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

INTEGRA
Redes y telecomunicaciones

GPON
Grupo de Profesionales Operadores de Networking S.C.

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 incluída 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 mejor drásticamente la forma de administrar el entorno de red. Escanea automáticamente todos los dispositivos dentro de subredes especificadas, dibuja y distribuye un mada 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 server

…. 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 syestem) 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:

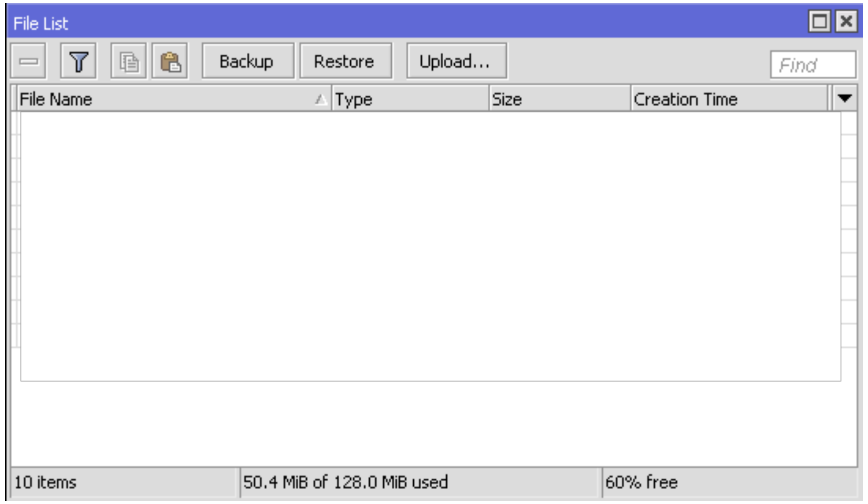
www.digitalocean.com

Script para montar el MikroTik:

https://www.digitalocean.com/community/questions/installing-mikrotik-routeros

Instalando:

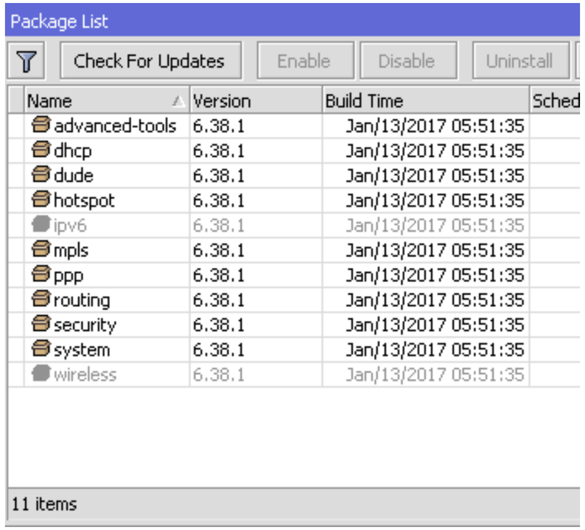
- Copiar el archivo .npk a nuestro equipo en files.



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

Instalando:

Verificamos:


Package List

Check For Updates | Enable | Disable | Uninstall

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	

11 items

- Accedemos a winbox y habilitamos dude:

dude set enabled=yes

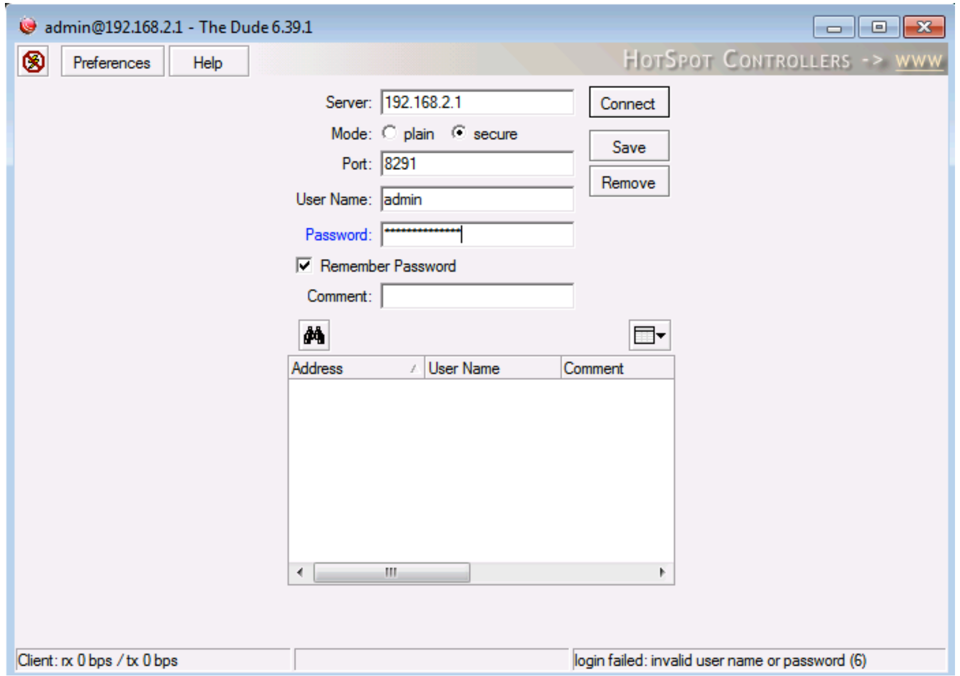
Instalando:

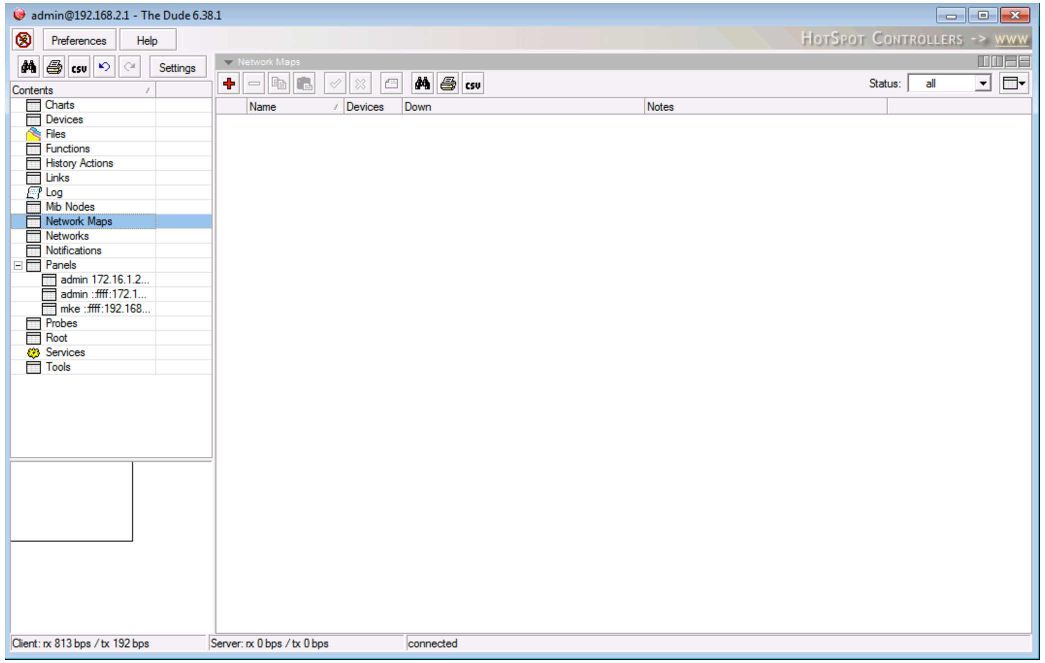
Descargamos el cliente desde la misma ubicación, sólo cliente windows:

https://mikrotik.com/download

Configuración inicial

Primer login:

