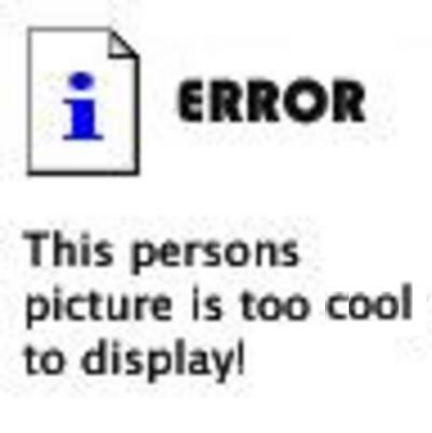
THE DUDE NOW & THE FUTURE

IDN foundation

ID NETWORKERS
Expert Trainer & Consultant

INTRODUCTION

ABOUT ROFIQ FAUZI



- 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

IDNFoundation

PESANTREN NETWORKING & PROGRAMMING

SMP & SMK IDN MADINATUL ILMI

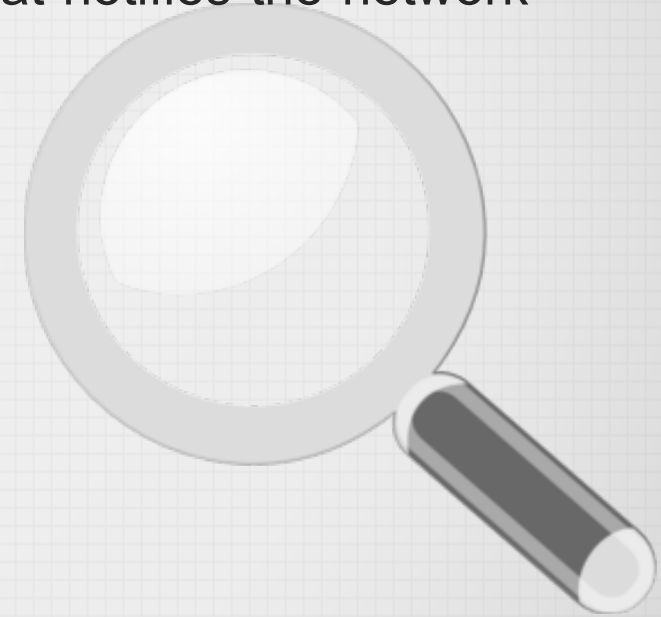
www.idn.sch.id

TRAINING GURU SMK

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?

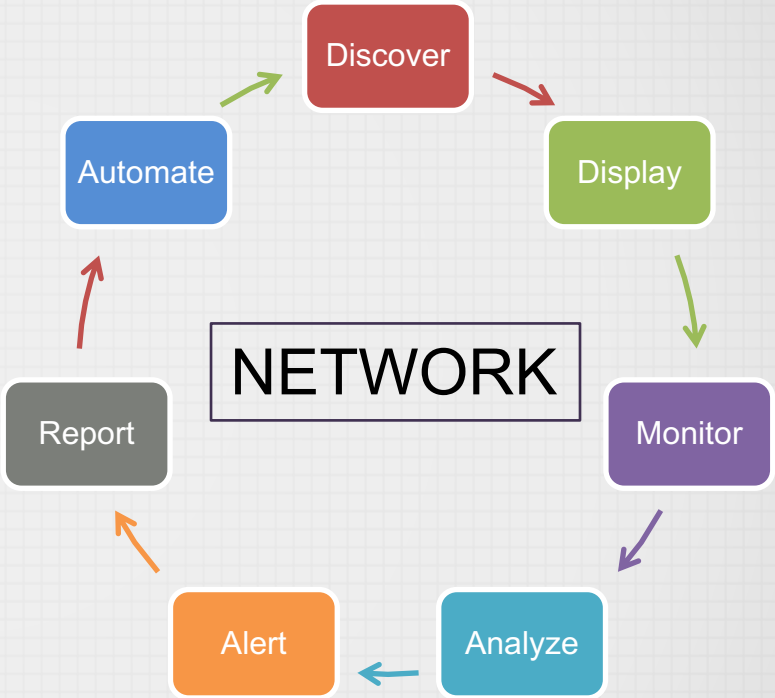


Image from www.freepik.com

WHY WE NEED NETWORK MONITORING?

