

Monitoreando con SNMP en Dude

MUM MÉXICO 2017

Acerca de mí:

- contactomexico@mkesolutions.net. Whatsapp: 951 3166271
- Propietario Integra Comunicaciones, WISP .- Miahuatlán Oaxaca

- Miembro adherente GPON SC
- Partner MKE Solutions en México (Próximos cursos Noviembre 2017)
- LSC, MTI
- MikroTik MTCNA, MTCRE, MTCTCE, MTCWE
- Cambium PTP650, ePMP
- Ubiquiti UAC
- Microsoft MCP, MCSA, MCSE
- CompTIA A+, Network+ , Server+, Security +
- Denwa DeECP
- ETA-I CST, CNST
- Access Data ACE



Objetivo:

Presentar de una forma fácil y simple una configuración básica del Dude Server para poder monitorear equipos en nuestra red independientemente de la marca.

*Se omite la configuración del Dude Server vía Winbox incluida en las nuevas distribuciones de RouterOS

* Configuraciones básicas se obvian

* No se ahonda en terminologías o configuraciones avanzadas, la meta es que los asistentes puedan implementarlo en sus redes.

Qué es el DUDE?

“Es una aplicación GRATUITA de MikroTik, que puede mejorar drásticamente la forma de administrar el entorno de red. Escanea automáticamente todos los dispositivos dentro de subredes especificadas, dibuja y distribuye un mapa de las redes, supervisa los servicios de los dispositivos y ejecuta acciones basadas en cambios de estado del dispositivo. No sólo puede monitorear sino también puede administrarlos. Actualizar masivamente los dispositivos RouterOS, configurar directamente desde la interfaz dude, ejecutar herramientas de supervisión de red, etc”.

https://wiki.mikrotik.com/wiki/Manual:The_Dude

- No solamente a dispositivos MikroTik, monitorea cualquier dispositivo con SNMP
- Corre como un servicio adicional en el routerboard (TILE, ARM, x86, MMIPS)
- También es un Syslog Server!
- Está en desarrollo, puede presentar bugs o tiene inhabilitadas funciones con respecto a las versiones anteriores

Alternativas:

- Cacti

- Se requiere una pc o un equipo en la nube
- Complicado
- Gratuito

-PRTG

- Muy caro (Gratuito con 100 sondas, Costo mas económico USD\$ 1600 por 500 sondas)
- Se requiere una pc o un equipo en la nube

Dude serve



.... Y bien amigable...

Qué es SNMP

- Simple Network Management Protocol

- A través de éste protocolo se obtiene información específica de los dispositivos monitoreados por un NMS (Network management system) y entregados por un agente vía OID (Identificador único de objeto)

- Existen 3 versiones:

- SNMPv1 .- Básica, valida por una cadena de “Comunidad” (plana)
- SNMPv2.- Seguridad intermedia, poco aceptada
- SNMPv3.- Versión segura de SNMP, cifrado , no todos los equipos son compatibles.

Instalando:

- <https://mikrotik.com/download>
- Seleccionar la plataforma compatible

TILE	CCR			
Main package			-	
Extra packages			-	
The Dude server			-	

- O instalarlo en un servidor en la nube, por ejemplo:

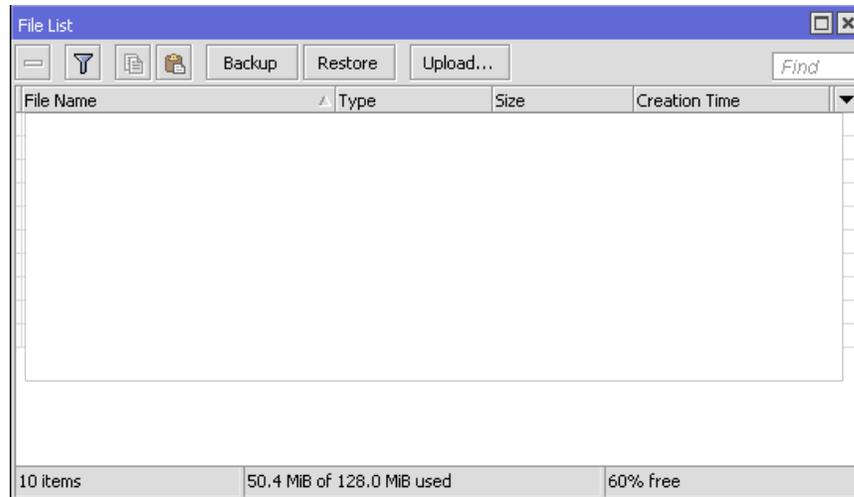
www.digitalocean.com

Script para montar el MikroTik:

<https://www.digitalocean.com/community/questions/installing-mikrotik-routers>

Instalando:

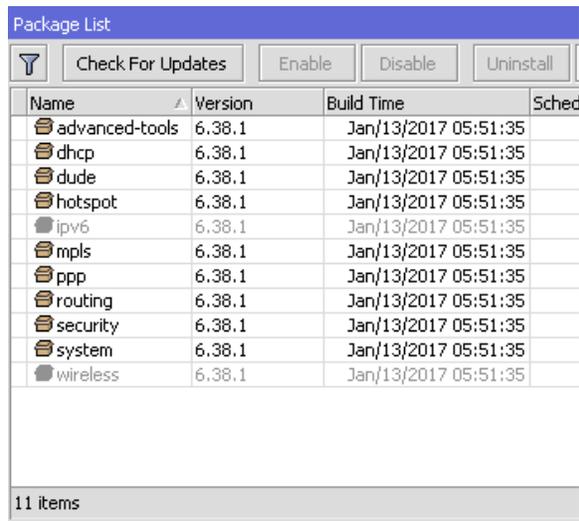
- Copiar el archivo .npk a nuestro equipo en files.



- system reboot
- la versión de dude DEBE ser igual a la versión de RouterOS

Instalando:

Verificamos:



The screenshot shows a window titled "Package List" with a blue header. Below the header are four buttons: "Check For Updates", "Enable", "Disable", and "Uninstall". The main area contains a table with the following columns: "Name", "Version", "Build Time", and "Sched". The table lists 11 packages, all with version 6.38.1 and build time Jan/13/2017 05:51:35. The packages are: advanced-tools, dhcp, dude, hotspot, ipv6, mpls, ppp, routing, security, system, and wireless. At the bottom of the window, a status bar indicates "11 items".

Name	Version	Build Time	Sched
advanced-tools	6.38.1	Jan/13/2017 05:51:35	
dhcp	6.38.1	Jan/13/2017 05:51:35	
dude	6.38.1	Jan/13/2017 05:51:35	
hotspot	6.38.1	Jan/13/2017 05:51:35	
ipv6	6.38.1	Jan/13/2017 05:51:35	
mpls	6.38.1	Jan/13/2017 05:51:35	
ppp	6.38.1	Jan/13/2017 05:51:35	
routing	6.38.1	Jan/13/2017 05:51:35	
security	6.38.1	Jan/13/2017 05:51:35	
system	6.38.1	Jan/13/2017 05:51:35	
wireless	6.38.1	Jan/13/2017 05:51:35	

- Accedemos a winbox y habilitamos dude:

dude set enabled=yes

Instalando:

Descargamos el cliente desde la misma ubicación, sólo cliente windows:

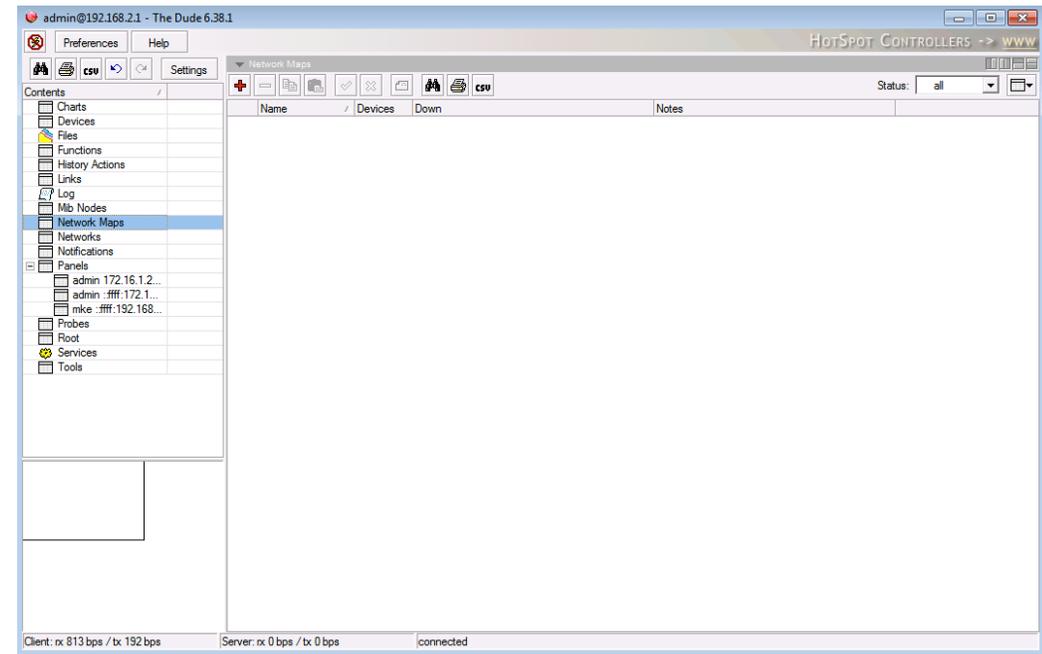
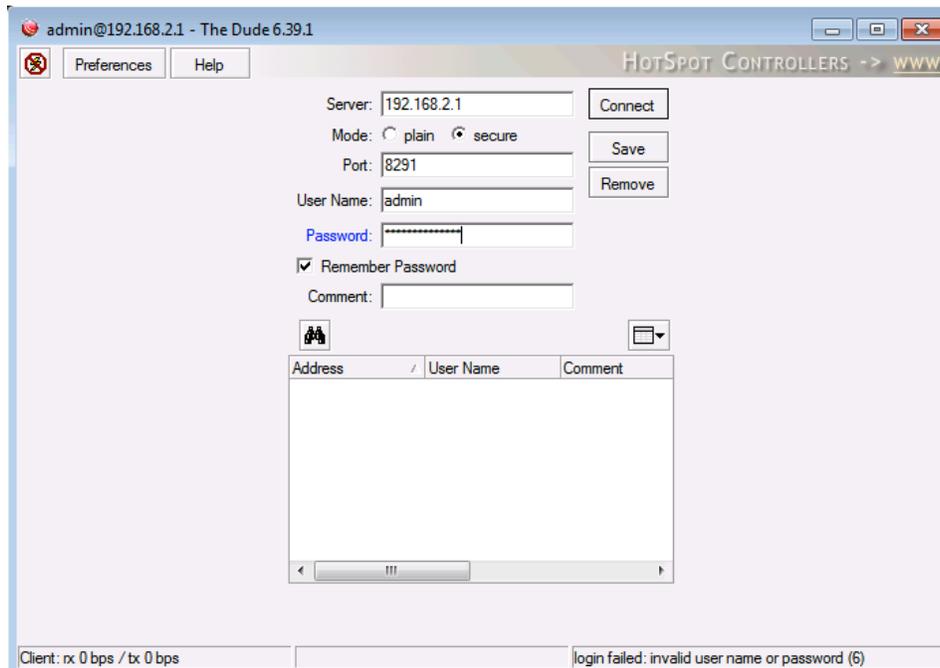
<https://mikrotik.com/download>