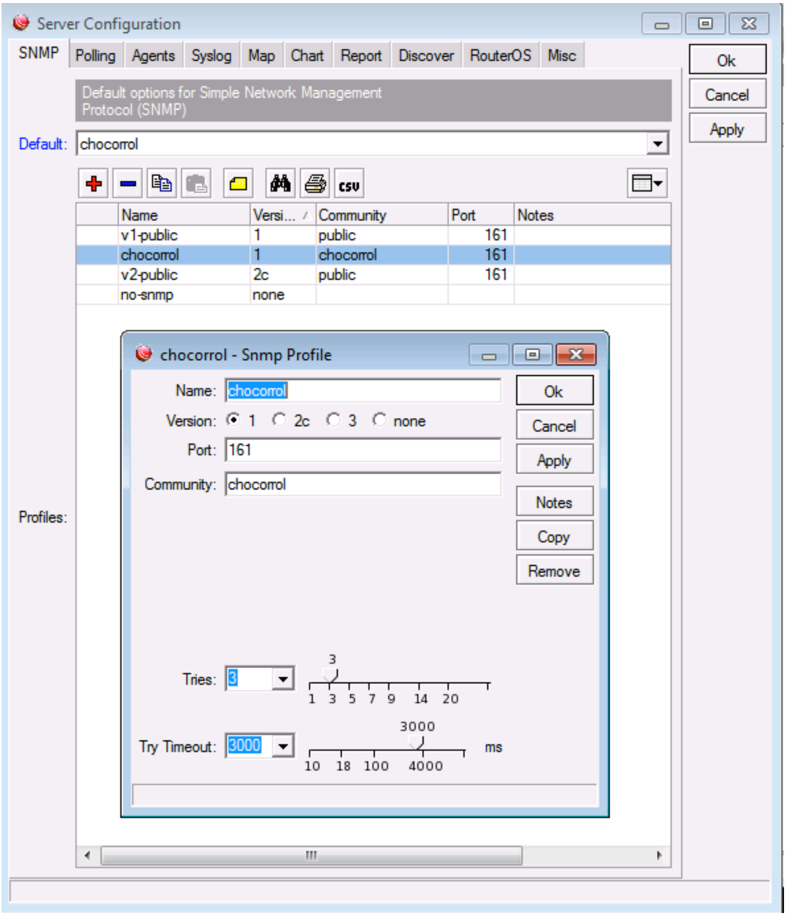




Configuración inicial

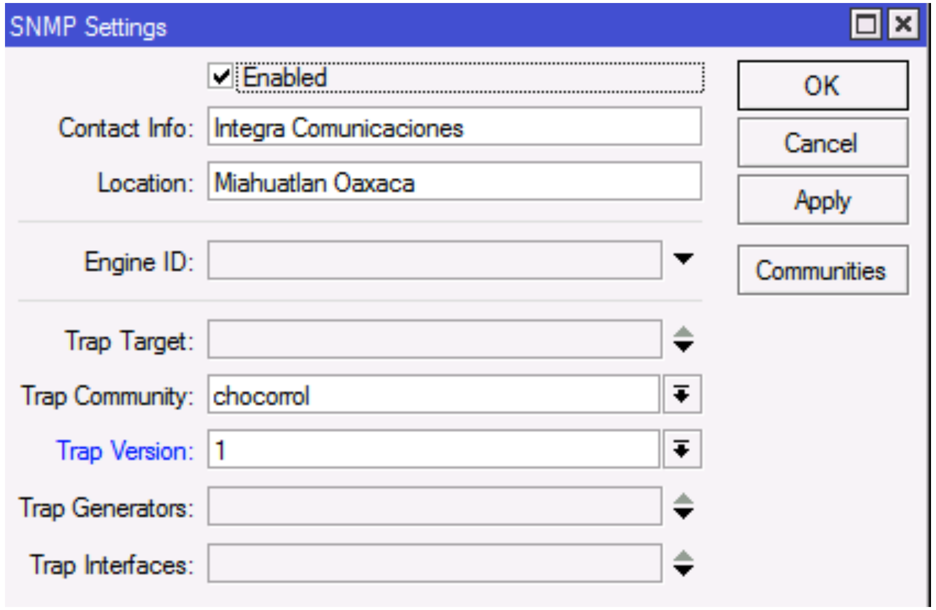
Tip: Antes de realizar un descubrimiento de equipos difinamos la comunidad de snmp por default. Marcas como Ubiquiti, Deliberant, TP-Link sólo permite SNMPv1 así que seamos ocurrentes en el nombre de la misma para darle un poco mas de “seguridad”.

