dec 5 10:06:26 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.114 on Vlan16
10:06:27	140.112.1.5	<13>751789: Dec 5 10:06:26 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.101 on Vlan16
10:06:27	140.112.1.5	<13>751790: Dec 5 10:06:26 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.114 on Vlan16
10:06:27	140.112.1.5	<13>751791: Dec 5 10:06:26 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.114 on Vlan16
10:06:28	140.112.1.5	<13>751792: Dec 5 10:06:26 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.114 on Vlan16
10:06:29	140.112.1.5	<13>751793: Dec 5 10:06:27 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.101 on Vlan10
10:06:29	140.112.1.5	<13>751794: Dec 5 10:06:28 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.101 on Vlan10
10:06:29	140.112.1.5	<13>751795: Dec 5 10:06:28 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.101 on Vlan10
10:06:29	140.112.1.5	<13>751796: Dec 5 10:06:28 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.101 on Vlan10
10:06:29	140.112.1.5	<13>751797: Dec 5 10:06:28 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.114 on Vlan10
10:06:29	140.112.1.5	<13>751798: Dec 5 10:06:28 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.101 on Vlan10
10:06:30	140.112.1.5	<13>751799: Dec 5 10:06:28 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.101 on Vlan10
10:06:30	140.112.1.5	<13>751800: Dec 5 10:06:28 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.101 on Vlan10
10:06:30	140.112.1.5	<13>751801: Dec 5 10:06:28 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.117 on Vlan16
10:06:39	140.112.1.5	<13>751802: Dec 5 10:06:37 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.117 on Vlan16
10:06:39	140.112.1.5	<13>751803: Dec 5 10:06:37 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.117 on Vlan16
10:06:39	140.112.1.5	<13>751804: Dec 5 10:06:37 ROC: %OSPFv3-5-ADJCHG: Process 1659, Nbr 192.192.0.117 on Vlan16