The Dude client



Configuración inicial

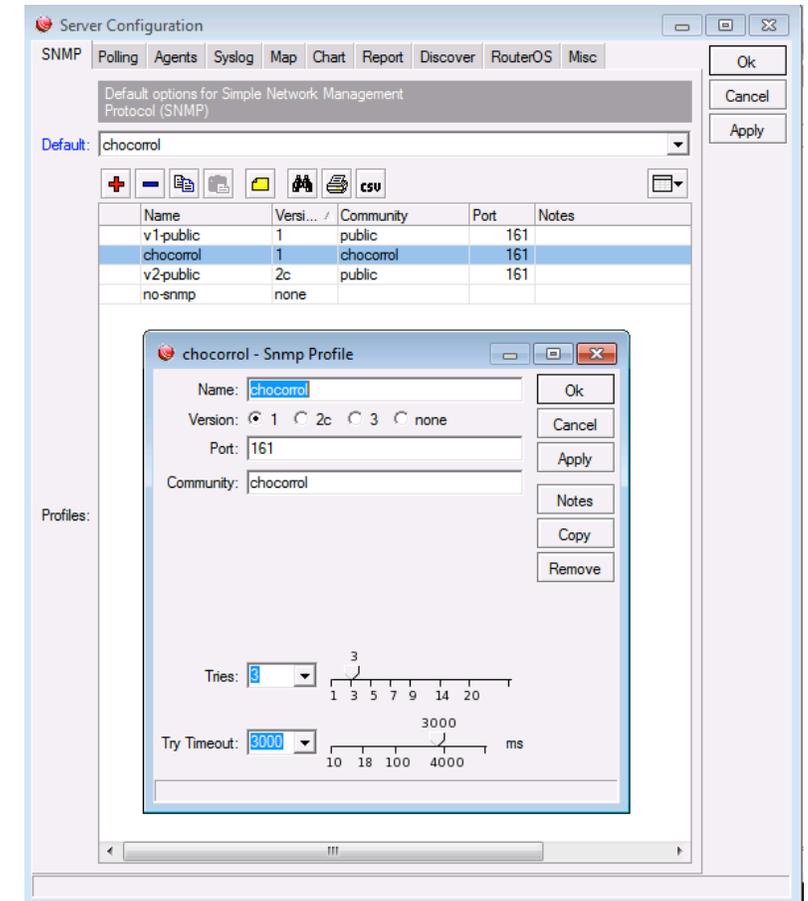
Primer login:



Configuración inicial

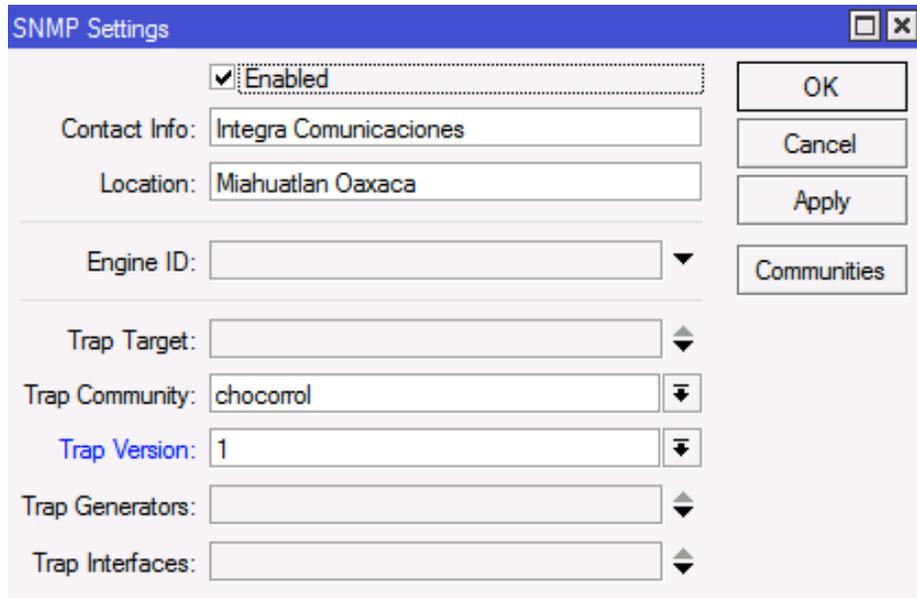
Tip: Antes de realizar un descubrimiento de equipos definamos la comunidad de snmp por default. Marcas como Ubiquiti, Deliberant, TP-Link sólo permite SNMPv1 así que seamos ocurrentes en el nombre de la misma para darle un poco mas de “seguridad”.

Definamos igualmente desde qué IP (Agente NMS) puede ser consultado



Configuración inicial

IP- SNMP



SNMP Settings

Enabled

Contact Info: Integra Comunicaciones

Location: Miahuatlan Oaxaca

Engine ID:

Trap Target:

Trap Community: chocorrol

Trap Version: 1

Trap Generators:

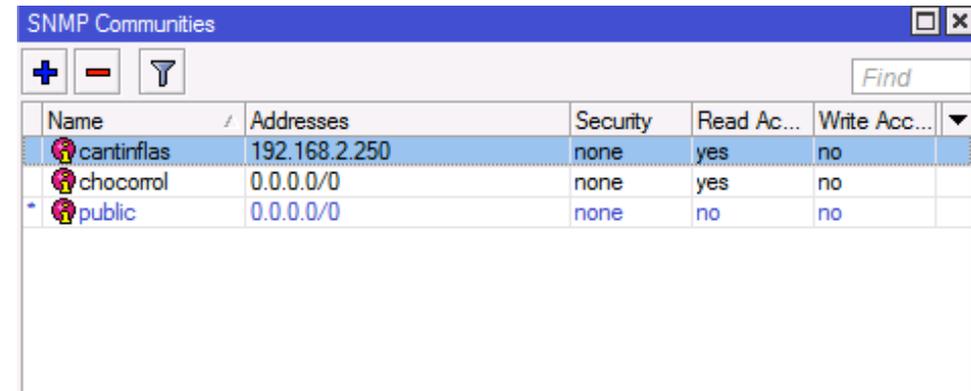
Trap Interfaces:

OK

Cancel

Apply

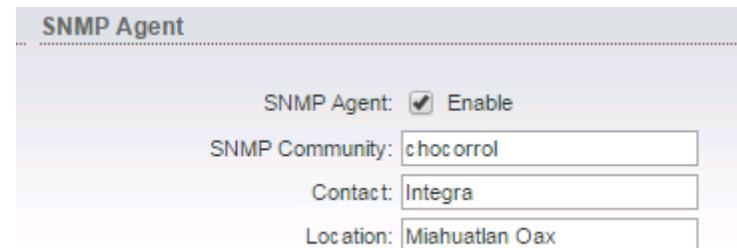
Communities



SNMP Communities

Name	Addresses	Security	Read Ac...	Write Acc...
cantinflas	192.168.2.250	none	yes	no
chocorrol	0.0.0.0/0	none	yes	no
public	0.0.0.0/0	none	no	no

Ubiquiti:
Pestaña services (sólo V1)



SNMP Agent

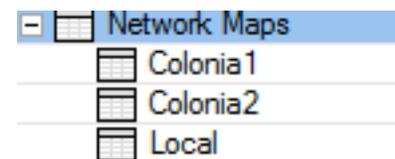
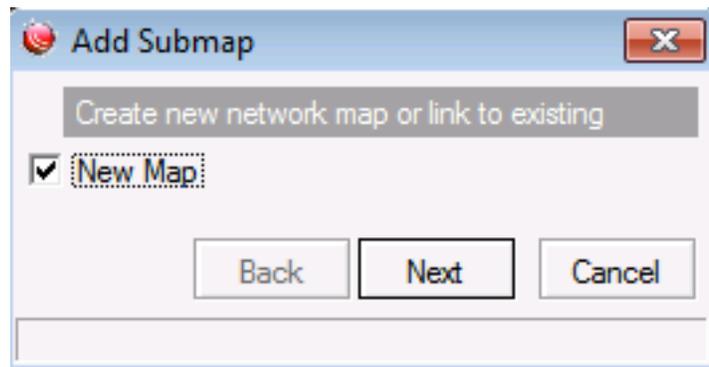
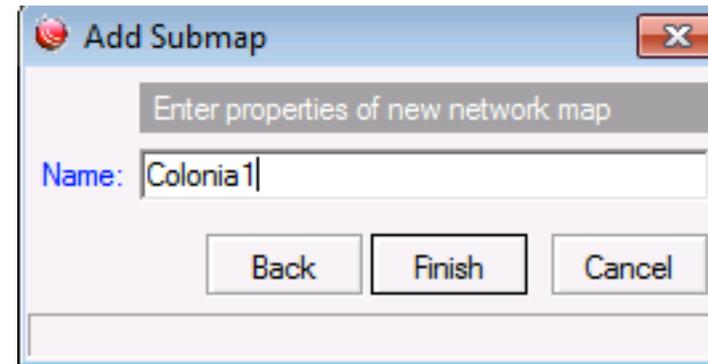
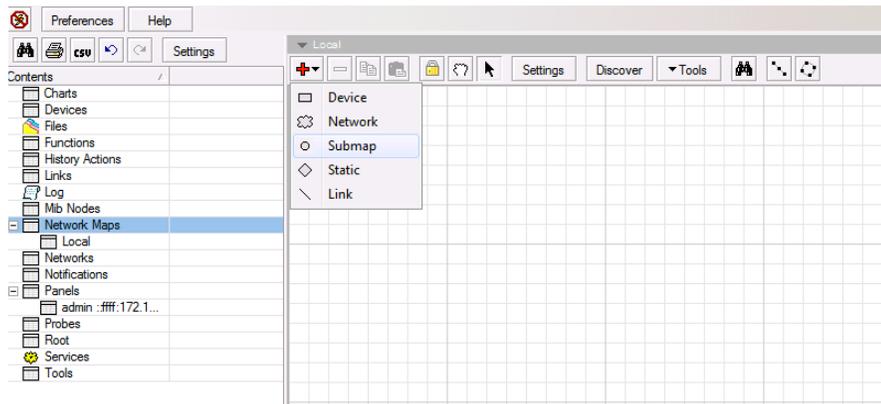
SNMP Agent: Enable

