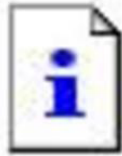




THE DUDE NOW & THE FUTURE

INTRODUCTION

ABOUT ROFIQ FAUZI



ERROR

This persons
picture is too cool
to display!

- MTCNA & MTC [all] E
- More than 10 year in Telco and Internet Industries
- 2012-Now, MikroTik Consultant & Trainer at [ID-Networkers](#).
- 2013-Now, Network Manager at small ISP in the small city
- 2013-Now, co-founder of IDNFoundation.org

CONSULTANT

<http://www.mikrotik.com/consultants/asia/indonesia>

CERTIFIED TRAINER

<http://www.mikrotik.com/training/partners/asia/indonesia>

ABOUT IDNFOUNDATION.ORG



- NGO as Yayasan IDN – Kemenkumham No. AHU – 0025185. AH .01.04 tahun 2016
- Program
 - ✓ Sekolah (SMP & SMK IDN Madinatul Ilmi)
 - ✓ Pesantren Networking & Programming (program pelatihan 1 tahun untuk lulusan SMK 1 tahun)
 - ✓ Pelatihan gratis untuk guru-guru SMK TKJ

PESANTREN NETWORKING & PROGRAMMING



SMP & SMK IDN MADINATUL ILMI

6



www.idn.sch.id

TRAINING GURU SMK

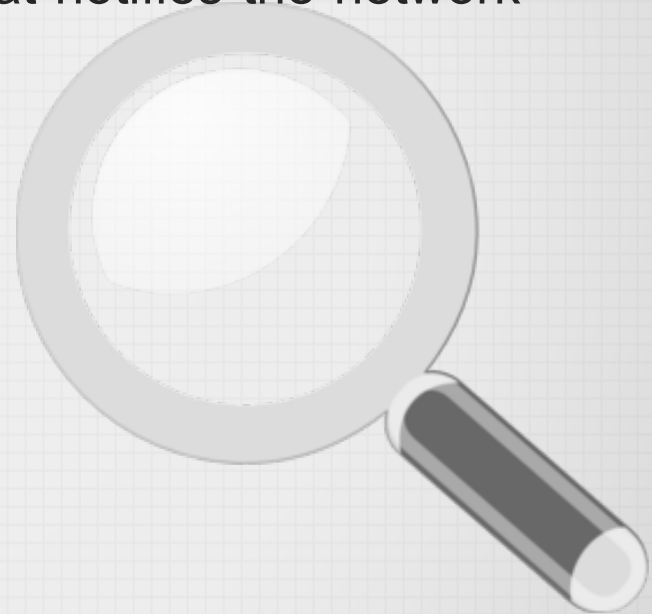
7



NETWORK MONITORING

WHAT IS NETWORK MONITORING

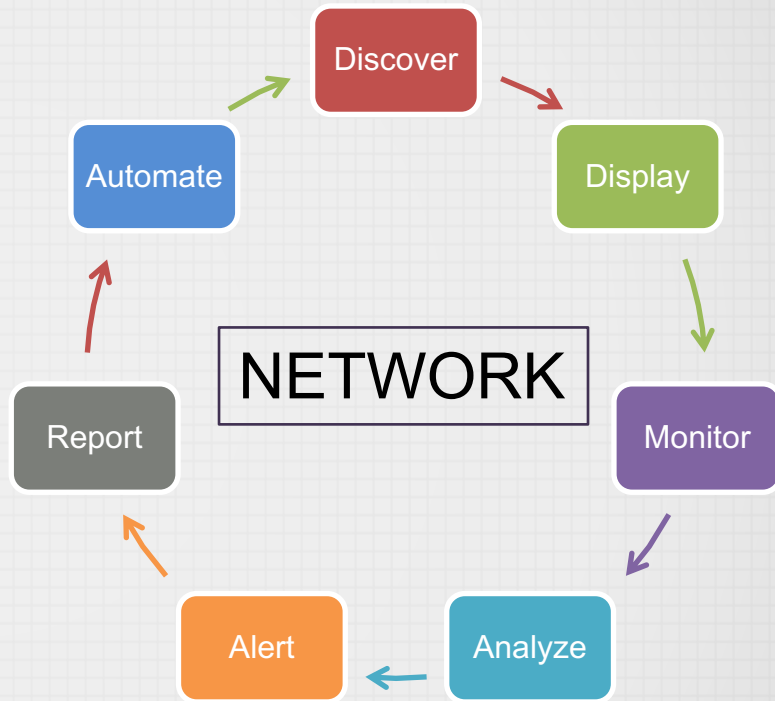
Network monitoring is a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator



WHAT IS NETWORK MONITORING?



