

m.it.sco

Morvarid. IT. Solutions Co.

MikroTik

MUM - Beirut, Lebanon - June 14th 2016

Dude Server

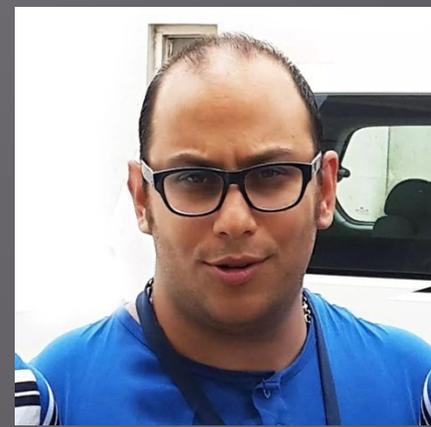
iGenTik

By
Mani Raissdana



Mani Raisdana

MikroTik Certified Trainer
CTO & Co. Founder

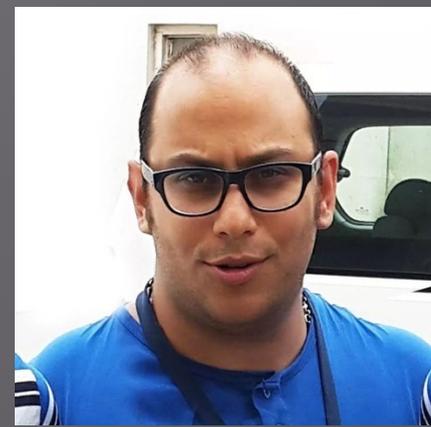


Being in IT technology business roughly around 14 years
Support & instruct Engineers more than 8 years all over the globe



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

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



SEARCH ENGINE DESIGN MEDIA
WEB SITE



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

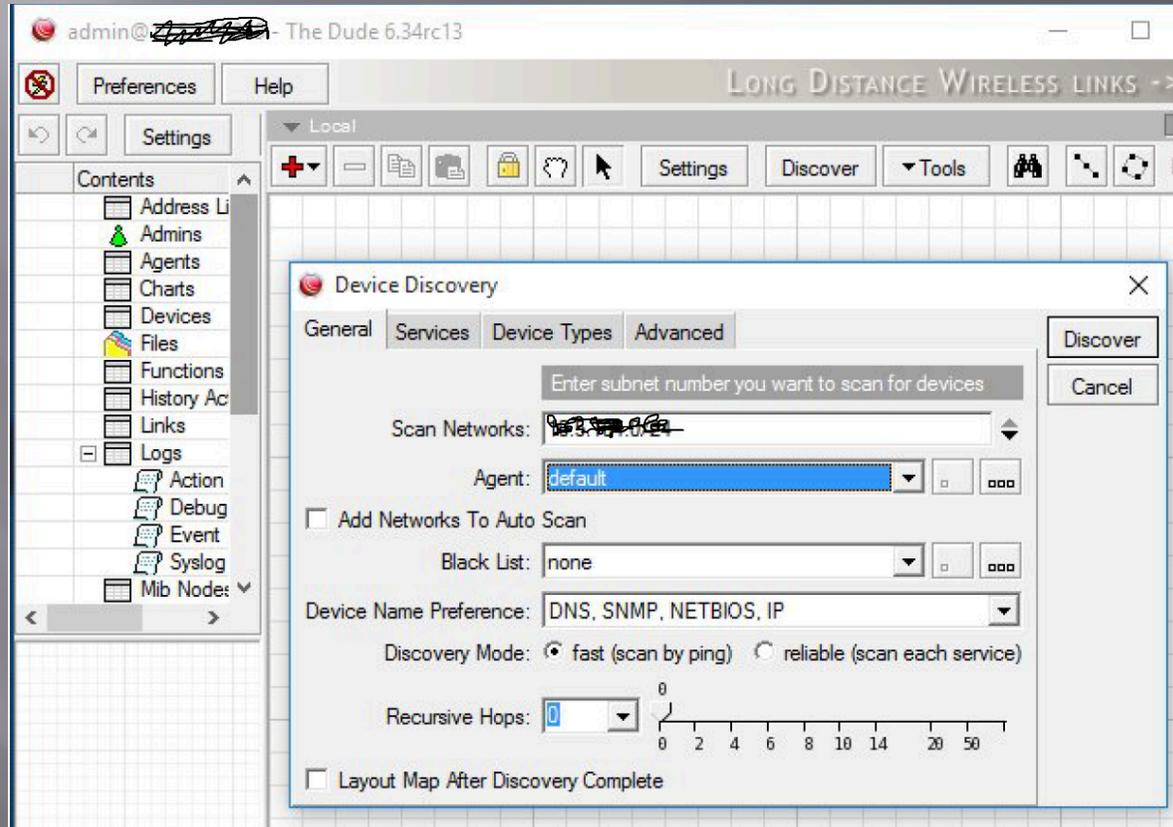
What it Does

- ▣ 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 distinct panes:

- Map Pane:** A network diagram showing a central router connected to various devices. A red box highlights this pane.
- Log Pane:** A Syslog log window showing a list of events. A red box highlights this pane.
- Panel:** The main interface area, which includes a left-hand menu and a bottom status bar.

Panel Contents:

- Left Menu:** Preferences, Help, csu, Settings, Contents (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, Panels, Probes, Services).
- Bottom Status Bar:** Client: rx 6.4 kbps / tx 248 bps, Server: rx

Log Pane 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
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. A red box highlights the left-hand menu, which is titled "Contents". A red arrow points from the word "Menu" to the highlighted menu area. The main area of the interface displays a network diagram with several nodes and connections. The nodes are represented by green icons with IP addresses and resource usage statistics. The connections are shown as black lines with associated statistics. The interface also includes a top navigation bar with "Preferences", "Local Server", and "Help" buttons, and a bottom status bar showing "Client: rx 1.17 kbps / tx 268 bps" and "Server: rx 2.81 kbps / tx 129 kbps".