SNMP Community: chocorrol

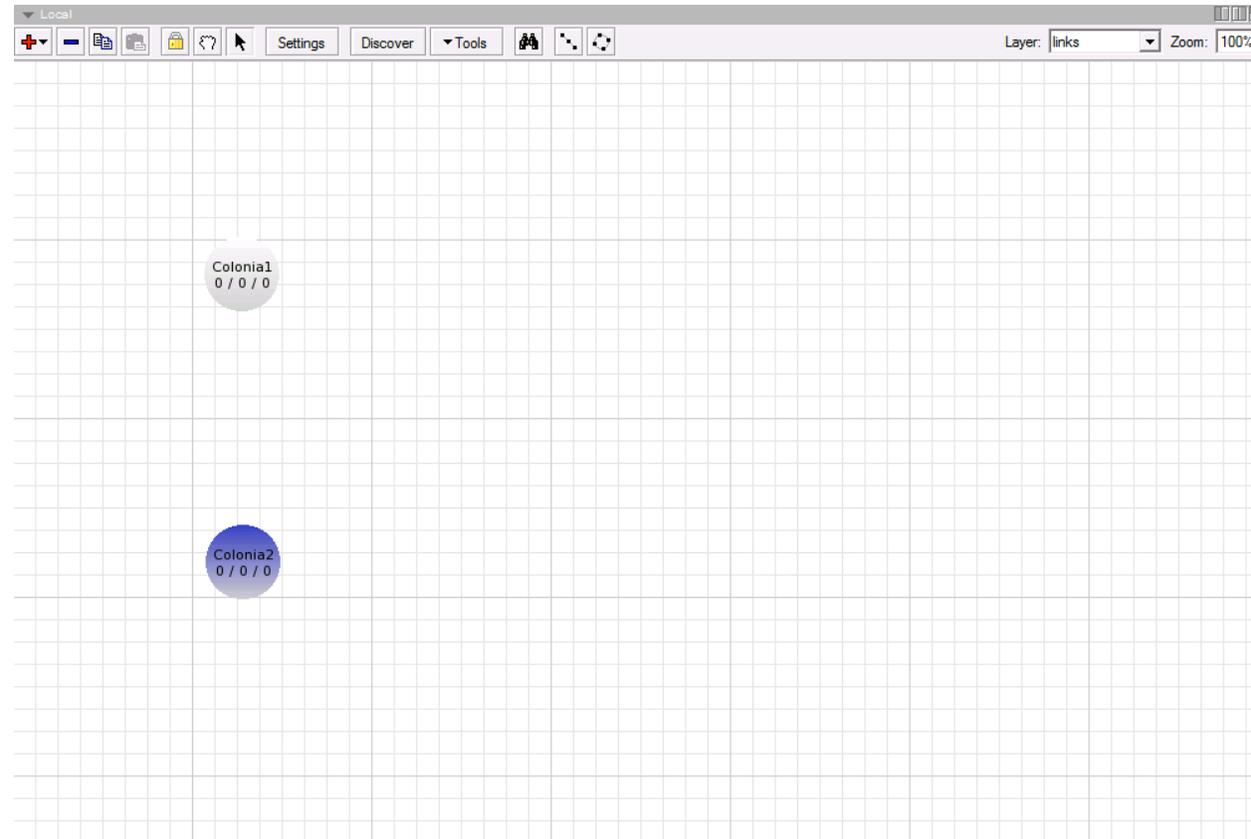
Contact: Integra

Location: Miahuatlan Oax

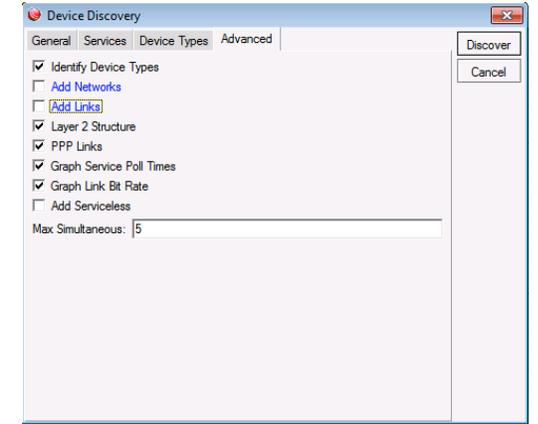
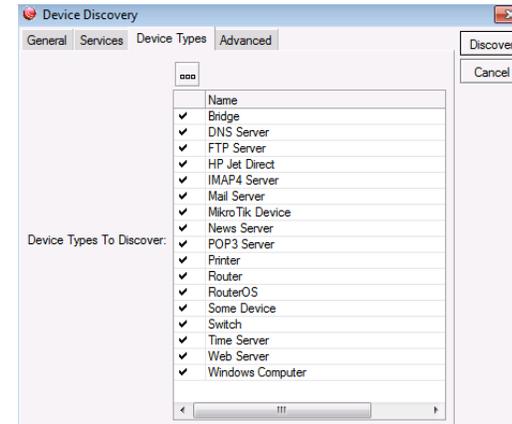
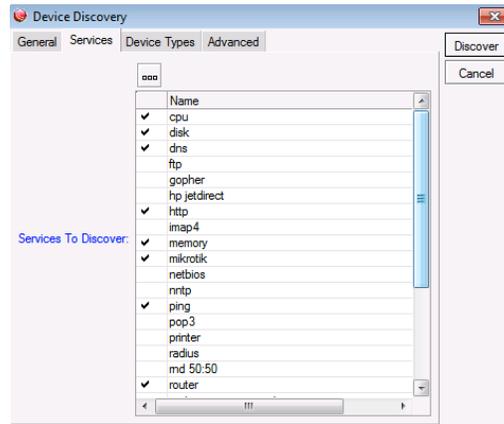
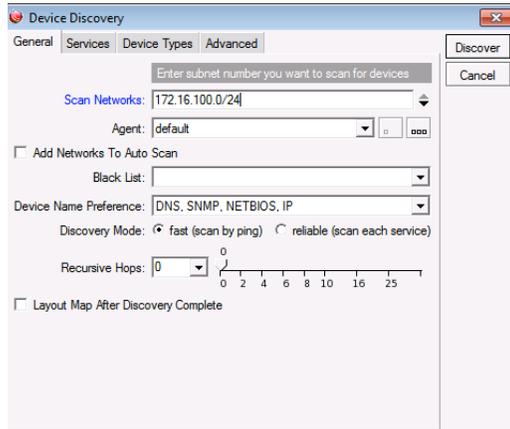
Definimos submapas “colonias”



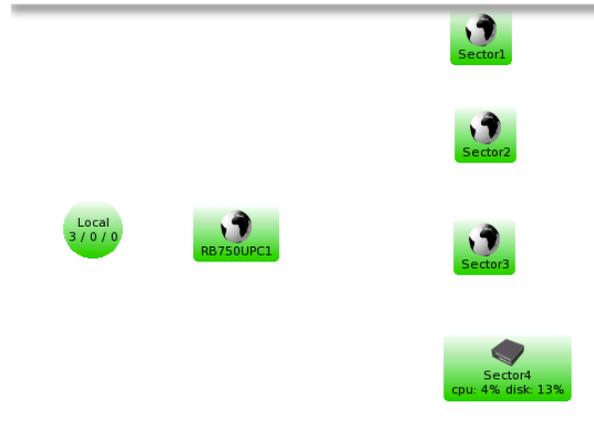
Definimos submapas “colonias”



Descubriendo dispositivos

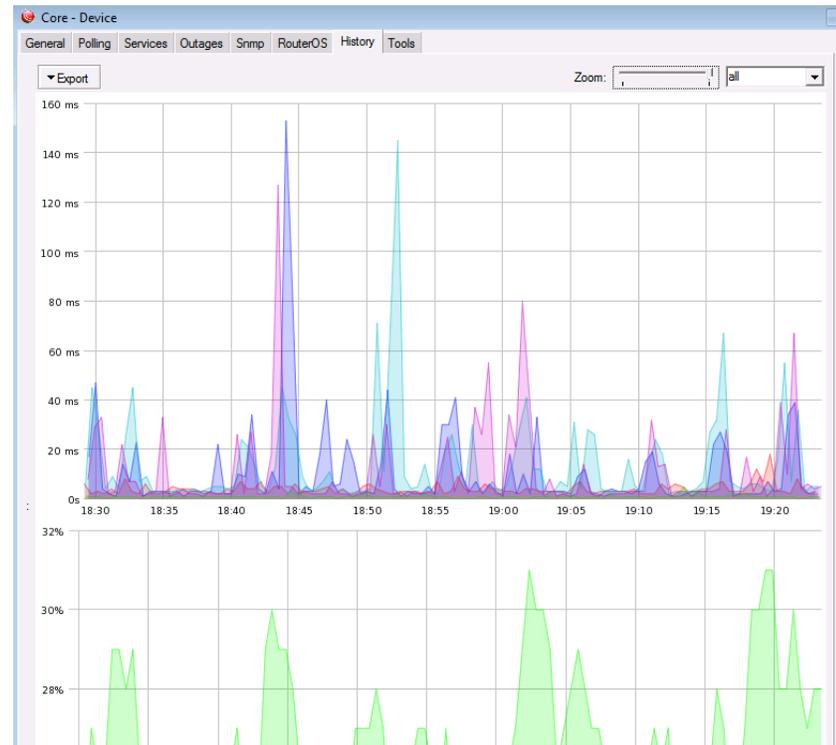


Descubriendo dispositivos



Tenemos un mapa principal y 2 submapas

Descubriendo dispositivos



Opciones

PtP2 - Device

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

Name: PtP2

Addresses:

DNS Names:

DNS Lookup: none address to name name to address

DNS Lookup Interval: 60 min

MAC Addresses: D4:CA:6D:B2:0A:58
D4:CA:6D:B2:0A:59

MAC Lookup: none ip to mac mac to ip

Type: RouterOS

Parents:

Custom Field 1:

Custom Field 2:

Custom Field 3:

Agent: default

Snmp Profile: chocorol

User Name: admin

Password:

Secure Mode
 Router OS
 Dude Server

Services:  Up - 12

Status: up

RouterOS Status: invalid user name or password (6), next attempt at May/17 23:31:50

Ok
Cancel
Apply
Notes
Remove
Tools
Reprobe
Ack
Unack
Reboot
Reconnect

Error in Addresses - ip address expected

Type: RouterOS

Parents: Bridge
DNS Server

Field 1: FTP Server
HP Jet Direct

Field 2: IMAP4 Server
Mail Server

Field 3: MikroTik Device
News Server
POP3 Server
Printer
Router
RouterOS
Some Device
Switch
Time Server
Web Server
Windows Computer
unknown

Opciones

Type	Problem	Notes
cpu		
disk		
dns		
ftp		
http		
mikrotik		
ping		
router		
routers manage...		
ssh		
switch		
telnet		

Enabled

Probe Interval: default
default 1s 2s 5s 10s 15s 30s 1m 2m 5m 10m 15m 30m 1h 2h 3h 6h 12h 1d

Probe Timeout: default
default 1s 2s 5s 10s 15s 30s 1m 2m 5m 10m 15m 30m 1h 2h 3h 6h 12h 1d

Probe Down Count: default
default 1 2 3 4 5 6 7 8 9 10 12 14 16 18 20 25 50 100

Use Notifications

Notifications:

Name
beep
flash
log to events
log to syslog
popup

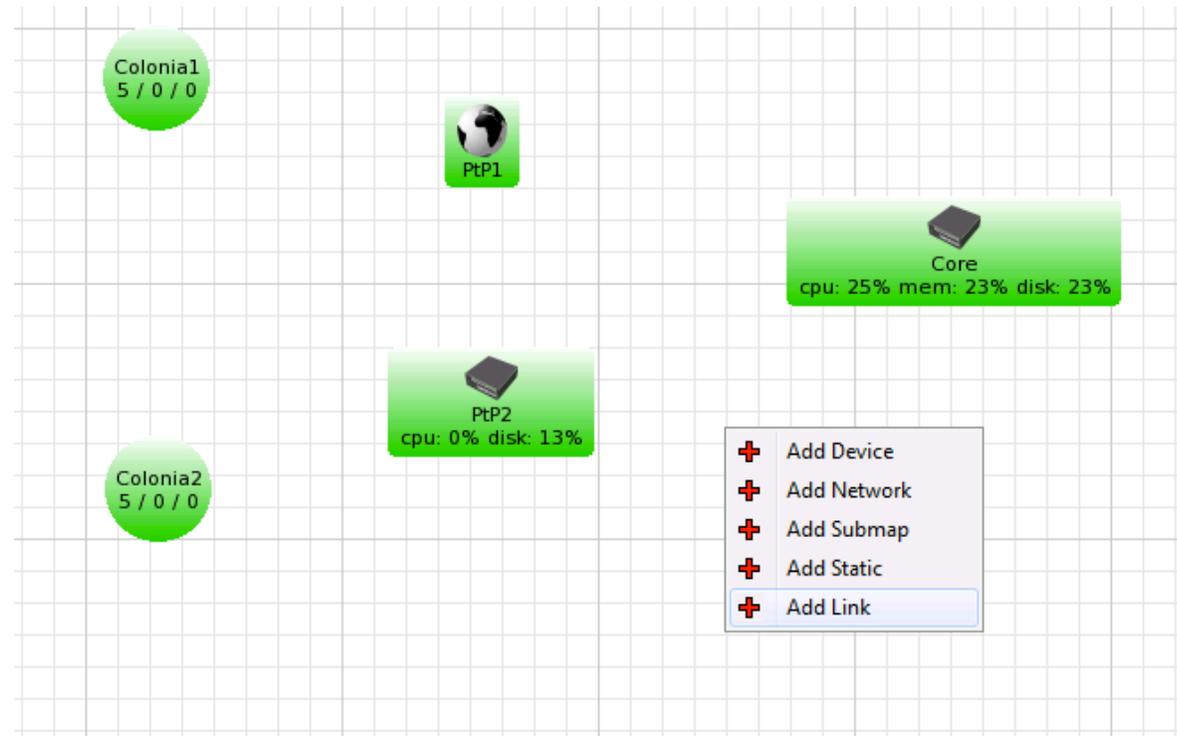
Probe interval: Cada cuánto deben ser encuestados los servicios (segundos)

Probe Timeout: Cuánto debe pasar desde el inicio de la encuesta hasta que se considere sin respuesta. El dispositivo seguirá en verde pero el servicio específico pasará a anaranjado.

Probe down count: Cuántas veces debe fallar la encuesta para que se considere abajo. El dispositivo se vuelve naranja pero el servicio individual pasa a rojo.

Añadimos links

Si tenemos correctamente configurada nuestra comunidad seremos capaces de visualizar las interfaces. Si es un dispositivo Mikrotik y seteamos el user y pass tenemos mas detalle.



Añadimos links

Links can be static things on map, or they can show some statistics about some interface, here you can set how link should be managed

Device: PtP2

Mastering Type: simple

- simple
- snmp
- routers

Speed: routers

Type: unknown

Finish Cancel

Links can be static things on map, or they can show some statistics about some interface, here you can set how link should be managed

Device: PtP2

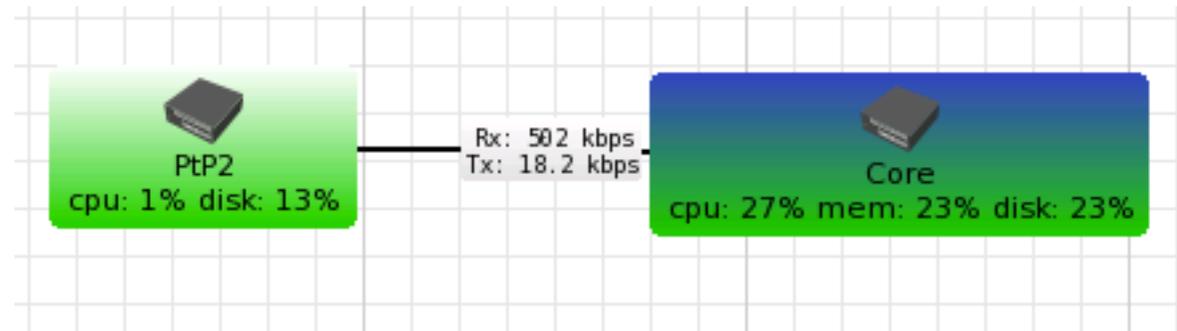
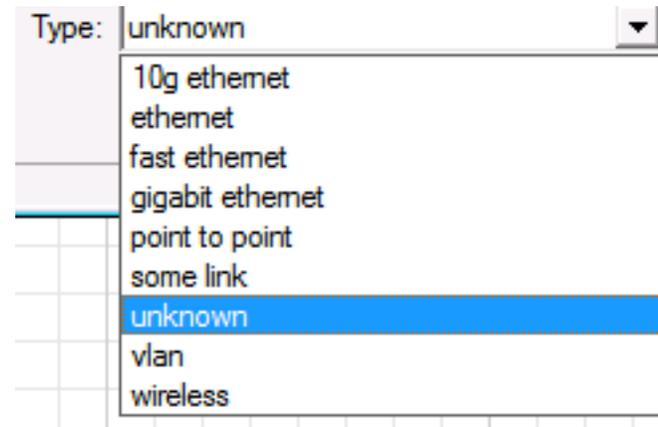
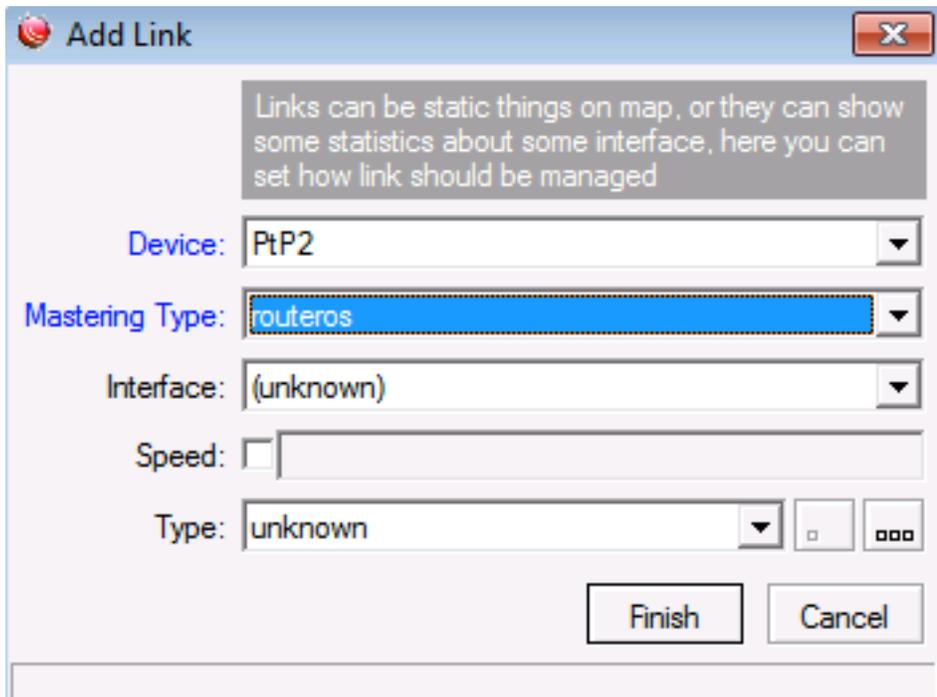
Mastering Type: snmp

