m.it.sco
Morvarid. IT. Solutions Co.

MikroTik

MUM -Kathmandu, Nepal
June 2nd 2017

# Dude Server
# iGenTik

By
Mani Raissdana

# MANI RAISSDANA

**MikroTik Certified Trainer**

**CTO & Co-Founder of**

m.it.sco

Morvarid. IT. Solutions Co.

**Being in IT technology business roughly around 14 years**

**Support & instruct Engineers more than 8 years all over the globe**

**Wireless, Routing, QoS, Firewall, The Dude**

# MANI RAISSDANA

- **MikroTik Certified Trainers**

http://www.mikrotik.com/training/partners/europe/turkey

- **MikroTik Certified Consultants**

http://www.mikrotik.com/consultants/europe/turkey

- **Mani Raissdana Certifications**

http://www.mikrotik.com/certificateSearch Check Mani Raissdana

http://www.mits-co.com/content/certificates

- **Ubiquiti Certified Trainers**

https://www.ubnt.com/training/partners/ Check Europe

- **elastiX Certified Trainers**

http://www.elastix.com/en/instructores/ Check Turkey

- **elastiX Official Resellers**

http://www.elastix.com/en/resellers-elastix/ Check Europe

- **Mani Raissdana Resume**

www.mits-co.com/sites/default/files/Mani%20Raissdana%20Resume.pdf

# TABLE OF CONTENTS

Dude

- What is Dude???
- What it does???
- How it works???
- How you should work with???
- Monitoring
- Notification

iGenTik

Interactive GSM/Email notification system

FORUM
SOCIAL NETWORK
CONTENT SHARING
MICROBLOGS
SOCIAL MEDIA
VIDEO
COMMUNICATION
CHAT
PICTURE
OUR BUSINESS
OK
CLIENT 1
CLIENT 2
CLIENT n.
FIREWALL
SERVER
INTERNET
VOIP
COMPANY HEADQUARTERS
GROWTH
DESIGN
MEDIA
OTHER
COMPETITOR
OUR COMPANY
YES
?
35%
STATISTICS
LAST YEAR
TIME
MONEY
BUSINESS
QUALITY
ROUTER
AUTHENTICATION SERVER
STRATEGY
SUCCESS
INNOVATION
RESEARCH
SOCIAL NETWORK

# WHAT IS DUDE

- MikroTik free Monitoring application
- Has 2 parts:
  1. Client application: (Windows, Mac, Linux)
  2. Server package: (RoS package) only for:
- MikroTik CCR Series
- RouterOS X86
- RouterOS CHR

**RouterOS Version should be 6.34rc13 or higher to be able to use Dude**

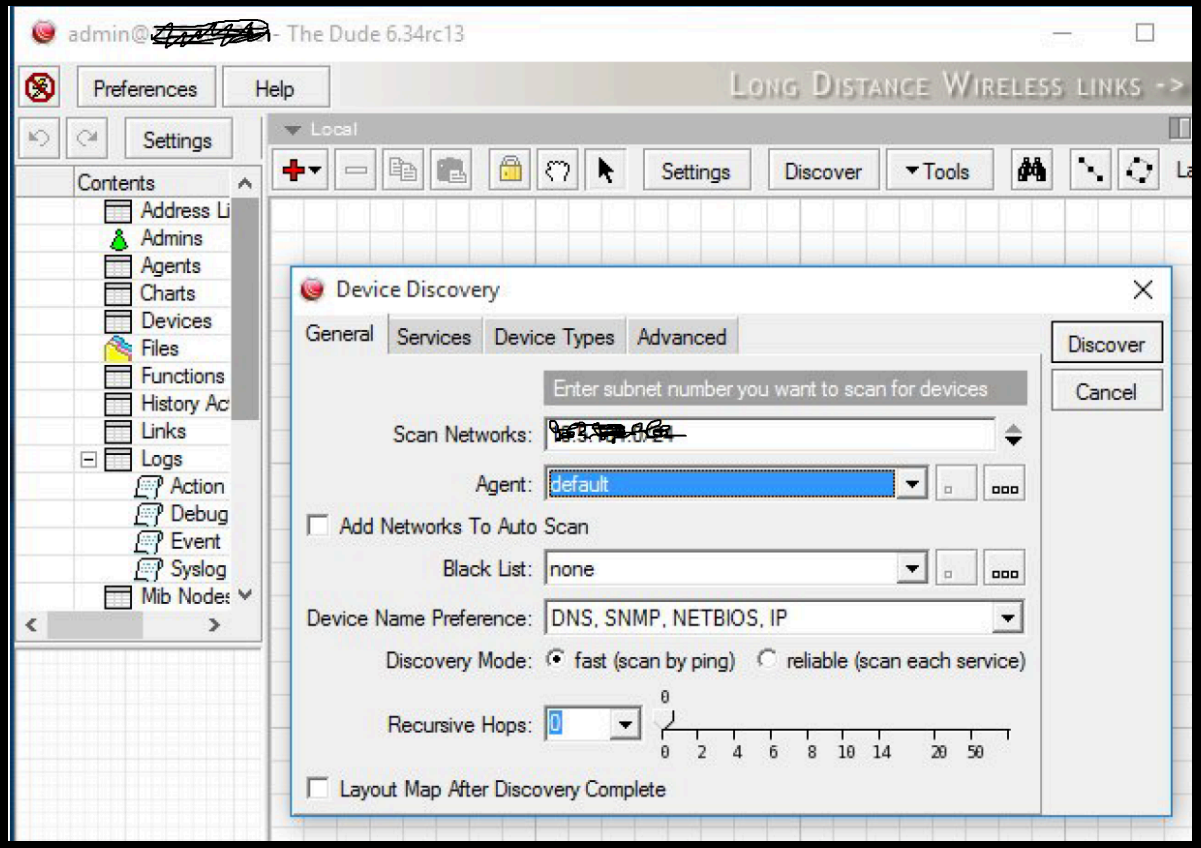
# WHAT IT DOES

- Scans (Discovers) your Network in layer 2
- Monitors availability of your network
- Keeps watching all your layer 3 devices
- Monitors all your links
- Supports layer 3 probes
- Supports SNMP
- Has direct access to your RouterOS (with Winbox)

**Here, we're talking about Dude V6, Which has some fundamental differences with legacy versions**

# HOW IT WORKS

- After successful Installation, login page comes up
- After Successful Login, Automatic Discovery feature will jump up,




- You may like to discover your Network automatically or add everything manually

# HOW IT WORKS

- If you are working with legacy versions (V3 or V4), you are still be able to import your old database here

```
/dude import-db backup-file=(file_name_path)
```

- Or maybe you'd like to change the path of database

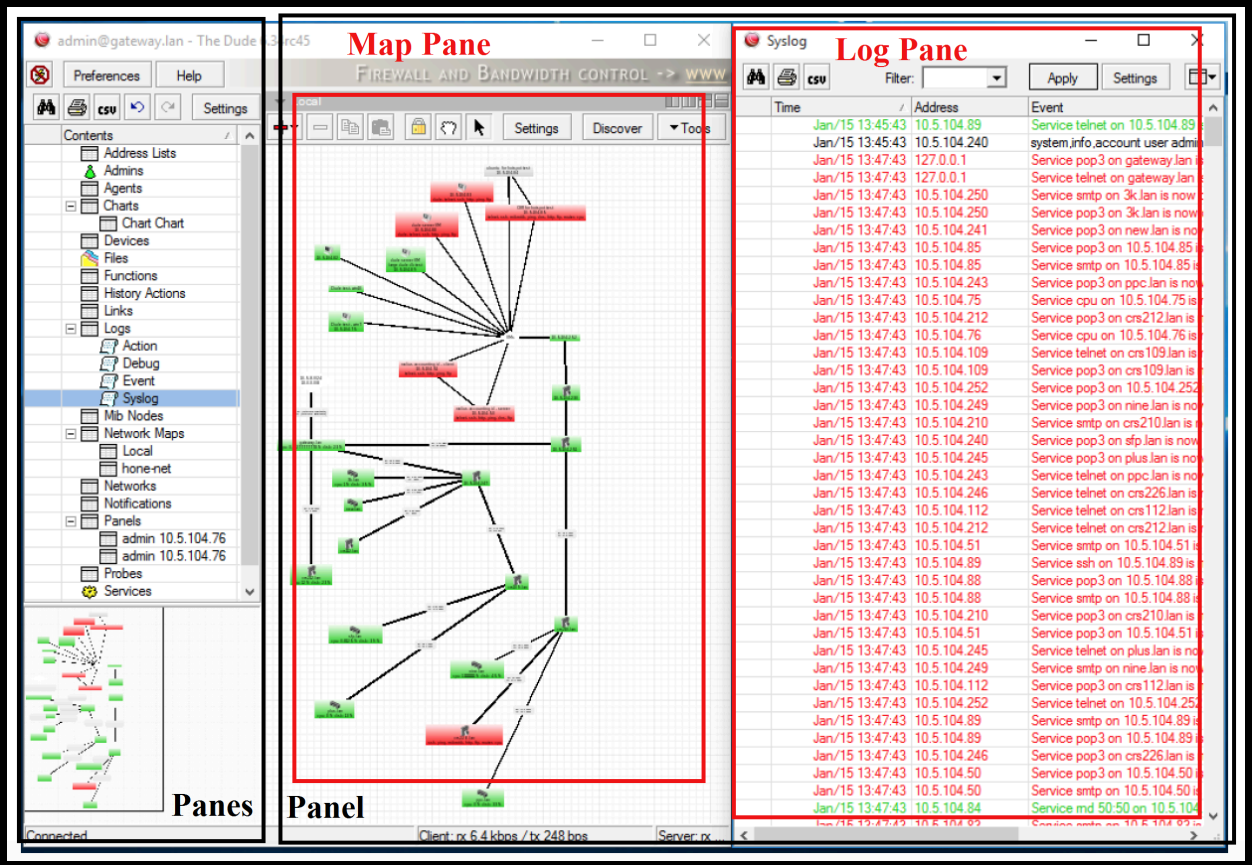
```
/dude set data-directory=(new_db_path)
```

Change path procedure:

1. Disable the Server
2. Move existing directory
3. Change the path of directory
4. Enable the Server

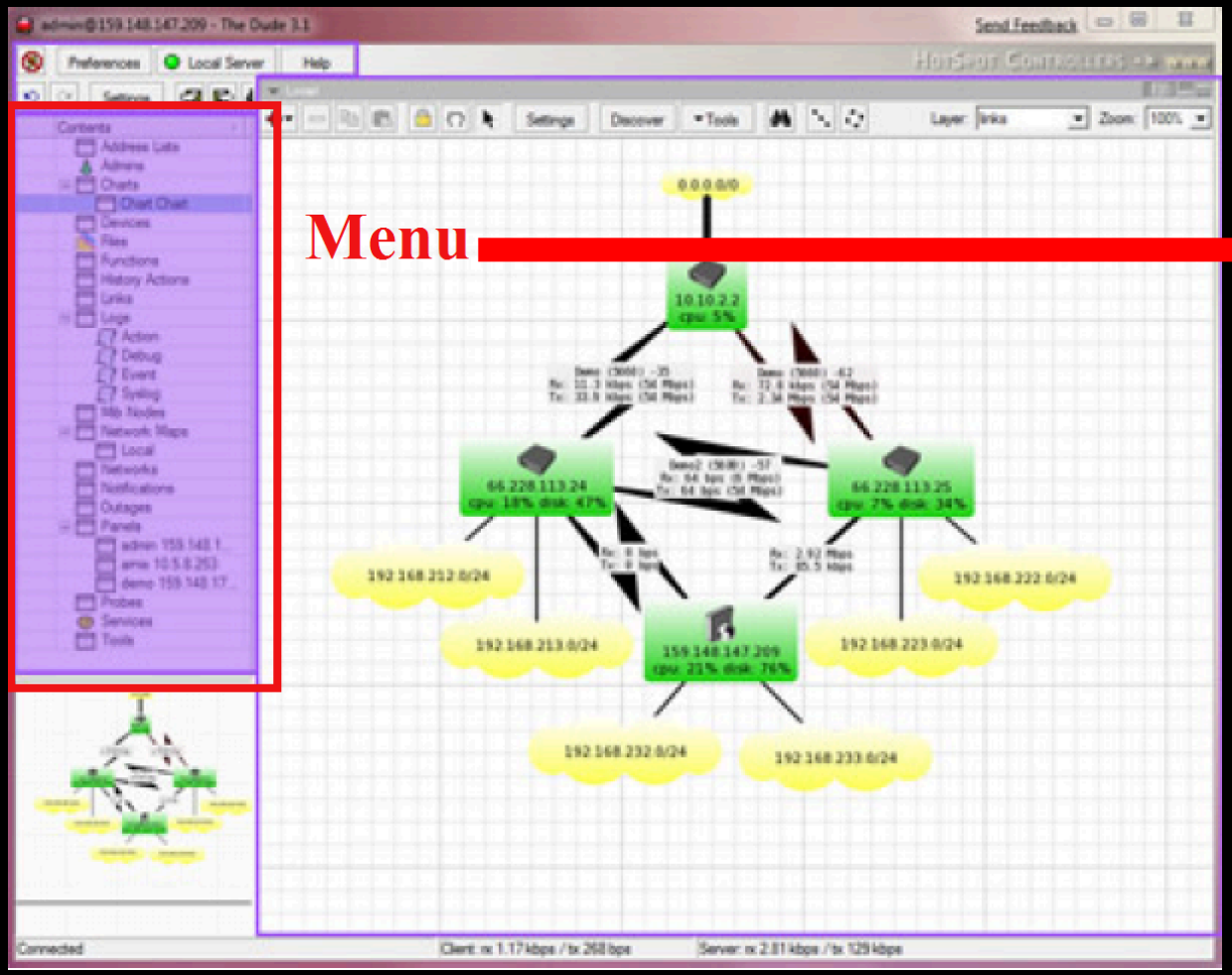
# HOW TO WORK WITH

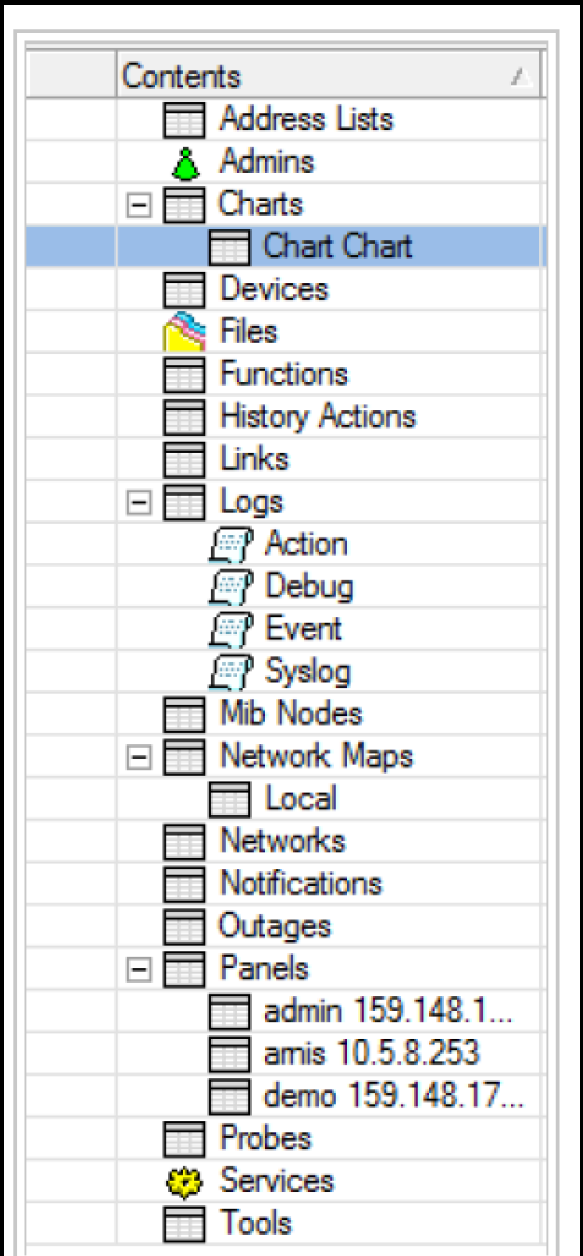
## Interface



# HOW TO WORK WITH

## Menu



# HOW TO WORK WITH

## Menu

Address lists: Lists of IP addresses to be used in Blocklist and other places

Admins: Users who can access this particular Dude server

Charts: Configure graphs based on any data source in the map

Devices: List of all the devices drawn on any of the network maps

Files: List of the files uploaded to the server, like images for network map backgrounds and sounds

Functions: Functions that can be used, includes scripts and advanced queries

History Actions: History of tasks performed by the admin, like adding or removing devices. Admin log.

Links: List of all links in all maps.

Logs: Logs of device statuses. Dude also includes a Syslog server, and can receive Logs from other devices.

MIB nodes: Information about MIBs

Network maps: All maps

Networks: List of all network segments places on the map

Notifications: Different ways to alert the admin of

Panels: Allows to configure separate dude window entities for use on multiple monitors or otherwise

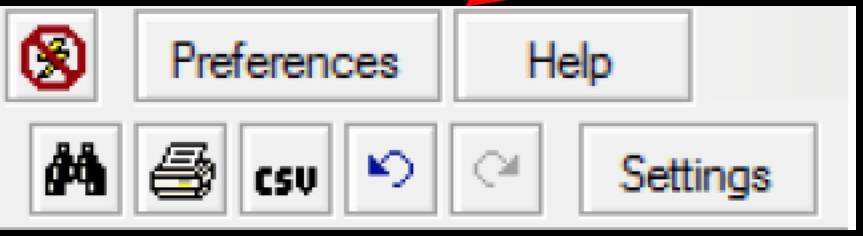
Probes: Probes are responsible for polling specific services on the defices

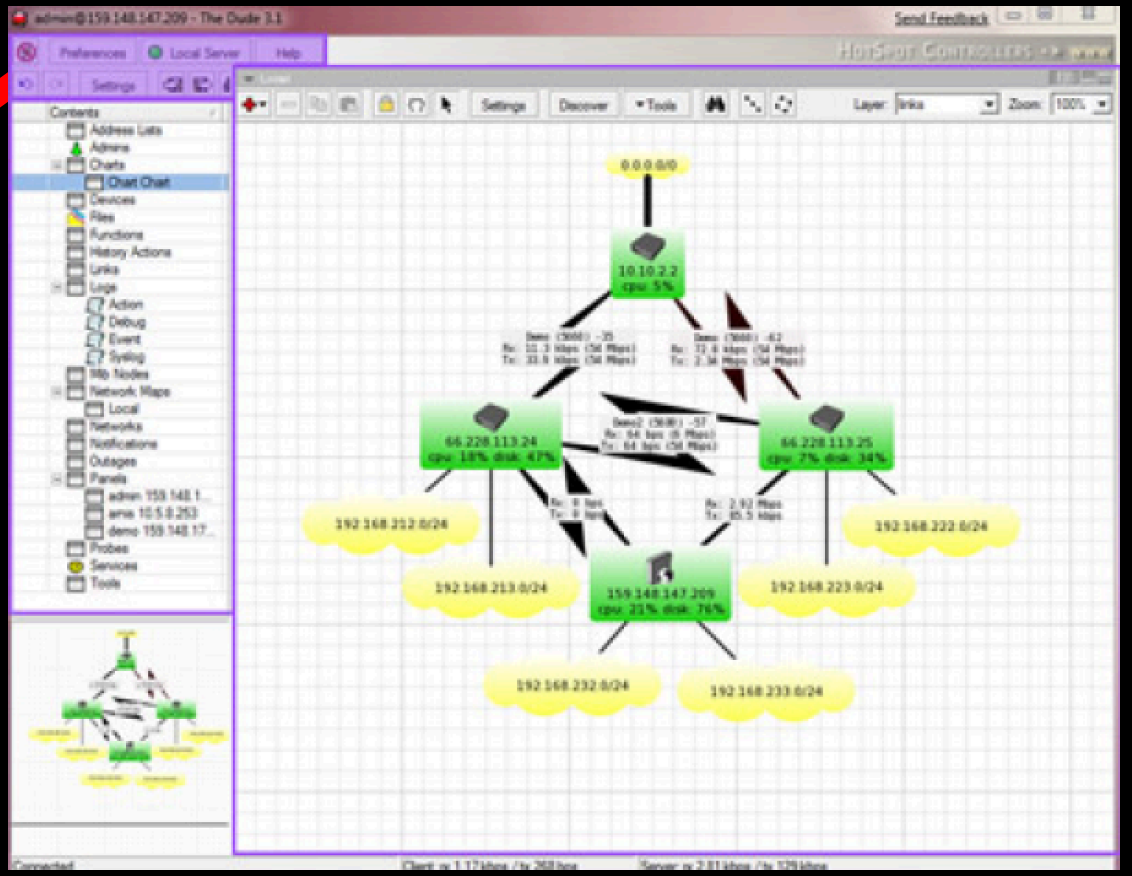
Services: Lists the currently monitored services on all devices

Tools: Configures the tools that can be run on each device (ie. connect with winbox, telnet, ftp, etc.)