Menu

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

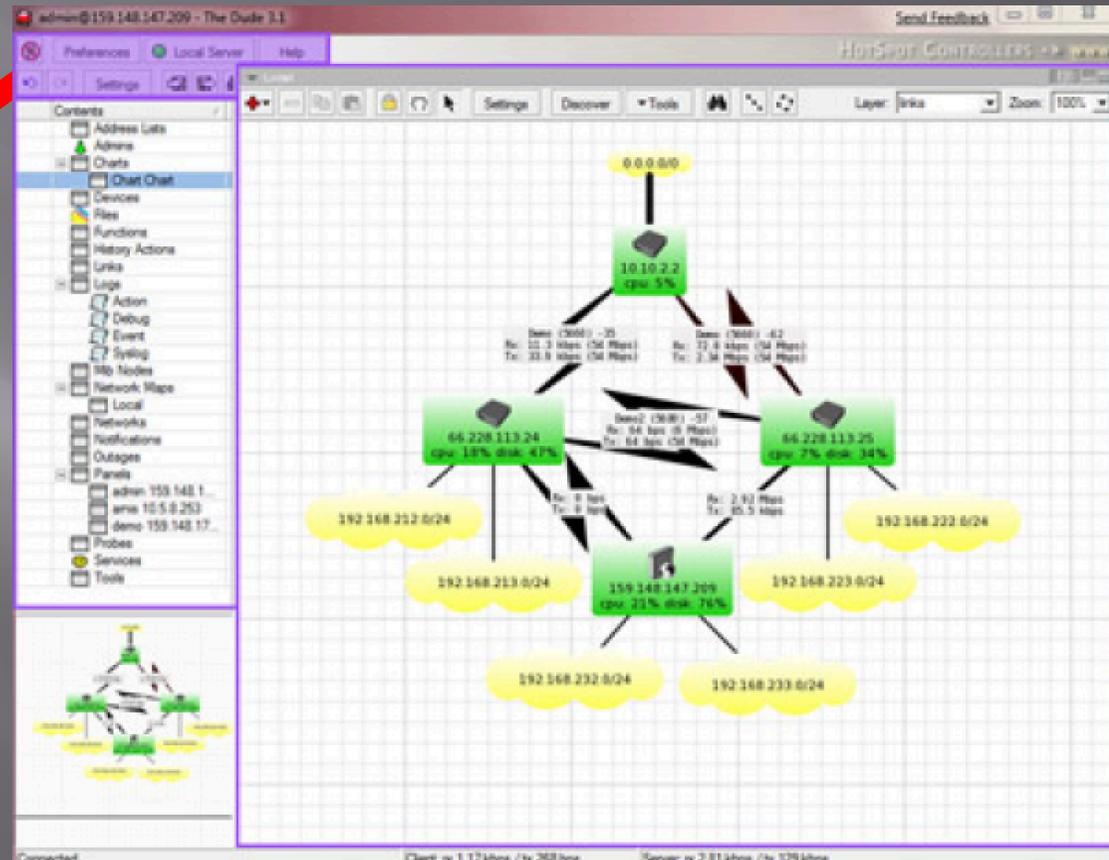
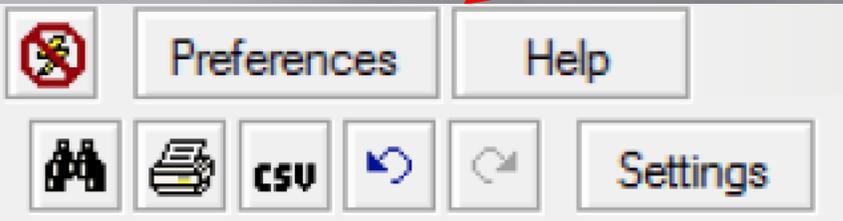
How you should work with

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.)