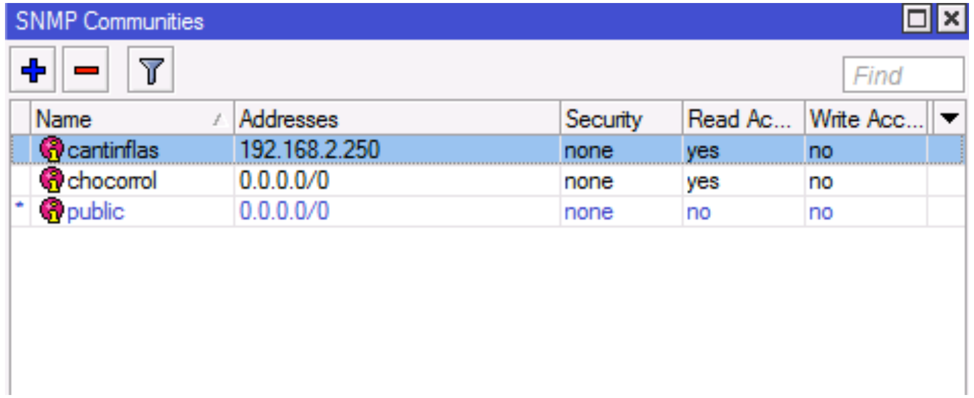
Definamos igualmente desde qué IP (Agente NMS) puede ser consultado