Interface: M900 ::ether5 (5)

Speed: M900 ::ether5 (5)

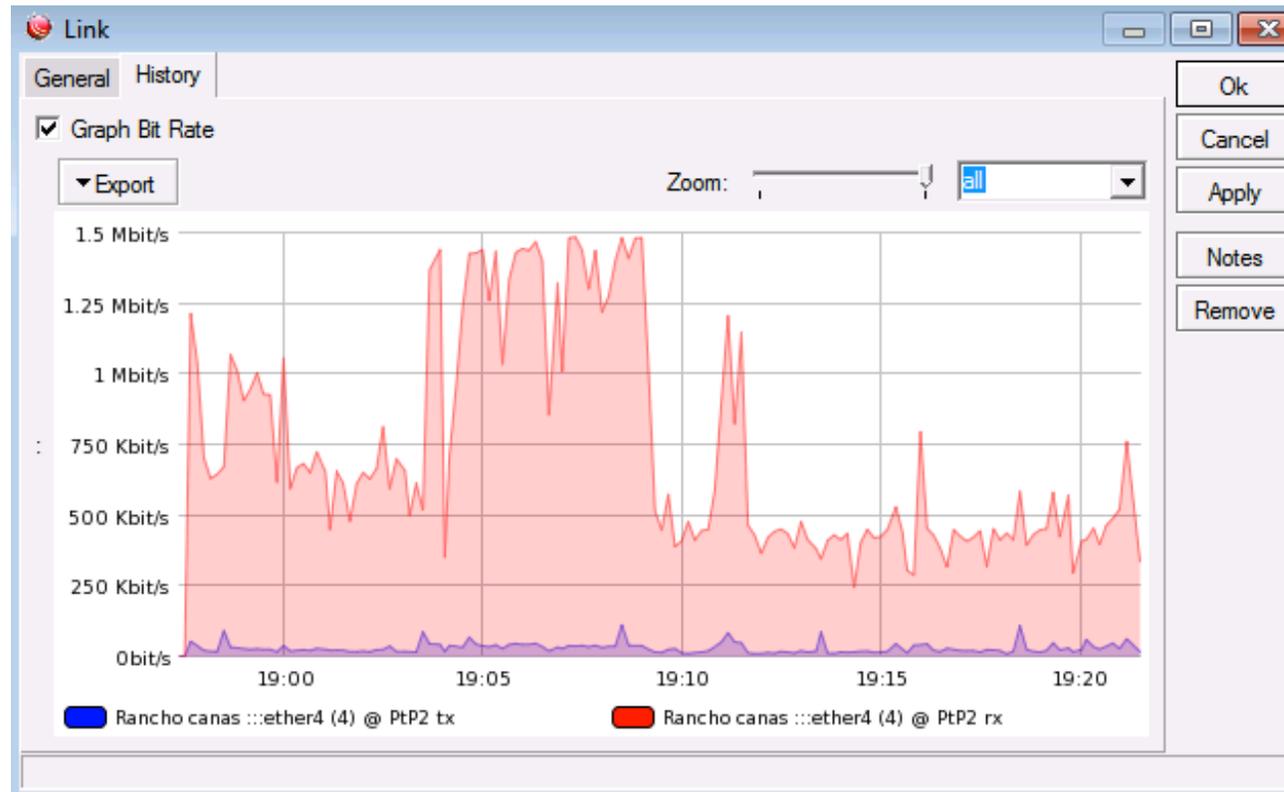
Type: bridge1 (6)
ether1 (1)
ether2 (2)
ether3 (3)

Añadimos links

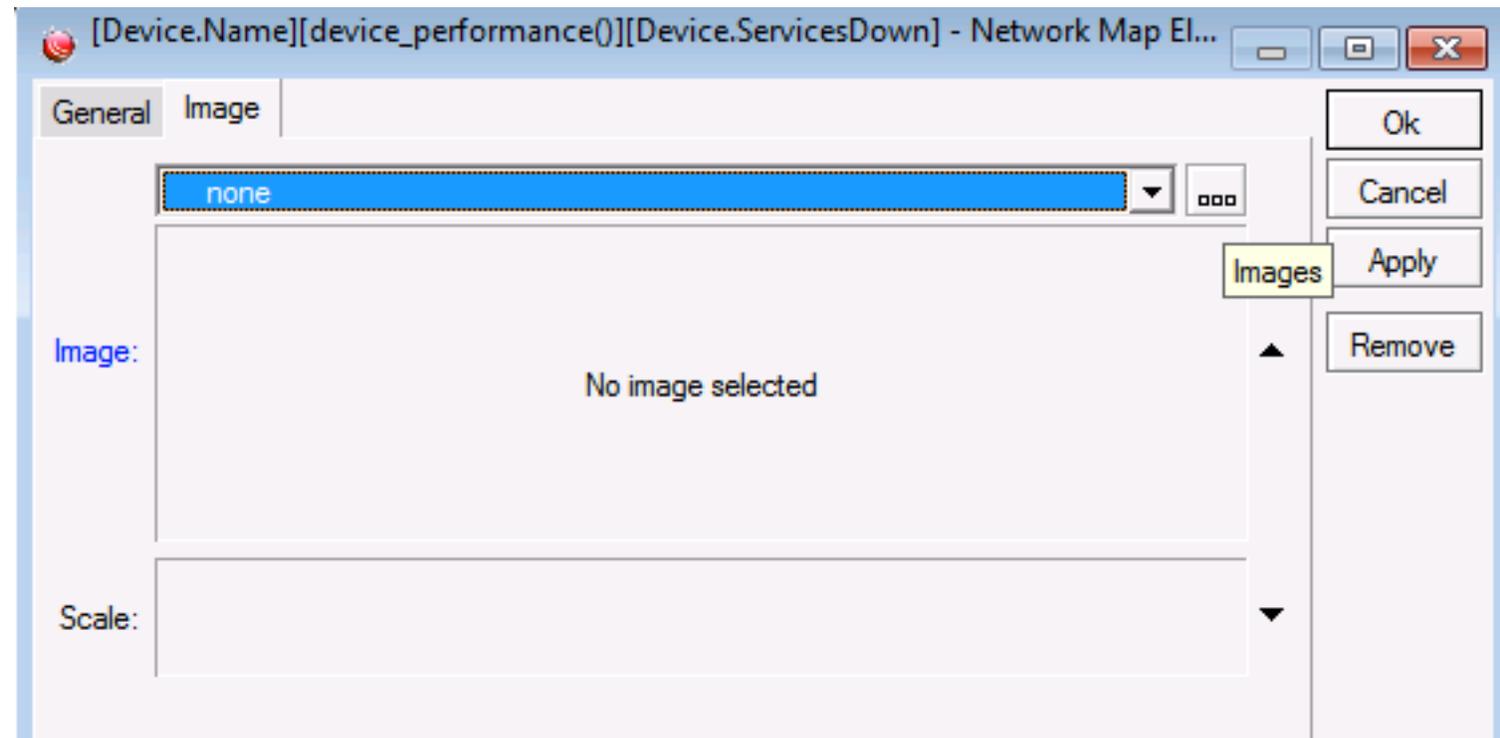
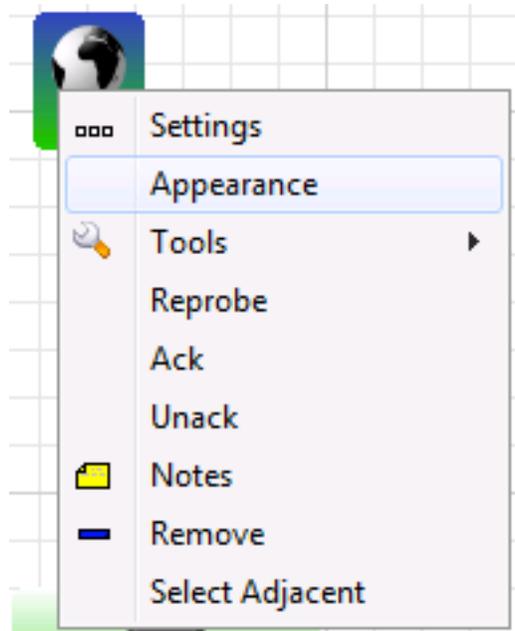