監控軟體設定備份

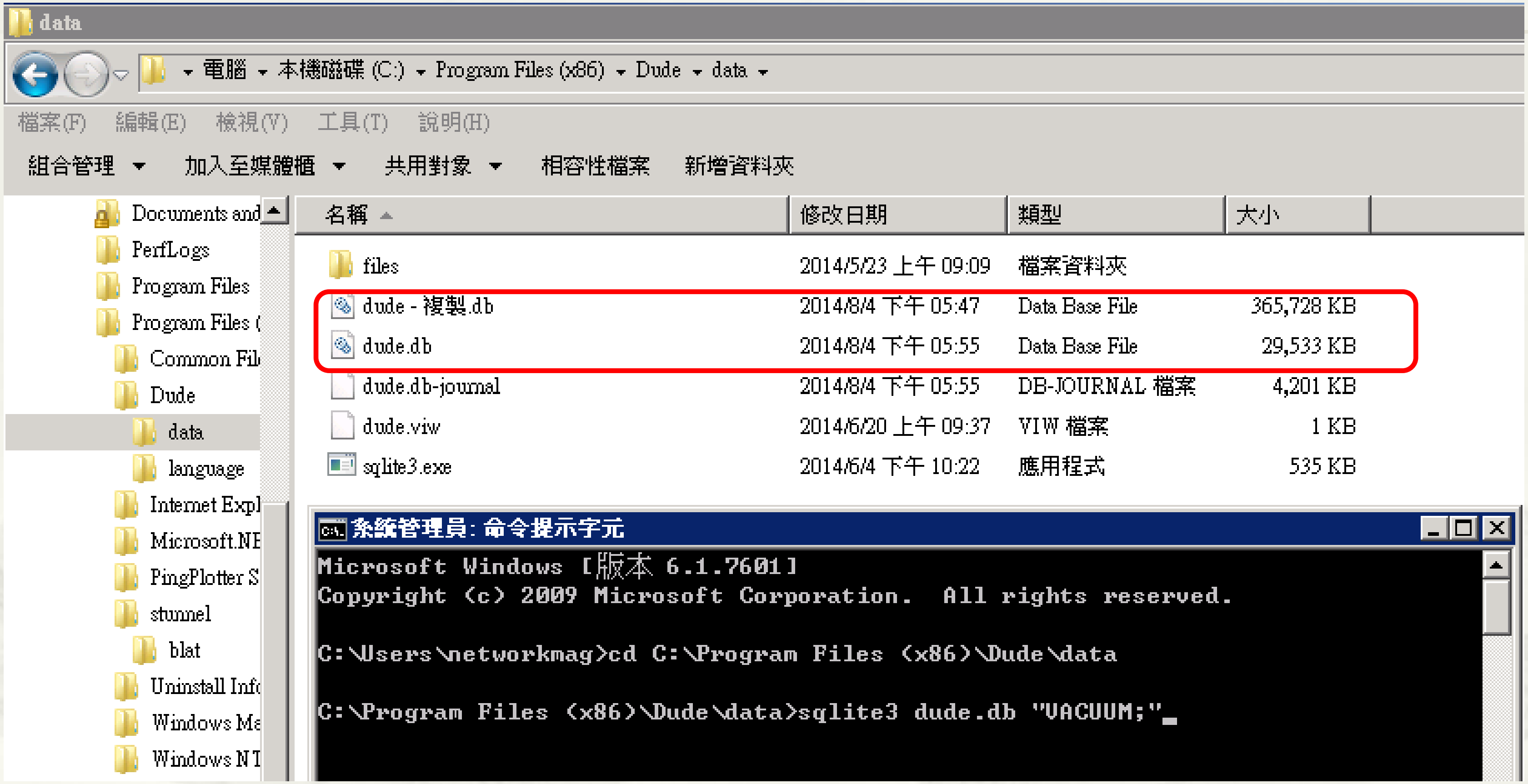
- 可以將監控的架構備份至檔案，以防遺失。



admin@140.112.3.91 - The Dude 4.0beta3

內容
Address Lists
Admins
Agents
Charts
Devices
Files
Functions
History Actions
Links

DB Optimization



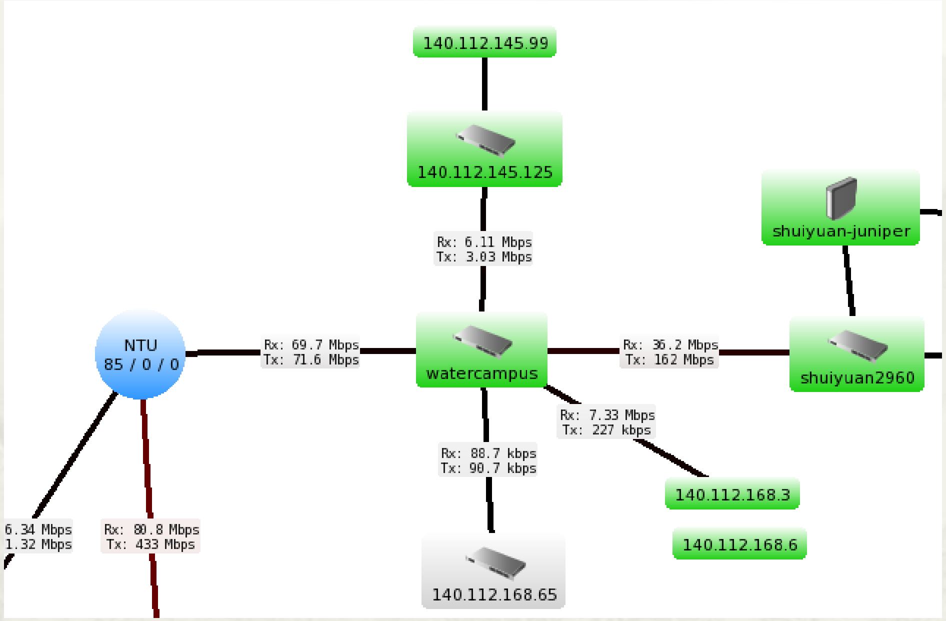
名稱	修改日期	類型	大小
files	2014/5/23 上午 09:09	檔案資料夾	
dude - 複製.db	2014/8/4 下午 05:47	Data Base File	365,728 KB
dude.db	2014/8/4 下午 05:55	Data Base File	29,533 KB
dude.db-journal	2014/8/4 下午 05:55	DB-JOURNAL 檔案	4,201 KB
dude.viw	2014/6/20 上午 09:37	VIW 檔案	1 KB
sqlite3.exe	2014/6/4 下午 10:22	應用程式	535 KB

```
Microsoft Windows [版本 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\networkmag>cd C:\Program Files (x86)\Dude\data

C:\Program Files (x86)\Dude\data>sqlite3 dude.db "VACUUM;"_
```