Image from www.freepik.com



WHY WE NEED NETWORK MONITORING?



WHY WE NEED NETWORK MONITORING?



Guys, there is an unplugged ethernet cable

Go fix it!!

Image from www.pinterest.com

WHAT ITS USE FOR?

- **Fault Detection:**
 - Discovering, locating, early warning and logging the failures.
- **Configuration:**
 - Maintain consistent configuration.
 - Record any configuration changes
- **Accounting:**
 - Resource /usage monitoring (bandwidth) for correct billing.
- **Performance:**
 - Diagnostic utilization of existing resources, for finding ways to increase performance in the future.
- **Security Assurance and Protection:**
 - Controlling access to the network

LIST OF NETWORK MONITORING SYSTEM

The Nagios logo, featuring the word "Nagios" in a bold, black, sans-serif font with a registered trademark symbol.The SolarWinds logo, featuring the word "solarwinds" in a lowercase, sans-serif font next to a stylized orange flame or wing icon.The Splunk logo, featuring the word "splunk" in a lowercase, sans-serif font followed by a green greater-than symbol.The Zabbix logo, featuring the word "ZABBIX" in white, uppercase letters on a red rectangular background.The Zenoss logo, featuring the word "zenoss" in a lowercase, sans-serif font with a stylized orange 'o'.The Netmon logo, featuring the word "netmon" in a blue, lowercase, sans-serif font with a blue double arrow icon above it.The WhatsUpGold logo, featuring the text "WhatsUpGold" in a green, sans-serif font.

https://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems



QUIZ?

15

WHAT IS THE SIMPLEST NETWORK MONITORING TOOL

PING AND TRACEROUTE

- **Ping**
 - measure the time for a packet to travel back from remote host to us
- **Traceroute**
 - list the router hops between us and a remote host.
 - The IP address and domain name (if there is one) of each router is returned to us

PING

```
mac:~ ropix$ ping 8.8.8.8
```

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
```

```
64 bytes from 8.8.8.8: icmp_seq=0 ttl=43 time=224.472 ms
```

```
64 bytes from 8.8.8.8: icmp_seq=1 ttl=43 time=206.019 ms
```

```
64 bytes from 8.8.8.8: icmp_seq=2 ttl=43 time=192.759 ms
```

```
64 bytes from 8.8.8.8: icmp_seq=3 ttl=43 time=84.939 ms
```

```
64 bytes from 8.8.8.8: icmp_seq=4 ttl=43 time=54.392 ms
```

```
64 bytes from 8.8.8.8: icmp_seq=5 ttl=43 time=24.057 ms
```

```
64 bytes from 8.8.8.8: icmp_seq=6 ttl=43 time=31.974 ms
```



Respond time from
8.8.8.8 to our pc



TTL = Time to live

TRACEROUTE

```
mac:~ ropix$ traceroute detik.com
```

```
traceroute: Warning: detik.com has multiple addresses; using 103.49.221.211
```