Image from www.quickmeme.com

WHY WE NEED NETWORK MONITORING?

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

Nagios®

cacti

solarwinds

MRTG
MULTI ROUTER TRAFFIC GRAPHER

splunk>

PAESSLER
PRTG

MUNIN

ZABBIX

PANDORAFMS

zenoss

syslog-ng
Open Source Edition

WhatsUpGold

icinga

netmon

ntop

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

QUIZ?

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

QUIZ

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 MikroTik , 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?

[redacted] Network Monitor Price List

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

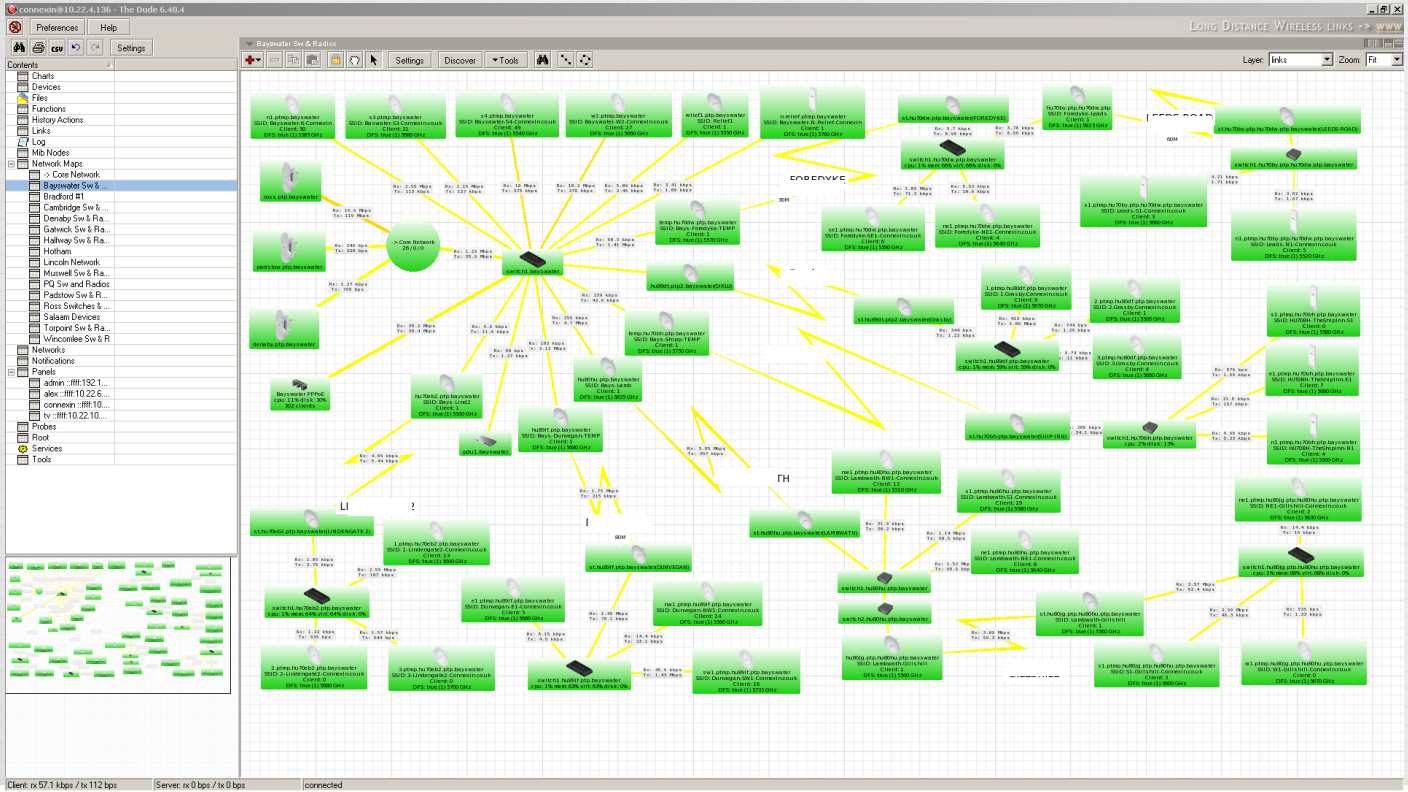
BUY NOW >>

THE DUDE VERSION

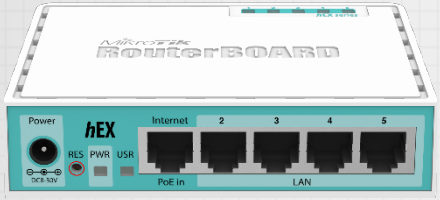
Version 4.x.x			Version 6.x.x	
Server	Client		Server	Client
Windows	Windows		TILE	Windows
MIPSBE			ARM	
MIPSLE			MMIPS	
X86			x86	
PPC			CHR	

2012 2016

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

@10.22.4.136 (The Dude Server) - WinBox v6.40.4 on RB1100AHx4 Dude Edition (arm)

Session Settings Dashboard

Safe Mode | Session: 10.22.4.136 | Memory: 741.5 MiB | CPU: 15% | Date: Oct/23/2017 | Time: 03:49:14 | Uptime: 2d 13:28:25

Quick Set
Interfaces
Bridge
Switch
Mesh
IP
System
Queues
Files
Log
Radius
Tools
New Terminal
Dude
Partition
Make Supout.rif
Manual
New WinBox
Exit