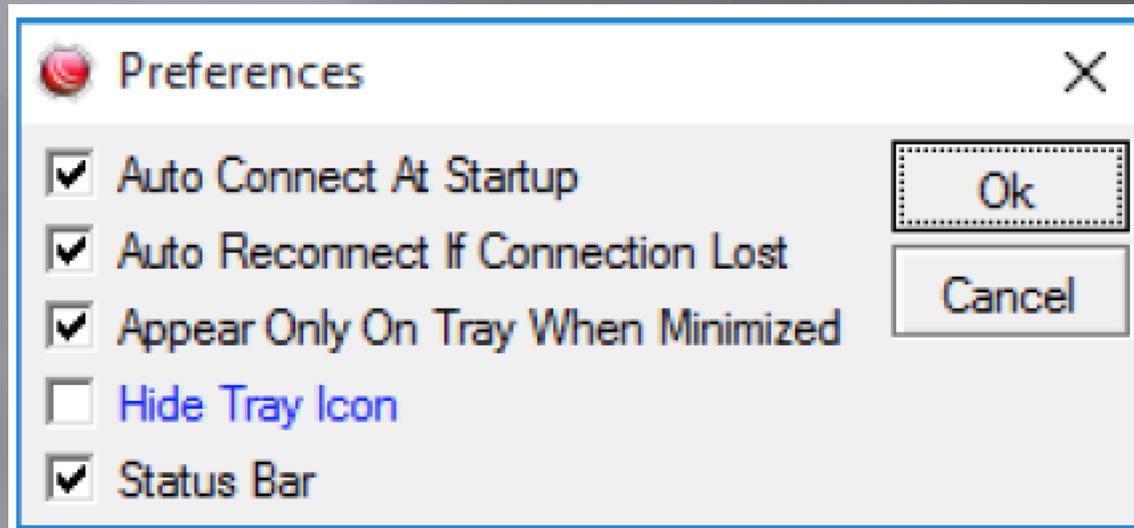
How you should work with

Server Settings



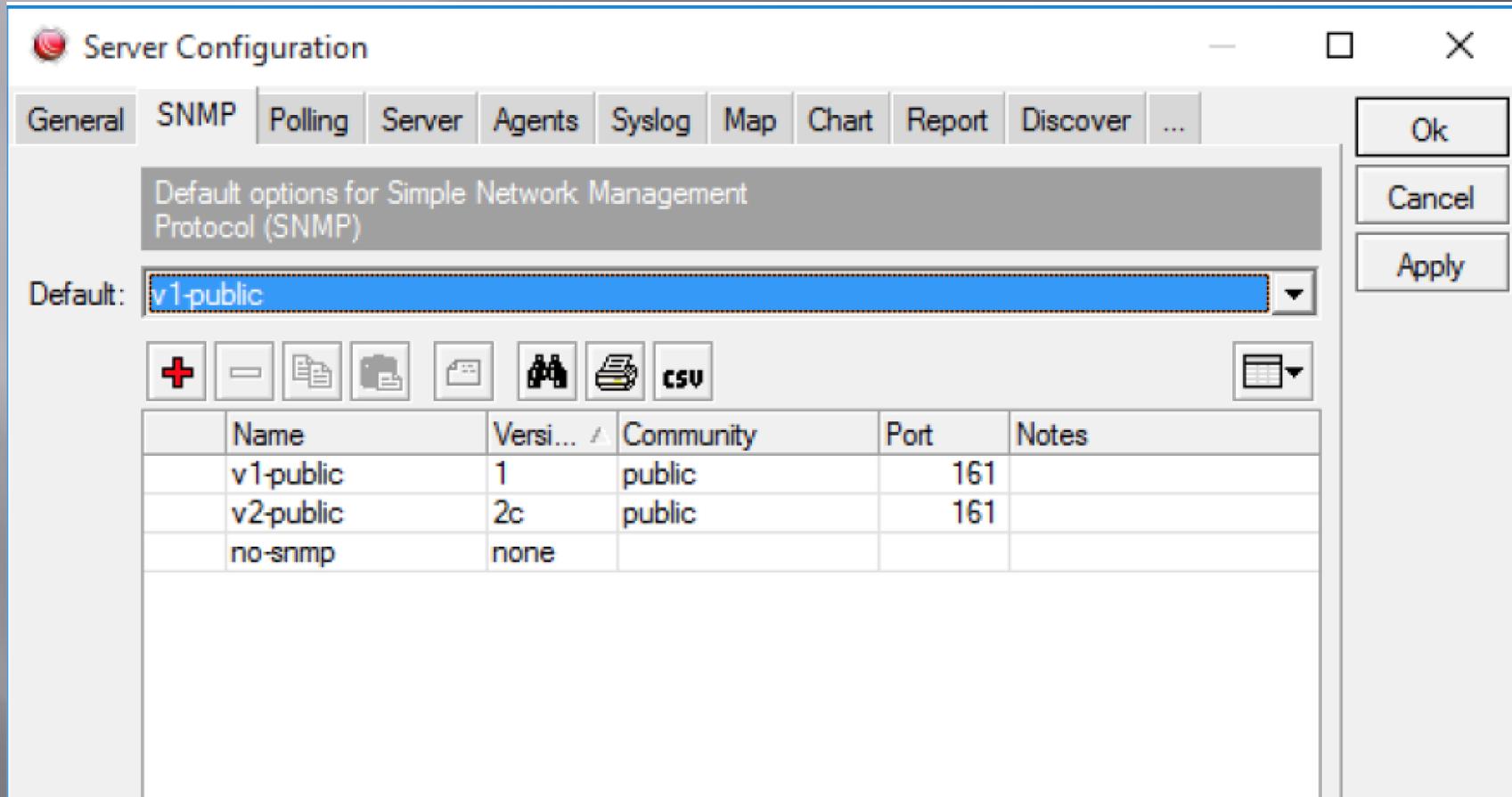
How you should work with

Preferences



How you should work with

Server Settings



The screenshot shows a 'Server Configuration' dialog box with the 'SNMP' tab selected. The title bar reads 'Server Configuration'. The tab bar includes 'General', 'SNMP', 'Polling', 'Server', 'Agents', 'Syslog', 'Map', 'Chart', 'Report', 'Discover', and an ellipsis. The main area is titled 'Default options for Simple Network Management Protocol (SNMP)'. A 'Default:' label is followed by a dropdown menu showing 'v1-public'. Below this is a toolbar with icons for adding (+), removing (-), creating a new entry (document with plus), deleting an entry (document with minus), a group of people icon, a printer icon, and the text 'CSV'. To the right of the toolbar is a calendar icon. Below the toolbar is a table with the following data:

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

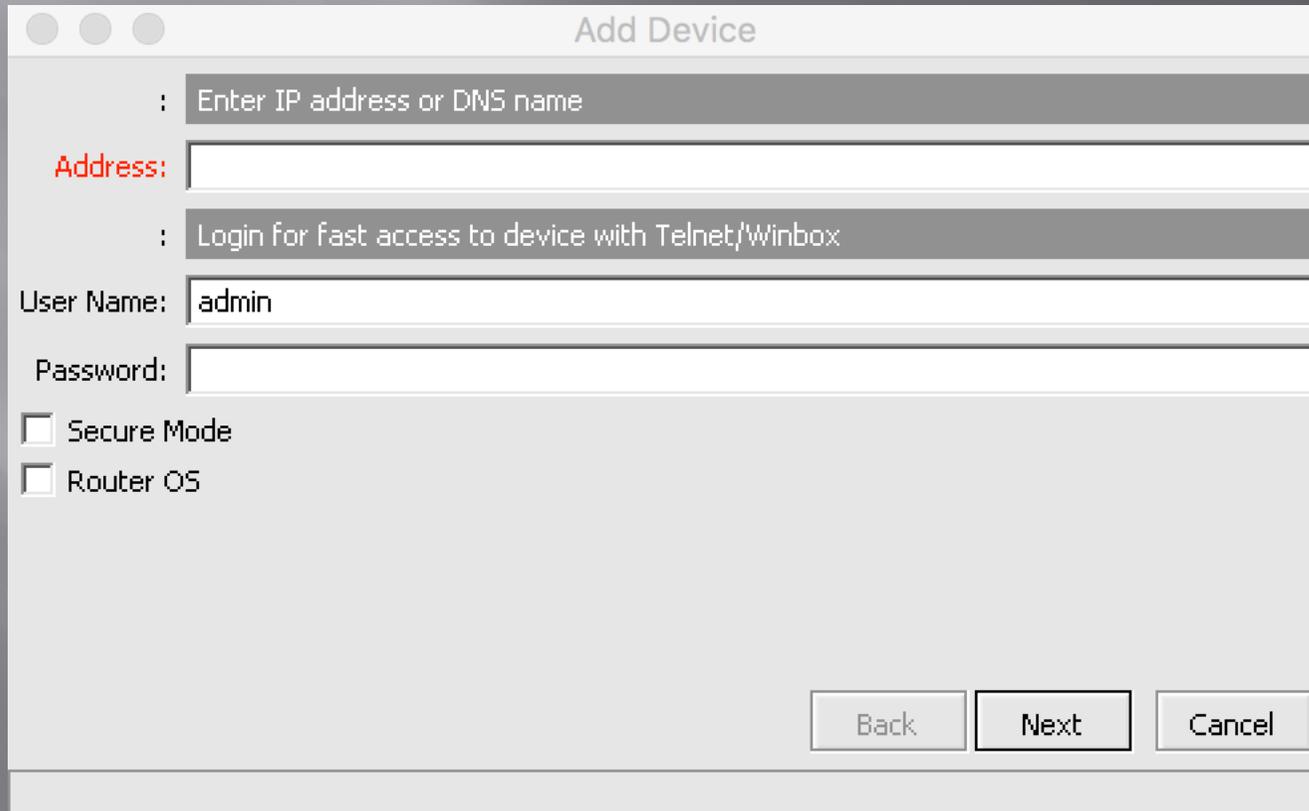
On the right side of the dialog, there are three buttons: 'Ok', 'Cancel', and 'Apply'.

