

m.it.sco

Morvarid. IT. Solutions Co.

MikroTik

MUM -Kathmandu, Nepal

June 2<sup>nd</sup> 2017

Dude Server  
iGenTik

By

Mani Raissdana

SAFE ZONE

# MANI RAISSDANA

MikroTik Certified Trainer  
CTO & Co-Founder of



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](http://www.mits-co.com/sites/default/files/Mani%20Raissdana%20Resume.pdf)

# TABLE OF CONTENTS

## Dude

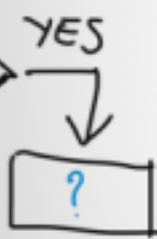
- What is Dude???
- What it does???
- How it works???
- How you should work with???
- Monitoring
- Notification

## iGenTik

Interactive GSM/Email notification system



FORUM SOCIAL NETWORK CONTENT SHARING  
MICROBLOGS SOCIAL MEDIA VIDEO  
COMMUNICATION CHAT PICTURE



35%  
\$



SEARCH ENGINE DESIGN MEDIA  
WEB SITE



STATISTICS

	LAST YEAR	THIS YEAR
\$	500.000	1.000.000

QUALITY STRATEGY VISION  
SUCCESS



# 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**

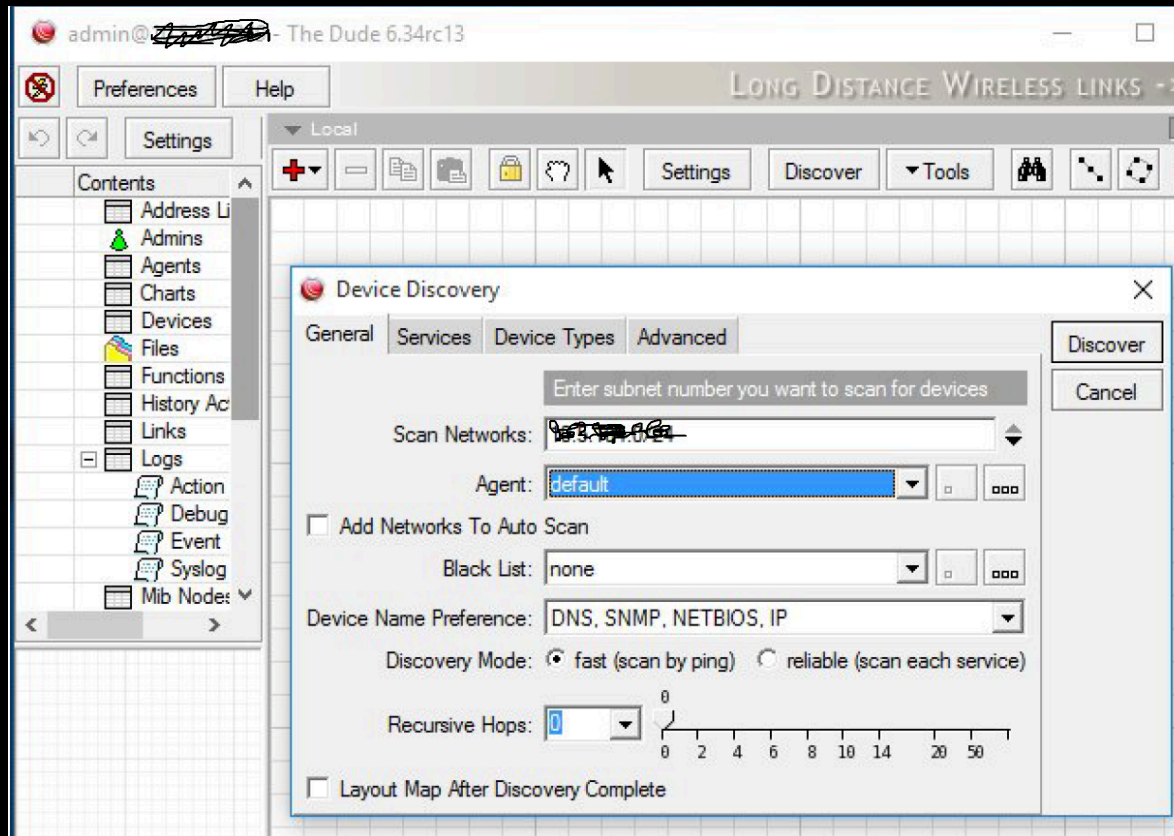
# WHAT IT DOES

- 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

# Interface

# HOW TO WORK WITH

The screenshot displays the Mikrotik WinBox interface, which is divided into several panes. The main window is titled "admin@gateway.lan - The Dude" and "rc45". The interface is organized into three main sections:

- Map Pane:** A central pane showing a network topology diagram with various nodes and connections. It is titled "Map Pane" and "FIREWALL AND BANDWIDTH CONTROL -> WWW".
- Log Pane:** A pane on the right displaying a Syslog log. It is titled "Syslog" and "Log Pane". The log shows a list of events with columns for Time, Address, and Event.
- Panes Panel:** A vertical panel on the left side of the interface, titled "Panels" and "Panels". It contains a tree view of the interface's contents, including Address Lists, Admins, Agents, Charts, Chart Chart, Devices, Files, Functions, History Actions, Links, Logs, Action, Debug, Event, Syslog, Mib Nodes, Network Maps, Local, hone-net, Networks, Notifications, Probes, and Services.

The Syslog log pane contains the following data:

Time	Address	Event
Jan/15 13:45:43	10.5.104.89	Service telnet on 10.5.104.89
Jan/15 13:45:43	10.5.104.240	system.info.account user admin
Jan/15 13:47:43	127.0.0.1	Service pop3 on gateway.lan is now
Jan/15 13:47:43	127.0.0.1	Service telnet on gateway.lan is now
Jan/15 13:47:43	10.5.104.250	Service smtp on 3k.lan is now
Jan/15 13:47:43	10.5.104.250	Service pop3 on 3k.lan is now
Jan/15 13:47:43	10.5.104.241	Service pop3 on new.lan is now
Jan/15 13:47:43	10.5.104.85	Service pop3 on 10.5.104.85 is now
Jan/15 13:47:43	10.5.104.85	Service smtp on 10.5.104.85 is now
Jan/15 13:47:43	10.5.104.243	Service pop3 on ppc.lan is now
Jan/15 13:47:43	10.5.104.75	Service cpu on 10.5.104.75 is now
Jan/15 13:47:43	10.5.104.212	Service pop3 on crs212.lan is now
Jan/15 13:47:43	10.5.104.76	Service cpu on 10.5.104.76 is now
Jan/15 13:47:43	10.5.104.109	Service telnet on crs109.lan is now
Jan/15 13:47:43	10.5.104.109	Service pop3 on crs109.lan is now
Jan/15 13:47:43	10.5.104.252	Service pop3 on 10.5.104.252 is now
Jan/15 13:47:43	10.5.104.249	Service pop3 on nine.lan is now
Jan/15 13:47:43	10.5.104.210	Service smtp on crs210.lan is now
Jan/15 13:47:43	10.5.104.240	Service pop3 on sfp.lan is now
Jan/15 13:47:43	10.5.104.245	Service pop3 on plus.lan is now
Jan/15 13:47:43	10.5.104.243	Service telnet on ppc.lan is now
Jan/15 13:47:43	10.5.104.246	Service telnet on crs226.lan is now
Jan/15 13:47:43	10.5.104.112	Service telnet on crs112.lan is now
Jan/15 13:47:43	10.5.104.212	Service telnet on crs212.lan is now
Jan/15 13:47:43	10.5.104.51	Service smtp on 10.5.104.51 is now
Jan/15 13:47:43	10.5.104.89	Service ssh on 10.5.104.89 is now
Jan/15 13:47:43	10.5.104.88	Service pop3 on 10.5.104.88 is now
Jan/15 13:47:43	10.5.104.88	Service smtp on 10.5.104.88 is now
Jan/15 13:47:43	10.5.104.210	Service pop3 on crs210.lan is now
Jan/15 13:47:43	10.5.104.51	Service pop3 on 10.5.104.51 is now
Jan/15 13:47:43	10.5.104.245	Service telnet on plus.lan is now
Jan/15 13:47:43	10.5.104.249	Service smtp on nine.lan is now
Jan/15 13:47:43	10.5.104.112	Service pop3 on crs112.lan is now
Jan/15 13:47:43	10.5.104.252	Service telnet on 10.5.104.252 is now
Jan/15 13:47:43	10.5.104.89	Service smtp on 10.5.104.89 is now
Jan/15 13:47:43	10.5.104.89	Service pop3 on 10.5.104.89 is now
Jan/15 13:47:43	10.5.104.246	Service pop3 on crs226.lan is now
Jan/15 13:47:43	10.5.104.50	Service pop3 on 10.5.104.50 is now
Jan/15 13:47:43	10.5.104.50	Service smtp on 10.5.104.50 is now
Jan/15 13:47:43	10.5.104.84	Service md 50:50 on 10.5.104.84