```
traceroute to detik.com (103.49.221.211), 64 hops max, 52 byte packets
```

```
1 192.168.2.1 (192.168.2.1)  7.568 ms  2.346 ms  1.384 ms
2 192.168.1.1 (192.168.1.1)  8.758 ms  74.343 ms  7.884 ms
3 10.90.0.1 (10.90.0.1)  2.805 ms  3.487 ms  3.013 ms
4 172.16.88.33 (172.16.88.33)  5.365 ms
  172.16.88.29 (172.16.88.29)  9.179 ms
  172.16.88.33 (172.16.88.33)  2.959 ms
5 172.16.88.134 (172.16.88.134)  2.926 ms
  172.16.88.146 (172.16.88.146)  3.245 ms
  172.16.88.134 (172.16.88.134)  10.214 ms
6 * * *
7 tengiga-0-0.openixp.net (218.100.27.128)  57.063 ms  3.339 ms  3.265 ms
8 detik.openixp.net (218.100.36.9)  3.949 ms  10.155 ms  3.713 ms
9 203.190.244.34 (203.190.244.34)  7.879 ms  3.556 ms  3.671 ms
10 103.49.221.211 (103.49.221.211)  4.602 ms  3.744 ms  3.911 ms
```

Number of hop from
laptop to detik.com

For **KIDs** Jaman NOW

**WHAT IS THE LAZIEST WAY FOR
MONITORING THE NETWORK ?**

THE LAZIEST



When the music stops playing, mean internet is down

THE DUDE

WHAT IS THE DUDE?

- free application by *Mikro**Tik*** , which can dramatically improve the way you manage your network environment.

THE DUDE MAIN FEATURES

- Draw and layout a map of your networks
- Supports various network monitoring tasks from simple ping checks to port probes and service checks.
- Support SNMP to access traffic individual link usage monitoring and graphs.
- Direct access to remote control tools for device management.
- Support syslog server.

WHY THE DUDE?

PRTO Network Monitor Price List

LICENSE	SENSORS	PRICE
Freeware Edition	100	Free
30 Day Trial	not restricted*	Free for 30 days
500	500	\$1,600.00