How you should work with

Device Settings

- ▣ Adding devices is just few steps:

1-



The screenshot shows a dialog box titled "Add Device" with a standard macOS-style title bar (three colored circles). The dialog contains several input fields and checkboxes:

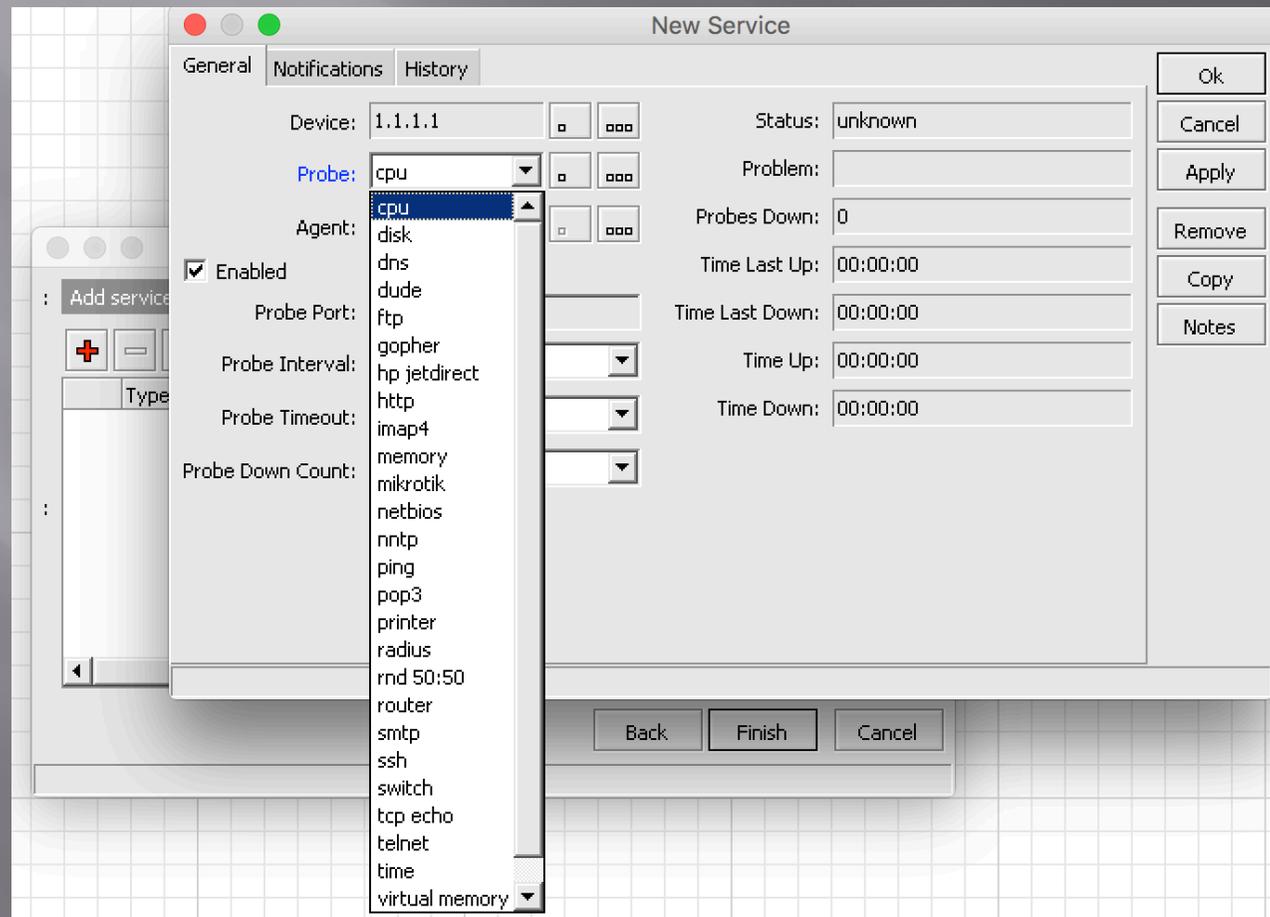
- A greyed-out label: " : Enter IP address or DNS name"
- A red label "Address:" followed by an empty text input field.
- A greyed-out label: " : Login for fast access to device with Telnet/Winbox"
- A label "User Name:" followed by a text input field containing the text "admin".
- A label "Password:" followed by an empty text input field.
- Two checkboxes, both unchecked:
 - Secure Mode
 - Router OS
- At the bottom right, three buttons: "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

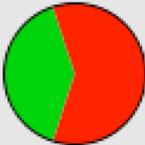
User Name: admin

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 for a device with IP 172.16.1.1. The window has 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

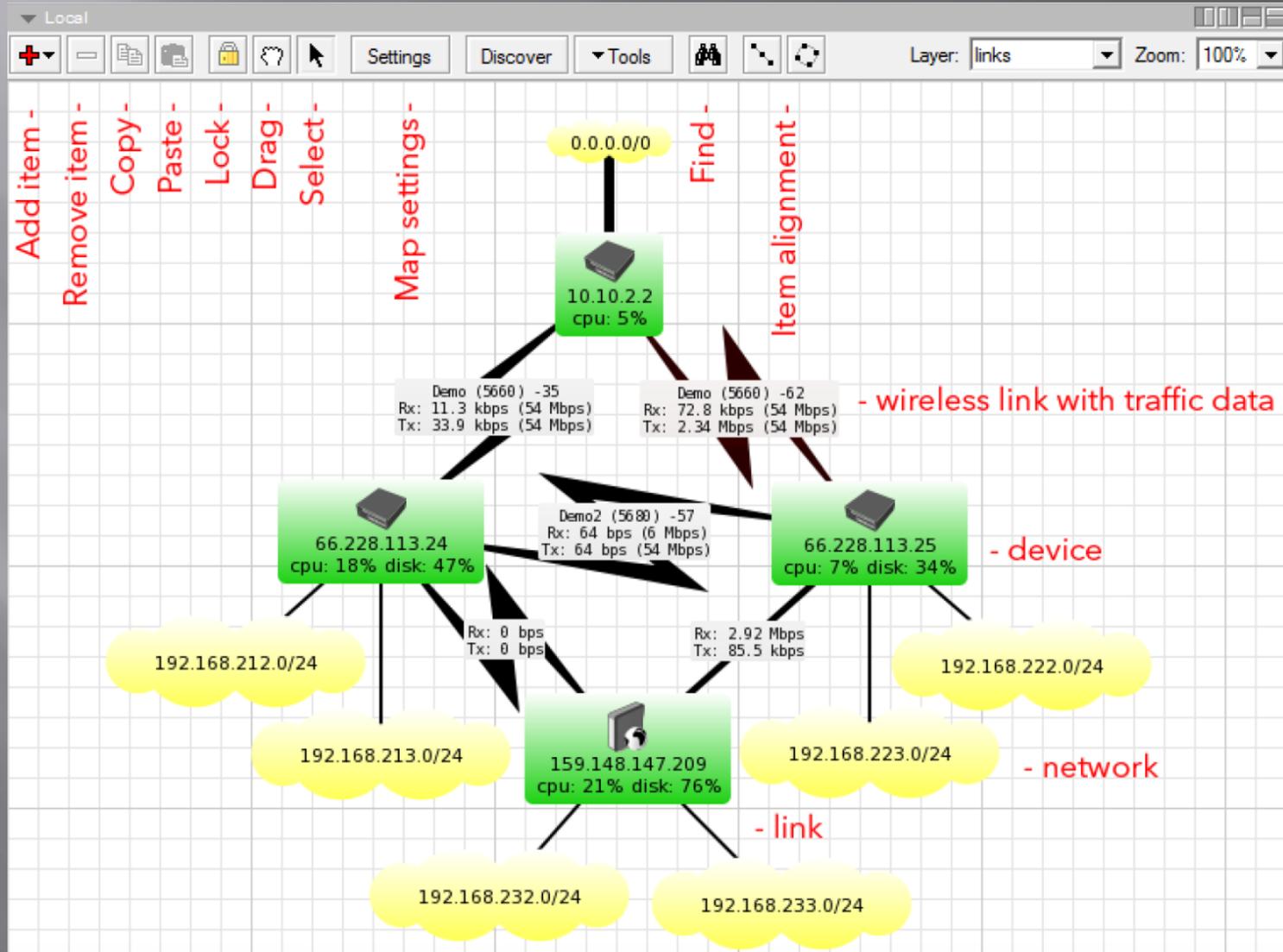
On the right side of the window, there are additional configuration options:

- 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

At the bottom 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.

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 the following settings:

- Enabled**
- Probe Interval:** default (dropdown), slider from default to 1d
- Probe Timeout:** default (dropdown), slider from default to 1d
- Probe Down Count:** default (dropdown), slider from default to 100
- Use Notifications**

Below the "Use Notifications" checkbox is a table of notification options:

	Name	/
	beep	
	flash	
	log to events	
	log to syslog	
	popup	

On the right side of the window, there are buttons for "Ok", "Cancel", "Apply", and "Notes".

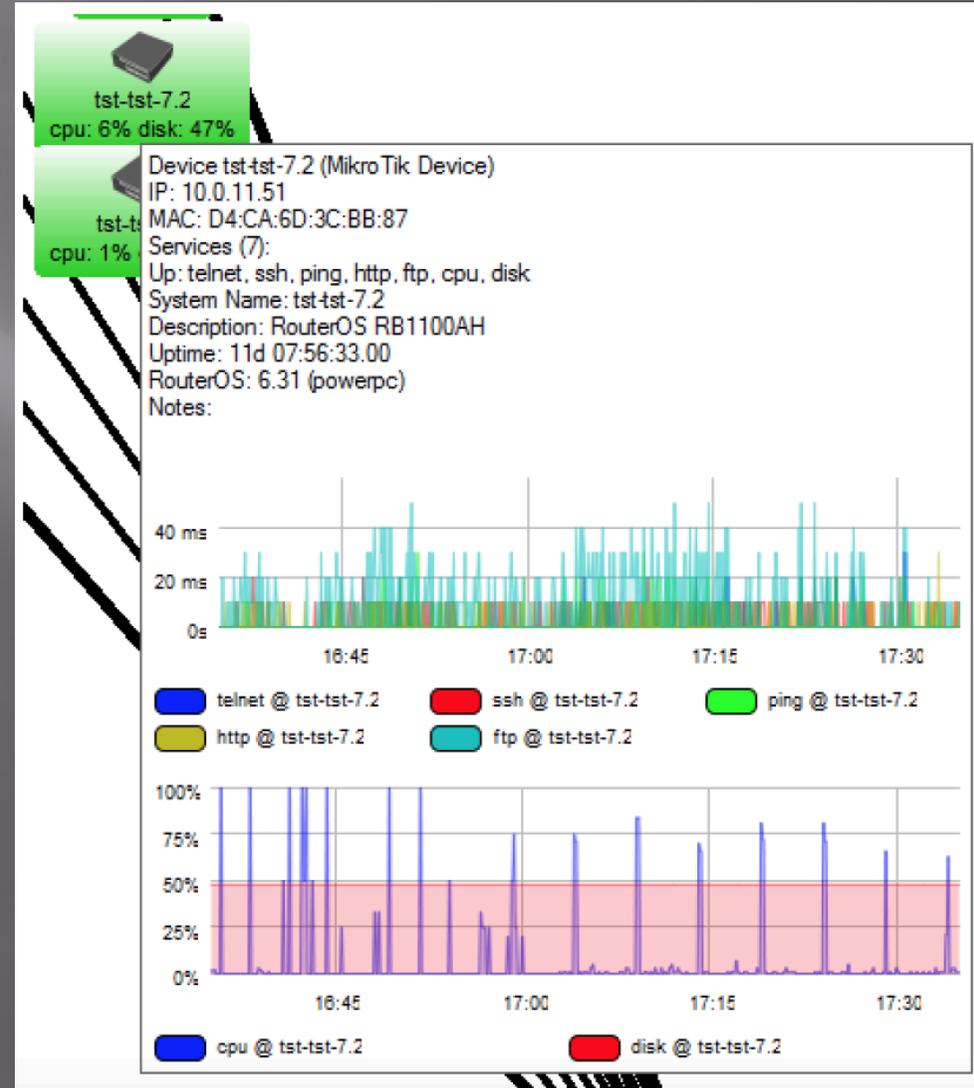
How you should work with

By The Way!!!!!!!