# HOW TO WORK WITH

## Menu

Menu

The screenshot shows the HotSpot Controller web interface. The main area displays a network diagram with several nodes and connections. A red box highlights the sidebar menu on the left, which contains various navigation options. A red arrow points from the word 'Menu' to the sidebar menu.

Client: rx 1.17 kbps / tx 268 bps Server: rx 2.81 kbps / tx 129 kbps

The screenshot shows the 'Contents' sidebar menu with the following items:

- Address Lists
- Admins
- Charts
- Chart Chart
- Devices
- Files
- Functions
- History Actions
- Links
- Logs
  - Action
  - Debug
  - Event
  - Syslog
- Mib Nodes
- Network Maps
  - Local
  - Networks
  - Notifications
  - Outages
- Panels
  - admin 159.148.1...
  - amis 10.5.8.253
  - demo 159.148.17...
- Probes
- Services
- Tools

# 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

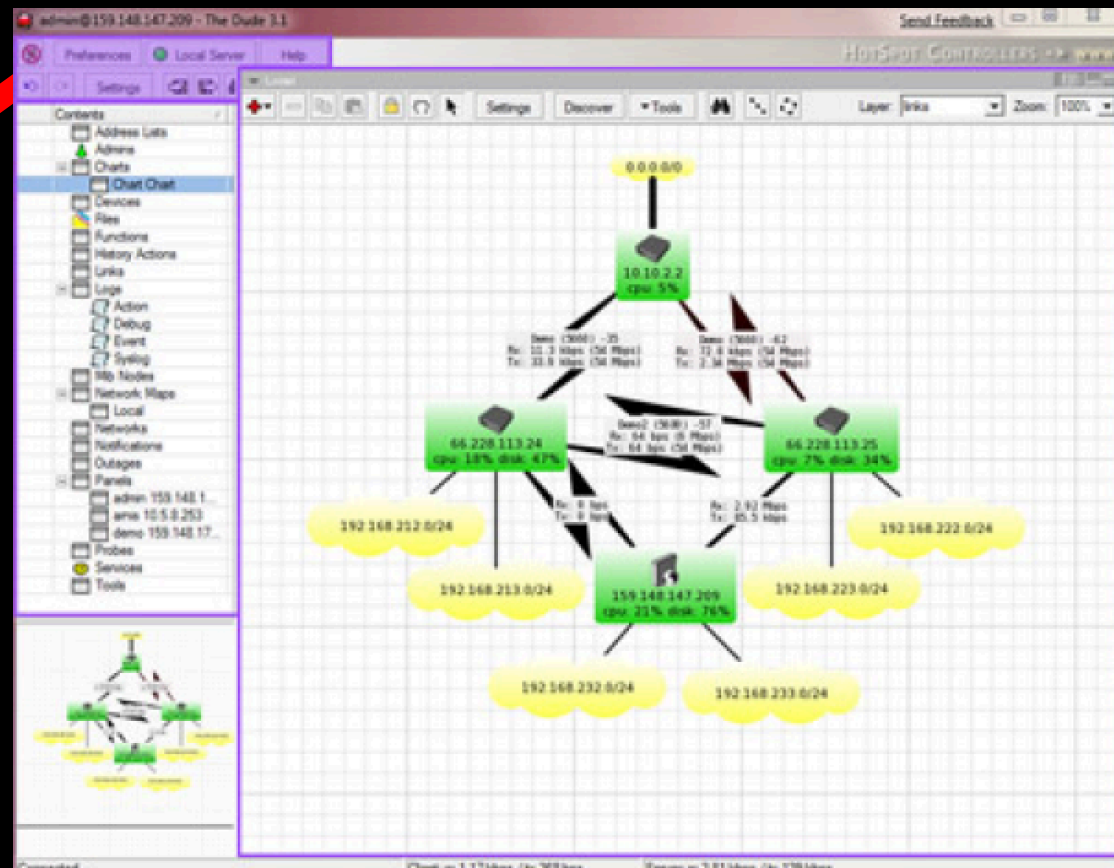
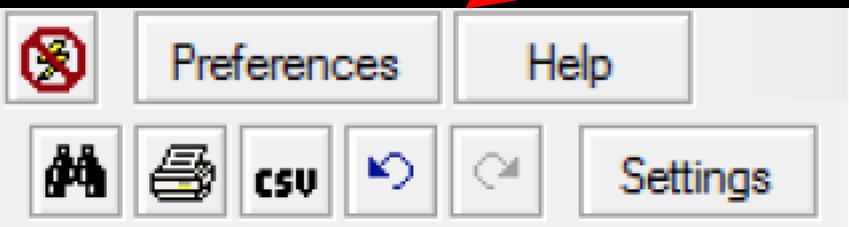
**Probes:** Probes are responsible for polling specific services on the defices