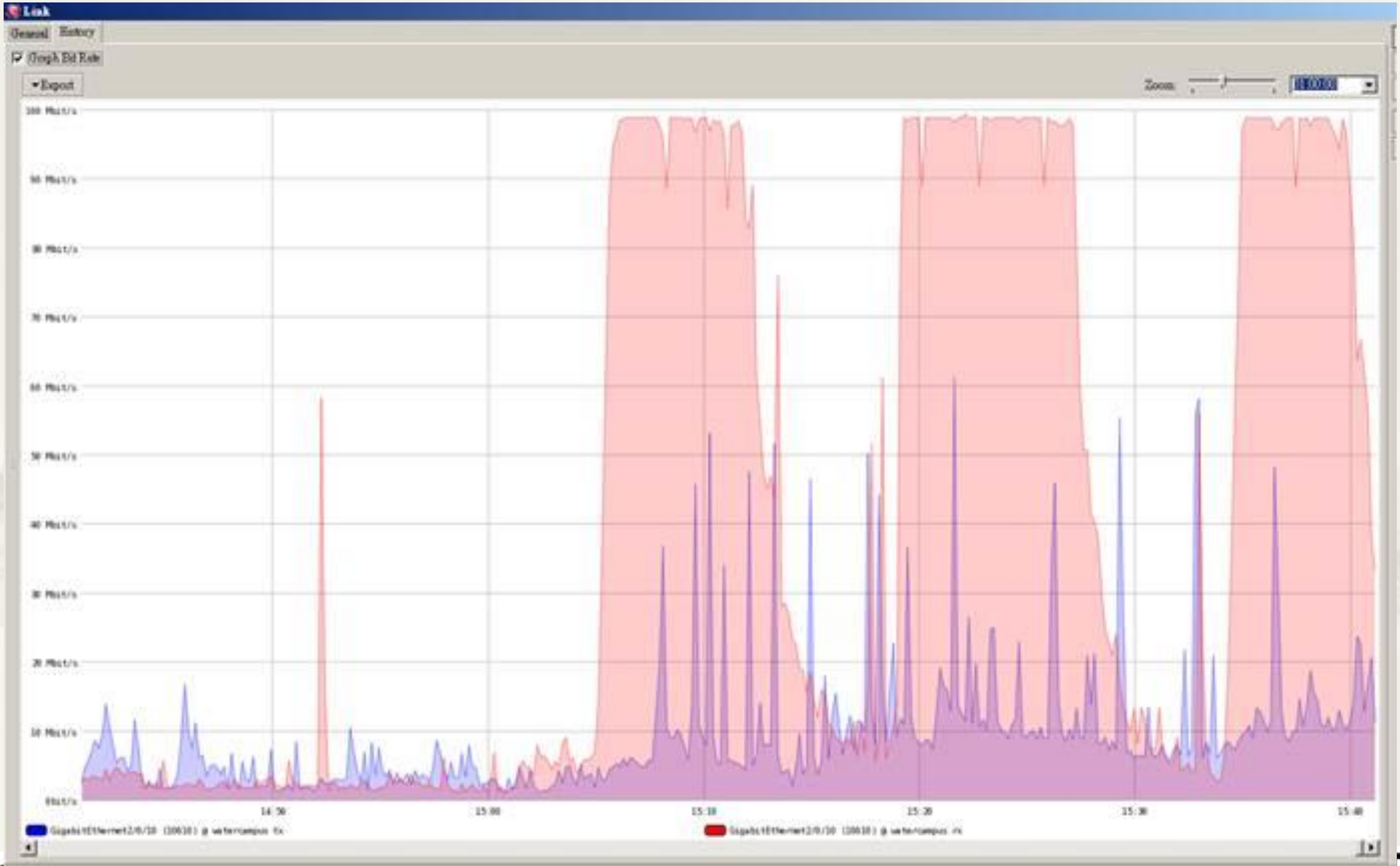
- http://www.sqlite.org/download.html
  - **Precompiled Binaries for Windows: sqlite-shell-win32-x86-3080500.zip**
- Compress DB
  - sqlite3 dude.db "VACUUM;"