# HOW TO WORK WITH

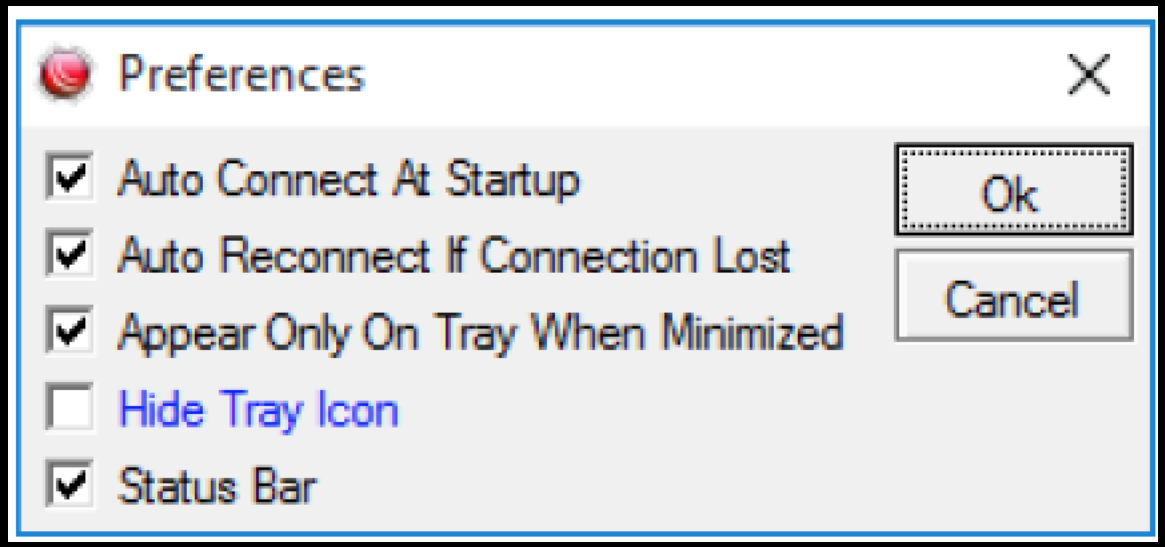
## Server Settings



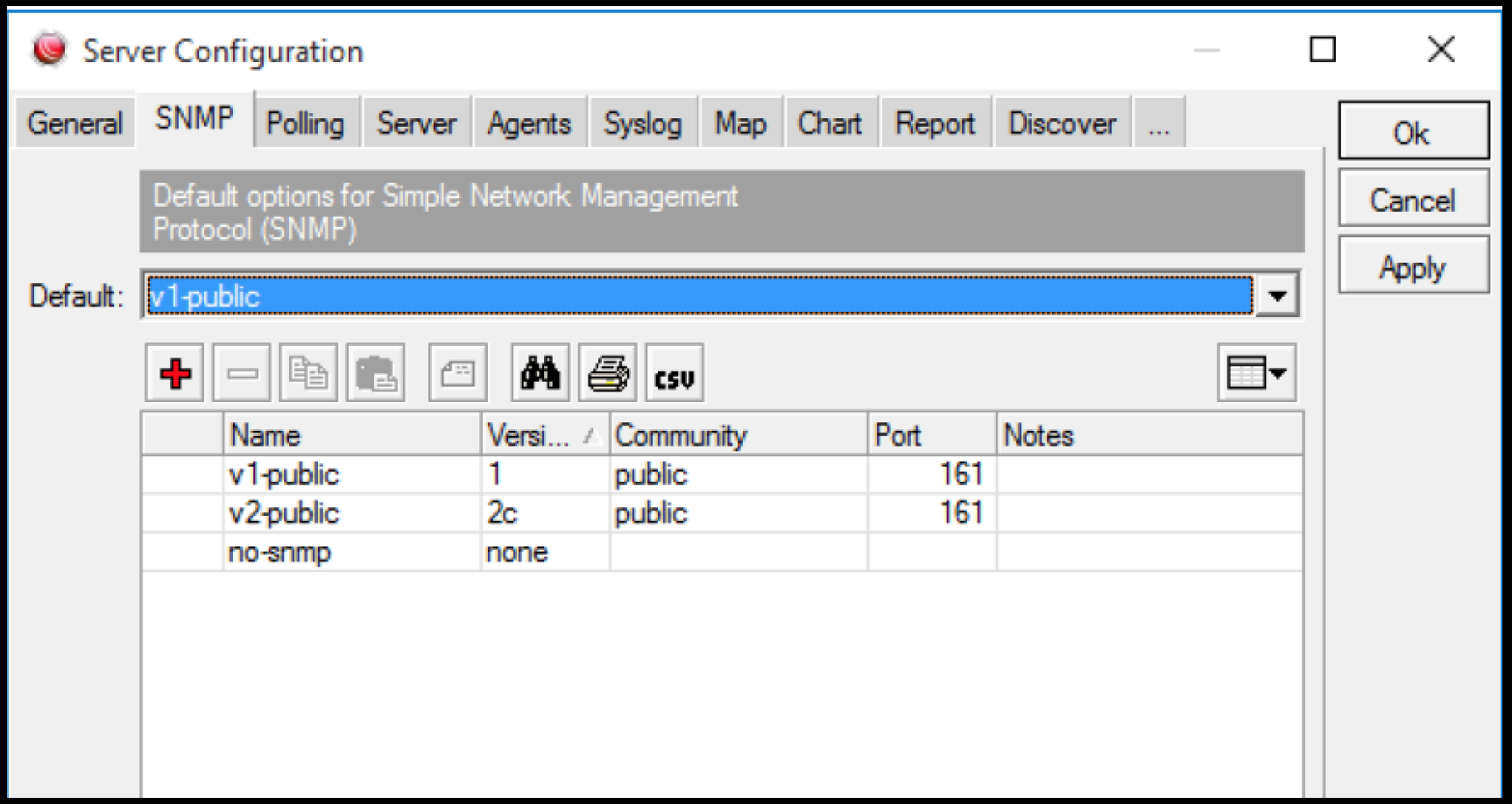
# HOW TO WORK WITH

## Preferences



# HOW TO WORK WITH

## Server Settings

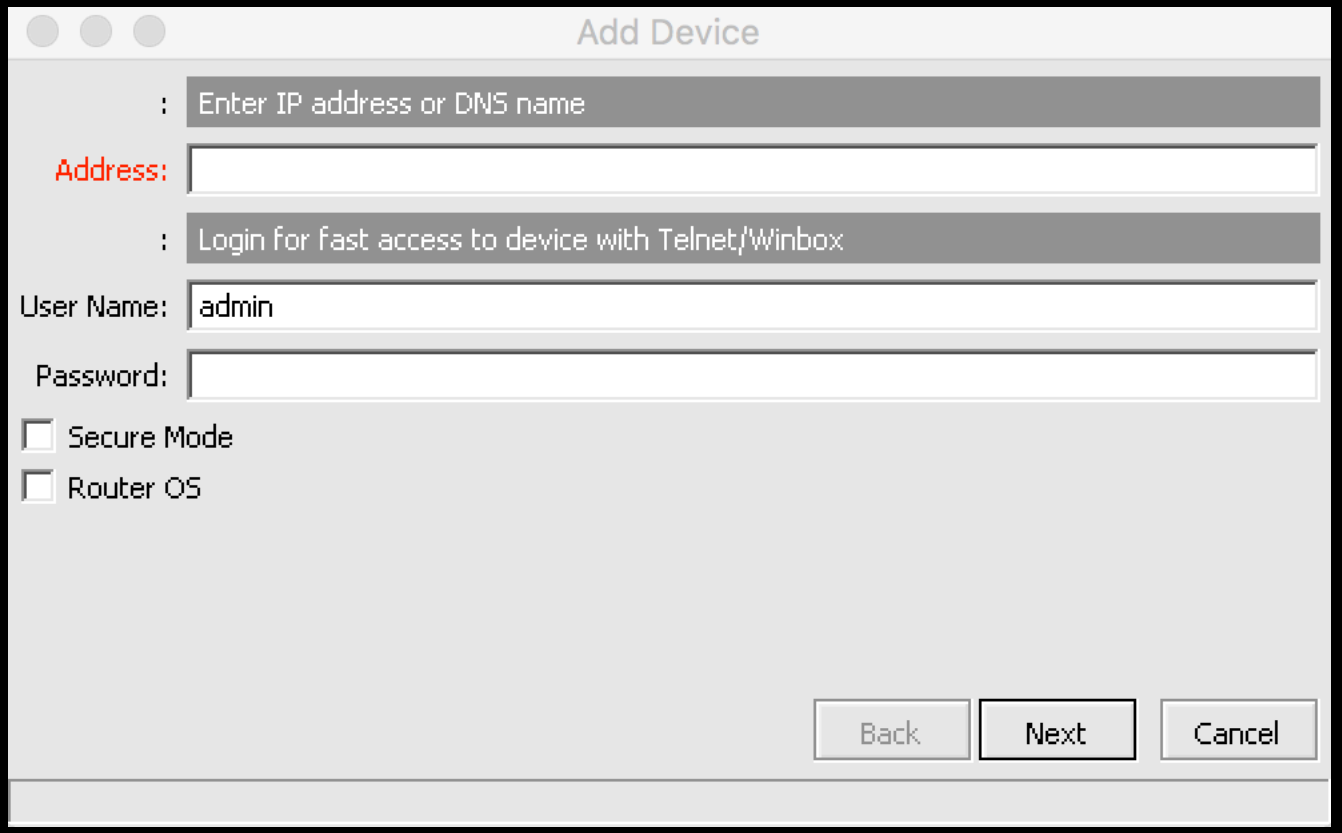


# HOW TO WORK WITH

## Device Settings

- Adding devices is just few steps:

1-

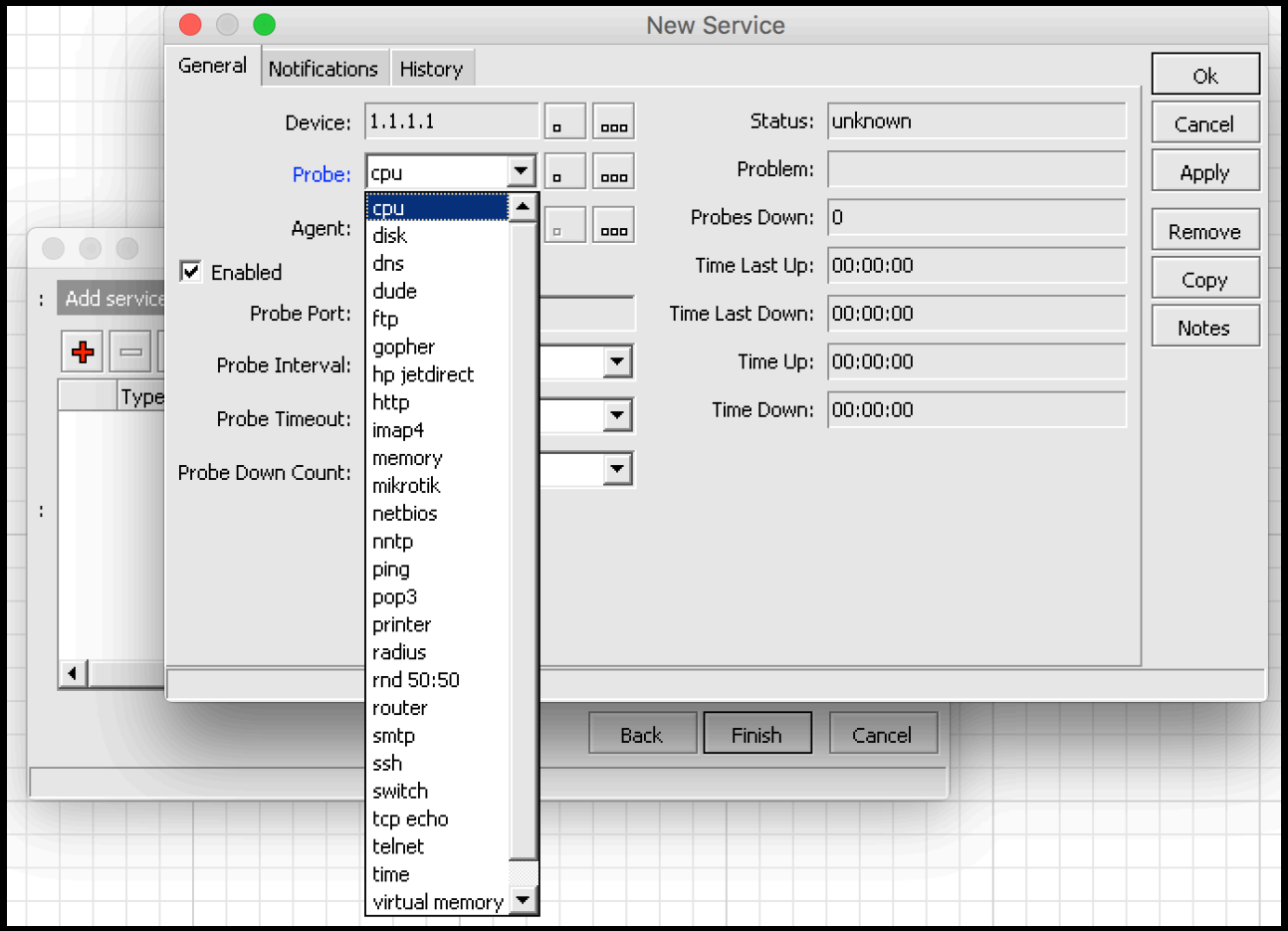


# HOW TO WORK WITH

## Device Settings

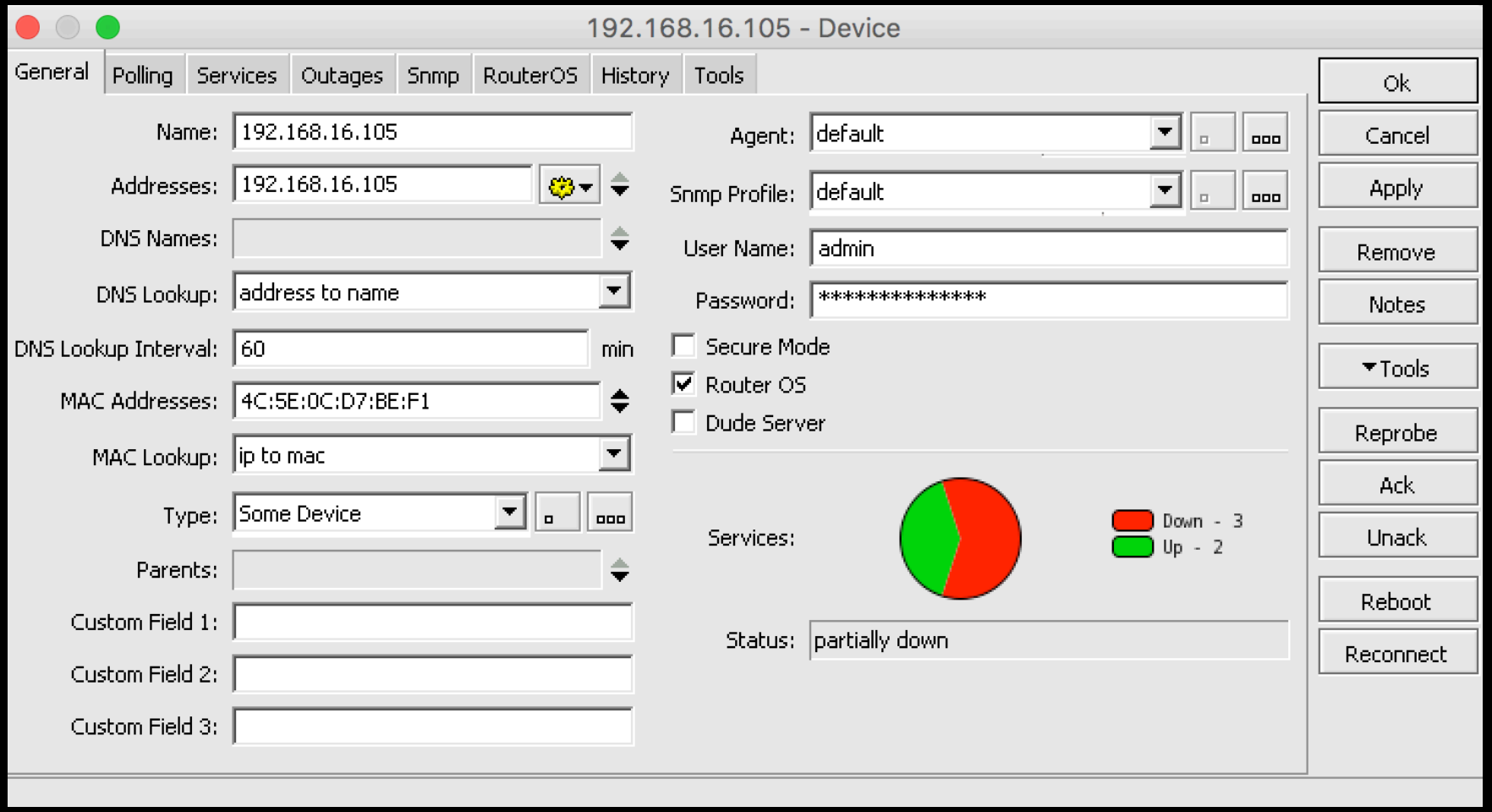
- Adding devices is just few steps:

2-



# HOW TO WORK WITH

## Device Settings



# HOW TO WORK WITH

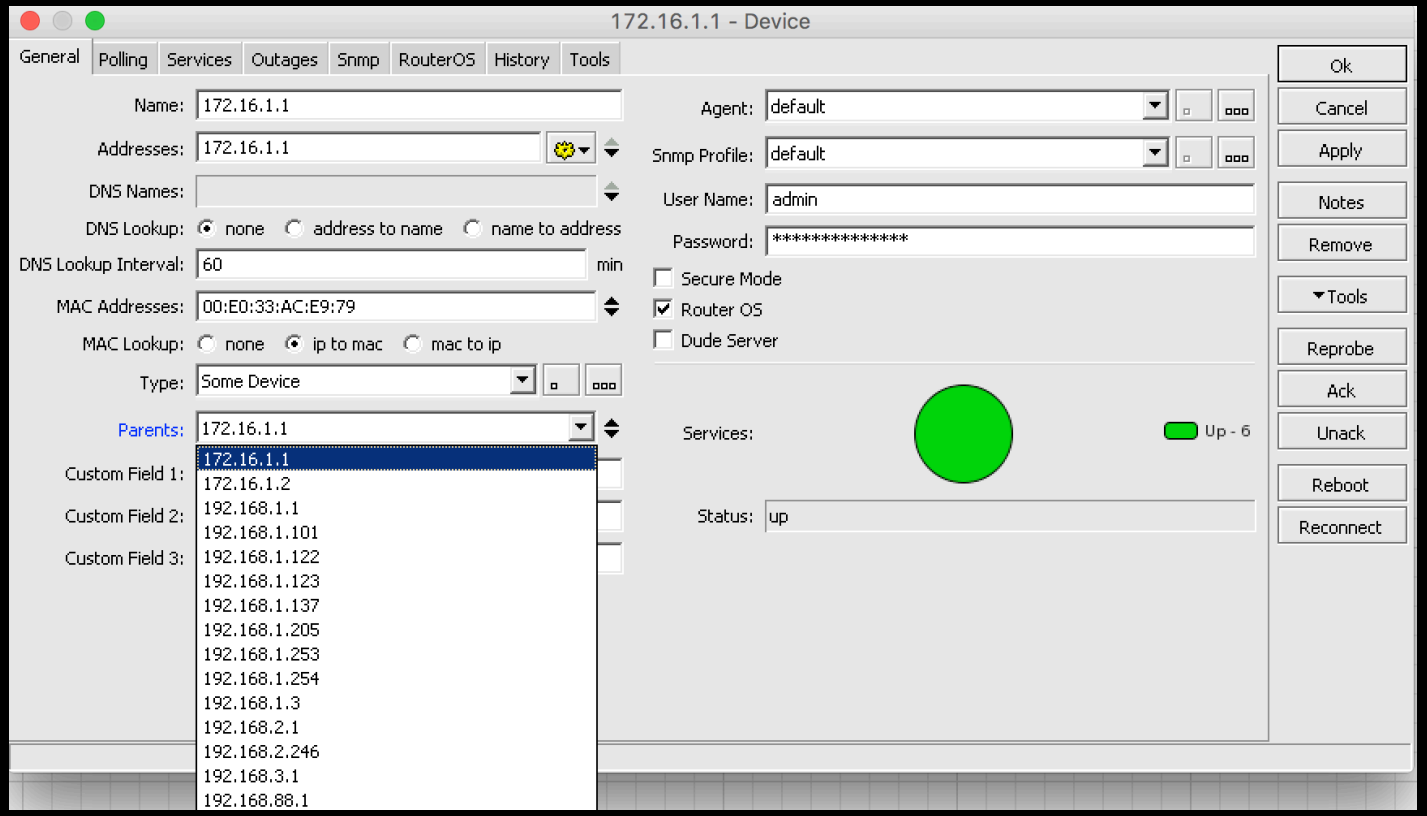
## Maps:

- Map Contains 2 Layers

  1- Device links

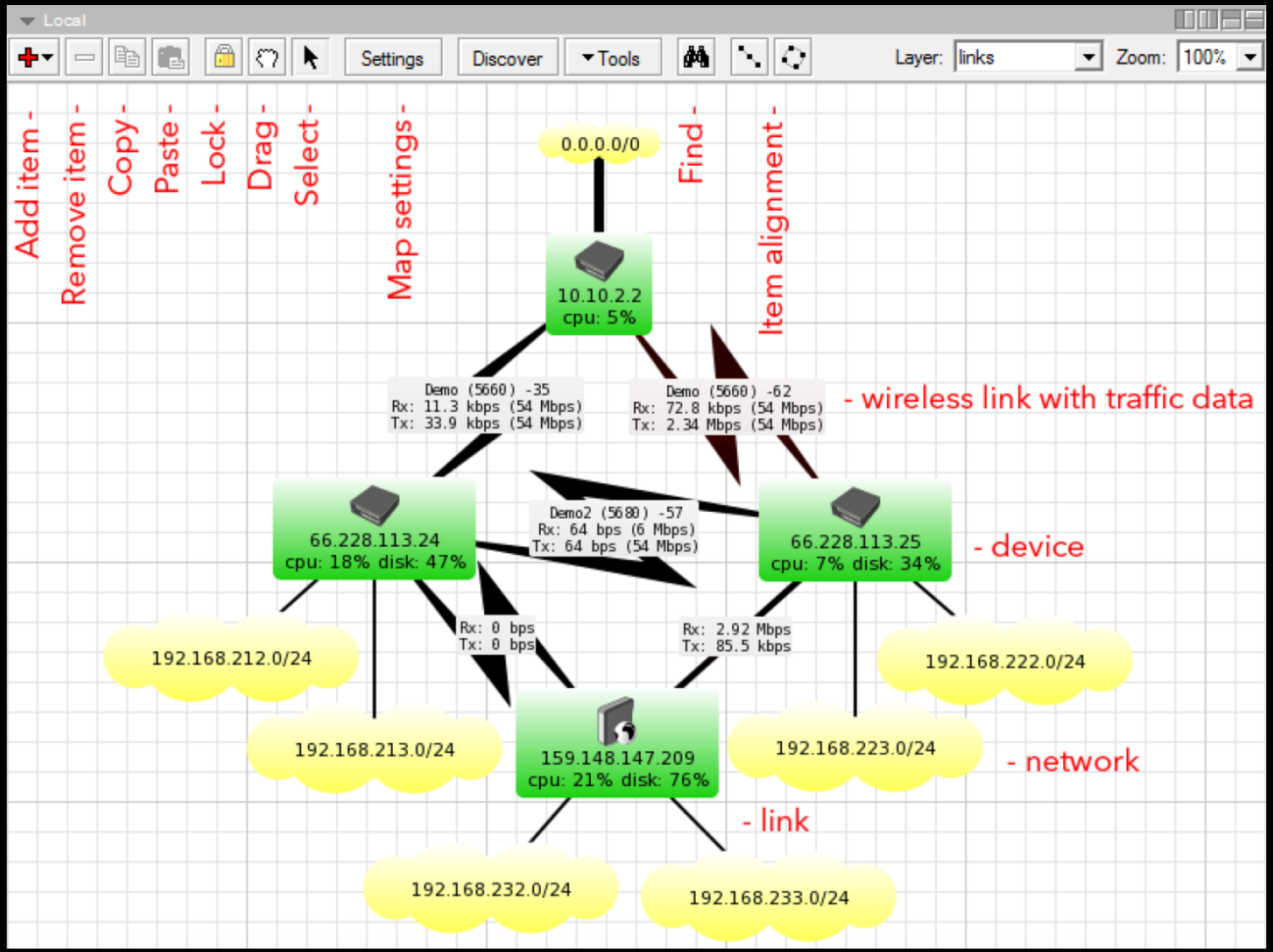
  2- Device dependencies

- To avoid receiving reports about each device status when a parent device is unreachable, you can make dependency between devices