**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.)

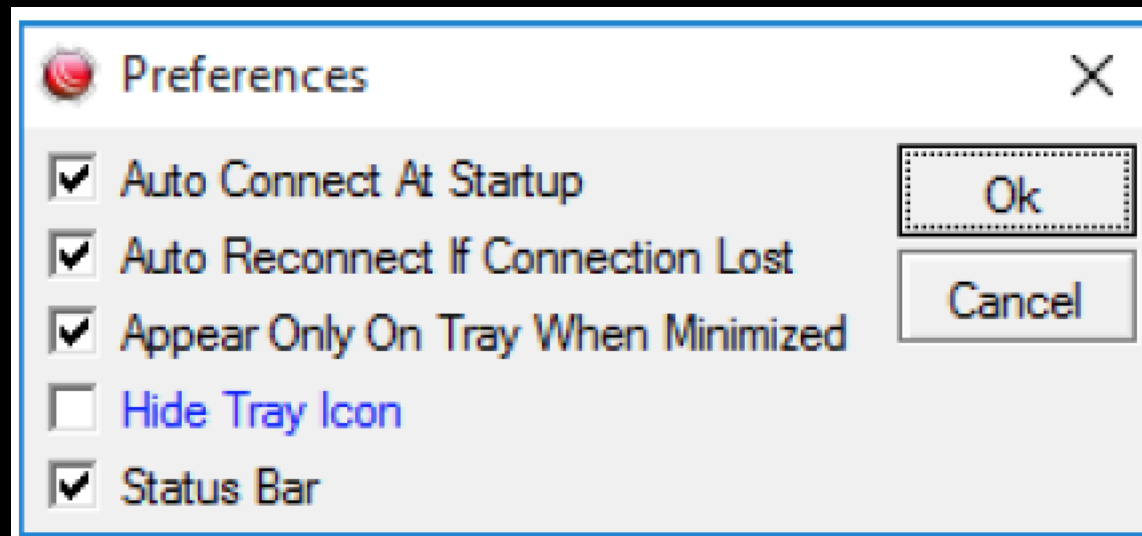
# HOW TO WORK WITH

## Server Settings



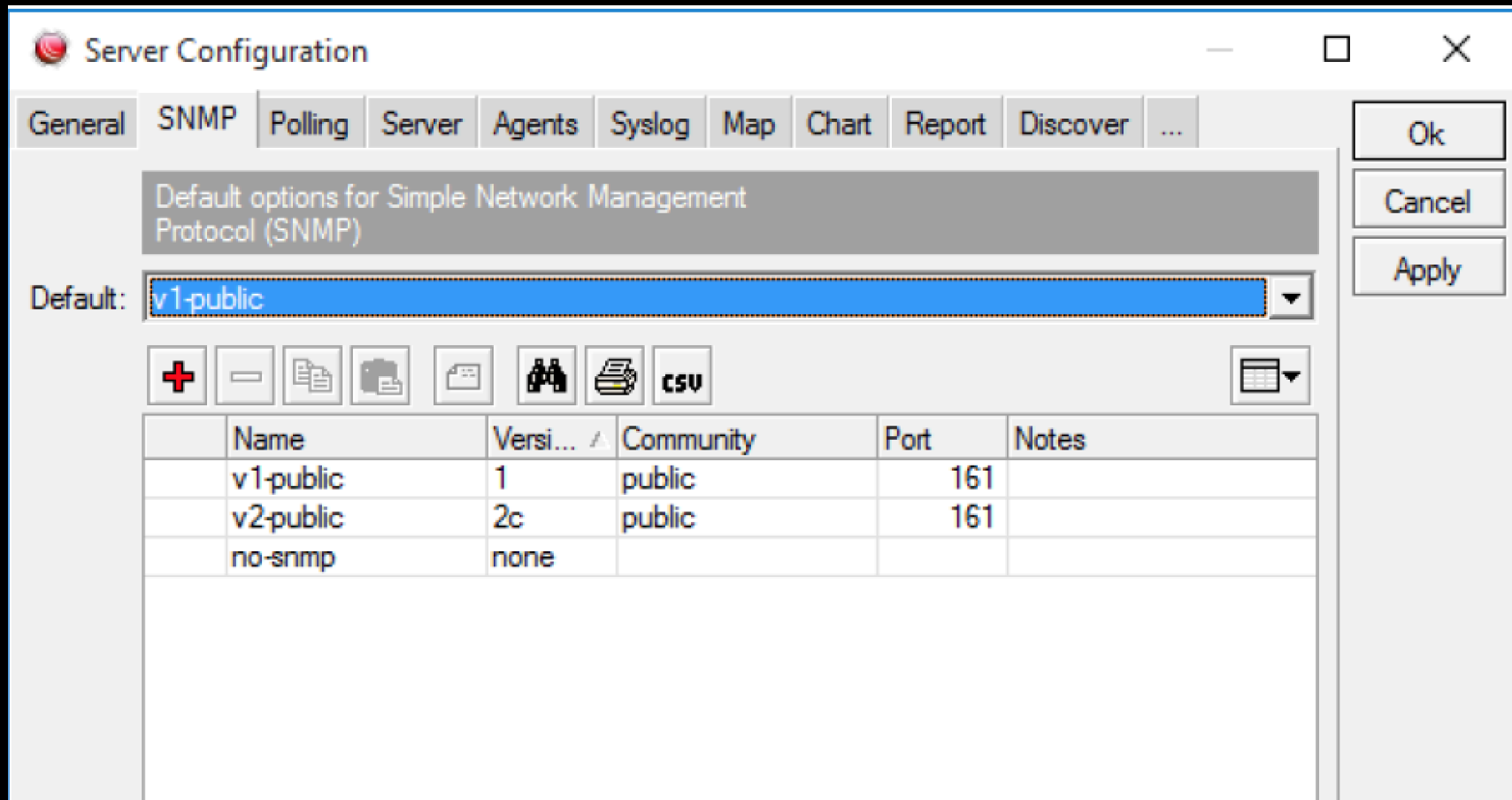
# HOW TO WORK WITH

## Preferences



# HOW TO WORK WITH

## Server Settings



Server Configuration

General | **SNMP** | Polling | Server | Agents | Syslog | Map | Chart | Report | Discover | ...

Default options for Simple Network Management Protocol (SNMP)

Default: v1-public

+ - [Icons] CSV

Name	Versi... /	Community	Port	Notes
v1-public	1	public	161	
v2-public	2c	public	161	
no-snmp	none			