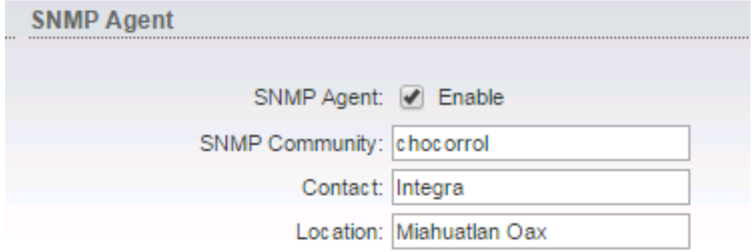
Configuración inicial

IP- SNMP

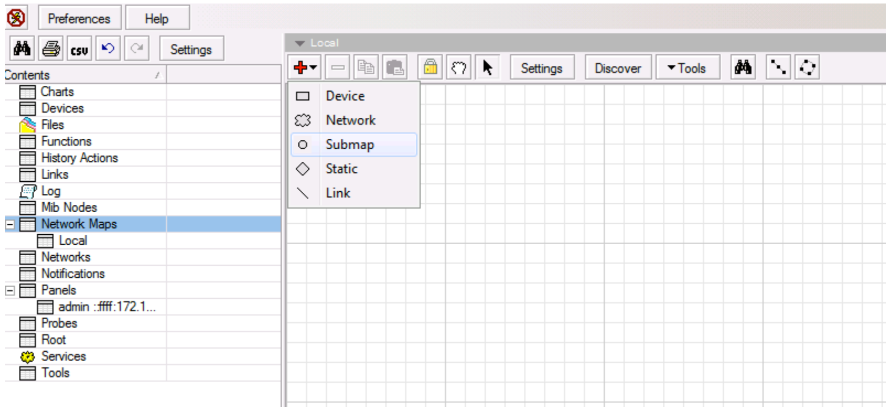


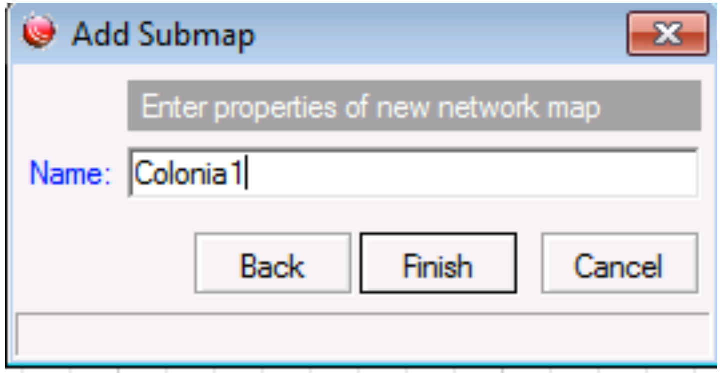


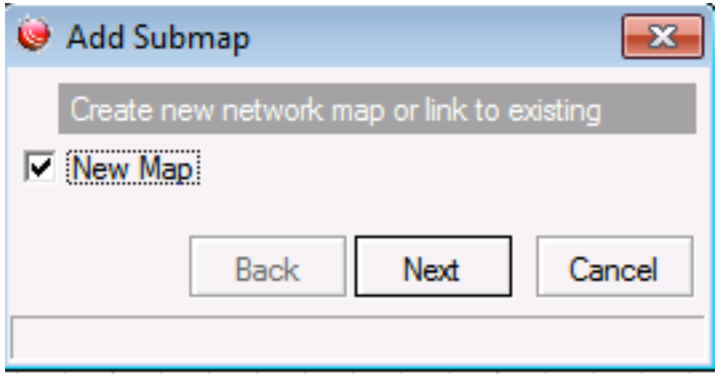
Ubiquiti:
Pestaña services (sólo V1)

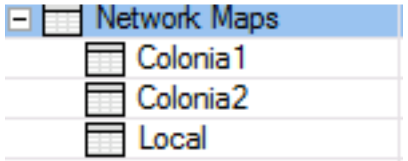


Definimos submapas “colonias”