# HOW TO WORK WITH

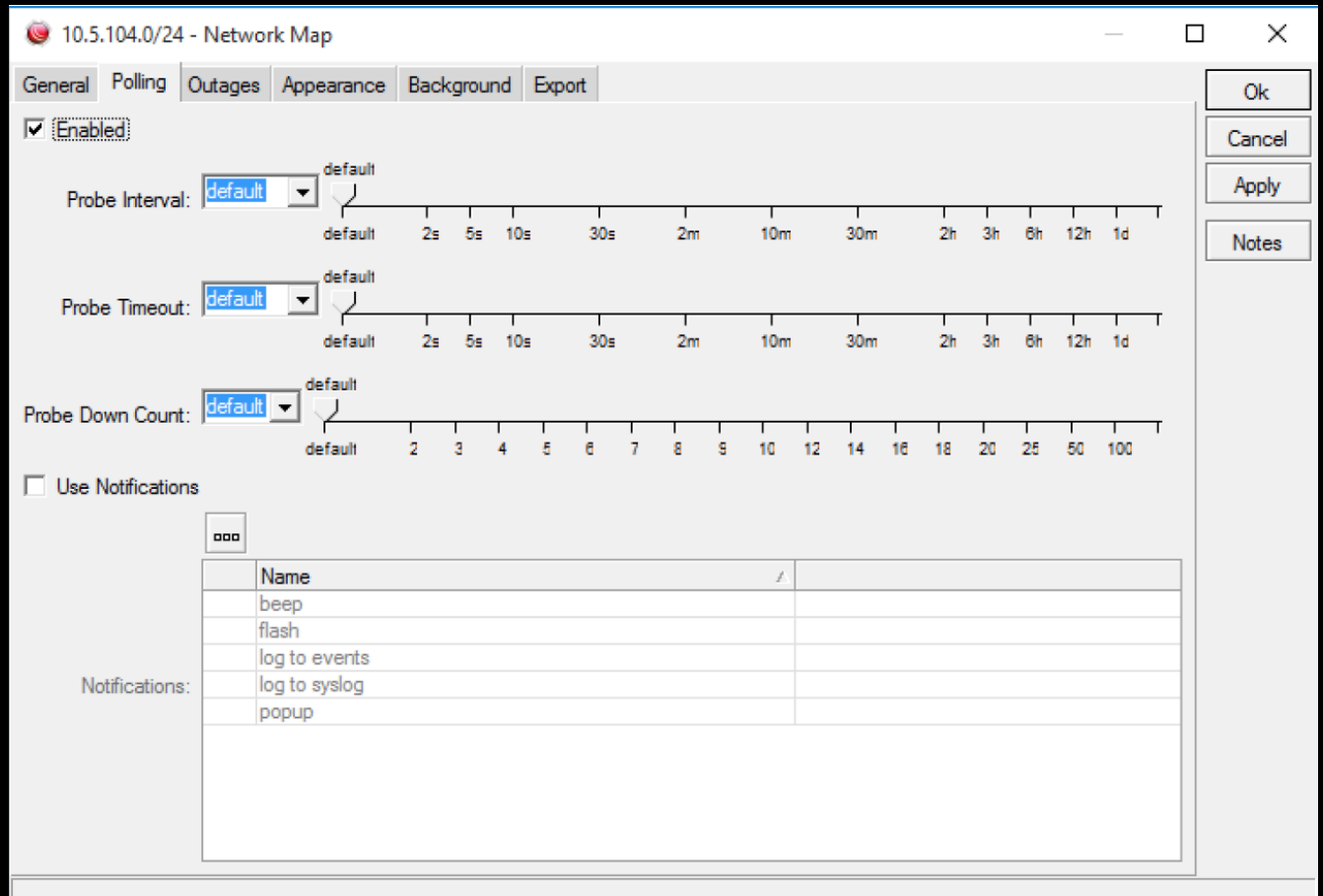
**Maps:**



# HOW TO WORK WITH Maps:

- Polling: This tab allows you to configure polling times and timeouts specifically for this map.

Map specific settings are always overriding general settings, but device specific settings take preference.



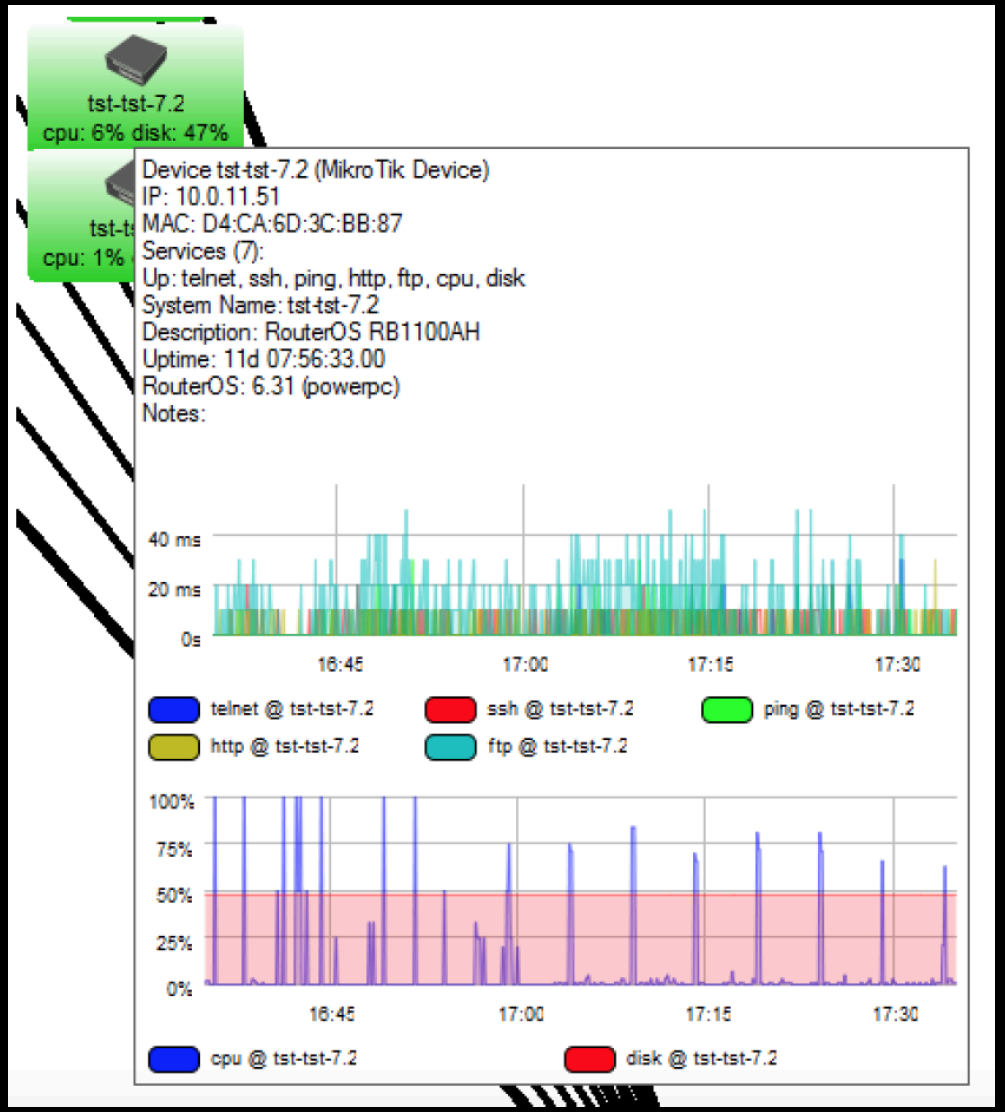
# HOW TO WORK WITH

## By The Way!!!!!!!

- You also can monitor and have a graph of device's Real Time traffic

**Interesting!!! Isn't it????**

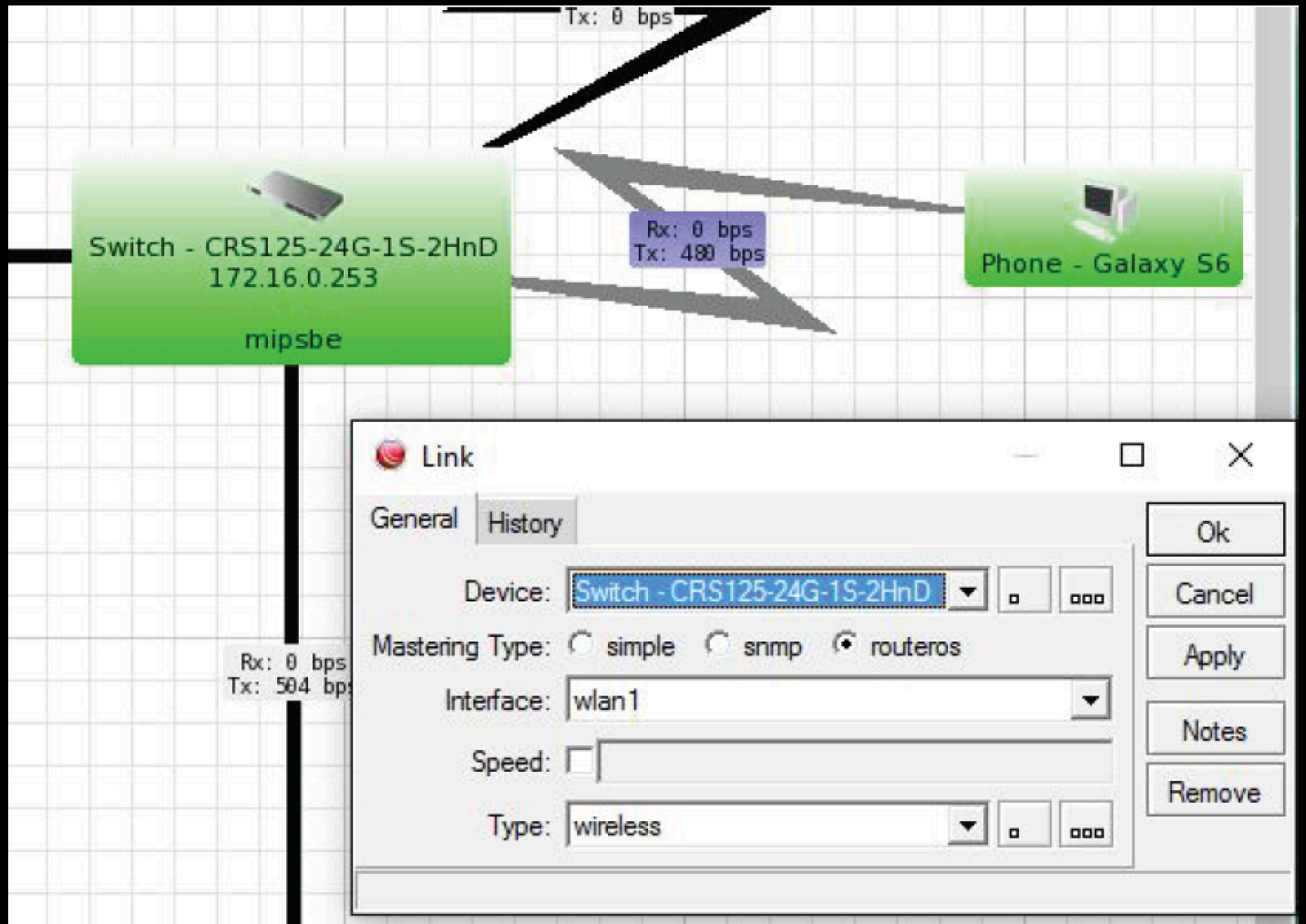
**:) :) :) :)**



# HOW TO WORK WITH

## Links

- Links list, shows all your links (different types)
- Also you can add links directly from the Map