1000	1000	\$2,850.00
2500	2500	\$6,150.00
5000	5000	\$10,500.00
XL1/Unlimited 	not restricted*	\$16,900.00
XL5/Unlimited 	not restricted*	\$60,000.00

BUY NOW >>

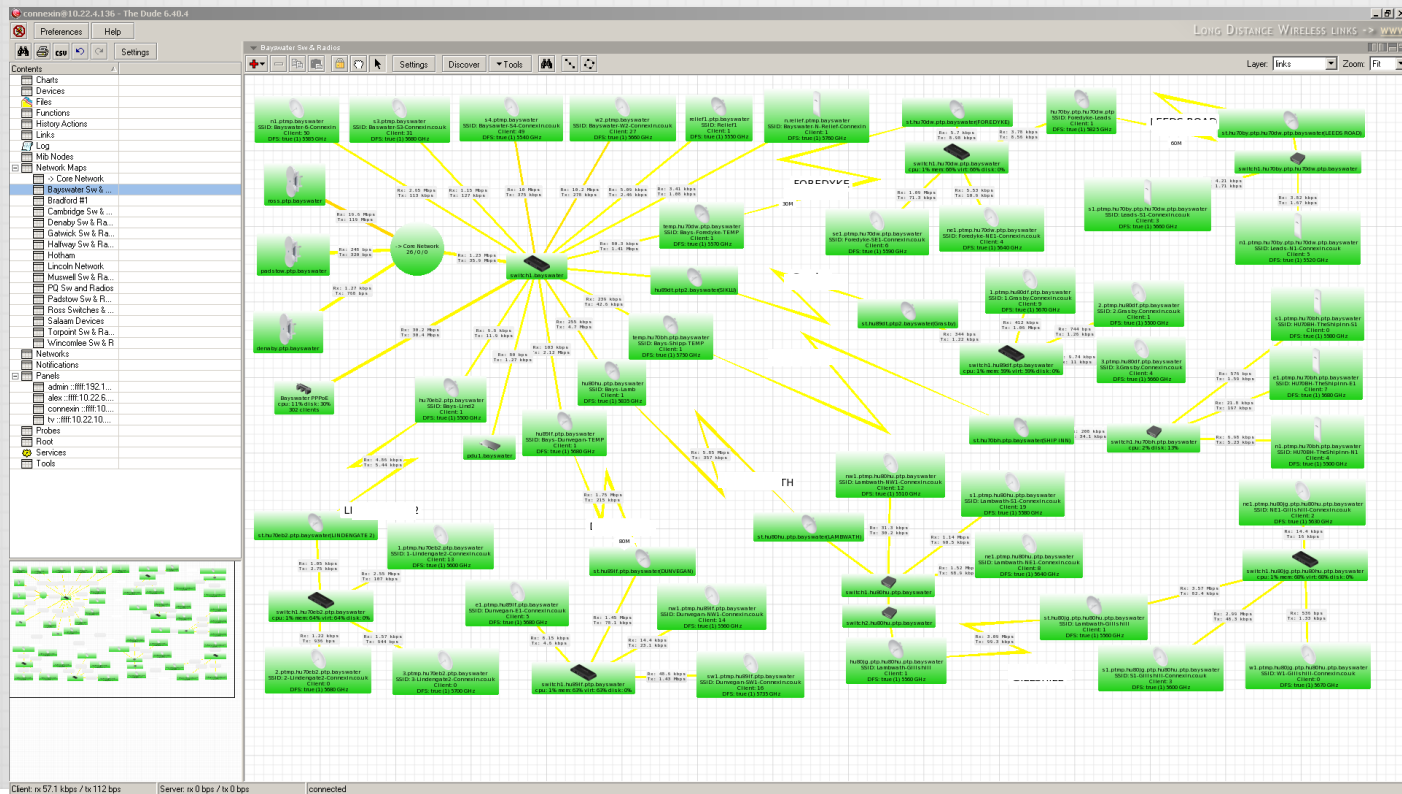


THE DUDE VERSION

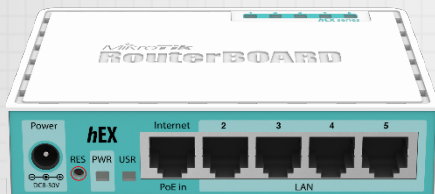
Version 4.x.x			Version 6.x.x	
Server	Client		Server	Client
Windows	Windows		TILE	Windows
MIPSBE			ARM	
MIPSLE			MMIPS	
X86			x86	
PPC			CHR	



THE DUDE LOOK LIKE



THE DUDE IN ROUTERBOARD



Details

Product code	RB750Gr3
CPU	MT7621A
CPU core count	2
CPU nominal frequency	880 MHz
CPU Threads count	4
Dimensions	113x89x28mm
License level	4
Operating System	RouterOS
Size of RAM	256 MB
Storage size	16 MB
Storage type	FLASH
Tested ambient temperature	-30 + 70 C
Suggested price	\$59.95

THE DUDE IN ROUTERBOARD



Details

Product code	RB1100Dx4
CPU	AL21400-1400-A0-E-1AN-8-C
CPU core count	4
CPU nominal frequency	1.4 GHz
CPU Threads count	4
Dimensions	444 x 148 x 47 mm
License level	6
Operating System	RouterOS
Size of RAM	1 GB
Storage size	128 MB
Storage type	NAND
Suggested price	\$349.00

RB1100DX4 DUDE EDITION

29

WinBox v6.40.4 on RB1100AHx4 Dude Edition (arm)

Session: 10.22.4.136

Memory: 741.5 MiB CPU: 15% Date: Oct/23/2017 Time: 03:49:14 Uptime: 2d 13:28:25

Resources

Uptime: 2d 13:28:25

Free Memory: 741.5 MiB

Total Memory: 1010.8 MiB

CPU: ARMv7

CPU Count: 4

CPU Frequency: 1400 MHz

CPU Load: 15 %

Free HDD Space: 90.8 MiB

Total HDD Size: 128.3 MiB

Architecture Name: arm

Board Name: RB1100AHx4 Dude Edition

Version: 6.40.4 (stable)

Build Time: Oct/02/2017 08:38:30

Factory Software: 6.38.4

Dude Settings

☒ Enabled