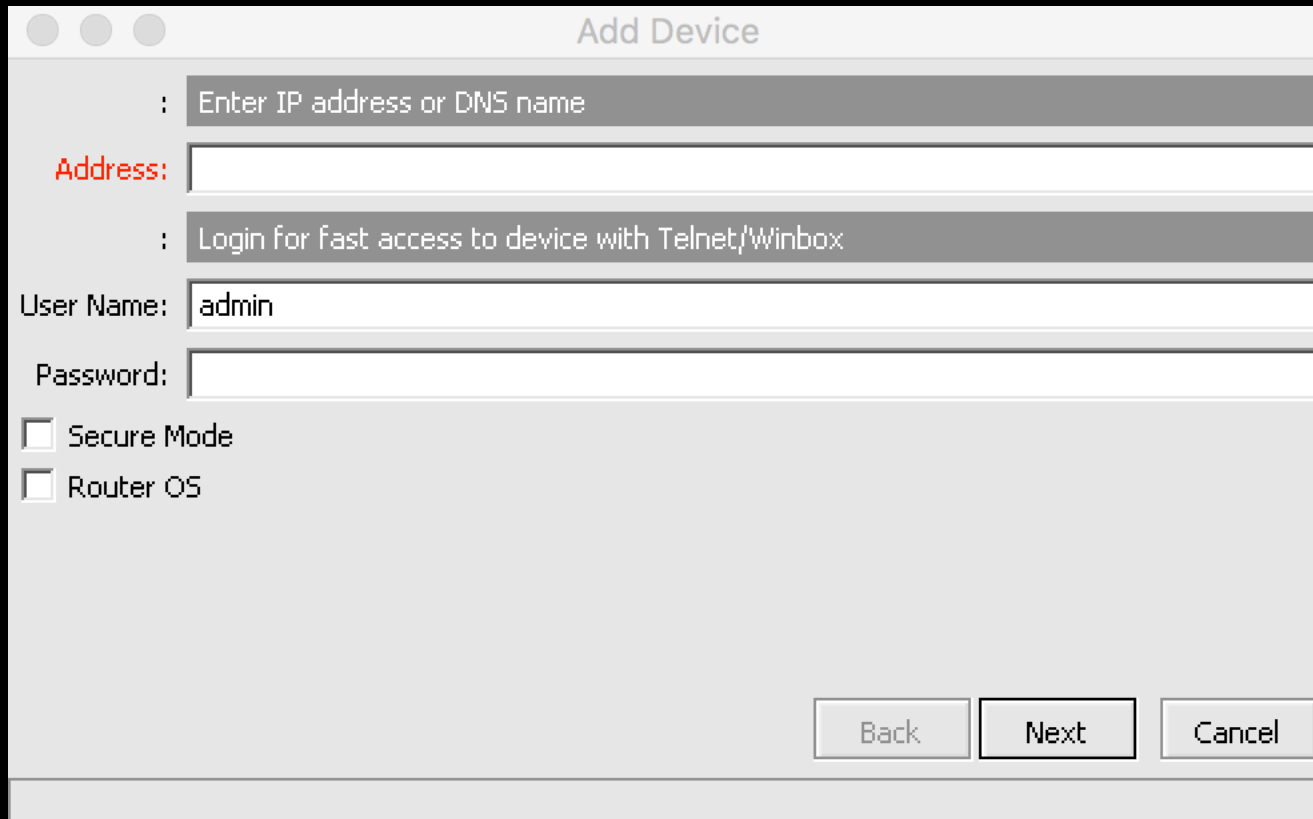
Ok  
Cancel  
Apply

# HOW TO WORK WITH

## Device Settings

- Adding devices is just few steps:

1-



The screenshot shows a dialog box titled "Add Device" with the following fields and options:

- A grey header bar with the text "Add Device".
- A grey bar with the text "Enter IP address or DNS name".
- A red label "Address:" followed by an empty text input field.
- A grey bar with the text "Login for fast access to device with Telnet/Winbox".
- A label "User Name:" followed by a text input field containing the text "admin".
- A label "Password:" followed by an empty text input field.
- Two unchecked checkboxes: "Secure Mode" and "Router OS".
- Three buttons at the bottom: "Back", "Next", and "Cancel".

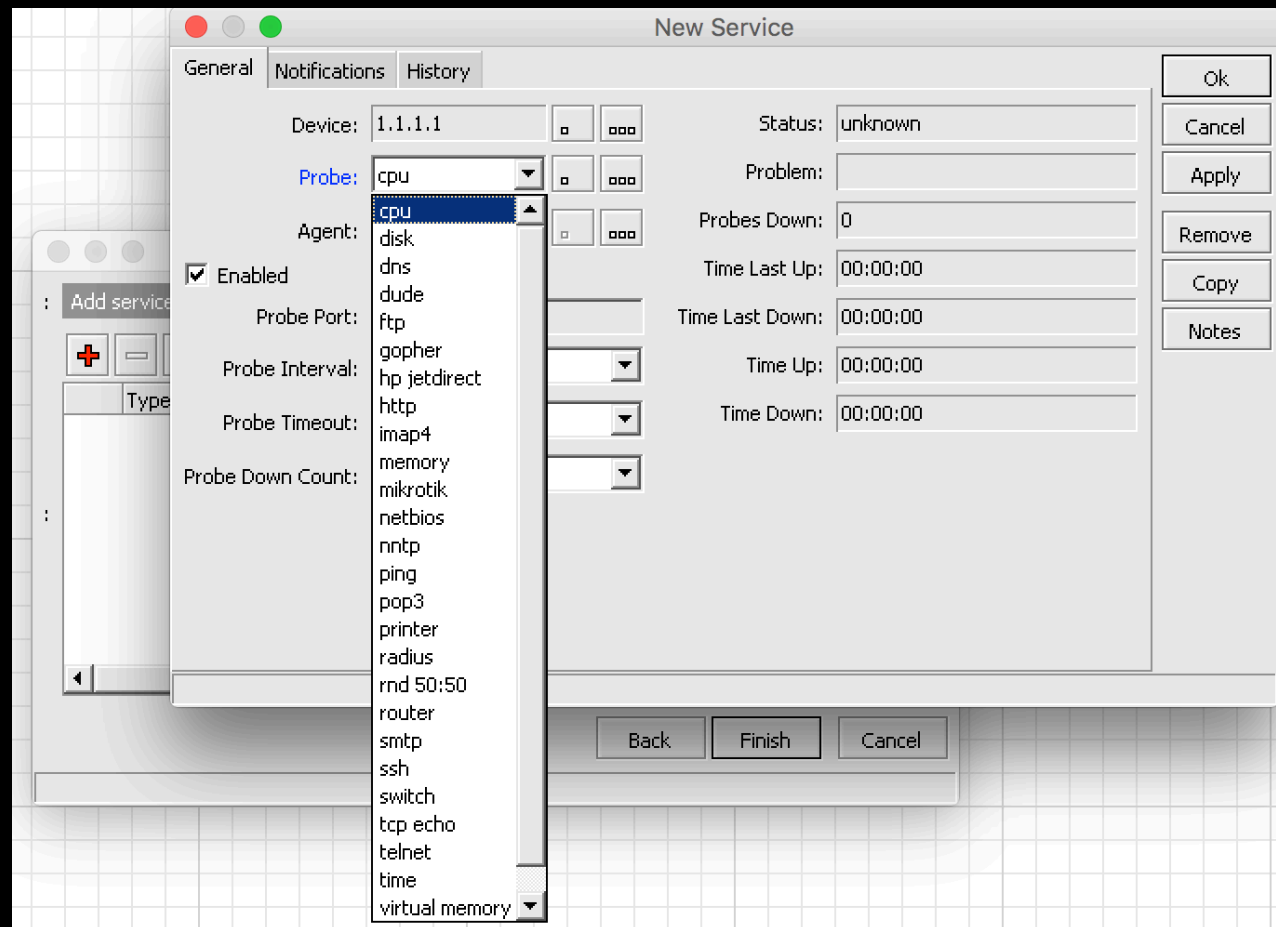


# Device Settings

# HOW TO WORK WITH

- Adding devices is just few steps:

2-





# HOW TO WORK WITH


## Device Settings


192.168.16.105 - Device

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


Name: 192.168.16.105


Addresses: 192.168.16.105  




DNS Names: 


DNS Lookup: address to name 

DNS Lookup Interval: 60 min

MAC Addresses: 4C:5E:0C:D7:BE:F1 

MAC Lookup: ip to mac 




Type: Some Device   




Parents: 

Custom Field 1:

Custom Field 2:

Custom Field 3:

Agent: default   

Snmp Profile: default   




User Name: admin

Password: \*\*\*\*\*

Secure Mode

Router OS

Dude Server

Services:   Down - 3  Up - 2

Status: partially down

Ok

Cancel

Apply

Remove

Notes

Tools

Reprobe

Ack

Unack

Reboot

Reconnect

# 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

The screenshot shows a configuration window for a device with IP 172.16.1.1. The 'Parents' field is set to 172.16.1.1, and the 'Status' is 'up'. The 'Services' field is set to 'Up - 6'. The 'Router OS' checkbox is checked.