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

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

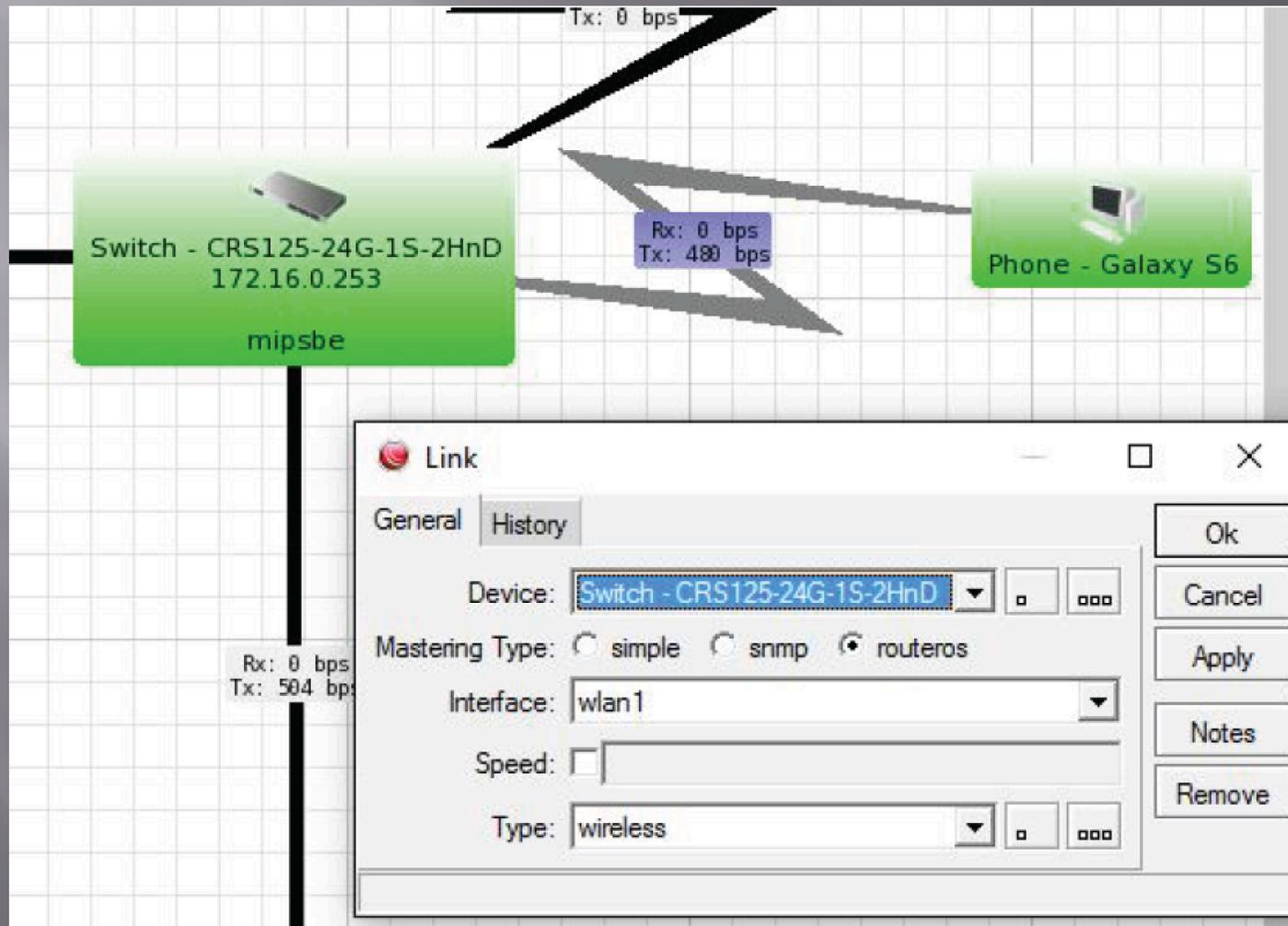
:) :) :) :)



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:

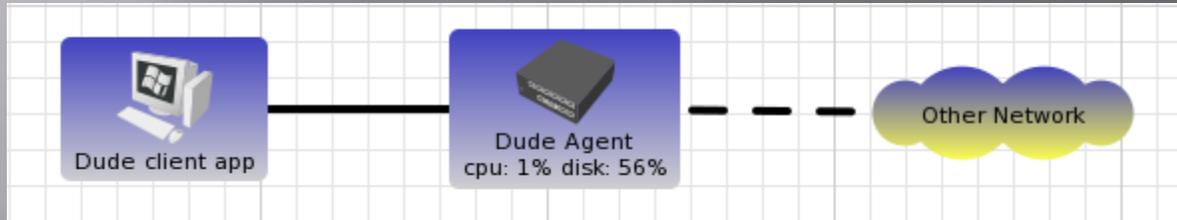
Snmp Type:

Snmp Speed:

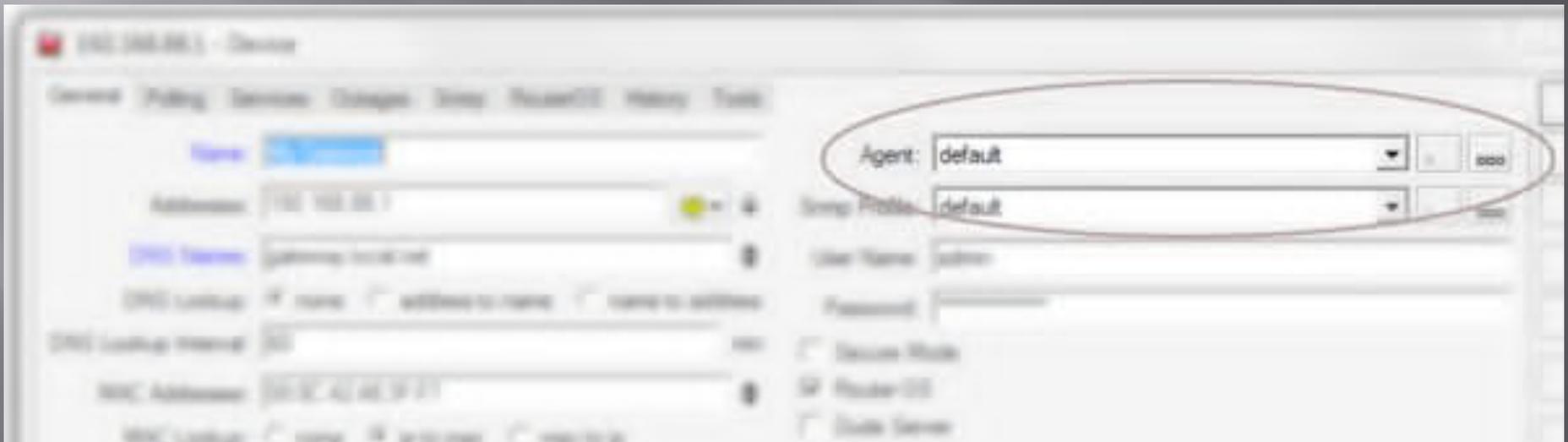
Ok
Cancel
Apply
Notes
Copy
Remove

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 is 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 bright orange color. The "i" is a simple dot and vertical line. "Gen" is in a clean, sans-serif font. "Tik" is in a bold, italicized sans-serif font. Above the "Tik" portion, there are two curved, crescent-like shapes, one slightly above and to the left of the other, suggesting motion or a stylized 'i'.