No lista nada, no es un dispositivo MikroTik

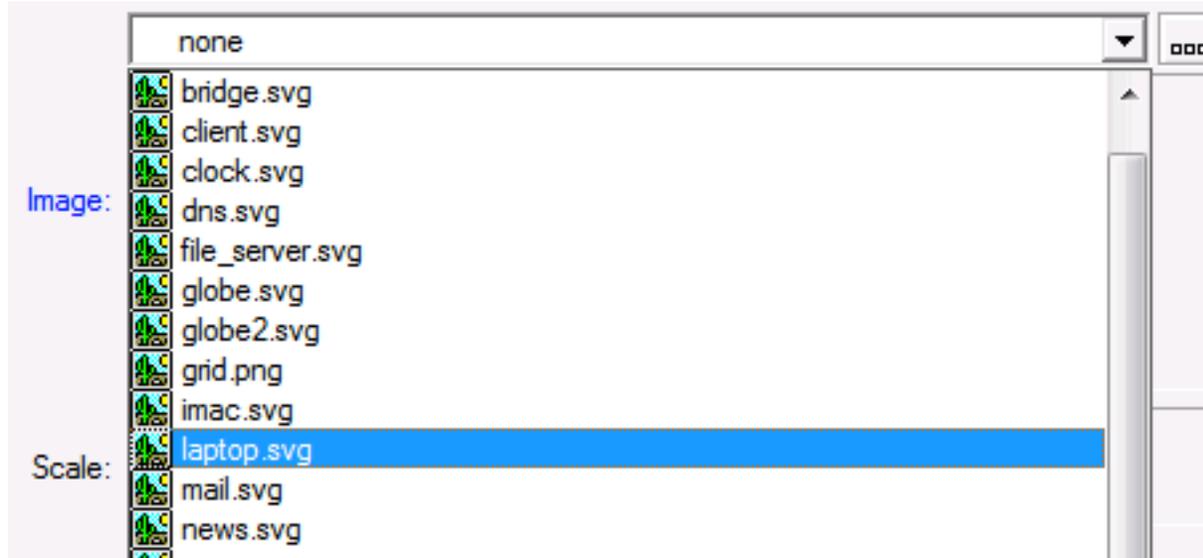
Añadimos links



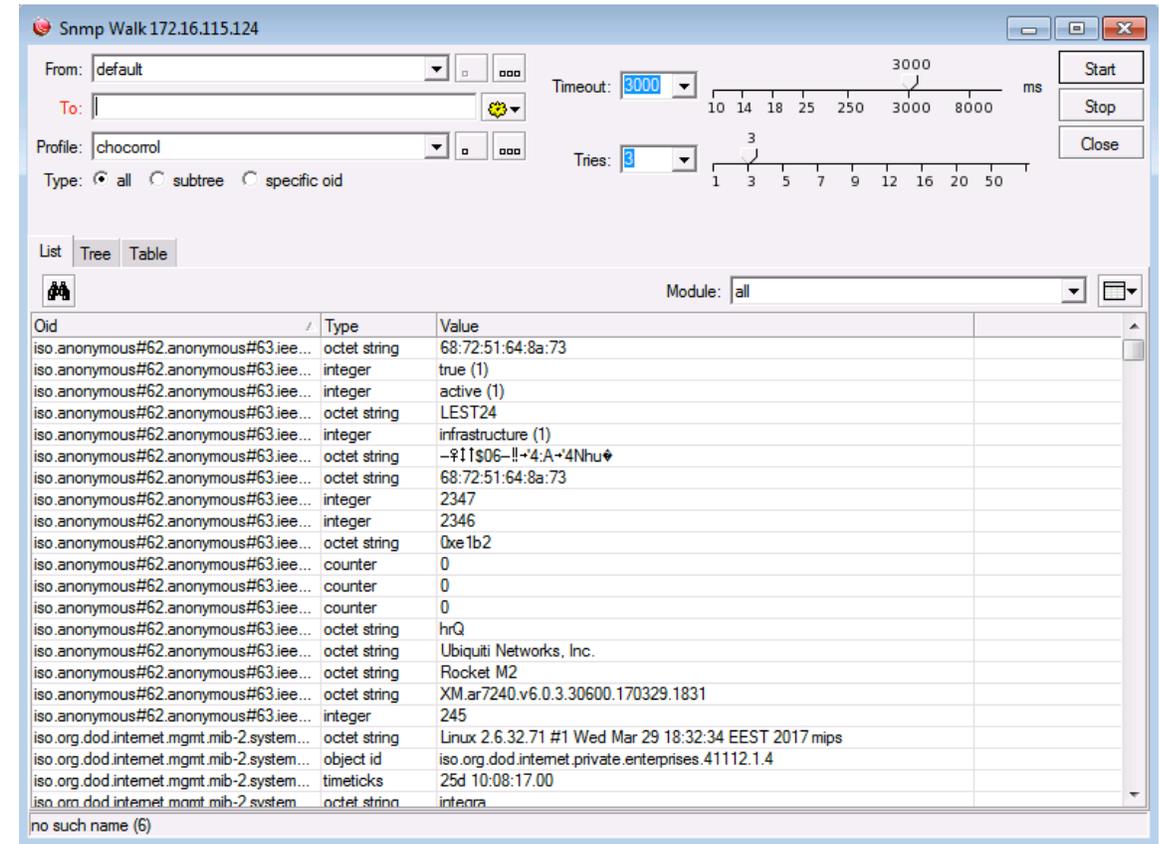
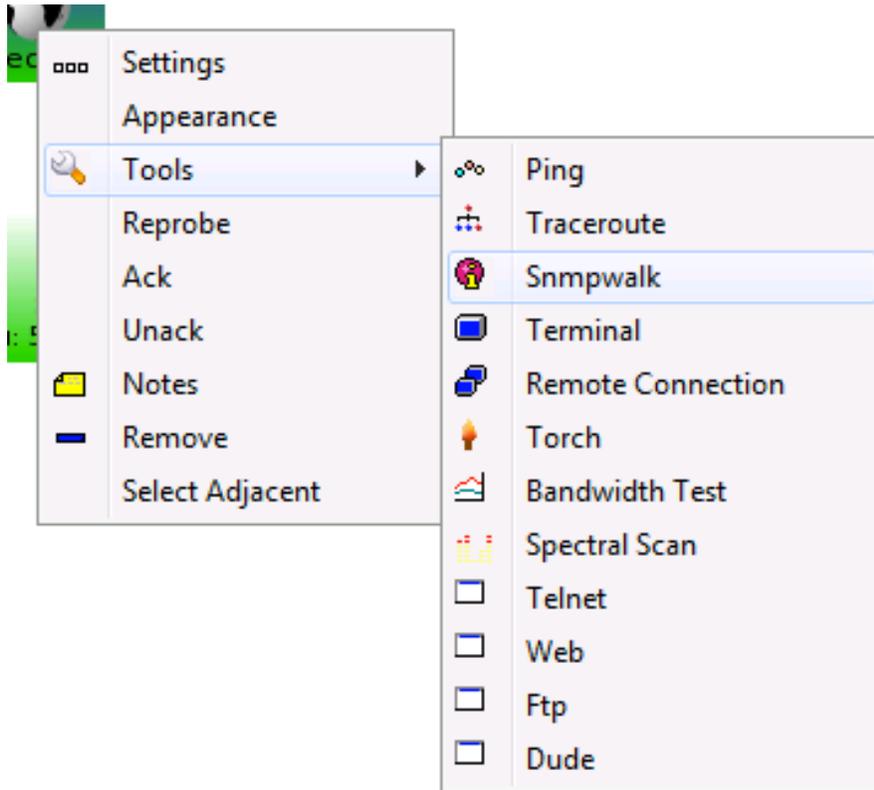
Personalizamos apariencia de dispositivos



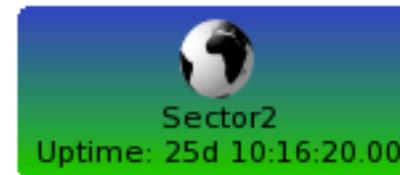
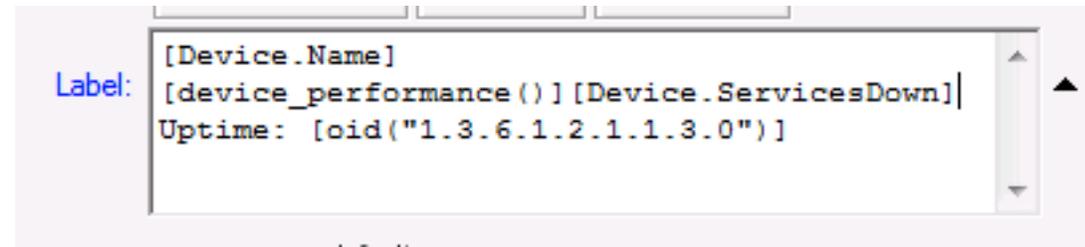
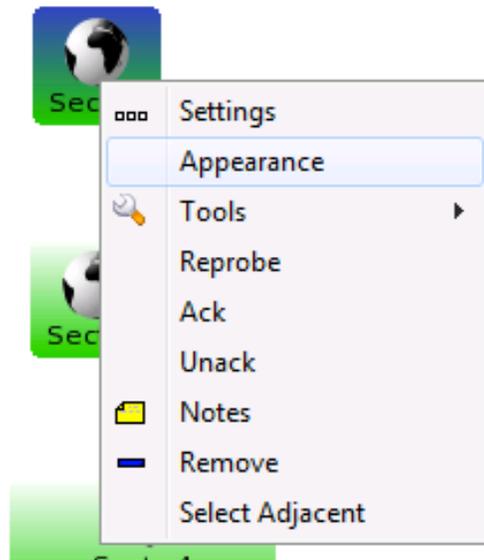
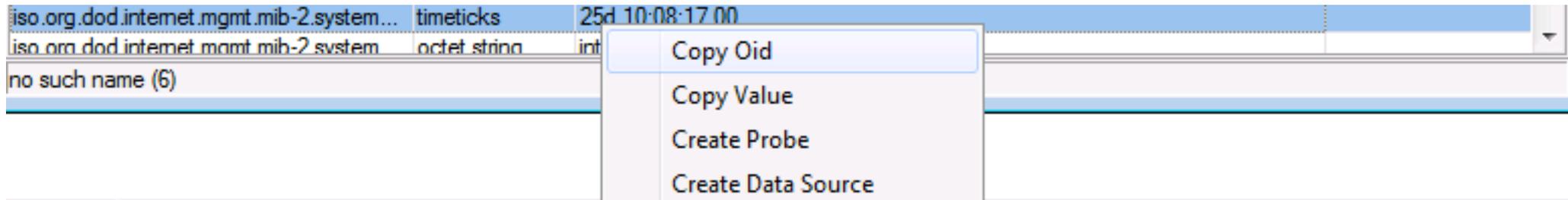
Personalizamos apariencia de dispositivos