Data Directory: disk1/dude

Status: running

Disk List

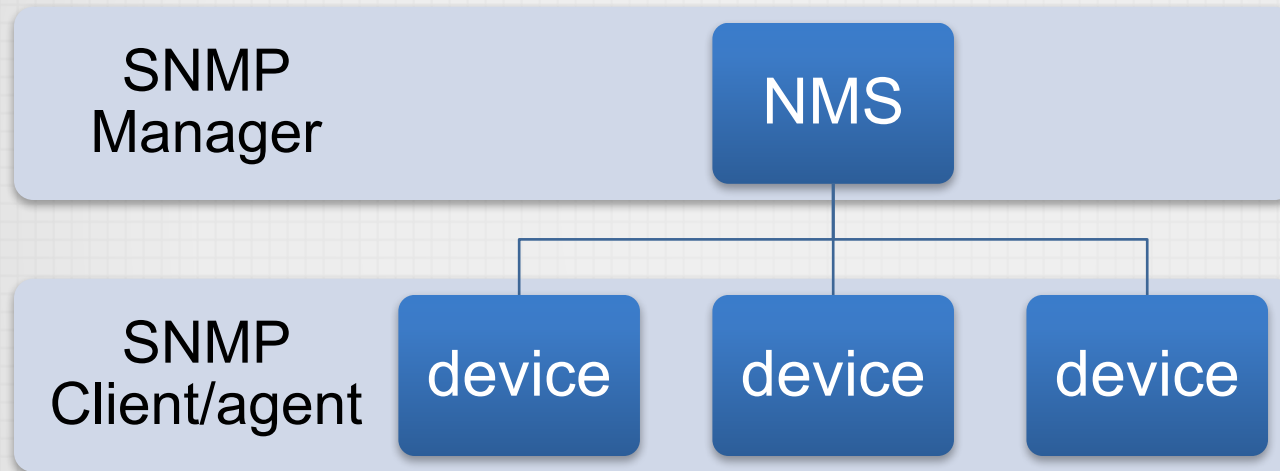
Eject Drive Format Drive Find

Name	Label	Type	Disk	Free	Size
disk1		ext3	FORESEE 60GB SSD	55.2 GiB	55.9 GiB

PROTOCOL FOR MONITORING NETWORK?

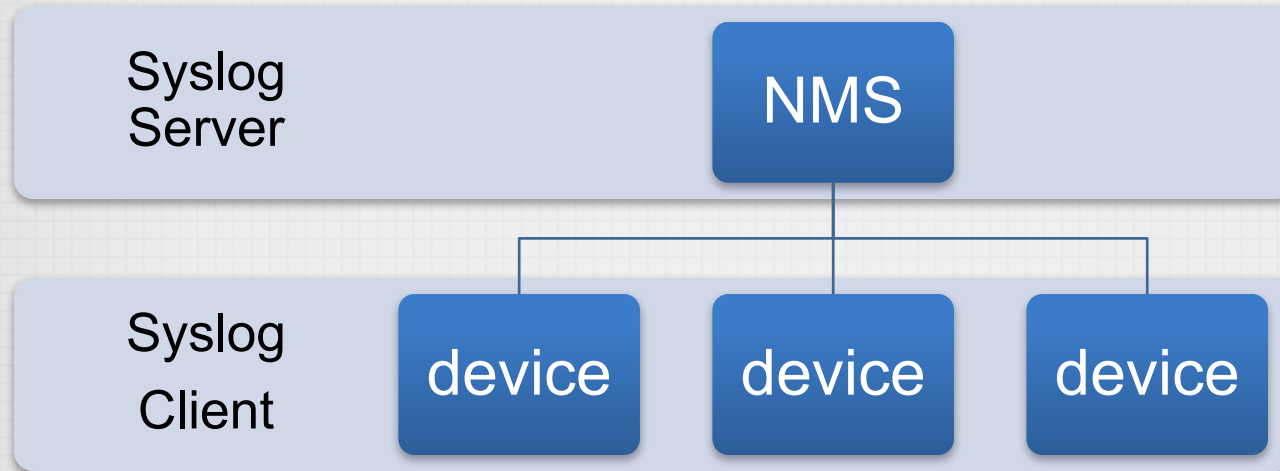
- **SNMP** (Simple Network Management Protocol).
 - Use for collecting and organizing information about managed network devices.
 - Also for modifying that information to change device behavior
- **Syslog** is a way for network devices to send event messages to a logging server
- **ROS** (proprietary MikroTik)

ELEMENT OF SNMP?



ELEMENT OF SYSLOG?

32



DEMO SECTION



THE DUDE DEMO AGENDA

- The dude installation
- Monitoring device
- Monitoring link utilization
- Playing with oid
- Notification (sms, email, line, telegram, etc)

THE DUDE INSTALLATION

- Download NPK File related with your routerboard architecture and version
- Upload to the routerboard
- Reboot the router
- The dude storage setting using winbox
- Download the dude client for your laptop/computer and start to add devices

DEVICE CHANGE

36

unmonitored

UP

Service down

Down

LINK UTILIZATION



PLAYING WITH **OID**

- An OID in SNMP is an "Object Identifier". It's an address used to identify devices and their statuses.
- Here is a sample structure of an OID:
`Iso(1).org(3).dod(6).internet(1).private(4).transition(868).products(2).chassis(4).card(1).slotCps(2).-cpsSlotSummary(1).cpsModuleTable(1).cpsModuleEntry(1).cpsModuleModel(3).3562.3`

Or

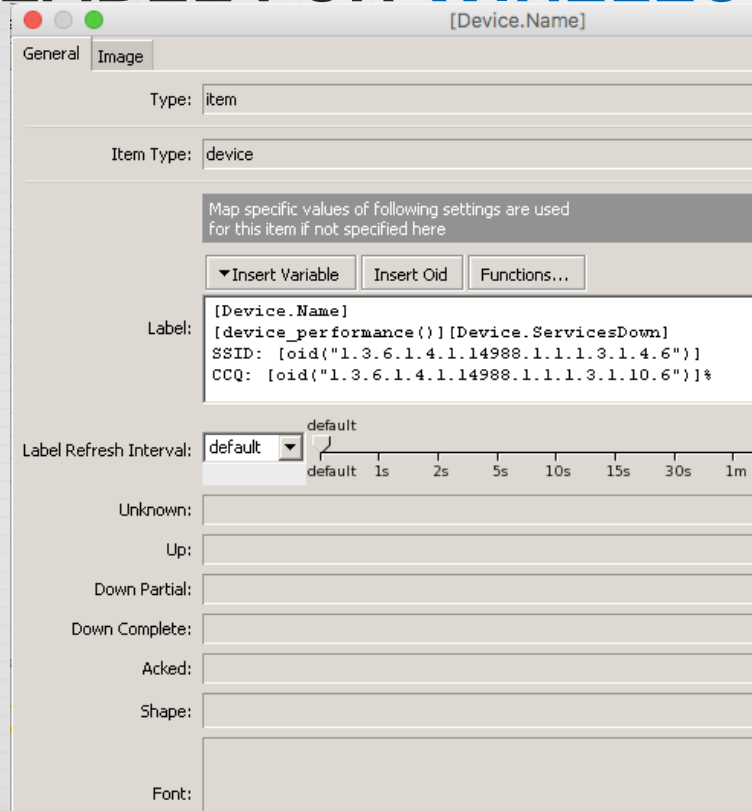
`1.3.6.1.4.868.2.4.1.2.1.1.1.3.3562.3`

PLAYING WITH **OID**