iGenTik

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

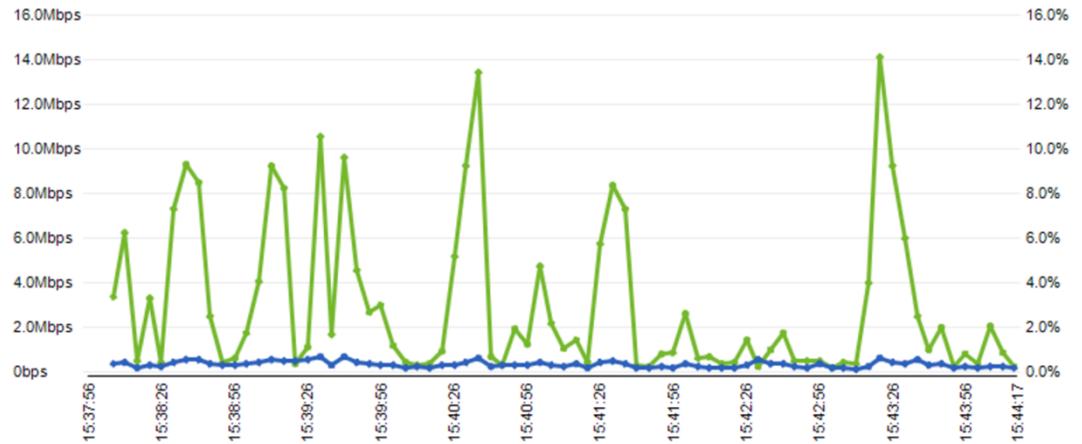
iGenTik

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



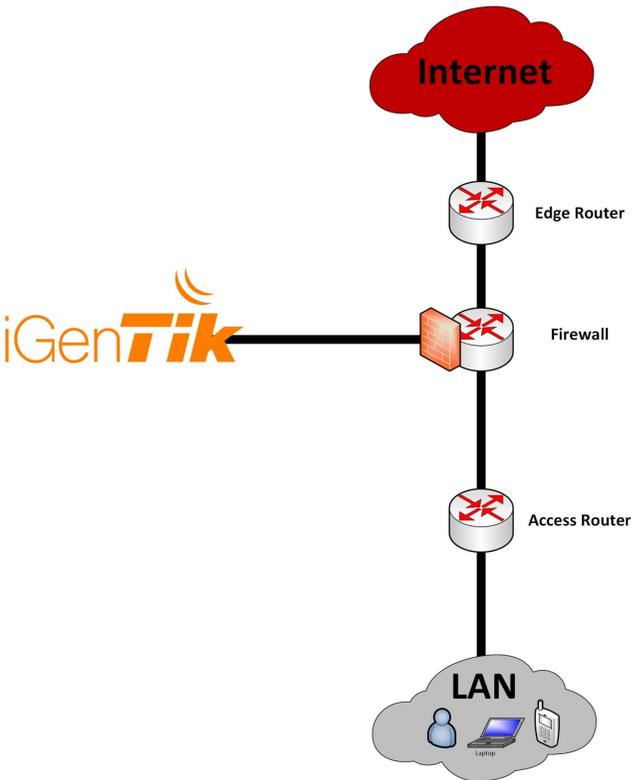
Key: Okay Dependent Partial Fail

iMS

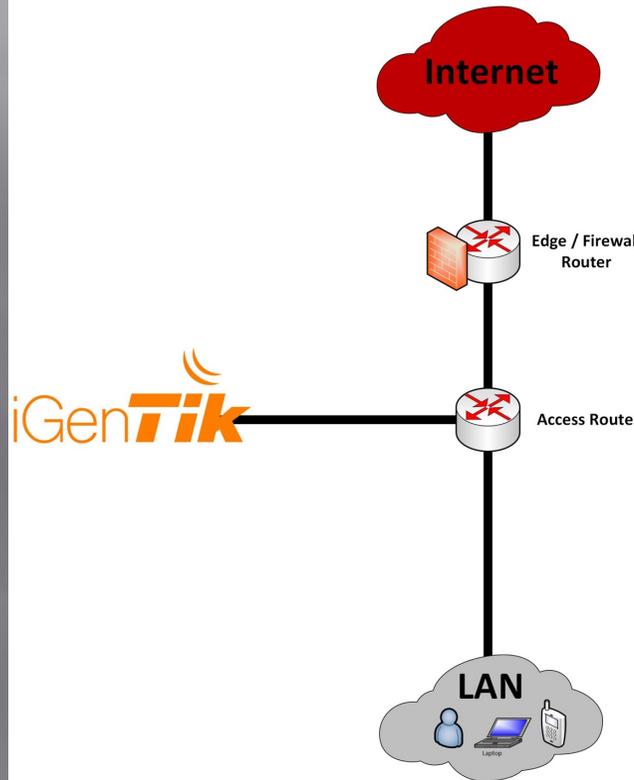
- IP status of all layer3 Devices including: Servers, Routers, Switches, End Points (Printers, Computers, Mobile Phones,)
- Public or Private host reachability and availability monitor
- Up Carrier gateway and reachability monitor: to monitor provider's availability and connectivity (with packet lost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

