

MUM - Manila, Philippines - April 13th 2016

Dude Server
iGenTik By
Mani Raissdana



Mani Raissdana

MikroTik Certified Trainer
Ubiquiti Certified Trainer
elastiX Certified Trainer

m.it.sco. CTO & Co. Founder
Morvarid. IT. Solutions Co.



Philippines Partner:

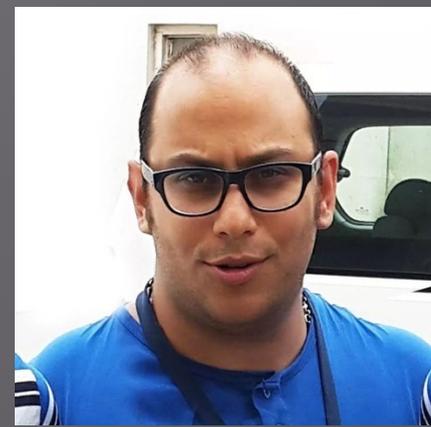


Being in IT technology business roughly around 14 years
Support & instruct Engineers more than 8 years all over the globe



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



Training Schedule

<http://www.mikrotik.com/training/> Check M.IT.S Co
<https://www.ubnt.com/training/calendar/> Check M.IT.S Co
<http://www.elastix.com/en/events-3/> Check M.IT.S Co

http://www.mits-co.com/training_mikrotik%20
http://www.mits-co.com/training_ubiquiti
http://www.mits-co.com/training_elastix

GALLERY



MITS & MICROTIK



Manila upcoming training sessions

April 14-16



April 17-18



April 19-20



April 21-22



April 23-24



April 25-26



April 26-30 (Elastix/ Asterisk)

elastix
CERTIFIED
ENGINEER

Table of contents

Dude

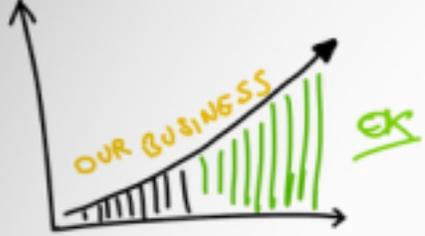
- ▣ What is Dude???
- ▣ What it does???
- ▣ How it works???
- ▣ How you should work with???
- ▣ Monitoring
- ▣ Notification

iGenTik

Interactive GSM/Email notification system



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



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

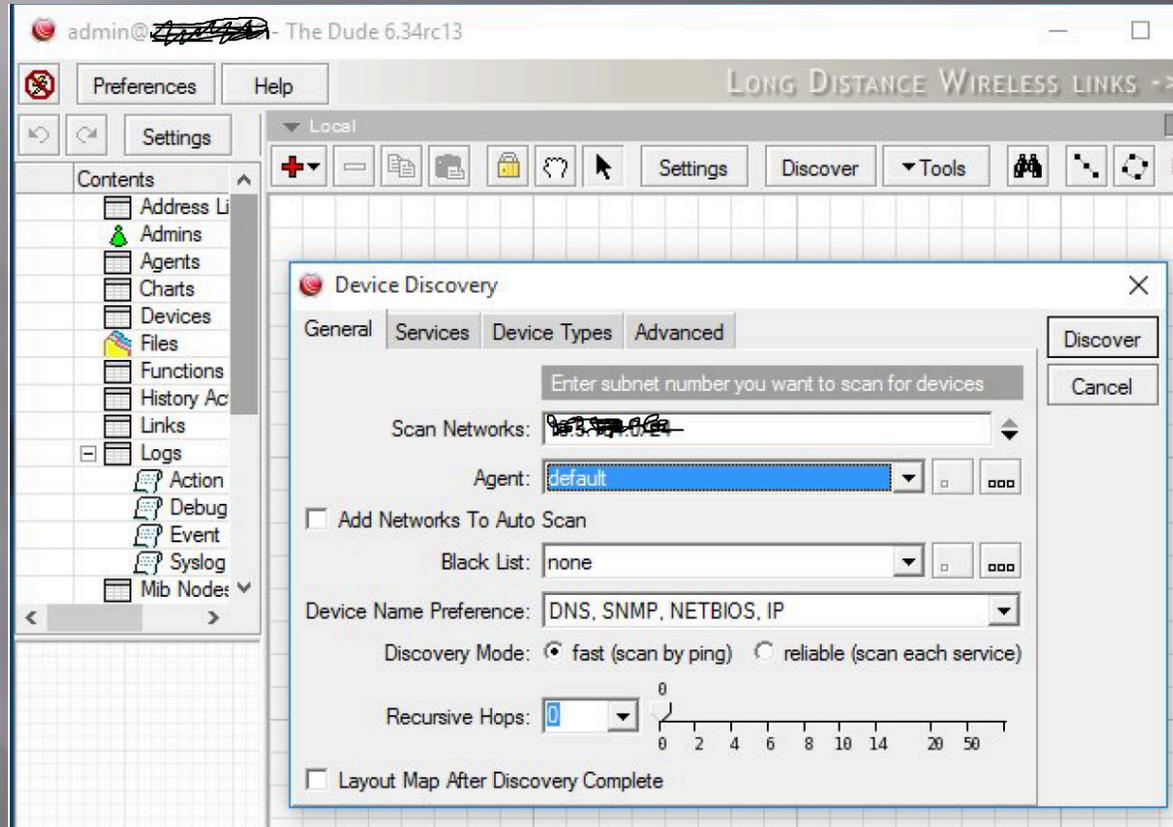
What it Does

- ▣ 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 you should work with

Interface

The screenshot displays the Mikrotik WinBox interface with three main panels highlighted:

- Map Pane:** A network diagram showing a central hub connected to multiple peripheral nodes, representing a network topology.
- Log Pane:** A Syslog window displaying a list of events with columns for Time, Address, and Event. The events include telnet, pop3, smtp, and ssh connections from various IP addresses.
- Panes:** A sidebar menu on the left containing various system management options such as Address Lists, Admins, Agents, Charts, Devices, Files, Functions, History Actions, Links, Logs, Mib Nodes, Network Maps, Networks, Notifications, Panels, Probes, and Services.