# HOW TO WORK WITH

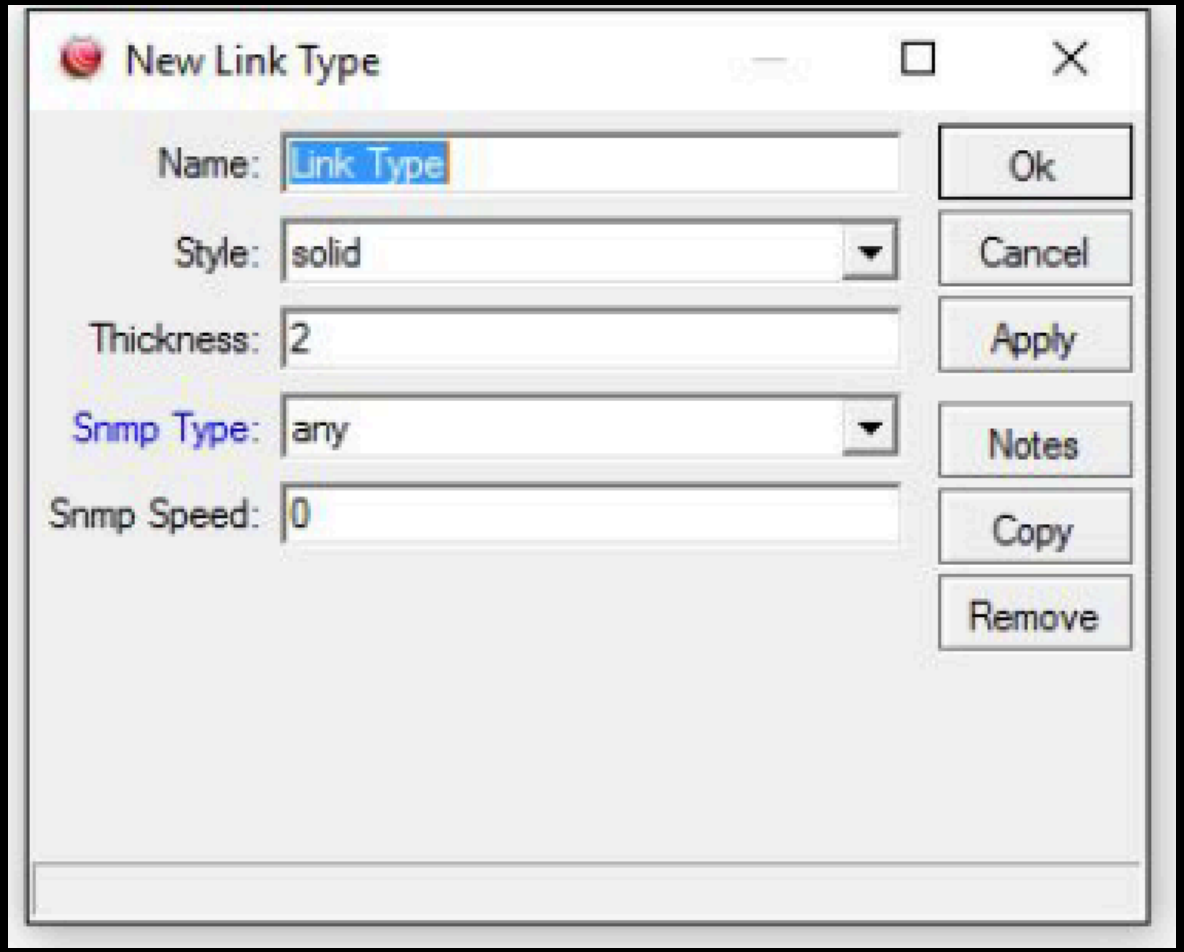
## Links

- By checking out link history, you can find out graphs

# HOW TO WORK WITH

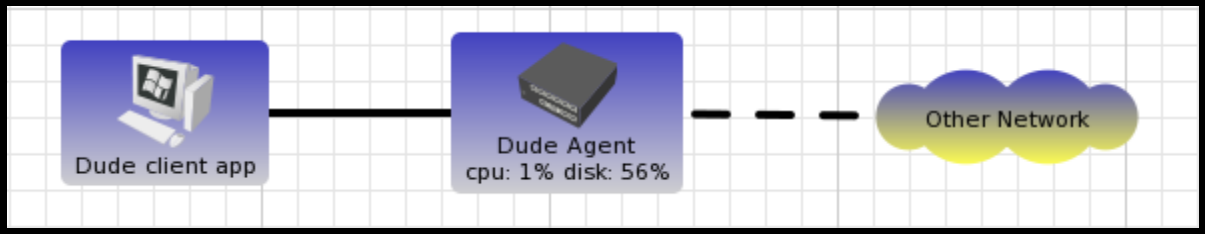
## Links

- There are some Link types by default, but also you can add your own type

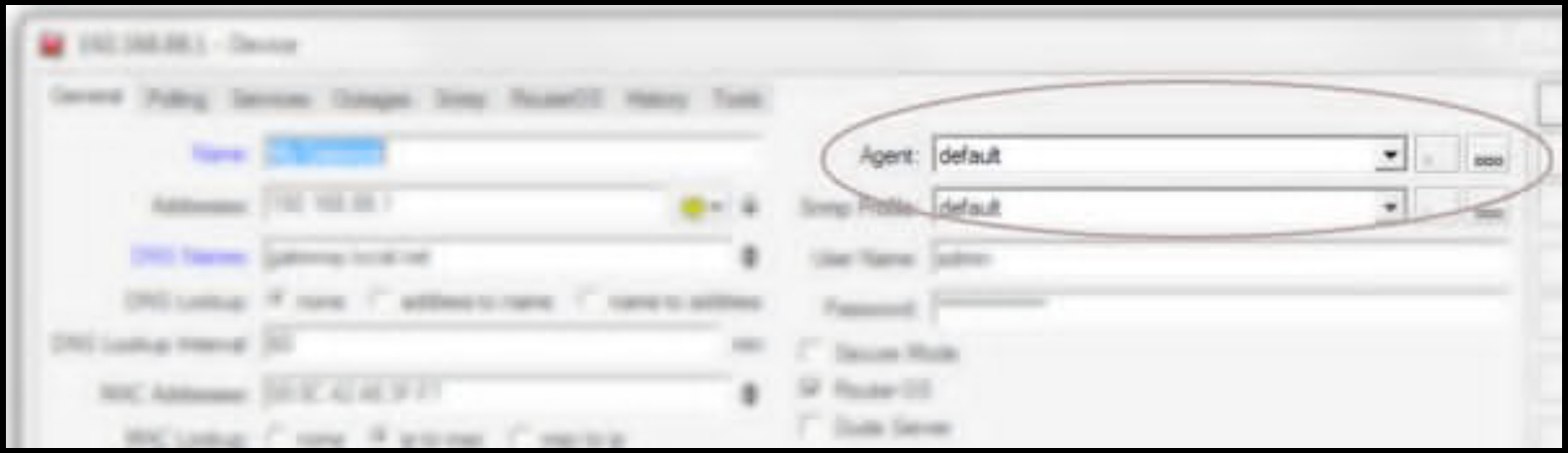


# MONITORING

## Agents




Agents are other Dude servers that can be used as intermediaries f
device monitoring.



# MONITORING

## Notifications:

- It's possible to configure any actions that can be taken when a device status changes.

The predefined Notifications are the following:

1-Beep: Makes a beeping from the PC speaker of the server 2-Flash: Flashes the Dude taskbar menu

3-Log to Events: Saves information to local Event log

4-Log to Syslog: Saves information to Syslog

5-Popup: Opens a small notification window

# MONITORING

**Notifications:**

You can also add new Notifications, more types are available

1-Email: Sends email, need to specify Server address

2-Execute locally: Run command on the local Windows machine (where Dude viewer runs), can pass variables

3-Sound: Plays sound. Sound files can be uploaded and chosen here

4-Group:Executes a group of actions

5-Speak: Uses Windows speech ability to say the message in a computerized voice

6-Log: Saves to local Dude Log file

7-Syslog: Saves to remote Syslog server. Need to specify Syslog address

# BUT SOMETHING IS MISSING HERE!!!!!!!

GSM Notification:
Sending text message to notify!!!!!!

**What??????????**

# NOW, LET'S TALK ABOUT

# iGenTik

- iGenTik is Interactive GSM/Email notification system,

Based on MikroTik platform

with customizable GUI Interface

To notify **anything you imagine**

# WHAT IS IGENTIK

**iGenTik** will be the first of it's kind on a linux system.

Flexible & Robust Monitoring/Notification system

**iGenTik** will be available in 2 format's as Monitoring Server:

iMS (Software only): Interactive Monitoring system

iCMS (Software and Hardware): Interactive Control and Monitoring System

Standard Features:
Monitors your network 24/7 365 days
Send Alerts via email, SMS

**Freeware limited to 100 Sensors:**

Anything which you want to monitor or get notification for, is a Sensor

# IGENTIK

iGenTik | Dashboard | Topology | Configuration | Logout

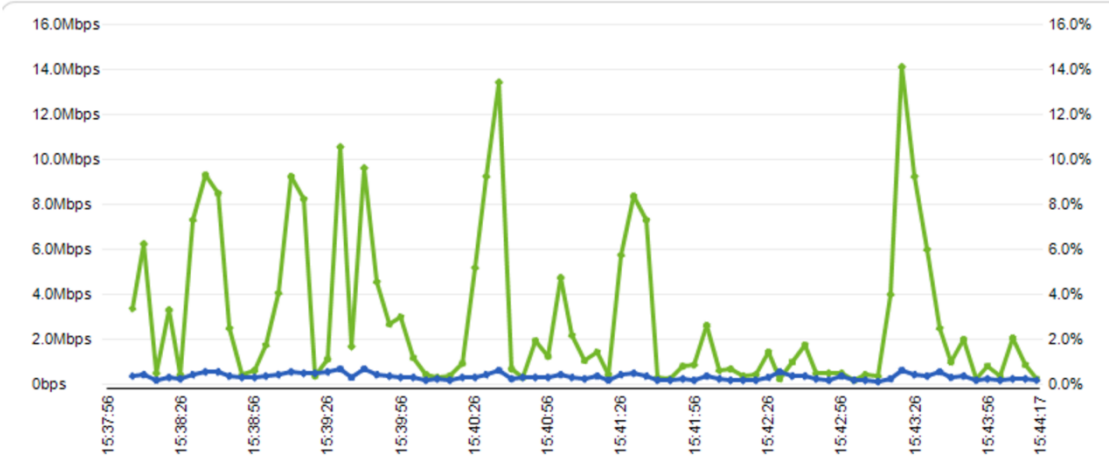
## Devices

⊖ Collapse All | ⊕ Expand All | Add Group

- Igentik
  - Routers
    - Router 1
      - Eth 0
      - Eth 1
      - Eth n
  - Switches
    - Switch 1
      - Eth 1
      - Eth 2
      - Eth 3
      - Eth n
  - Access Points
    - AP 1
      - Sensor 1

## Ethernet 1(Sensor)

| Sensor | Status |
|---|---|
| Sensor 1 | Ok |




Edit | Delete

Key: Okay | Dependent | Partial | Fail

ecnx.net electronic connections limited

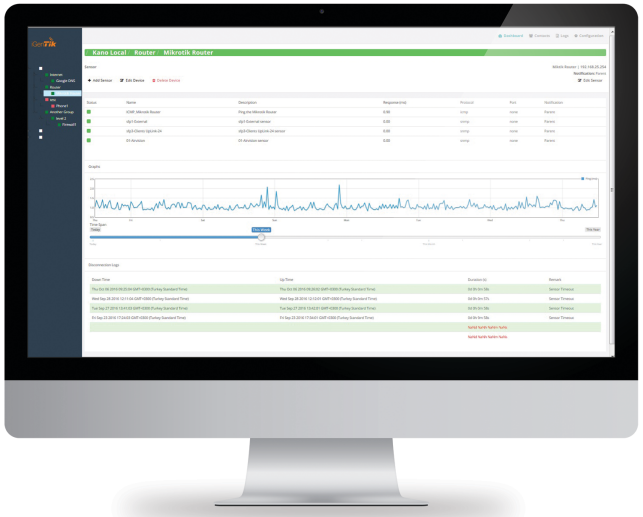
Copyright © 2016 m.it.sco

# iMS

- IP status of all layer3 Devices including: Servers, Routers, Switches, End Points (Printers, Computers, Mobile Phones,)
- Public or Private host reachability and availability monitor
- Up Carrier gateway and reachability monitor: to monitor provider's availability and connectivity (with packet lost monitor feature)
- Standard SNMP Monitoring support
- Power and UPS Monitoring (with special features for APC)
- Logs notification: receiving, managing, analyzing, reporting and notifying of all Standard log files (syslog)
- Full categorised Graphing and historical Data Analysis (RRD Tool for graphing and archiving) (with SNMP or through API)
- Hierarchical topology support (Master, Slave viewer)
- Live Update
- Traffic Control (weird TX/RX bandwidth Monitor)
- Protocol check (weird UDP/TCP.ICM traffic Monitor)

**Extra Modules:**

- iGenApp (Android/iOS APP)
- Cloud Master Control
- Remote (DC,AC) (Solar) Power Network monitoring and Control
- Antivirus Management system integration and notification (Kaspersky special features)
- Elastix (Any VOIP Call Center) logs and reports.