Informamos por OIDS



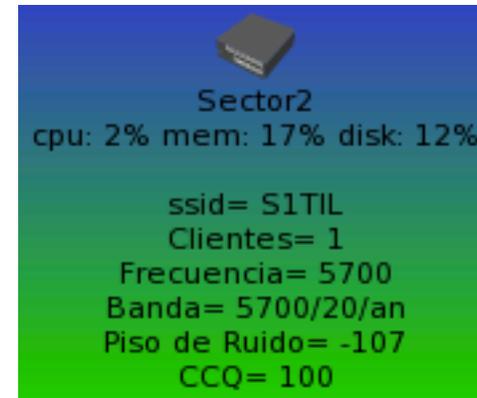
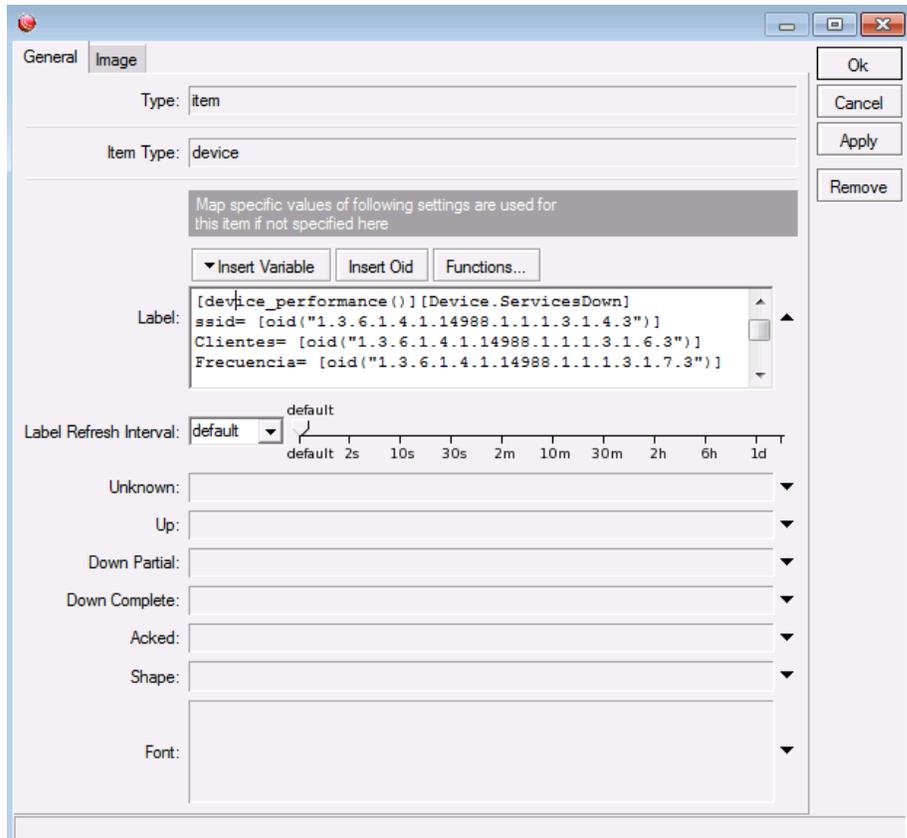
Informamos por OIDS



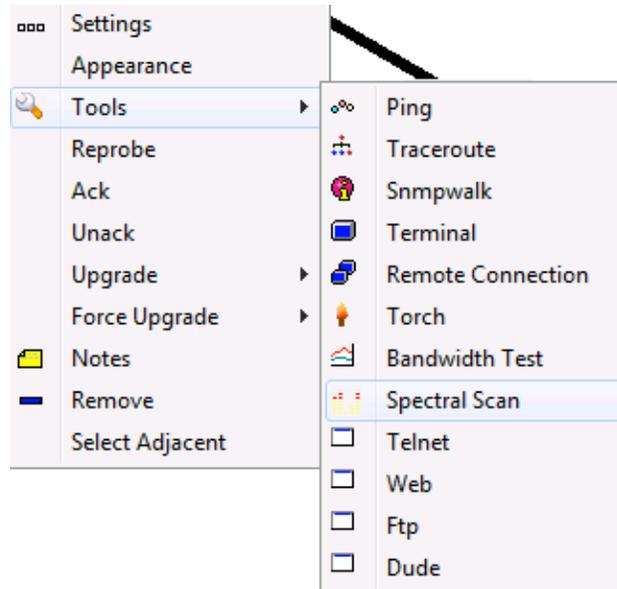
Informamos por OIDS

```
[admin@ASILO S3] > int wire
[admin@ASILO S3] /interface wireless> print oid
0 tx-rate=.1.3.6.1.4.1.14988.1.1.1.3.1.2.5
  rx-rate=.1.3.6.1.4.1.14988.1.1.1.3.1.3.5
  ssid=.1.3.6.1.4.1.14988.1.1.1.3.1.4.5  bssid=.1.3.6.1.4.1.14988.1.1.1.3.1.5.5
  client-count=.1.3.6.1.4.1.14988.1.1.1.3.1.6.5
  frequency=.1.3.6.1.4.1.14988.1.1.1.3.1.7.5
  band=.1.3.6.1.4.1.14988.1.1.1.3.1.8.5
  noise-floor=.1.3.6.1.4.1.14988.1.1.1.3.1.9.5
  overall-ccq=.1.3.6.1.4.1.14988.1.1.1.3.1.10.5
```

Informamos por OIDS

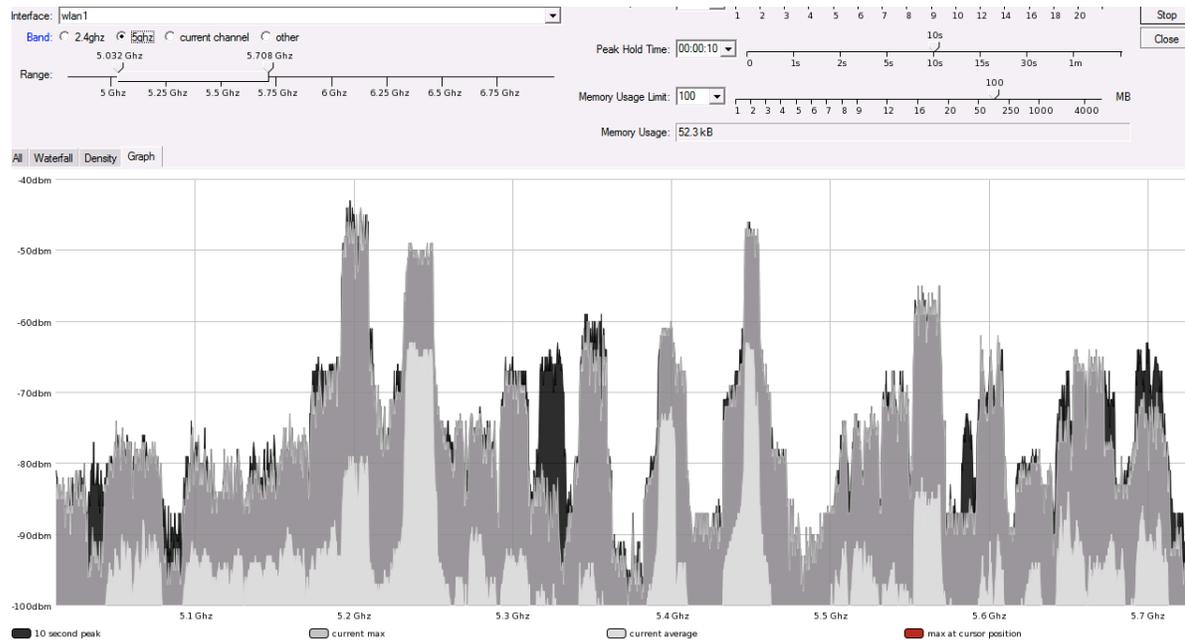


Otras herramientas (Spectral scan)

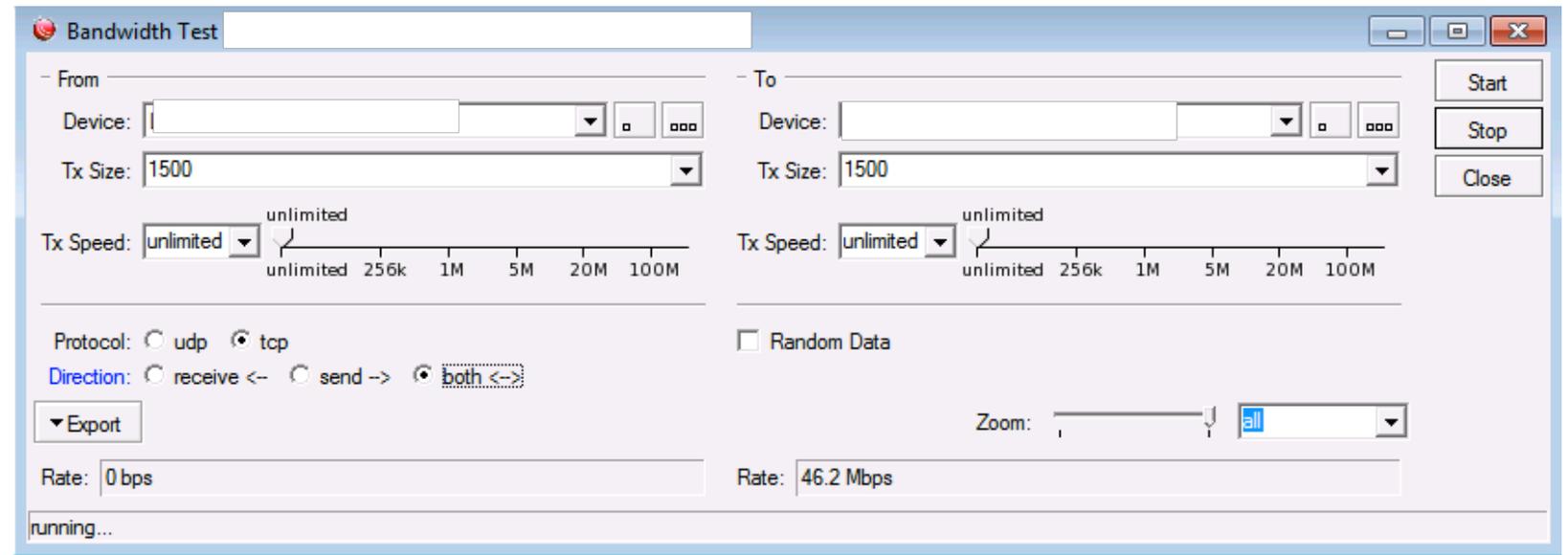
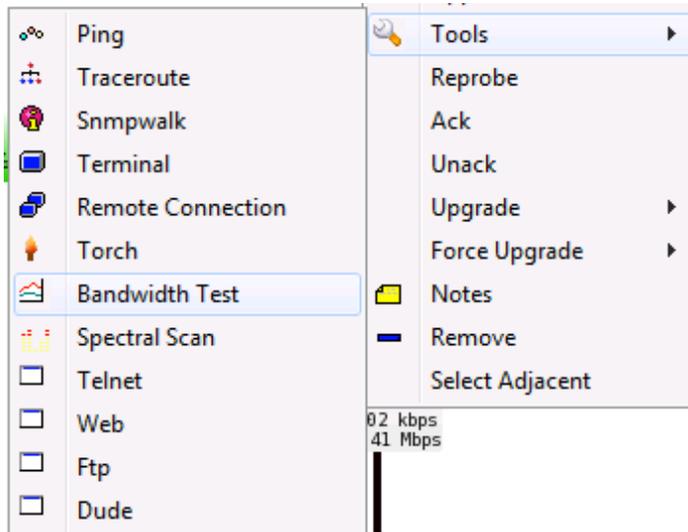