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
Jan/15 13:47:43	127.0.0.1	Service telnet on gateway.lan
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 no
Jan/15 13:47:43	10.5.104.85	Service pop3 on 10.5.104.85
Jan/15 13:47:43	10.5.104.85	Service smtp on 10.5.104.85
Jan/15 13:47:43	10.5.104.243	Service pop3 on ppc.lan is no
Jan/15 13:47:43	10.5.104.75	Service cpu on 10.5.104.75
Jan/15 13:47:43	10.5.104.212	Service pop3 on crs212.lan is
Jan/15 13:47:43	10.5.104.76	Service cpu on 10.5.104.76
Jan/15 13:47:43	10.5.104.109	Service telnet on crs109.lan is
Jan/15 13:47:43	10.5.104.109	Service pop3 on crs109.lan is
Jan/15 13:47:43	10.5.104.252	Service pop3 on 10.5.104.252
Jan/15 13:47:43	10.5.104.249	Service pop3 on nine.lan is no
Jan/15 13:47:43	10.5.104.210	Service smtp on crs210.lan is
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 no
Jan/15 13:47:43	10.5.104.243	Service telnet on ppc.lan is no
Jan/15 13:47:43	10.5.104.246	Service telnet on crs226.lan is
Jan/15 13:47:43	10.5.104.112	Service telnet on crs112.lan is
Jan/15 13:47:43	10.5.104.212	Service telnet on crs212.lan is
Jan/15 13:47:43	10.5.104.51	Service smtp on 10.5.104.51
Jan/15 13:47:43	10.5.104.89	Service ssh on 10.5.104.89
Jan/15 13:47:43	10.5.104.88	Service pop3 on 10.5.104.88
Jan/15 13:47:43	10.5.104.88	Service smtp on 10.5.104.88
Jan/15 13:47:43	10.5.104.210	Service pop3 on crs210.lan is
Jan/15 13:47:43	10.5.104.51	Service pop3 on 10.5.104.51
Jan/15 13:47:43	10.5.104.245	Service telnet on plus.lan is no
Jan/15 13:47:43	10.5.104.249	Service smtp on nine.lan is no
Jan/15 13:47:43	10.5.104.112	Service pop3 on crs112.lan is
Jan/15 13:47:43	10.5.104.252	Service telnet on 10.5.104.252
Jan/15 13:47:43	10.5.104.89	Service smtp on 10.5.104.89
Jan/15 13:47:43	10.5.104.89	Service pop3 on 10.5.104.89
Jan/15 13:47:43	10.5.104.246	Service pop3 on crs226.lan is
Jan/15 13:47:43	10.5.104.50	Service pop3 on 10.5.104.50
Jan/15 13:47:43	10.5.104.50	Service smtp on 10.5.104.50
Jan/15 13:47:43	10.5.104.84	Service md 50:50 on 10.5.104

How you should work with

Menu

The screenshot shows the HotSpot Controllers web interface. On the left, a purple sidebar menu is highlighted with a red box and labeled "Menu" with a red arrow. The main area displays a network diagram with several green nodes and yellow cloud nodes. The top status bar shows "Client: rx 1.17 kbps / tx 268 bps" and "Server: rx 2.81 kbps / tx 129 kbps".

Contents	
	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

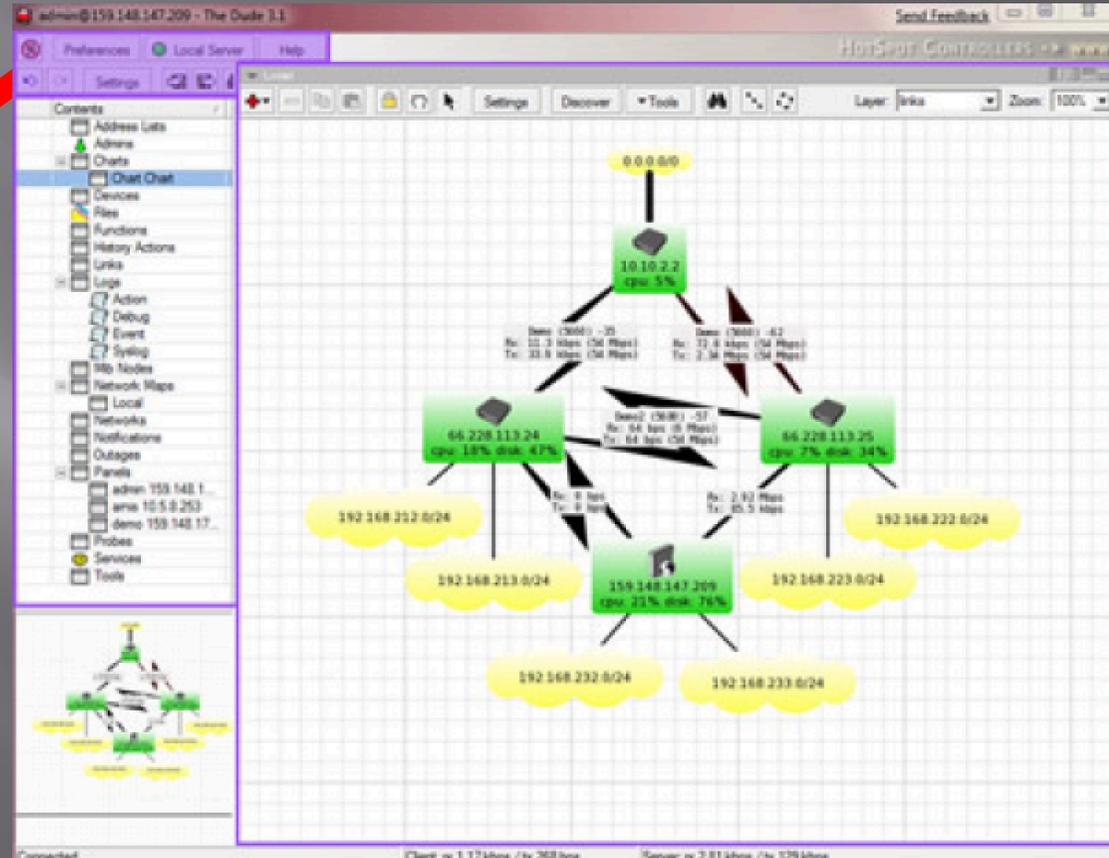
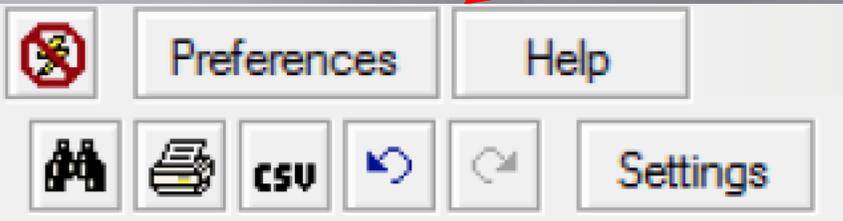
How you should work with