# iCMS More than all iMS Features!

- Dedicated Firewall Hardware with pass throw relays, Battery backup, SMS - GSM Card.
- Built-in battery for the Monitoring Server to have an one hour power Backup.
- Multi Sensors System support (Temperature, humidity monitor and weather Status check)
- Environment Monitoring
- Power Failure detection.
- Pass Throw with Cache, Proxy and Control.
- Sending notification by Text Message
  - Replying Text Messages by receiving any Text Message (means you can send commands to it by messages or emails (trusted numbers or Email Addresses) to get reports or to push doing something) including:
  - Sending remote commands to get reports and logs
  - Sending remote commands to any other device in the Network to
  - Disable/Enable Interface
  - Block/Unblock Users
  - Allow/Terminate any connections
  - Turn on/turn off or restart Servers, routers … via APC Master Switch

## MikroTik Features only

**Any kind of attack:**

- IP/Port Scan
- UDP Flood (i.e. DNS)
- DDOS Attack
- Phishing Attack
- Hijack Attack
- Buffer Attack
- Password Attack
- IP Spoofing
- Sniffing
- Application Layer Attack

**Wireless Control**

- Providing wrong pass by clients for several times
- Registration table reports (list of connected clients)

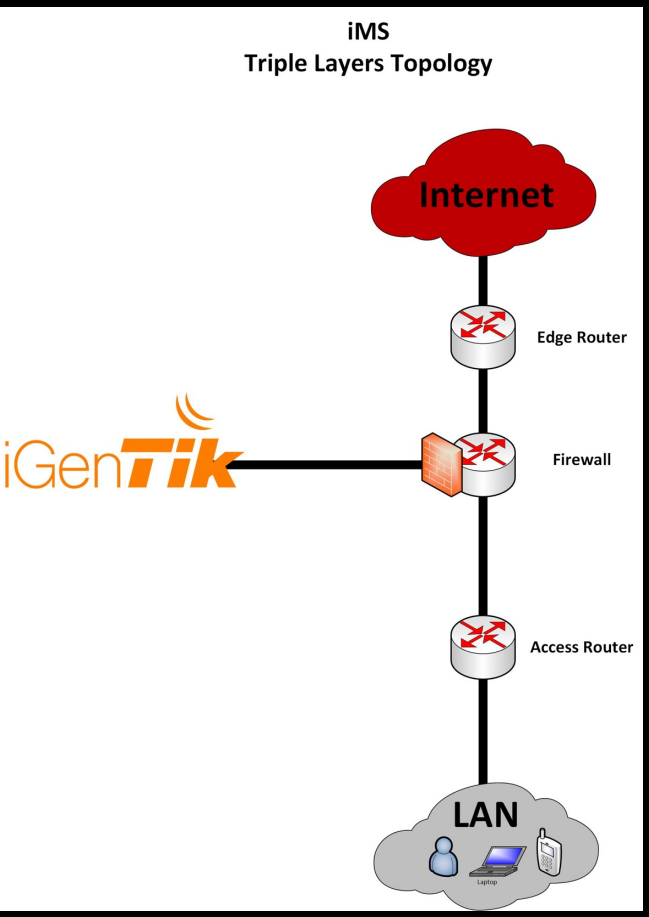
- VPN Connections: Alert as soon as a VPN connection get connected.
- Tunnel Connections: Alert as soon as a Tunnel connection get connected.
- Queuing Control : Alert if one queue rule gets 50%, 75% or 100% of Bandwidth
- By Adding any route (Static, Dynamic) in routing table.
- Firewall/NAT/Mangle Control: Adding any rules in these tables
- Full Control by Add and Removing Rule to any part of the Router Dynamically depending on Rules and trigger's.

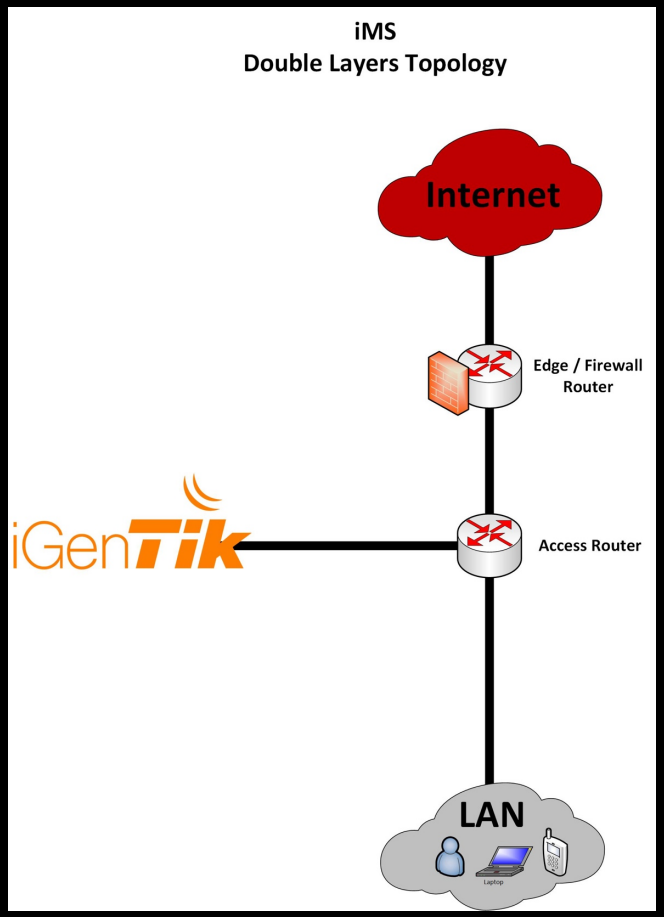

IGENTIK.MITS-CO.COM

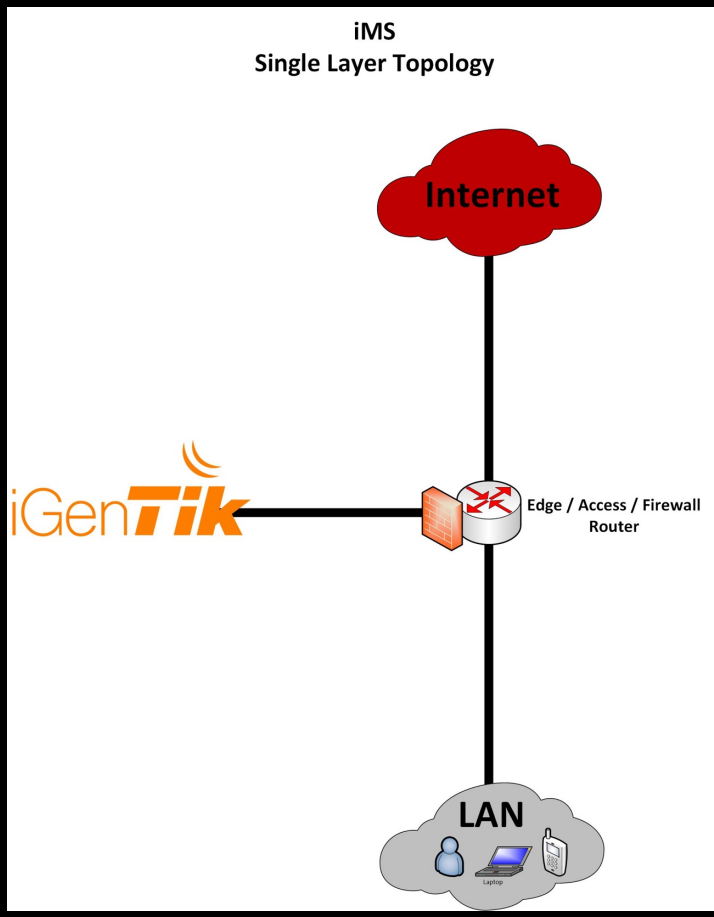
# IMS

- IP status of all layer3 Devices including: Servers, Routers, Switches, End Points (Printers, Computers, Mobile Phones,)
- Public or Private host reachability and availability monitor
- Up Carrier gateway and reachability monitor: to monitor provider's availability and connectivity (with packet lost monitor feature)
- Standard SNMP Monitoring support
- Power and UPS Monitoring (with special features for APC)
- Logs notification: receiving, managing, analyzing, reporting and notifying of all Standard log files (syslog)
- Full categorized Graphing and historical Data Analysis (RRD2 Tool for graphing and archiving) (with SNMP or through API)
- Hierarchical topology support (Master, Slave viewer)
- Live Update
- Traffic Control (weird TX/RX bandwidth Monitor)
- Protocol check (weird UDP/TCP.ICM traffic Monitor)

# IMS


iMS
Triple Layers Topology
Internet
Edge Router
Firewall
Access Router
LAN
iGenTik


iMS
Double Layers Topology
Internet
Edge / Firewall Router
Access Router
LAN
iGenTik