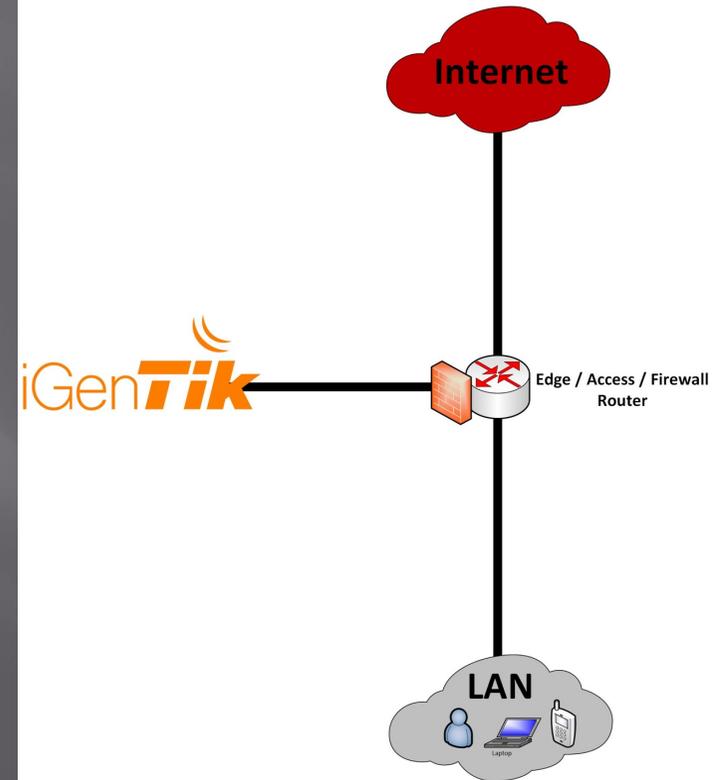
iMS
Triple Layers Topology



iMS
Double Layers Topology



iMS
Single Layer Topology

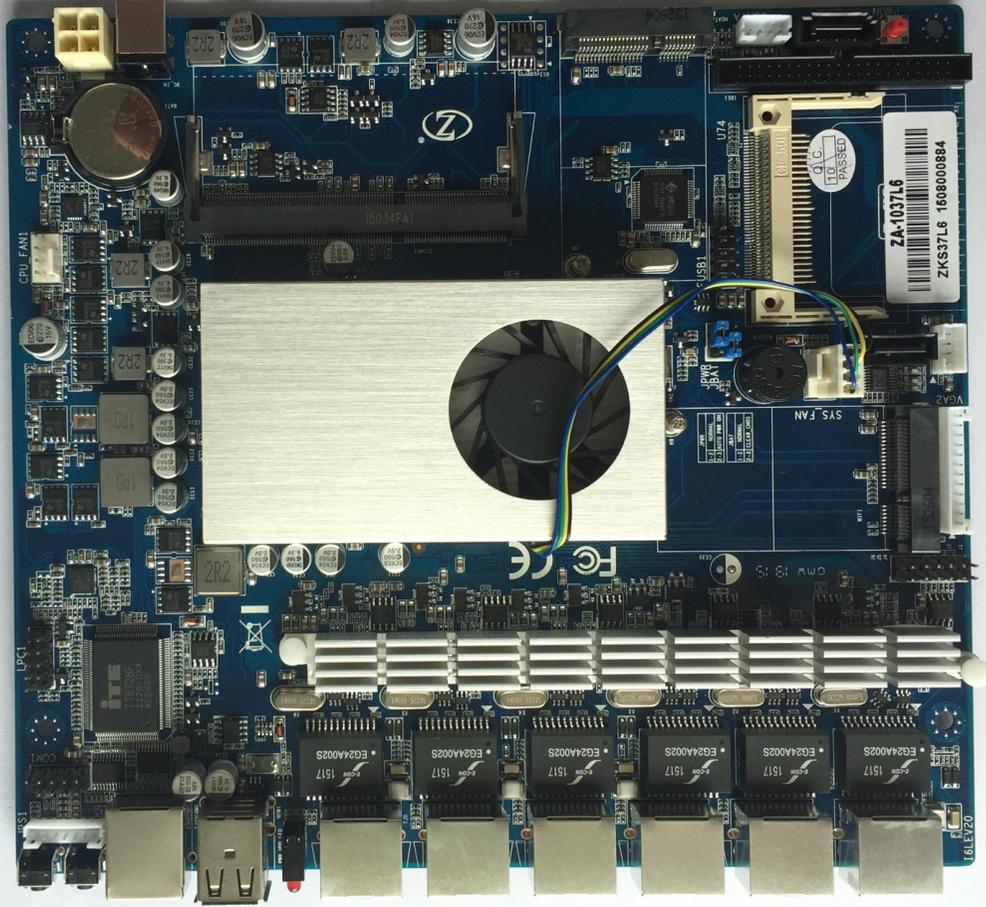


iCMS

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

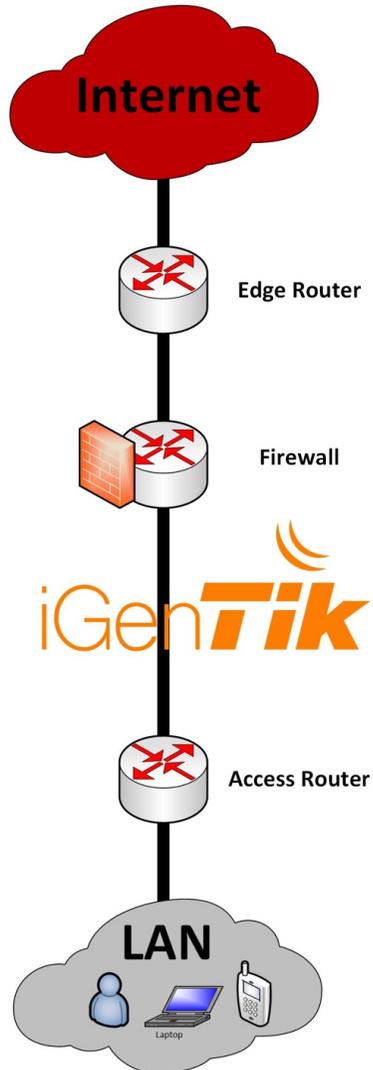


iCMS



iCMS

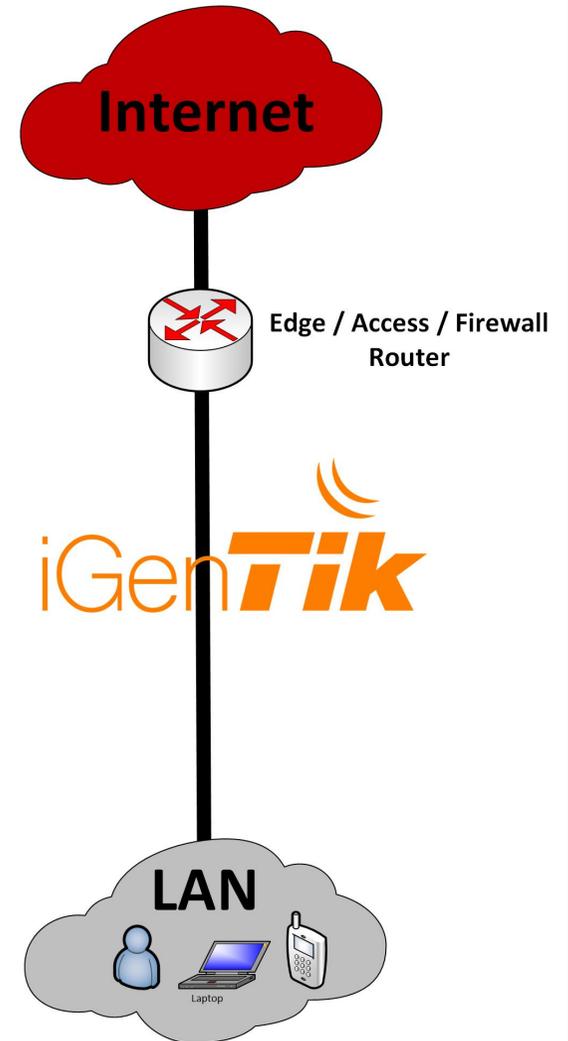
**iCMS
Triple Layers Topology**



**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  

Persian Cell: +98 (912) 149 7009  

International Cell: +37259431151

Skype: mani_raissdana

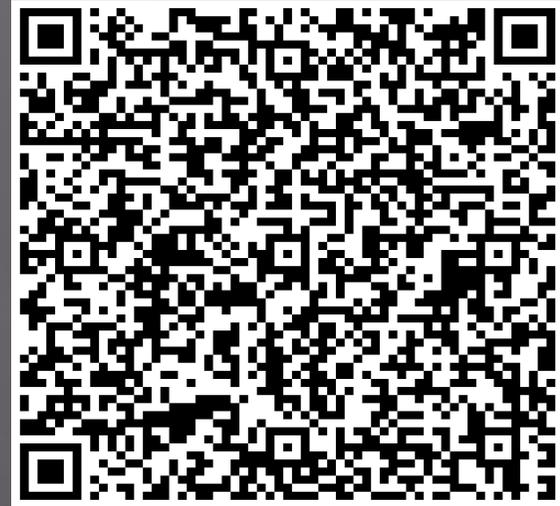
m.raissdana@mits-co.com

raissdana.mani@gmail.com

www.mits-co.com



MikroTikEngineers



mani_raissdana



mikrotikiran



@mani_raissdana



Mani Raissdana

Good Luck

&

Enjoy MUM