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.)

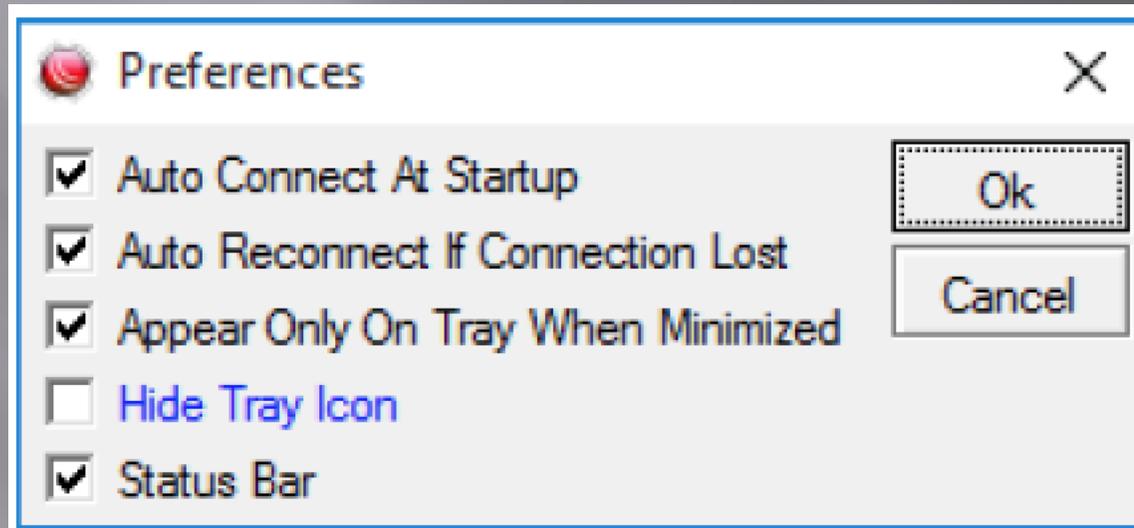
How you should work with

Server Settings



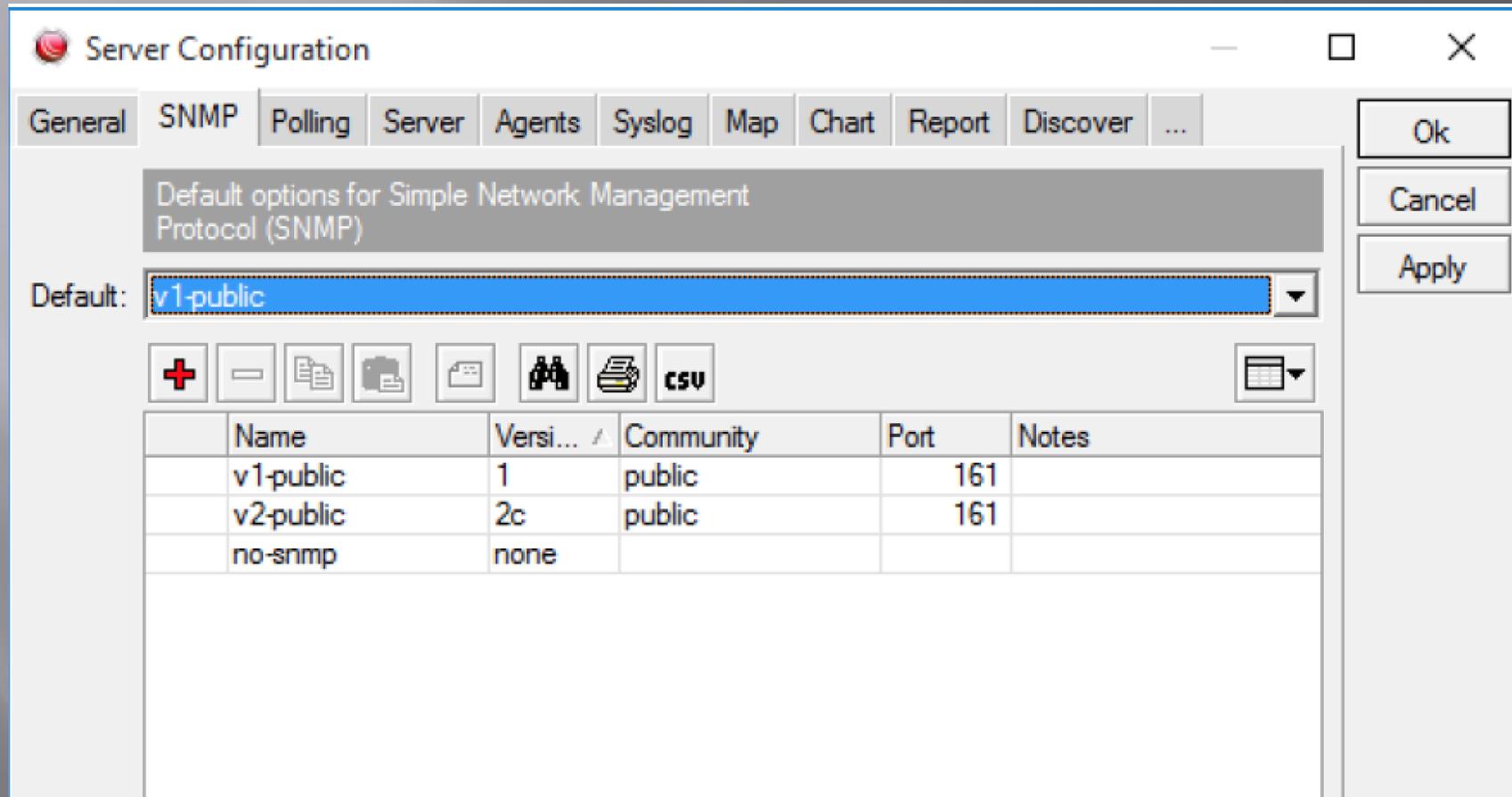
How you should work with

Preferences



How you should 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 you should work with

Device Settings

- ▣ Adding devices is just few steps:

1-



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

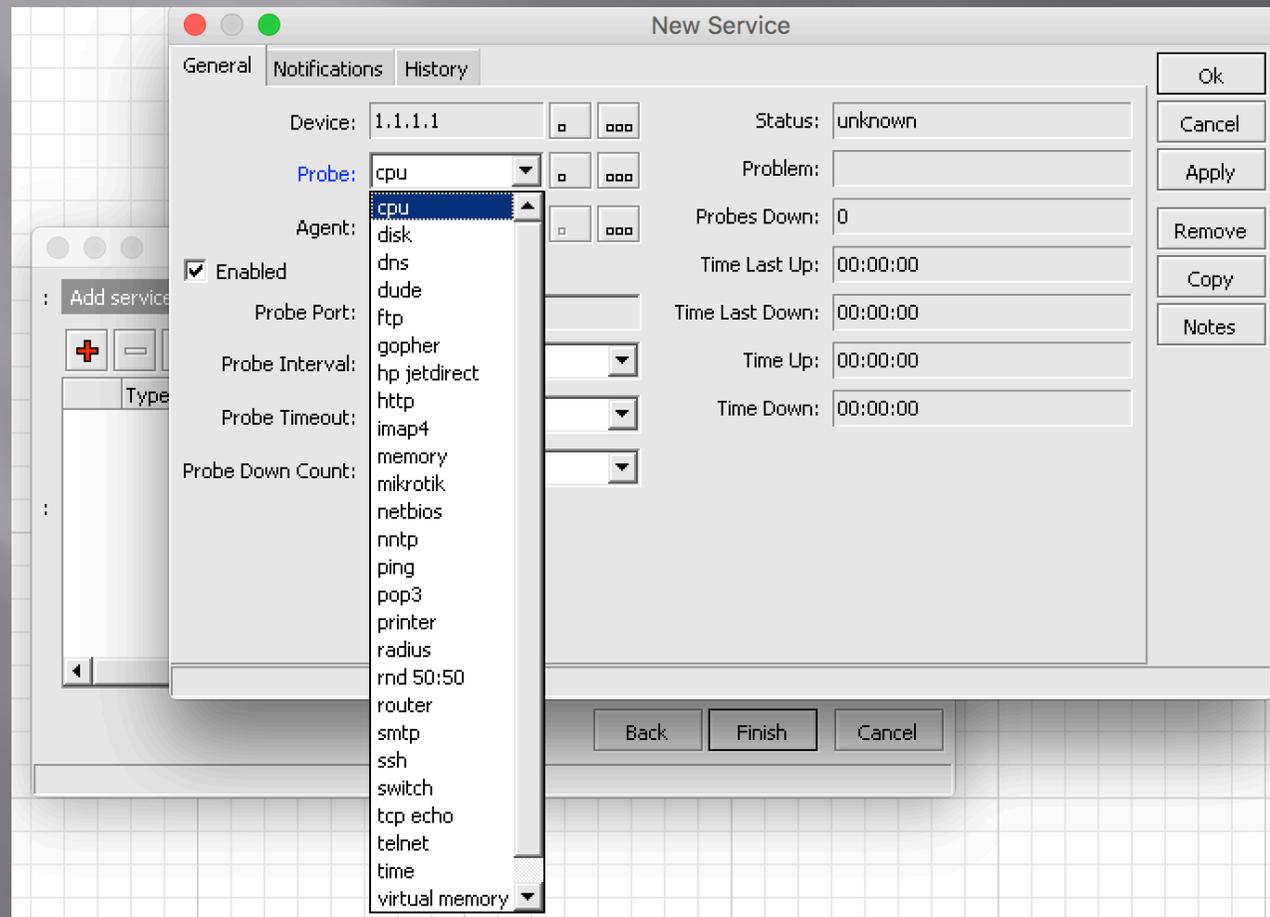
- A greyed-out instruction field: "Enter IP address or DNS name"
- An "Address:" label in red text next to an empty text input field.
- A greyed-out instruction field: "Login for fast access to device with Telnet/Winbox"
- A "User Name:" label next to a text input field containing the text "admin".
- A "Password:" label next to an empty text input field.
- Two unchecked checkboxes: "Secure Mode" and "Router OS".
- Three buttons at the bottom right: "Back", "Next", and "Cancel".