No todos los chipsets de MikroTik son soportados

Otras herramientas (Spectral scan)



Otras herramientas (Bandwidth test)



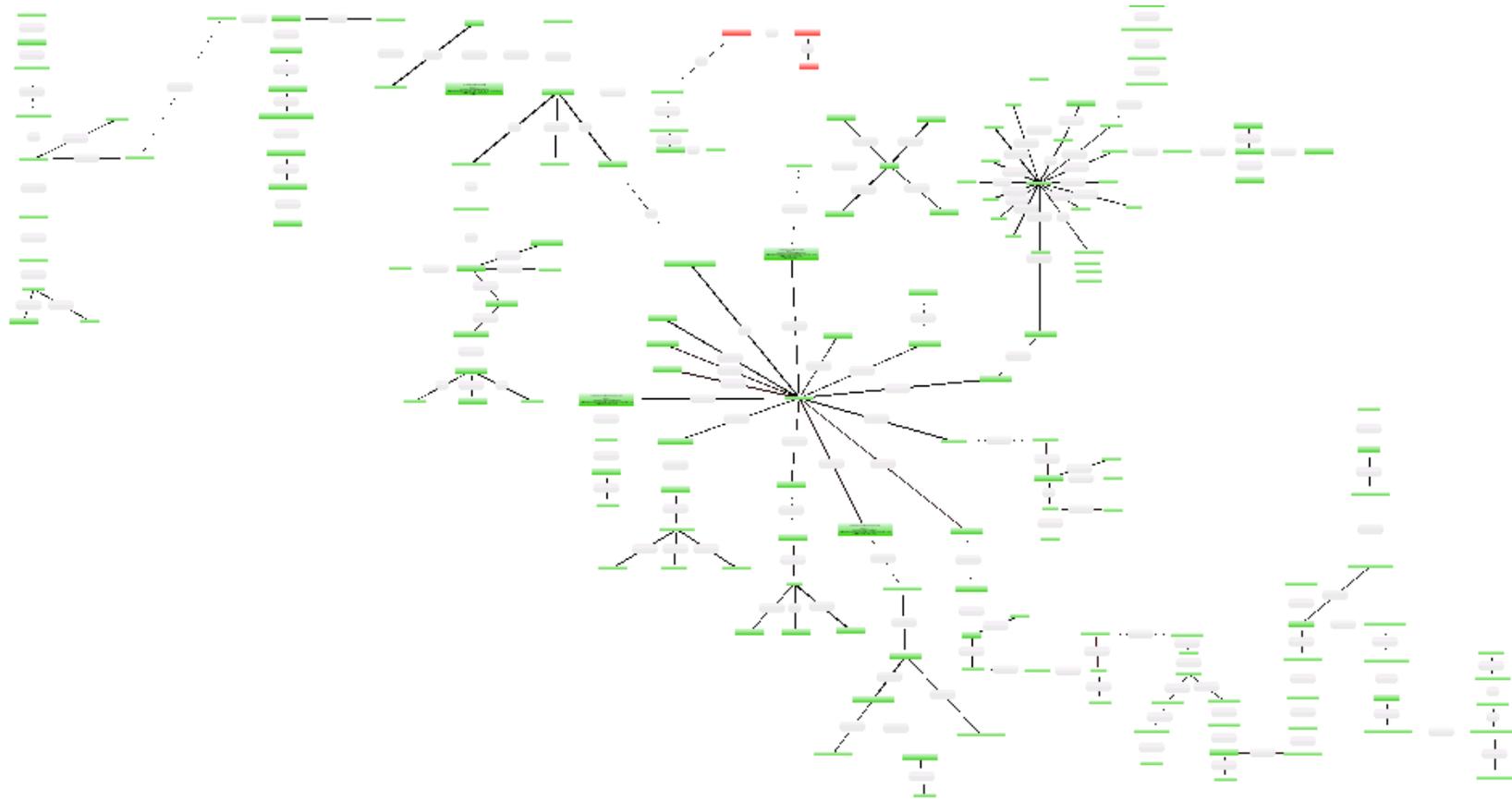
Otras herramientas (Torch)

A screenshot of a network tool menu. The 'Tools' menu is open, showing various options. 'Torch' is highlighted with a blue selection bar. Other options include Ping, Traceroute, Snmpwalk, Terminal, Remote Connection, Bandwidth Test, Spectral Scan, Telnet, Web, Ftp, and Dude. The 'Tools' sub-menu includes: Reprobe, Ack, Unack, Upgrade, Force Upgrade, Notes, Remove, and Select Adjacent.

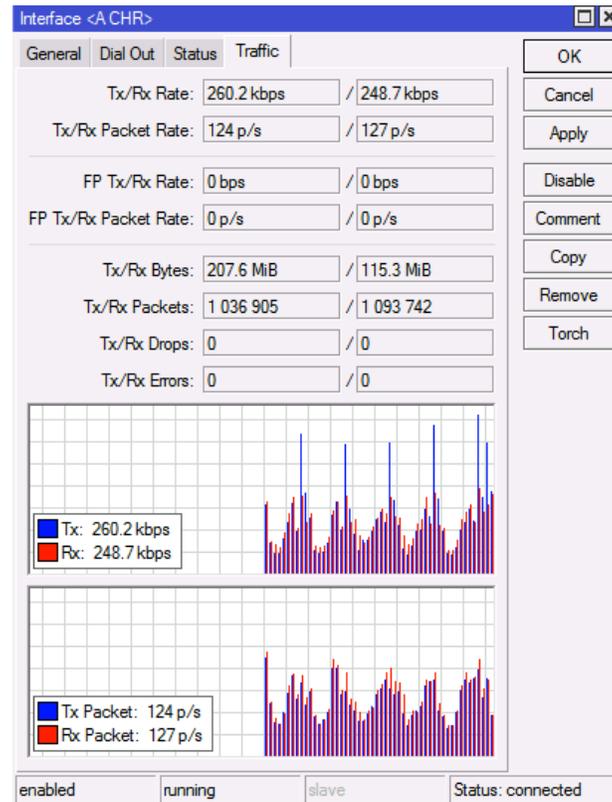
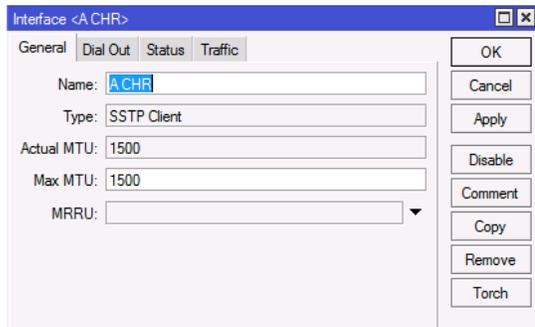
A screenshot of the Torch application interface. The 'General' tab is active, showing the interface set to 'ether1' and an average time of 00:00:10. The 'Filter' section is empty. Below the filters is a table of network traffic. The table has columns for #, Eth Proto, IP Pr..., Vlan ID, Src Address, Src Port, Dst Address, Dst Port, Dscp, Cpu, Tx Bps, Fx Bps, Tx Pps, and Fx Pps. The table contains 9 rows of data.

#	Eth Proto	IP Pr...	Vlan ID	Src Address	Src Port	Dst Address	Dst Port	Dscp	Cpu	Tx Bps	Fx Bps	Tx Pps	Fx Pps
1	ip				0		0			387 kbps	2.75 M...	204	
2	ip	tcp		46.166.139.210	http		62014			15 kbps	382 kbps	29	
3	ip	tcp		204.79.197.223	http		61999			13.4 kbps	461 kbps	26	
4	802.2				0		0			0 bps	9.73 kbps	0	
5	ip	udp		189.203.232.19	https		49681			18.3 kbps	523 kbps	28	
6	ip	tcp		10.254.253.1	43043		winbox			14.8 kbps	1.66 kbps	2	
7	ip	tcp		187.189.89.14	https		32775			30.9 kbps	786 kbps	53	
8	ip	tcp		172.16.61.31	42100		9081			0 bps	0 bps	0	
9	ip	tcp		187.190.54.18	https		39492			0 bps	0 bps	0	

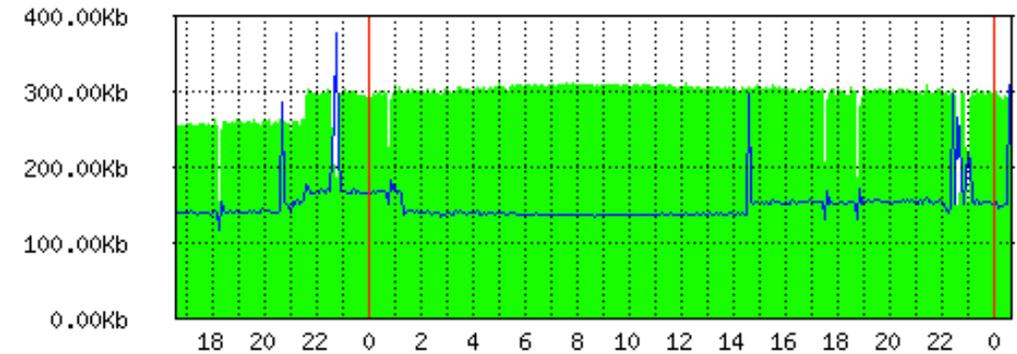
Mi dude ;)



Mi dude ;)



"Daily" Graph (5 Minute Average)



Saludos banda!
Whatsapp Wisp México
Whatsapp Wisp Oaxaca

Gracias