簡報完畢
謝謝

Case Study


140.112.145.99
140.112.145.125
Rx: 6.11 Mbps
Tx: 3.03 Mbps
shuiyuan-juniper
NTU
85 / 0 / 0
Rx: 69.7 Mbps
Tx: 71.6 Mbps
watercampus
Rx: 36.2 Mbps
Tx: 162 Mbps
shuiyuan2960
Rx: 7.33 Mbps
Tx: 227 kbps
Rx: 88.7 kbps
Tx: 90.7 kbps
140.112.168.3
140.112.168.6
6.34 Mbps
1.32 Mbps
Rx: 80.8 Mbps
Tx: 433 Mbps
140.112.168.65

Case Study


Link
General
History
☑ Graph Bit Rate
▾ Export
Zoom
100 Mbit/s
90 Mbit/s
80 Mbit/s
70 Mbit/s
60 Mbit/s
50 Mbit/s
40 Mbit/s
30 Mbit/s
20 Mbit/s
10 Mbit/s
0bit/s
14:50
15:00
15:10
15:20
15:30
15:40
🟦 GigabitEthernet2/0/10 (10610) @ watercampus tx
🟥 GigabitEthernet2/0/10 (10610) @ watercampus rx

- 由以下情況判斷, G0/3 Port 佔據了 96% 之 Uplink 上傳頻寬.

```
Switch#sh int counters
Port         InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Gi0/1         2082901         4581             0             0
Gi0/2          403844          295             0             0
Gi0/3       345965276       319264            91            21
  --> 此 Port佔據了 96% 之 Uplink 上傳頻寬.
Gi0/20       37621472       194975           167           207

Port        OutOctets   OutUcastPkts   OutMcastPkts   OutBcastPkts
Gi0/1         1416620         5154          223           149
Gi0/2           87908          342          223           149
Gi0/3        34180984       183987           132           128
Gi0/20      358330002       328251            74            20   --> Uplink
```

- 但因為此 Port 之後應該還有接 Switch, 因此目前尚無法判斷是哪台電腦.

```
Switch#sh mac address-table | in 0/3
 10   000e.7fe1.9f68    DYNAMIC     Gi0/3
 10   000e.e301.92f9    DYNAMIC     Gi0/3
 10   0011.322d.038c    DYNAMIC     Gi0/3
 10   001a.6422.91eb    DYNAMIC     Gi0/3
 10   0024.8121.abd0    DYNAMIC     Gi0/3
 10   0860.6e47.06bf    DYNAMIC     Gi0/3
 10   0860.6e61.5464    DYNAMIC     Gi0/3
 10   10bf.48d6.aa27    DYNAMIC     Gi0/3
 10   10bf.48d6.abde    DYNAMIC     Gi0/3
 10   10fe.edab.177d    DYNAMIC     Gi0/3
 10   20cf.30ec.8a33    DYNAMIC     Gi0/3
 10   4061.86ec.2452    DYNAMIC     Gi0/3
 10   5046.5d51.88fd    DYNAMIC     Gi0/3
 10   5046.5d51.8a0c    DYNAMIC     Gi0/3
 10   60a4.4ccf.acdc    DYNAMIC     Gi0/3
 10   78e3.b5a0.3b91    DYNAMIC     Gi0/3
 10   b8a3.8649.96e9    DYNAMIC     Gi0/3
```

Sqlite -- Database Browser

- Database Browser 5.1.0.10
  - http://www.dbsoftlab.com/database-editors/database-browser/overview.html
  - Support Oracle, MS Sql Server, ODBC, MySql, OleDB, PostgreSQL, SQLite, MS Sql Server Compact, Interbase and Firebird