How you should work with

Device Settings

- ▣ Adding devices is just few steps:

2-



How you should work with

Device Settings

Important to configure accurately

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

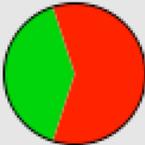
User Name: admin

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 you should 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 titled "172.16.1.1 - Device" with several tabs: General, Polling, Services, Outages, Snmp, RouterOS, History, and Tools. The "General" tab is active. The configuration fields are as follows:

- Name: 172.16.1.1
- Addresses: 172.16.1.1
- DNS Names: (empty)
- DNS Lookup: none, address to name, name to address
- DNS Lookup Interval: 60 min
- MAC Addresses: 00:E0:33:AC:E9:79
- MAC Lookup: none, ip to mac, mac to ip
- Type: Some Device
- Parents: 172.16.1.1 (selected)
- Custom Field 1: 172.16.1.2
- Custom Field 2: 192.168.1.1
- Custom Field 3: 192.168.1.101

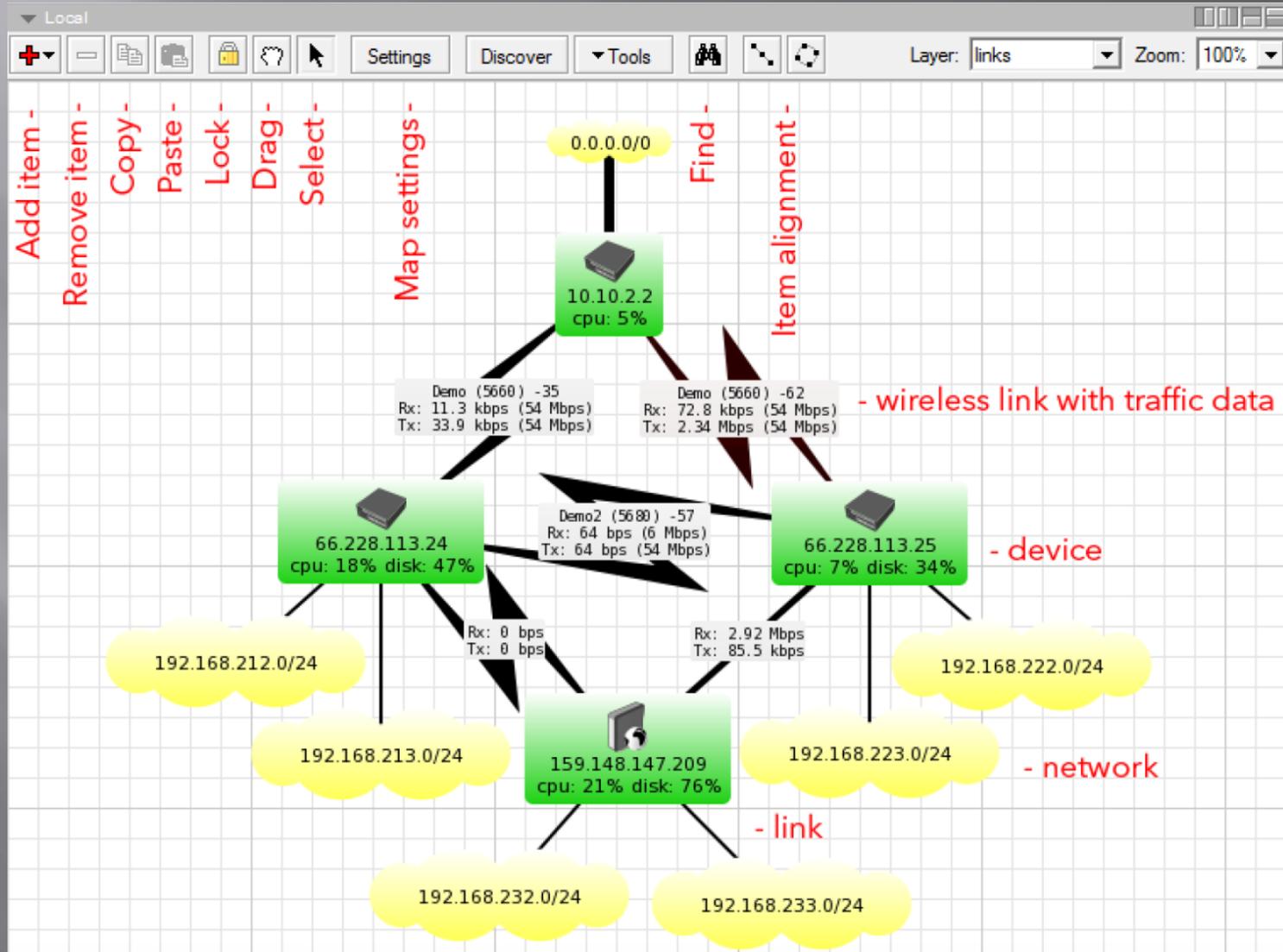
On the right side of the configuration panel:

- Agent: default
- Snmp Profile: default
- User Name: admin
- Password: (masked with asterisks)
- Secure Mode
- Router OS
- Dude Server
- Services: (represented by a large green circle)
- Status: up

On the far right, there is a vertical stack of buttons: Ok, Cancel, Apply, Notes, Remove, Tools (dropdown), Reprobe, Ack, Unack, Reboot, and Reconnect.

How you should work with

Maps:

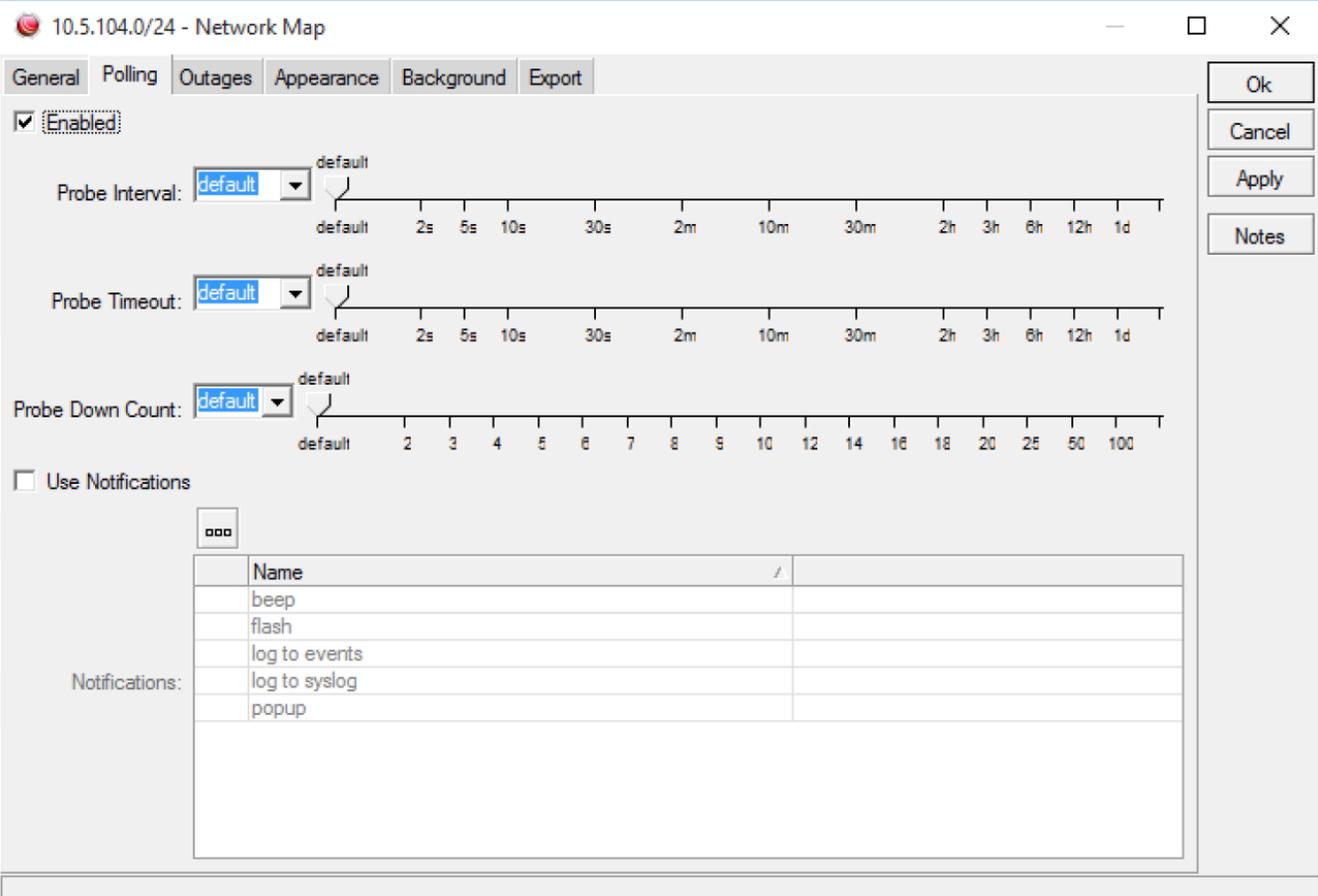


How you should work with

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.



10.5.104.0/24 - Network Map

General Polling Outages Appearance Background Export

Enabled

Probe Interval: default [default] default 2s 5s 10s 30s 2m 10m 30m 2h 3h 6h 12h 1d

Probe Timeout: default [default] default 2s 5s 10s 30s 2m 10m 30m 2h 3h 6h 12h 1d

Probe Down Count: default [default] default 2 3 4 5 6 7 8 9 10 12 14 16 18 20 25 50 100

Use Notifications

ooo

Name	
beep	
flash	
log to events	
log to syslog	
popup	

Notifications:

Ok Cancel Apply Notes

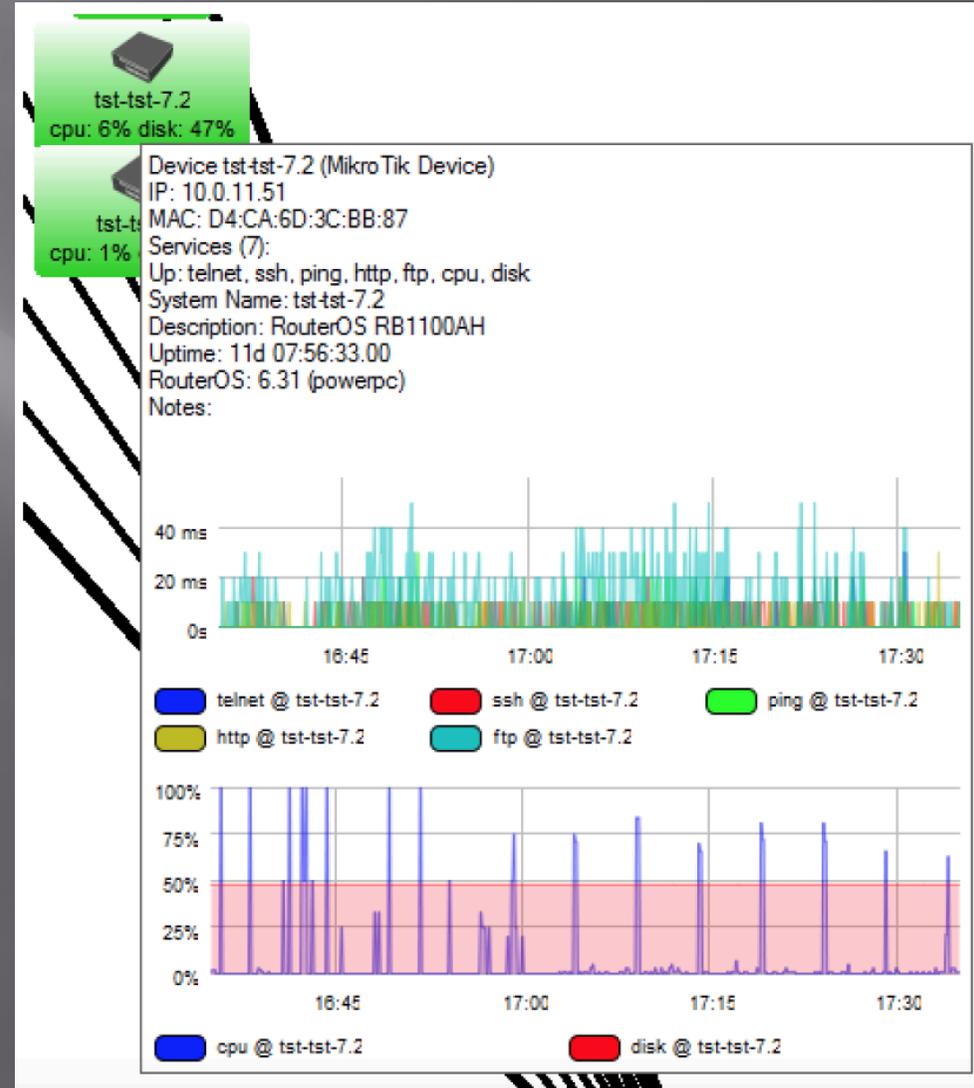
How you should work with

By The Way!!!!!!!

- ▣ You also can monitor and have a graph of real time device's traffic

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

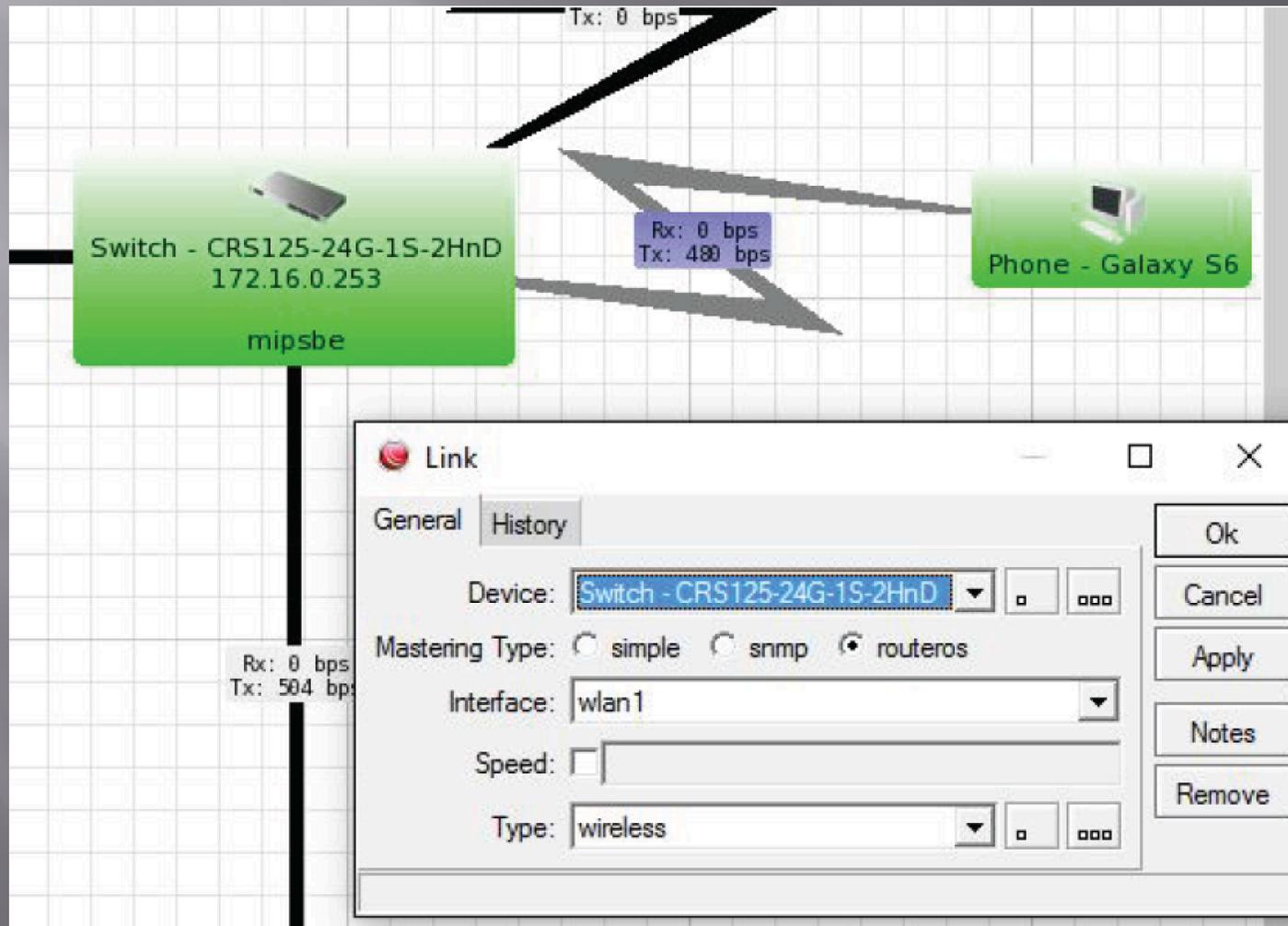
:) :) :) :)



How you should work with

Links

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



How you should work with

Links

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



How you should 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:

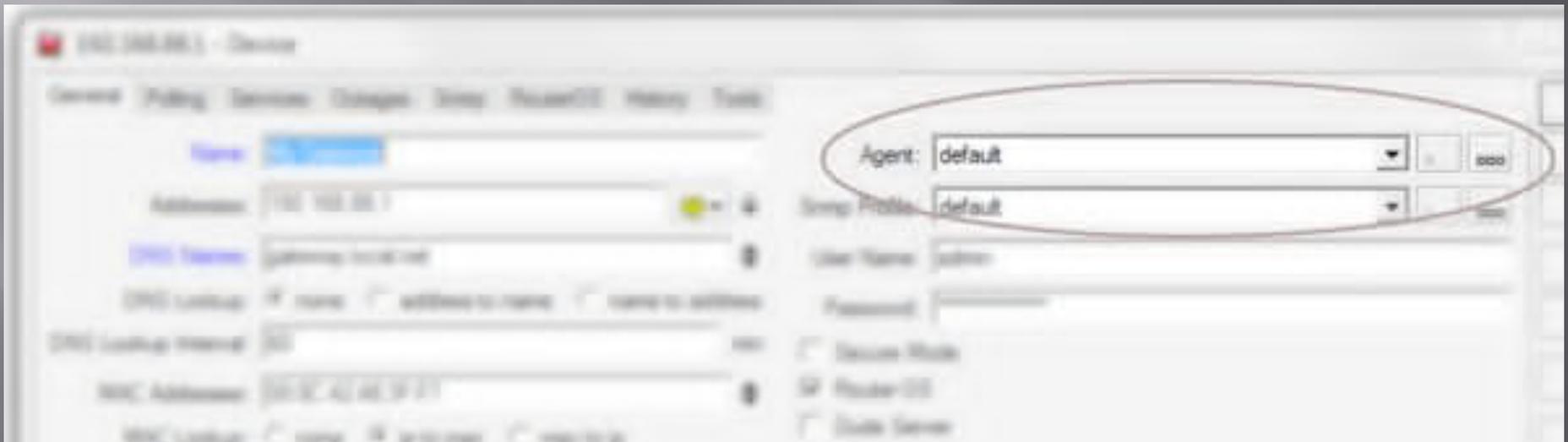
Ok
Cancel
Apply
Notes
Copy
Remove

Monitoring

Agents



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 missing here!!!!!!

GSM Notification:

Sending text message to notify!!!!!!

What???????????

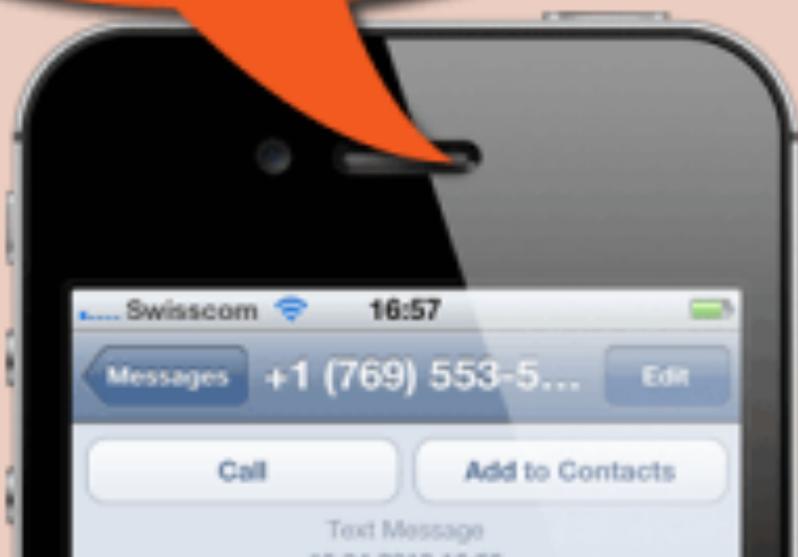
Now, let's talk about



The logo for iGenTik features the text "iGenTik" in a stylized orange font. The "i" is lowercase and has a dot. "Gen" is in a rounded, lowercase sans-serif font. "Tik" is in a bold, italicized, lowercase sans-serif font. Above the "Tik" portion, there are two curved orange lines that resemble a stylized flame or a signal. The entire logo is set against a dark gray background with diagonal light gray stripes.

iGenTik

Order
Notification
SMS



iGenTik

- ▣ iGenTik is Interactive GSM/Email notification system,

Based on MikroTik platform

with customizable GUI Interface

To notify **anything you imagine**

iGenTik

- built-in battery that can be alive for around an hour
- Sending notification by Text Message or Email about all Device's activities in the Network including:
 1. Any Public or Private host reachability
 2. VPN Connections: as soon as any VPN connections get connected,
 3. Queuing: if one queue rule gets 50%, 75% or 100% bandwidth
 4. by adding any route (Static, Dynamic) in routing table
 5. main/failover upstream replacement
 6. check ISP gateway: to make sure the availability of providers
 7. Firewall/NAT/Mangle Control: by adding any rules in these tables
 8. Logs notifications
 9. Traffic Control: weird TX/RX bandwidth
 10. Protocol check: weird UDP/TCP/ICMP... traffic
 11. Any kind of attack:
 - I. IP/Port Scan
 - II. DDOS Attack
 - III. Phishing Attack
 - IV. Hijack Attack
 - V. Buffer Attack
 - VI. Password Attack
 - VII. IP Spoofing
 - VIII. Sniffing
 - IX. Application Layer Attack

iGenTik

12. Wireless Control:
 - I. providing wrong pass by clients for several times
 - II. registration table reports (list of connected clients)
 - III. unwanted wireless login
13. City/UPS Power Check
 - I. voltage balance
 - II. Ampere balance
 - III. City Power up/down
 - IV. UPS power up/down
14. Elastix (Any VOIP Call Center) logs and reports including:
 - I. Emergency Calls
 - II. Call Duration
 - III. Trunk Failure
 - IV. Call Center Failure
 - V. Operator timeout
15. Antivirus Management notification (Kaspersky, Node, ...)

iGenTik

The Most interesting default features

- Replying Text Messages by receiving any Text Message (means you can send commands to it by messages or emails 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 for
 - I. Disable/Enable Interface
 - II. Block/Unblock Users
 - III. Allow/Terminate any connections
 - IV. Turn on/turn off or restart Servers, routers ...

iGenTik

Has not released yet

Will announced as MikroTik MfM Project in a month

And will be ready to use soooooooooon....

ANY

questions?

CONTACT DETAILS

Turk Cell: +90 (537) 495 3233  

Persian Cell: +98 (912) 149 7009  

International Cell: +37259431151

Skype: mani_raissdana

m.raissdana@mits-co.com

raissdana.mani@gmail.com

www.mits-co.com



MikroTikEngineers



mani_raissdana



mikrotikiran



@mani_raissdana



Mani Raissdana

Good Luck

&

Enjoy MUM