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

OK | Cancel | Apply

Disk List

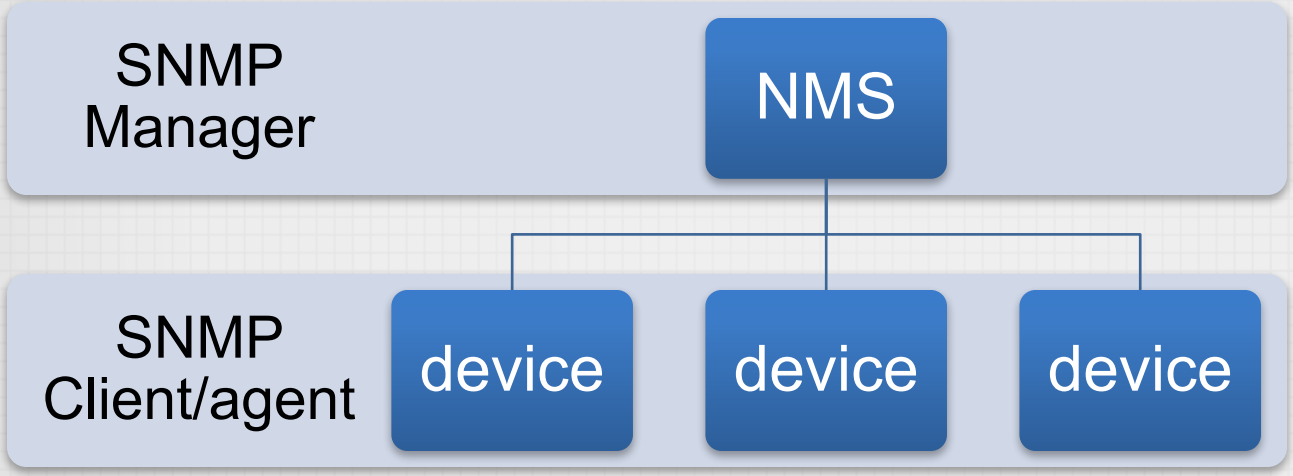
Eject Drive | Format Drive | Find

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

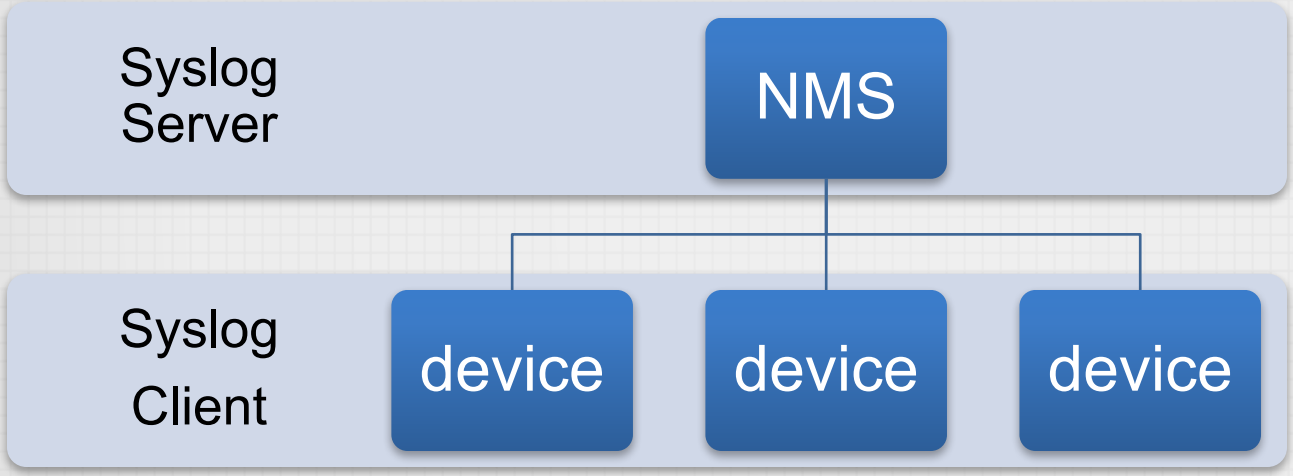
PROTOCOL FOR MONITORING NETWORK?

- **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?