```
Terminal
[admin@AP-ropix] > interface wireless print oid
0 tx-rate=.1.3.6.1.4.1.14988.1.1.1.3.1.2.6
  rx-rate=.1.3.6.1.4.1.14988.1.1.1.3.1.3.6
  ssid=.1.3.6.1.4.1.14988.1.1.1.3.1.4.6 bssid=.1.3.6.1.4.1.14988.1.1.1.3.1.5.6
  client-count=.1.3.6.1.4.1.14988.1.1.1.3.1.6.6
  frequency=.1.3.6.1.4.1.14988.1.1.1.3.1.7.6
  band=.1.3.6.1.4.1.14988.1.1.1.3.1.8.6
  noise-floor=.1.3.6.1.4.1.14988.1.1.1.3.1.9.6
  overall-ccq=.1.3.6.1.4.1.14988.1.1.1.3.1.10.6

1 tx-rate=.1.3.6.1.4.1.14988.1.1.1.3.1.2.7
  rx-rate=.1.3.6.1.4.1.14988.1.1.1.3.1.3.7
  ssid=.1.3.6.1.4.1.14988.1.1.1.3.1.4.7 bssid=.1.3.6.1.4.1.14988.1.1.1.3.1.5.7
  client-count=.1.3.6.1.4.1.14988.1.1.1.3.1.6.7
  frequency=.1.3.6.1.4.1.14988.1.1.1.3.1.7.7
  band=.1.3.6.1.4.1.14988.1.1.1.3.1.8.7
  noise-floor=.1.3.6.1.4.1.14988.1.1.1.3.1.9.7
  overall-ccq=.1.3.6.1.4.1.14988.1.1.1.3.1.10.7
[admin@AP-ropix] >
```

LABEL FOR WIRELESS LINK QUALITY



The screenshot shows a configuration window titled "[Device.Name]". It has two tabs: "General" and "Image". The "General" tab is active. It contains the following fields and options:

- Type: item
- Item Type: device
- A greyed-out section with the text: "Map specific values of following settings are used For this item if not specified here". Below it are buttons: "▼Insert Variable", "Insert Oid", and "Functions...".
- Label:

```
[Device.Name]  
{device_performance()} [Device.ServicesDown]  
SSID: {oid("1.3.6.1.4.1.14988.1.1.1.3.1.4.6")}  
CCQ: {oid("1.3.6.1.4.1.14988.1.1.1.3.1.10.6")}%
```
- Label Refresh Interval: A dropdown menu set to "default" and a slider ranging from "default" to "1m" with intermediate marks at 1s, 2s, 5s, 10s, 15s, and 30s.
- Unknown: (empty field)
- Up: (empty field)
- Down Partial: (empty field)
- Down Complete: (empty field)
- Acked: (empty field)
- Shape: (empty field)
- Font: (empty field)



Access Point
cpu: 1% mem: 41% disk: 91%
SSID: ~the dude~
CCQ: 65%

LABEL FOR UPS TEMPERATURE & LOAD

[Device.Name]

General Image

Type: item

Item Type: device

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

▼ Insert Variable Insert Oid Functions...

Label:

```
[Device.Name]  
Temp: [oid("1.3.6.1.4.1.318.1.1.1.2.3.2.0")/10]*C  
Load: [oid("1.3.6.1.4.1.318.1.1.1.4.3.3.0")/10]*  
[device_performance()][Device.ServicesDown]
```

Label Refresh Interval: default default 1s 2s 5s 10s 15s 30s 1m 2m 5m 10m

Unknown:

Up:

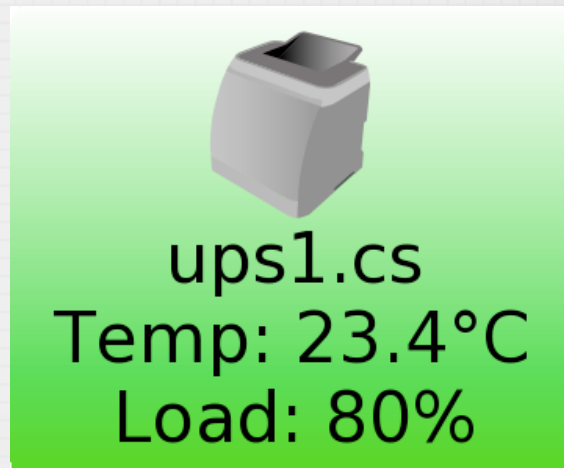
Down Partial:

Down Complete:

Acked:

Shape:

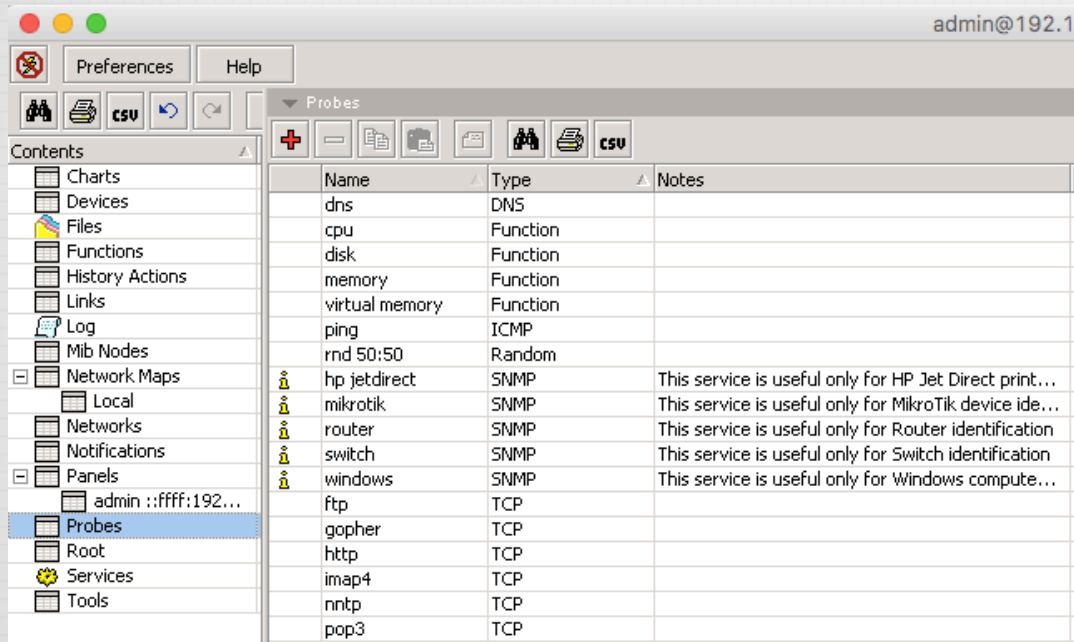
Font:



PROBE

42

Methods of checking for device services



The screenshot shows the CSU Probes interface. The top bar includes a status indicator (red, yellow, green), a username 'admin@192.1', and buttons for 'Preferences' and 'Help'. Below the top bar is a toolbar with icons for adding, deleting, and saving probes, along with a 'CSU' button. The main area is divided into a 'Contents' sidebar on the left and a table of probes on the right. The 'Contents' sidebar lists various categories like Charts, Devices, Files, Functions, History Actions, Links, Log, Mib Nodes, Network Maps, Local, Networks, Notifications, Panels, Root, Services, and Tools. The 'Probes' category is selected. The table of probes has three columns: Name, Type, and Notes. It lists various services such as dns, cpu, disk, memory, virtual memory, ping, rnd 50:50, hp jetdirect, mikrotik, router, switch, windows, ftp, gopher, http, imap4, nntp, and pop3.

Name	Type	Notes
dns	DNS	
cpu	Function	
disk	Function	
memory	Function	
virtual memory	Function	
ping	ICMP	
rnd 50:50	Random	
hp jetdirect	SNMP	This service is useful only for HP Jet Direct print...
mikrotik	SNMP	This service is useful only for MikroTik device ide...
router	SNMP	This service is useful only for Router identification
switch	SNMP	This service is useful only for Switch identification
windows	SNMP	This service is useful only for Windows compute...
ftp	TCP	
gopher	TCP	
http	TCP	
imap4	TCP	
nntp	TCP	
pop3	TCP	

PROBE FOR FREQ CHANGES

43

Freq-5500 - Probe

Name:

Type:

Agent:

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:

☐ Treat service as available only if up

Oid:

Oid Type:

Compare Method:

Integer Value:

Buttons: Ok, Cancel, Apply, Notes, Copy, Remove