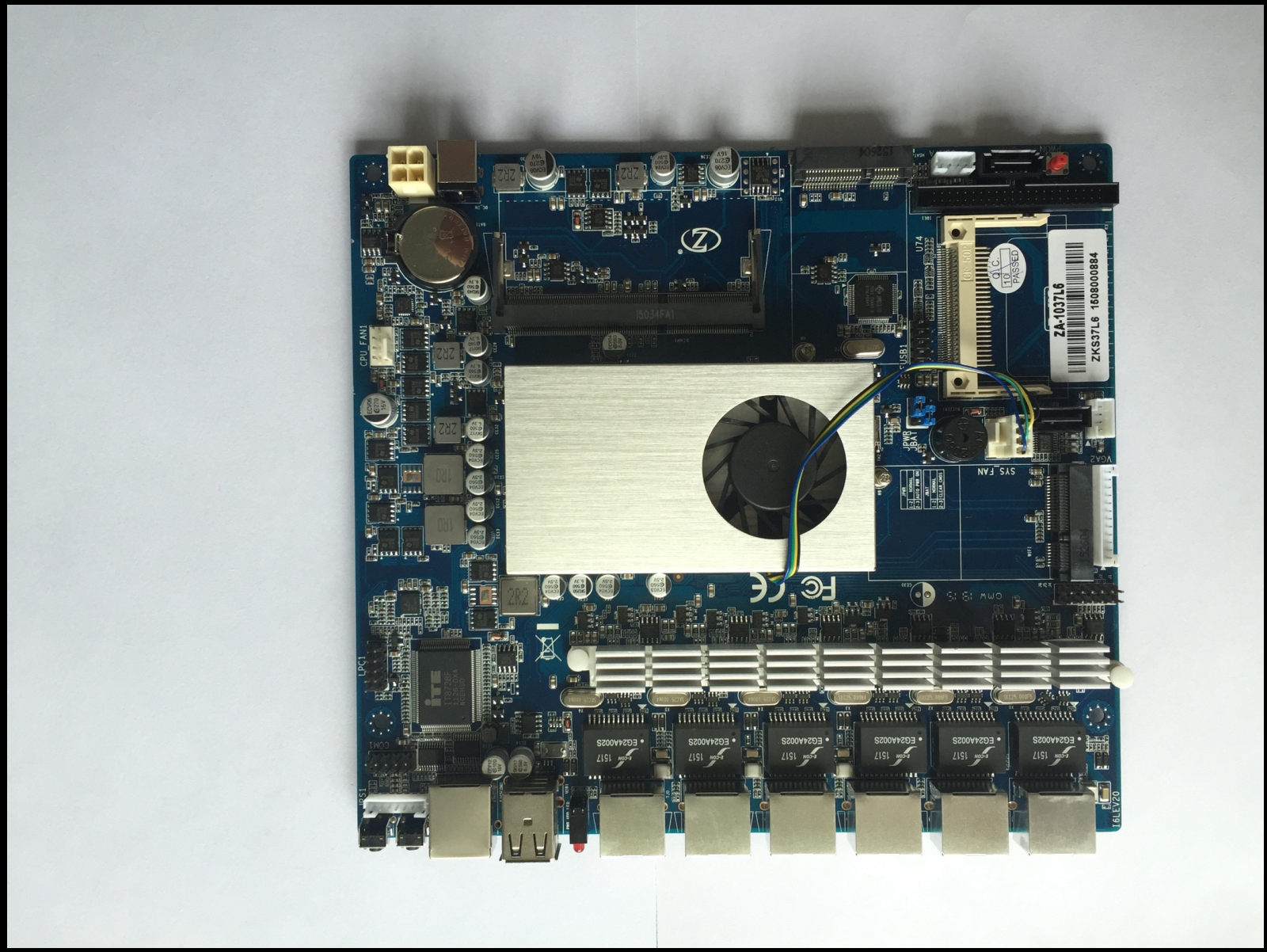

iMS
Single Layer Topology
Internet
Edge / Access / Firewall Router
LAN
iGenTik

# ICMS

More than all iMS Features!

- Dedicated Firewall Hardware with pass throw relays, Battery backup, SMS - GSM Card.
- Built-in battery for the Monitoring Server to have an one hour power Backup.
- Multi Sensors System support (Temperature, humidity monitor and weather Status check)
- Environment Monitoring
- Power Failure detection.
- Pass Throw with Cache, Proxy and Control.
- Sending notification by Text Message
  - Replying Text Messages by receiving any (means you can send commands to it by messages or emails (trusted numbers or Email Addresses) to get reports or to push doing something) including:
  - Sending remote commands to get reports and logs
  - Sending remote commands to any other device in the Network to
  - Disable/Enable Interface
  - Block/Unblock Users
  - Allow/Terminate any connections
  - Turn on/turn off or restart Servers, routers … via APC Master Switch

# ICMS


CPU_FAN1
SYS_FAN
ZA-1037L6
ZKS37L6 1608000884
PASSED
EG24A00ZS

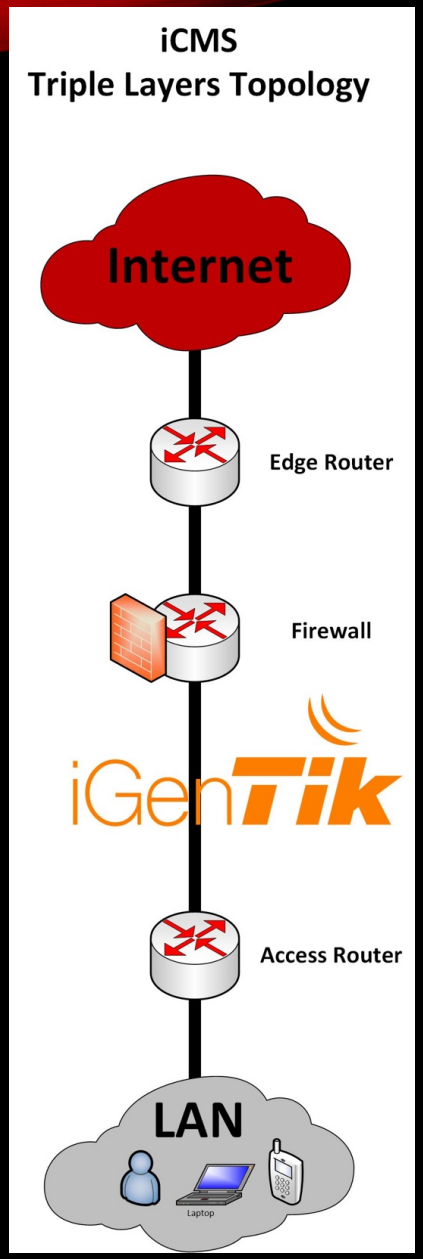
# ICMS

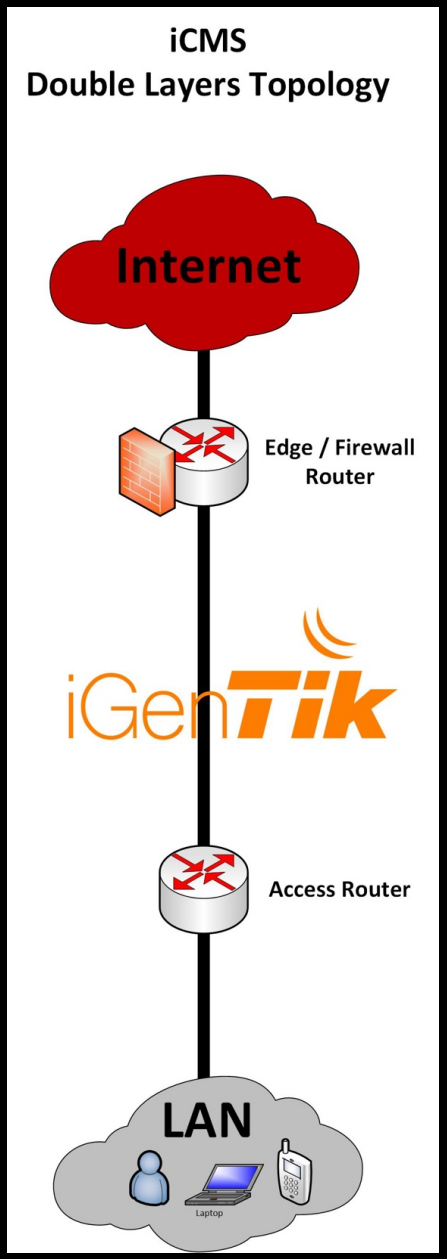
POWER
HDD
USB1/2
CONSOLE
ETH0
ETH1
ETH2
ETH3
ETH4
ETH5
BYPASS_SW
OFF
ON

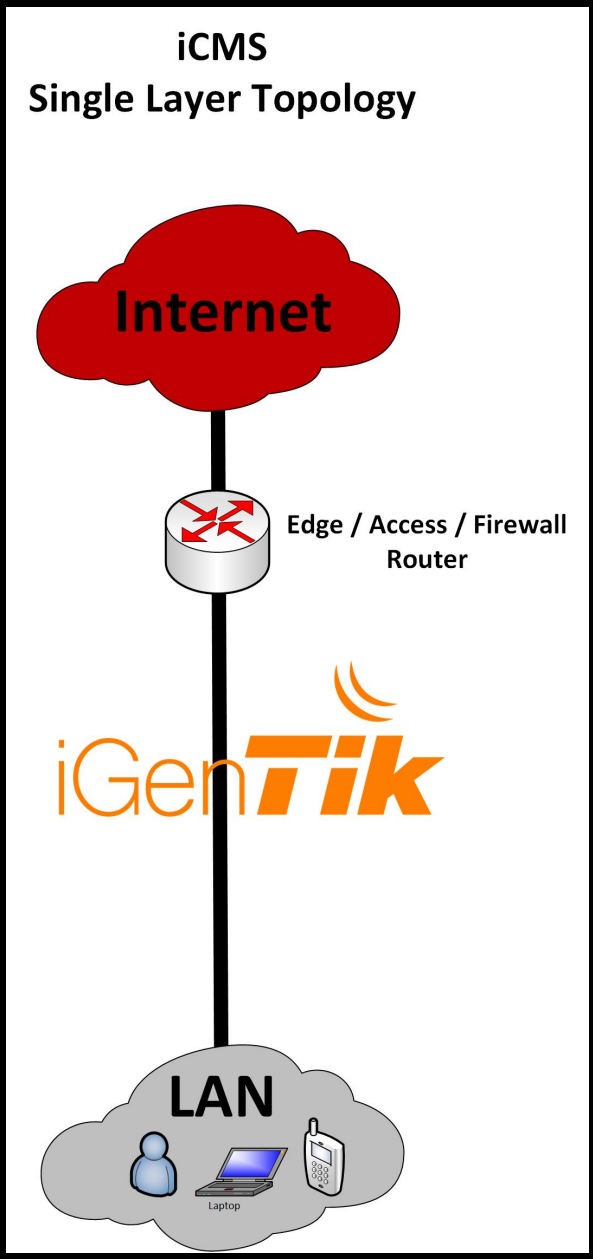
m.it.s co
www.mits-co.com
Console
USB
ETH0
ETH1
ETH2
ETH3
ETH4
ETH5
SW
HDD
PWR
iGenTik
I(C)MS-6GU

m.it.s co
www.mits-co.com
Console
USB
ETH0
ETH1
ETH2
ETH3
ETH4
ETH5
SW
HDD
PWR
iGenTik
i(C)MS-6GU

# ICMS


iCMS
Triple Layers Topology
Internet
Edge Router
Firewall
iGenTik
Access Router
LAN
Laptop


iCMS
Double Layers Topology
Internet
Edge / Firewall
Router
iGenTik
Access Router
LAN
Laptop


iCMS
Single Layer Topology
Internet
Edge / Access / Firewall
Router
iGenTik
LAN
Laptop

# IGENTIK EXTRA MODULES

- iGenApp (Android/iOS APP)
- Cloud Master Control
- Remote (DC,AC) (Solar) Power Network monitoring and Control
- Antivirus Management system integration and notification (Kaspersky special features)
- Elastix (Any VOIP Call Center) logs and reports.

# MIKROTIK FEATURES ONLY

## Any kind of attack:

- IP/Port Scan
- UDP Flood (i.e. DNS)
- DDOS Attack
- Phishing Attack
- Hijack Attack
- Buffer Attack
- Password Attack
- IP Spoofing
- Sniffing
- Application Layer Attack

## Wireless Control

- Providing wrong pass by clients for several times
- Registration table reports (list of connected clients)
- Unwanted wireless login

- VPN Connections: Alert as soon as a VPN connection get connected.
- Tunnel Connections: Alert as soon as a Tunnel connection get connected.
- Queuing Control : Alert if one queue rule gets 50%, 75% or 100% of Bandwidth
- By Adding any route (Static, Dynamic) in routing table.
- Firewall/NAT/Mangle Control: Adding any rules in these tables
- Full Control by Add and Removing Rule to any part of the Router Dynamically depending on Rulesand trigger's.

ANY
questions?

# CONTACT DETAILS


Turk Cell: +90 (537) 495 3233

Skype: mani_raissdana

m.raissdana@mits-co.com

raissdana.mani@gmail.com

www.mits-co.com


YouTube

MikroTikEngineers

mani_raissdana mikrotikiran @mani_raissdana Mani Raissdana

GOOD LUCK
&
ENJOY MUM