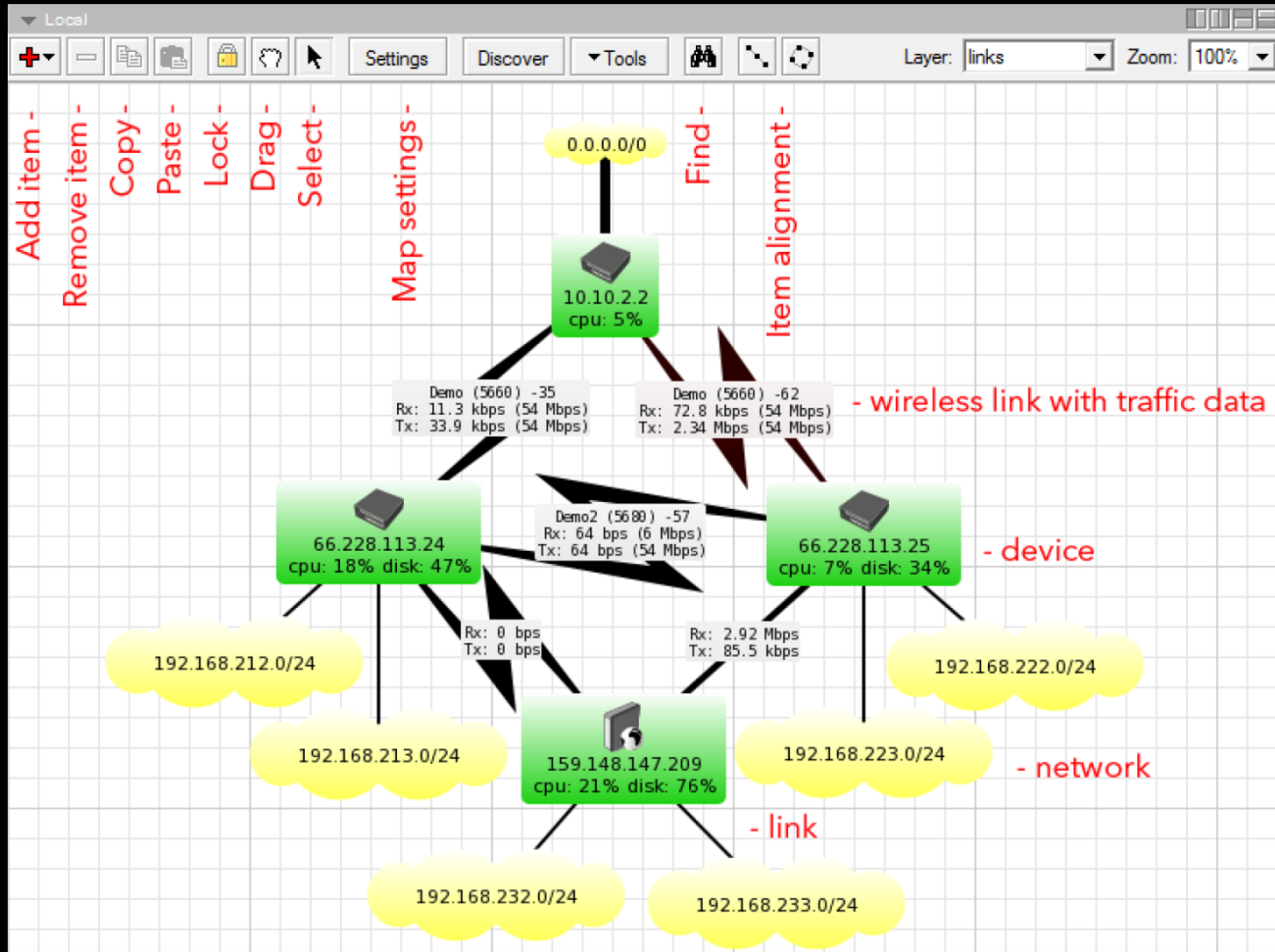
Field	Value
Name	172.16.1.1
Addresses	172.16.1.1
DNS Names	
DNS Lookup	none
DNS Lookup Interval	60 min
MAC Addresses	00:E0:33:AC:E9:79
MAC Lookup	ip to mac
Type	Some Device
Parents	172.16.1.1
Custom Field 1	172.16.1.2
Custom Field 2	192.168.1.1
Custom Field 3	192.168.1.101

Services: Up - 6

Status: up

# HOW TO WORK WITH

## Maps:



# Maps:

# HOW TO WORK WITH

**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.

The screenshot shows the configuration window for a network map. The title bar reads "10.5.104.0/24 - Network Map". The "Polling" tab is selected, showing settings for "Probe Interval", "Probe Timeout", and "Probe Down Count". Each setting has a dropdown menu set to "default" and a corresponding slider control. Below these are checkboxes for "Use Notifications" and a table for selecting notification types.

Name
beep
flash
log to events
log to syslog
popup

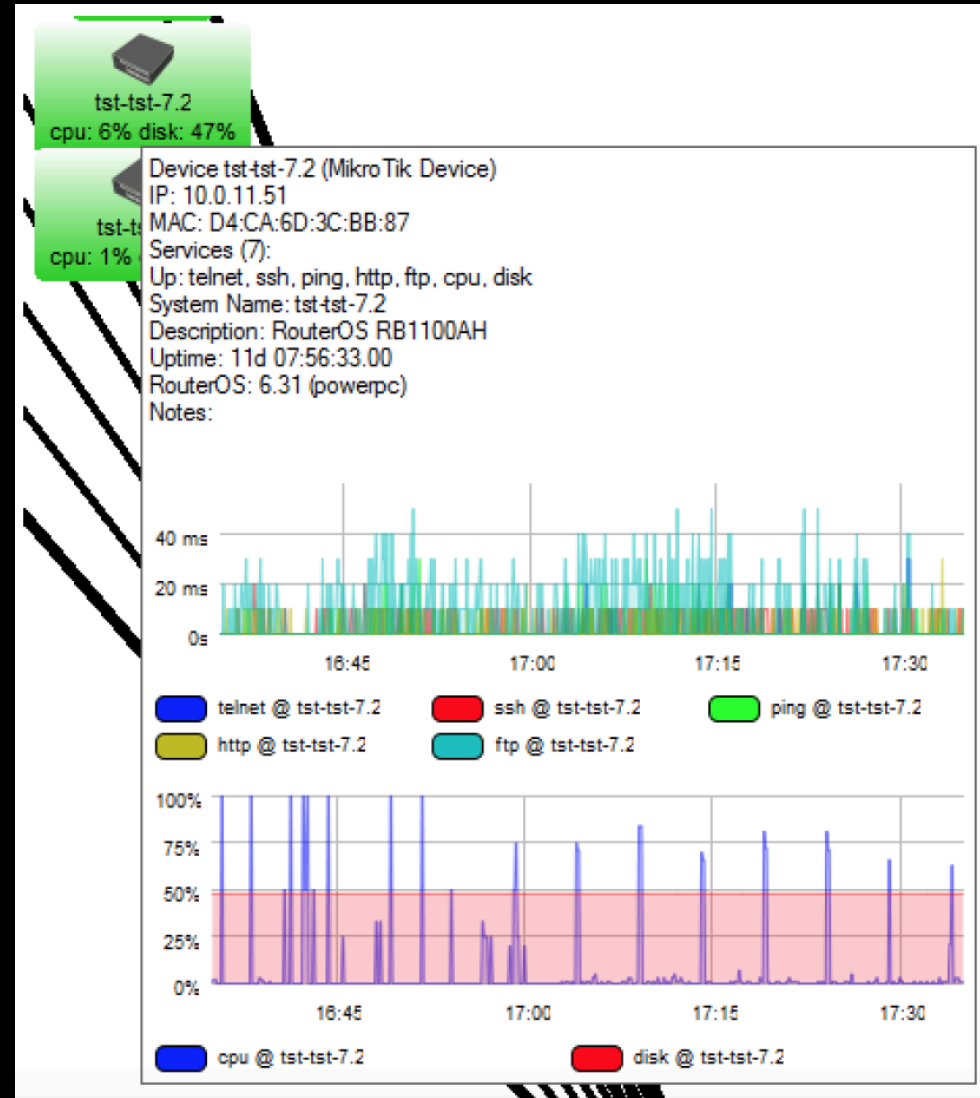
By The Way!!!!!!!