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

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

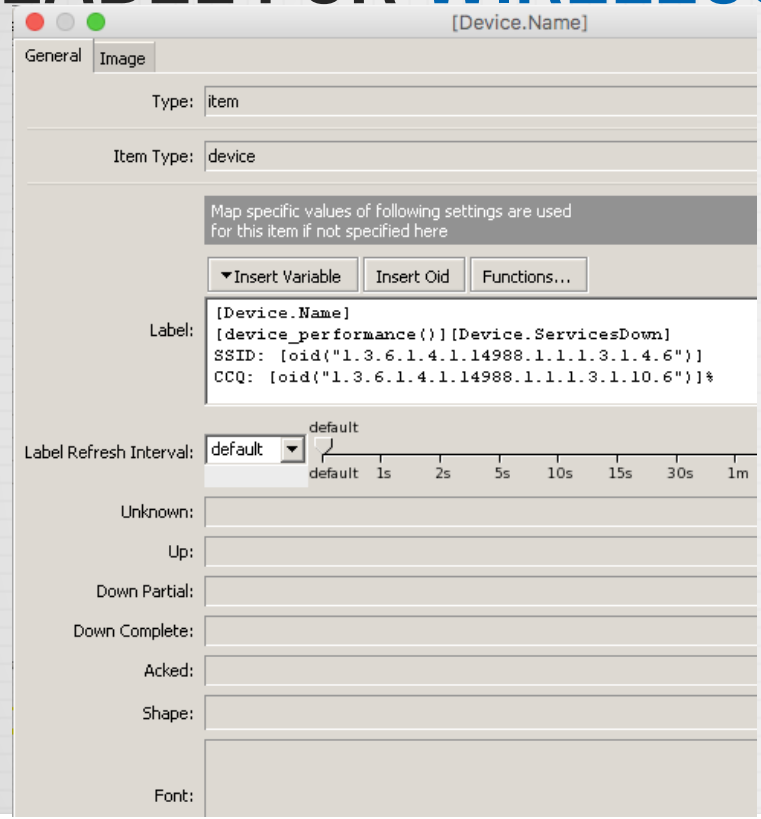
PLAYING WITH OID

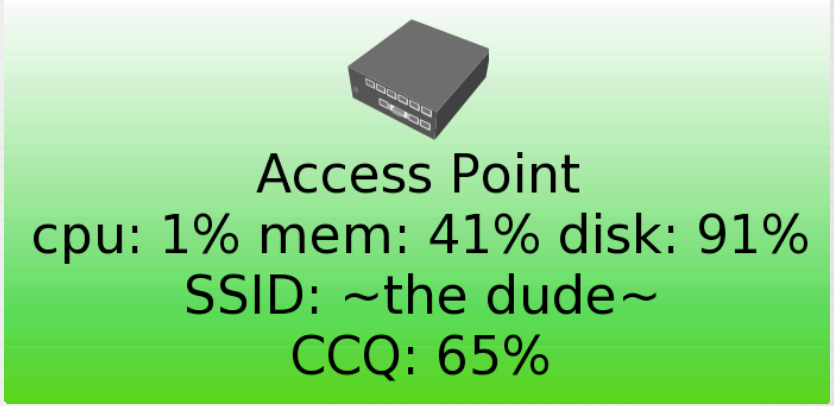
Terminal

```
[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





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:

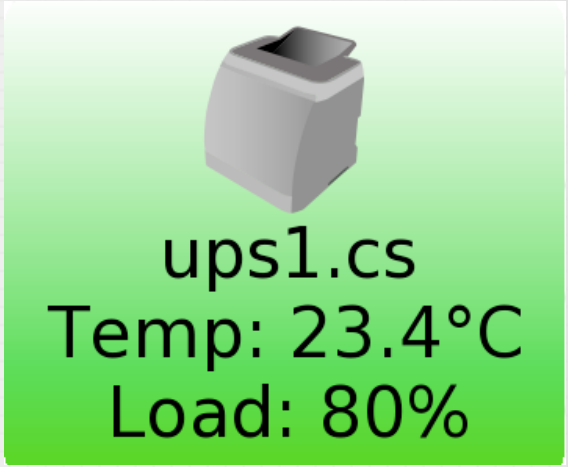
Down Partial:

Down Complete:

Acked:

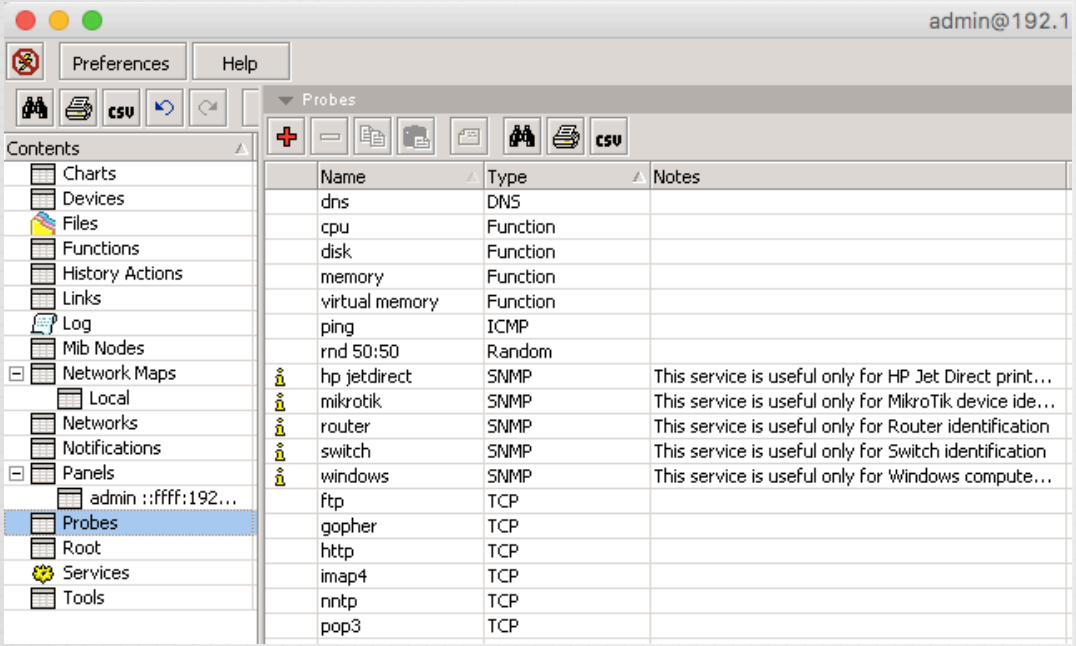
Shape:

Font:

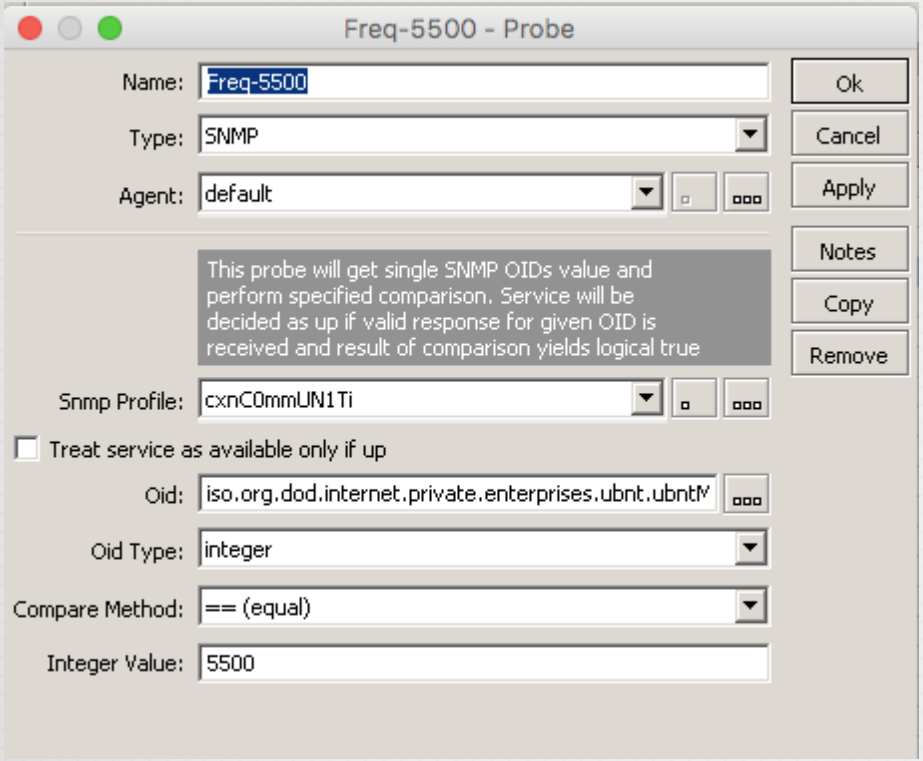


PROBE

Methods of checking for device services



PROBE FOR FREQ CHANGES



PROBE FOR PPP ACTIVE CONNECTION DROP

ppp active - Probe

Name: ppp active

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: 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

Remove

getUserActive - Function

Name: getUserActive

Description: get active ppp user

Code:

```
oid("1.3.6.1.4.1.9.9.150.1.1.1.0")
```

Ok

Cancel

Apply

Notes

Copy

Remove

CHART FOR PPP ACTIVE CONNECTION

General | Chart

☑ Enabled

Name: cambridge

Unit: users

Device: Cambridge PPPoE

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

Interval: 00:00:30 — 1s 2s 5s 1

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 — default 2s 5s 10s 15s 30s 1m 2m 5m

10 Min Value Keep Time: default — default 10m 15m 30m 1h 2h 3h 6h

2 Hour Value Keep Time: default — default 2h 3h 6h 12h 1d 2

1 Day Value Keep Time: default — default 1d 2d 3d 5d

Approximate Storage Size: 122.9 kB

cambridge - Data Source

General | Chart

Export

400users
350users
300users
250users
200users
150users
100users
50users
0users

Oct/21 Oct/22 Oct/23 Oct/24

cambridge

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)*