PROBE FOR PPP ACTIVE CONNECTION DROP

44

The image shows two overlapping windows from a network monitoring application. The background window is titled 'ppp active - Probe' and contains the following fields and text:

- Name:** ppp active
- Type:** Function
- Agent:** default
- Description:** 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:** if(getActiveUser())>0, 1,-1)
 - If return string is empty then service is assumed up
- Error:** if(getActiveUser())<200, "", "PPPOE bellow 200 users")
 - Should return value to graph if up
- Value:** getActiveUser()
- Unit:** Users

The foreground window is titled 'getUserActive - Function' and contains the following fields and buttons:

- Name:** getUserActive
- Description:** get active ppp user
- Code:** oid("1.3.6.1.4.1.9.9.150.1.1.1.0")
- Buttons:** Ok, Cancel, Apply, Notes, Copy, Remove

Below the 'Code' field in the foreground window is a 'Remove' button.

CHART FOR PPP ACTIVE CONNECTION

45

General Chart

☒ Enabled

Name: cambridge

Unit: users

Device: Cambridge PPPoE

Code: `ros_command("/ppp active print count-only")`

Interval: 00:00:30

Last Value Time: 03:15:27

Last Value: 380

Settings that control how much detail is stored for how long time

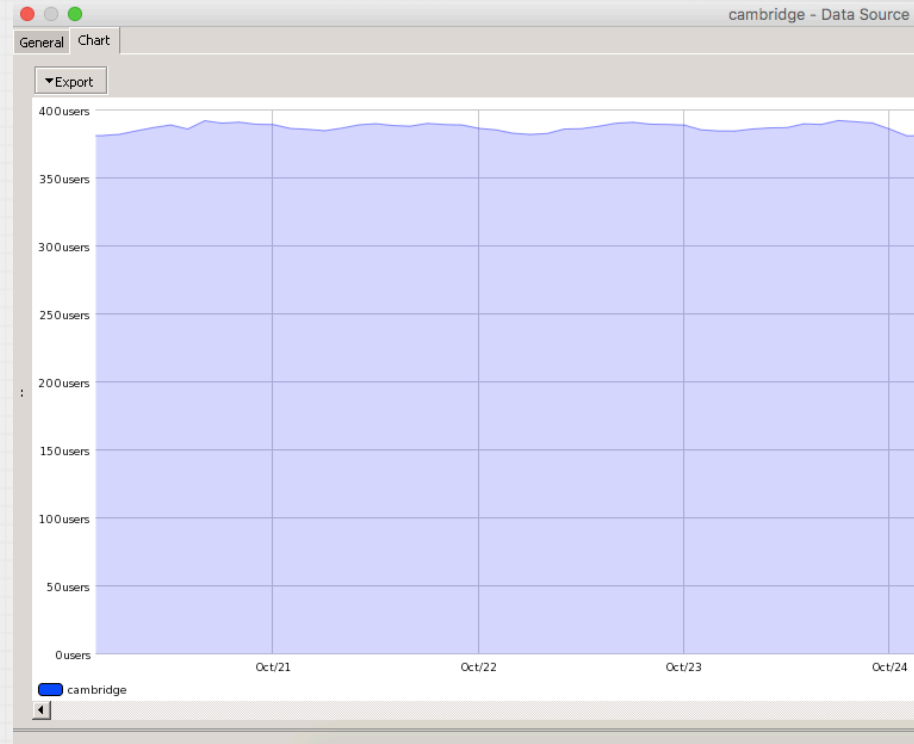
Raw Value Keep Time: default

10 Min Value Keep Time: default

2 Hour Value Keep Time: default

1 Day Value Keep Time: default

Approximate Storage Size: 122.9 kB



CONCLUSIONS

- The dude is powerful, cheap and easy
- The dude is "almost anything impossible" network monitoring system
- Need some improvement especially in read/write database to the storage.



If you have any other questions or would like me to clarify anything else, please, let me know. I am always glad to help in any way I can

CONTACT

ADDRESS: Jakarta & Semarang, Indonesia

WEBSITE: www.trainingmikrotik.com

EMAIL: rrofiq@idn.id

TELEPHONE: +62 8156583545



@mymikrotik



www.facebook.com/ropix



id.linkedin.com/in/ropix/



[rofiq.fauzi](#)

“If you cannot survive in the tired of learning, then you will be suffering by the pain of stupidity” (*Imam Syafi'i*)