# HOW TO WORK WITH

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

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

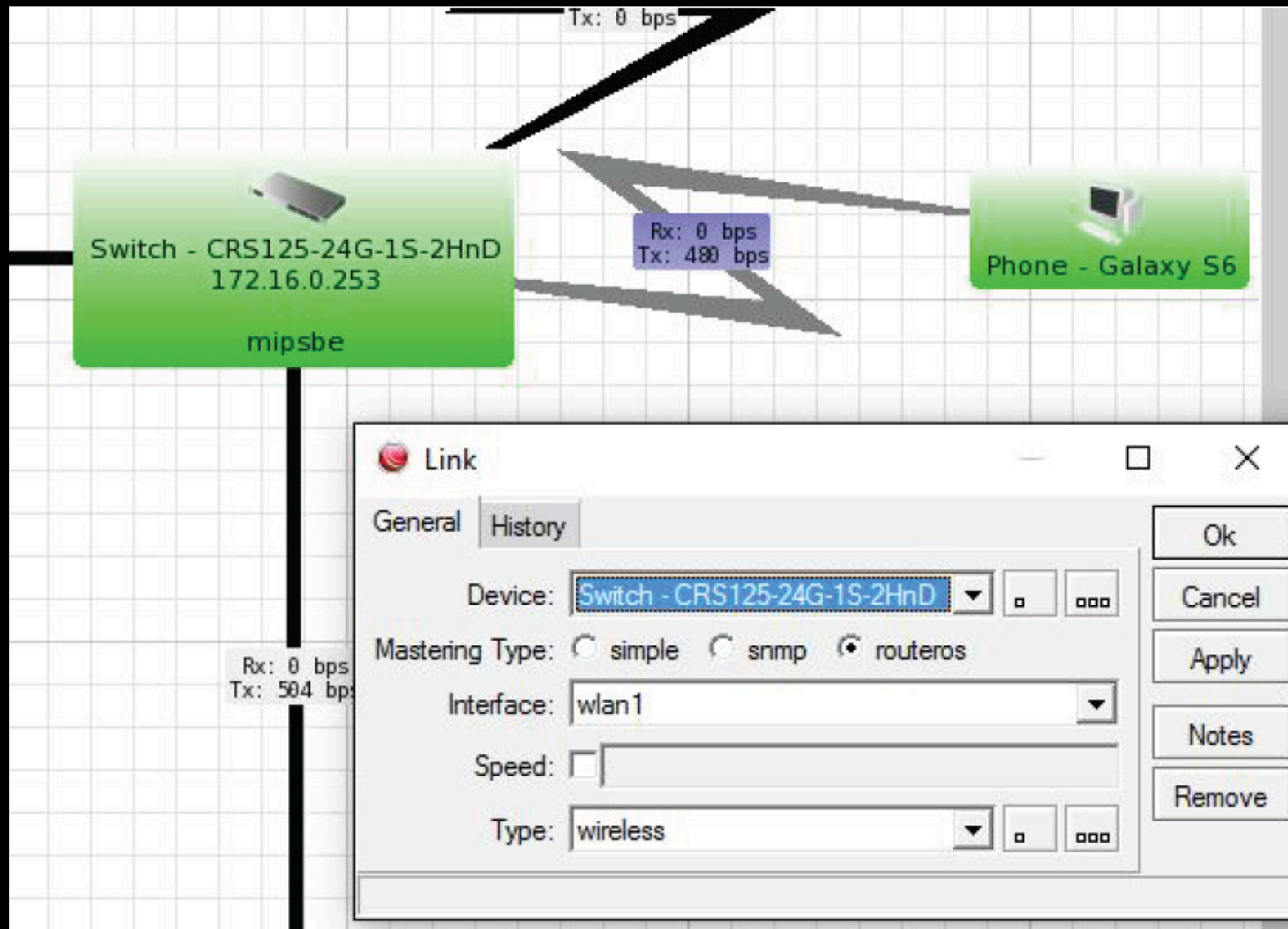
:) :) :) :)



# Links

# HOW TO WORK WITH

- 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

New Link Type

Name:

Style:

Thickness:

Snmp Type:

Snmp Speed:

Ok

Cancel

Apply

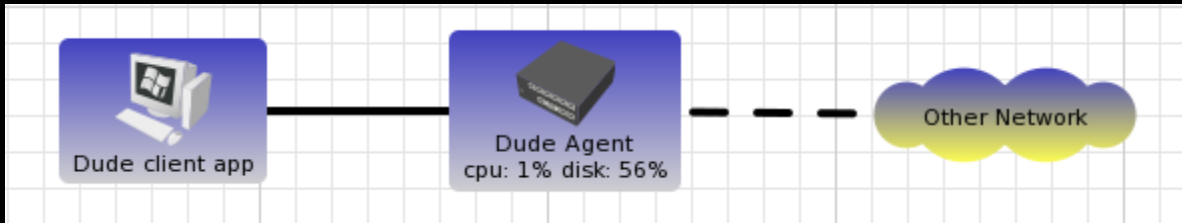
Notes

Copy

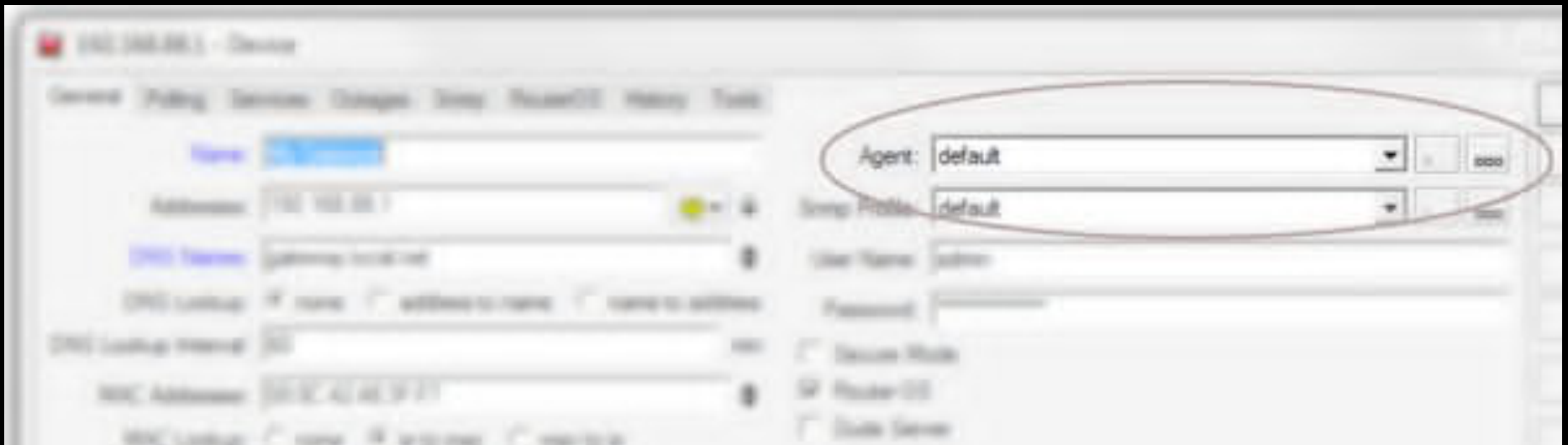
Remove

# Agents

# MONITORING



Agents are other Dude servers that can be used as intermediaries for 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



iGen**TIK**



- 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**

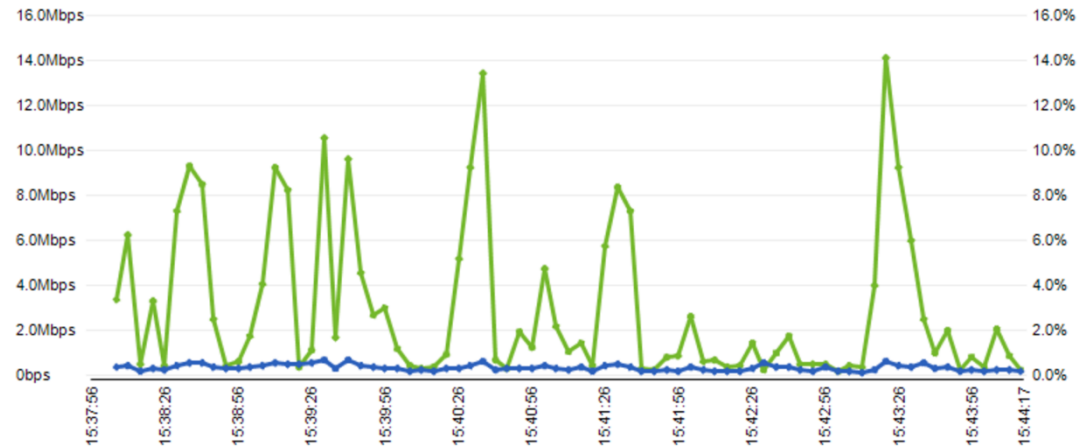


## Devices

- 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



Key:  Okay  Dependent  Partial  Fail

# 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

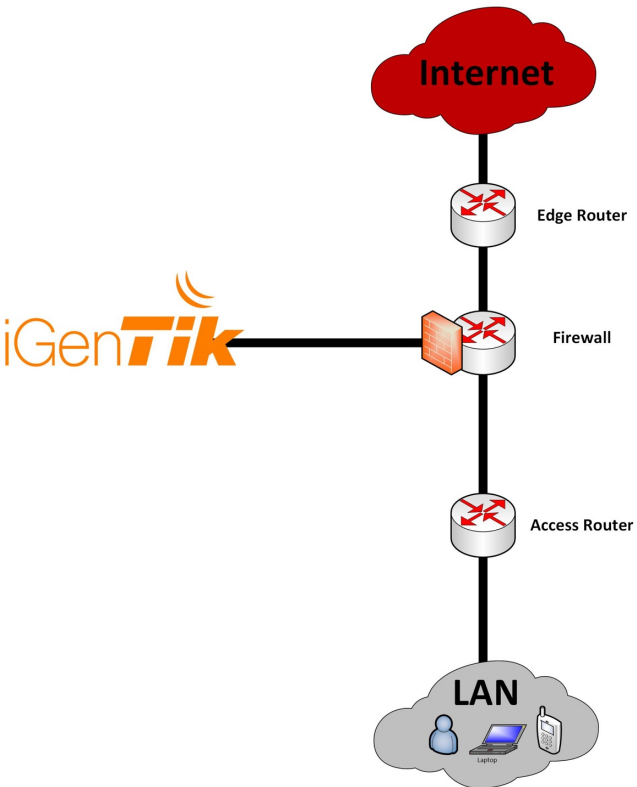
- Providing wrong pass by clients for several times
- Registration table reports (list of connected clients)

- 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.

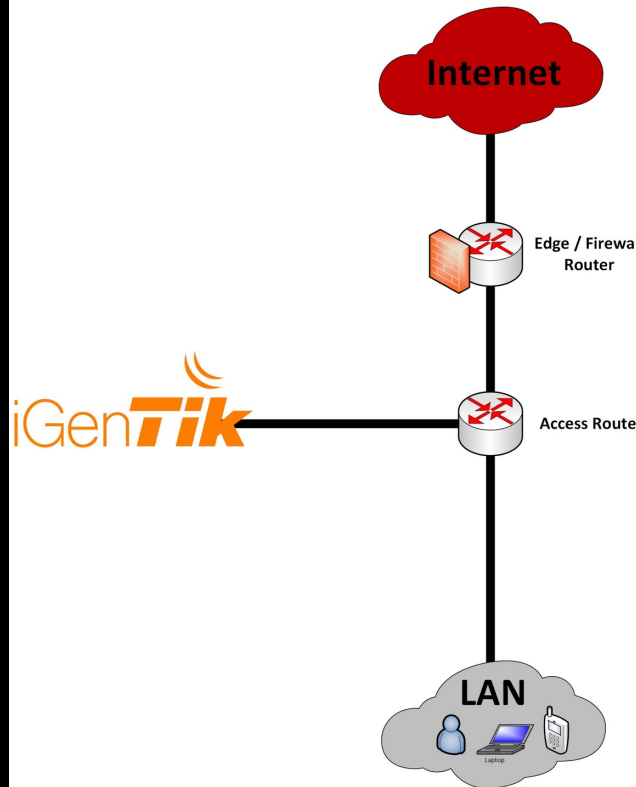
- IP status of all layer3 Devices including: Servers, Routers, Switches, End Points (Printers, Computers, Mobile Phones,)
- Public or Private host reachability and availability monitor
- Up Carrier gateway and reachability monitor: to monitor provider's availability and connectivity (with packet lost 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

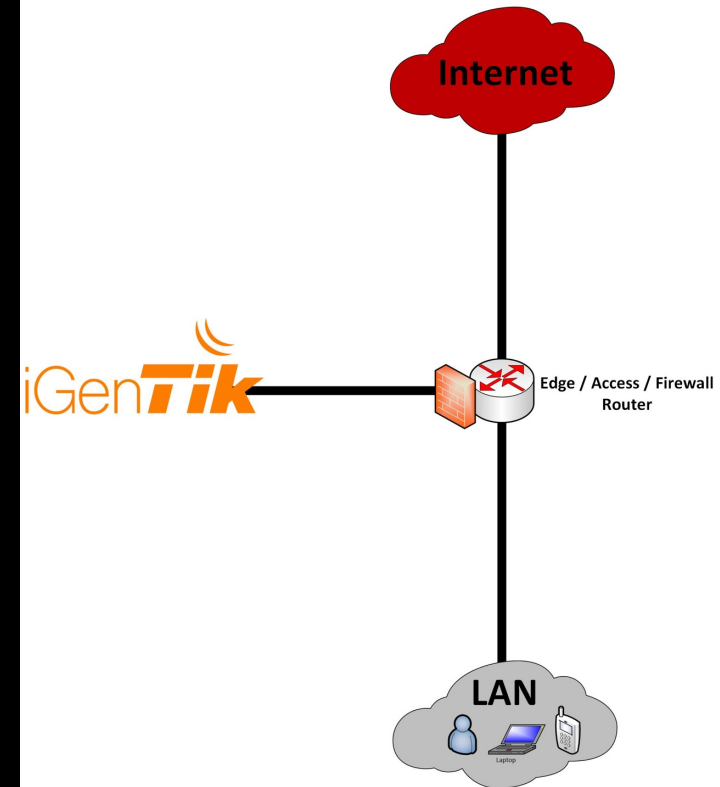
iMS  
Triple Layers Topology



iMS  
Double Layers Topology



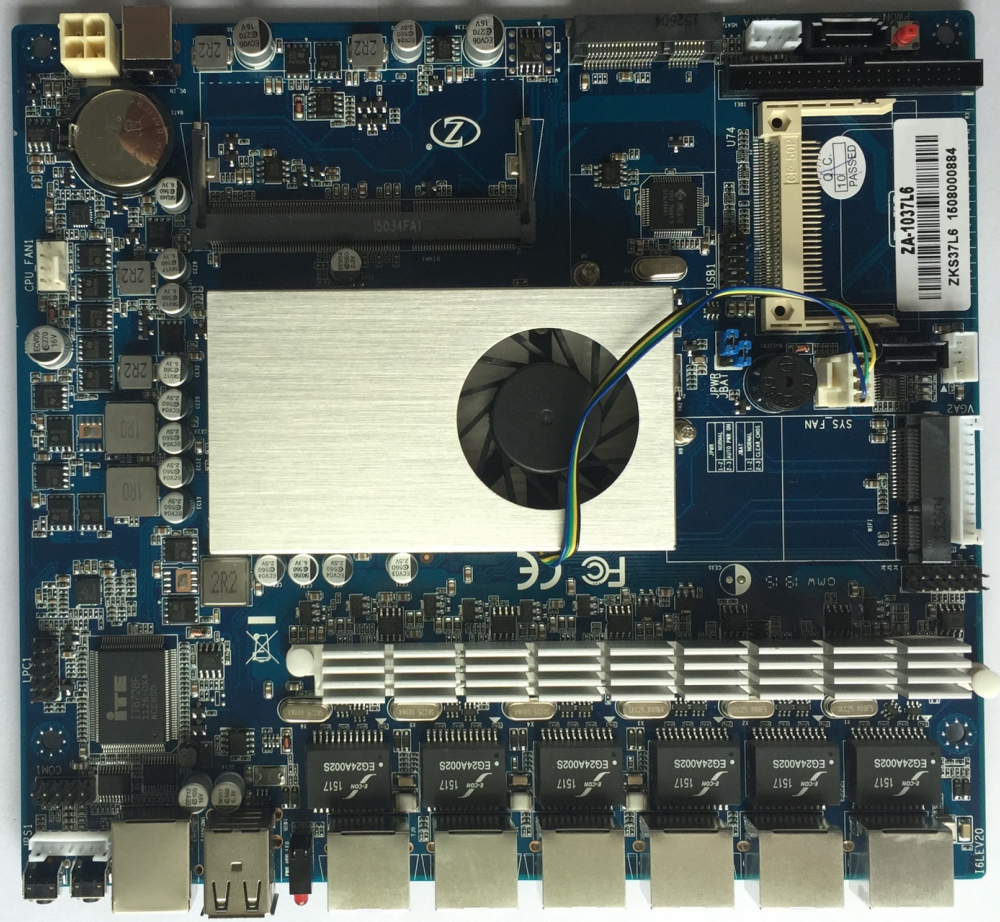
iMS  
Single Layer Topology



## 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



# ICMS



m.it.sco.  
www.mits-co.com

Console



USB



ETH0



ETH1



ETH2



ETH3



ETH4



ETH5



SW

HDD



PWR



iGenTik  
iCIMS-6GU



m.it.sco  
www.mits-co.com

Console

USB

ETH0

ETH1

ETH2

ETH3

ETH4

ETH5

SW

HDD

PWR

iGenTik  
ICMS-6GU



# ICMS

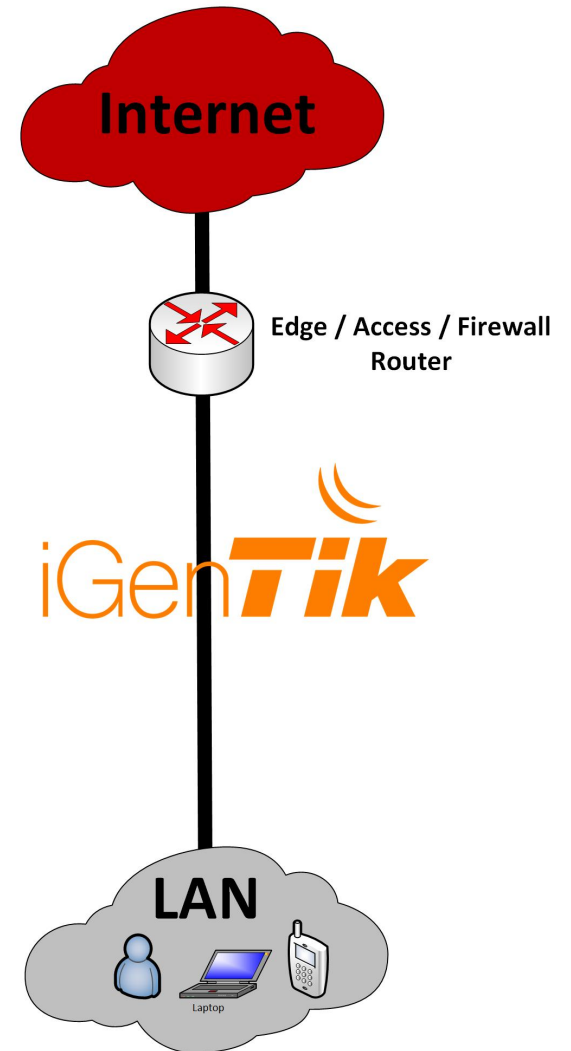
iCMS  
Triple Layers Topology



iCMS  
Double Layers Topology



iCMS  
Single Layer Topology



# 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 Rules and trigger's.

ANY

questions?

# CONTACT DETAILS

Turk Cell: +90 (537) 495 3233  

Skype: mani\_raissdana

[m.raissdana@mits-co.com](mailto:m.raissdana@mits-co.com)

[raissdana.mani@gmail.com](mailto:raissdana.mani@gmail.com)

[www.mits-co.com](http://www.mits-co.com)



MikroTikEngineers



mani\_raissdana



mikrotikiran



@mani\_raissdana



Mani Raissdana



GOOD LUCK  
&  
ENJOY MUM