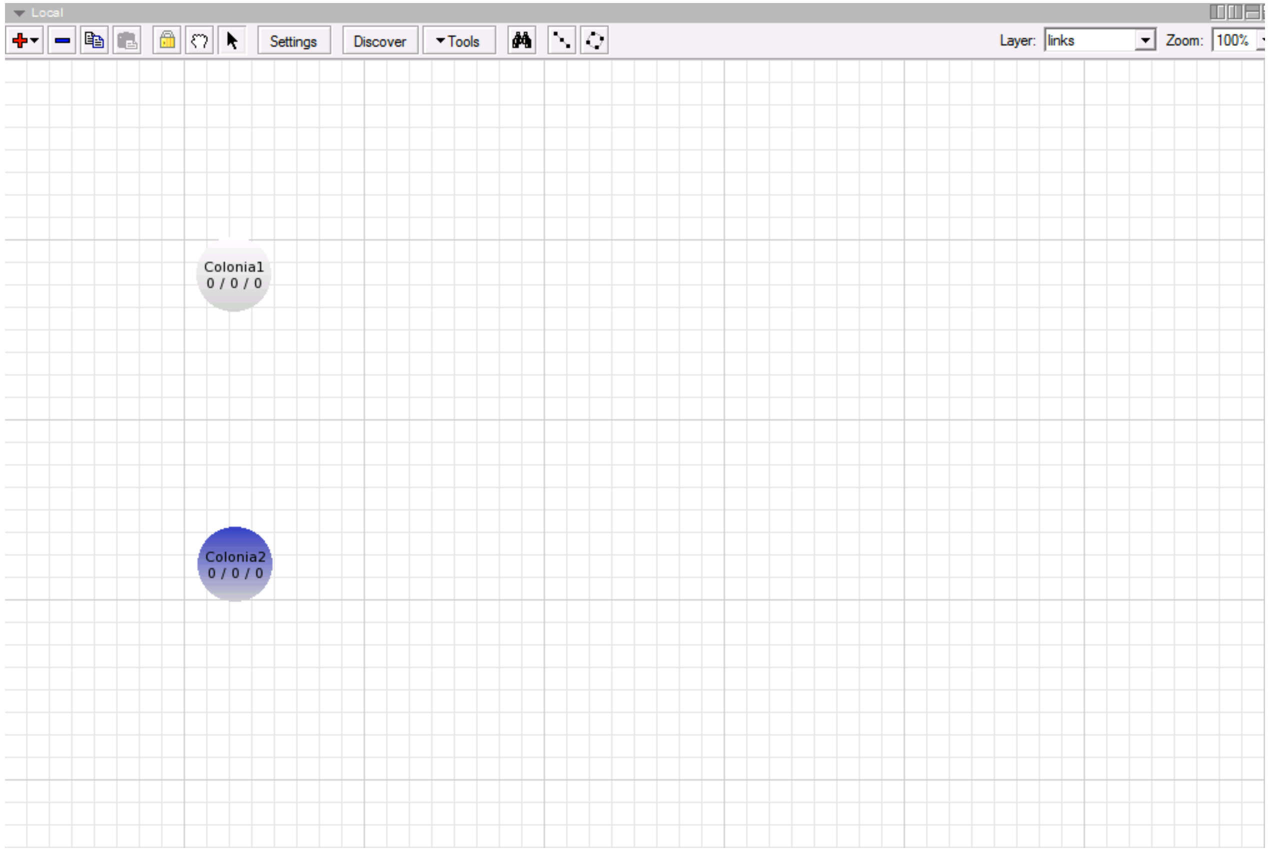




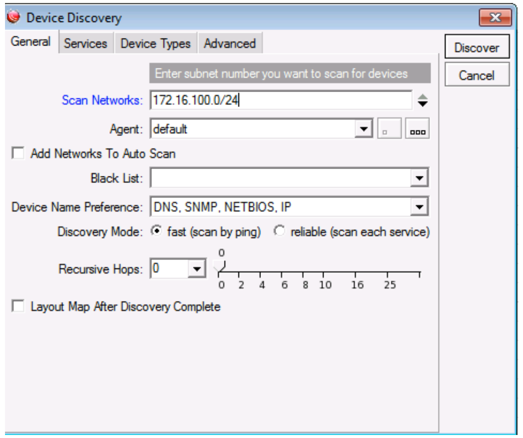


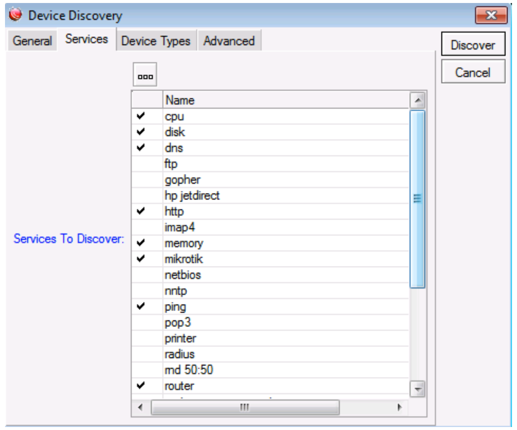


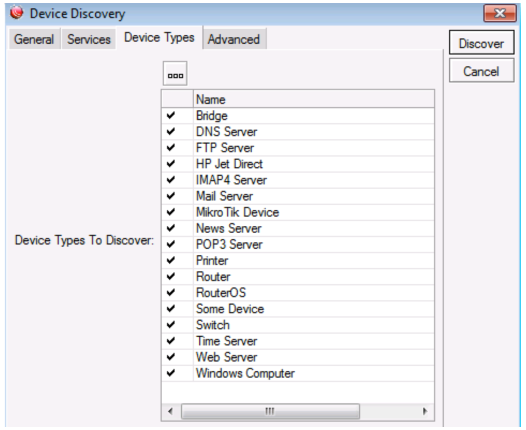
Definimos submapas “colonias”

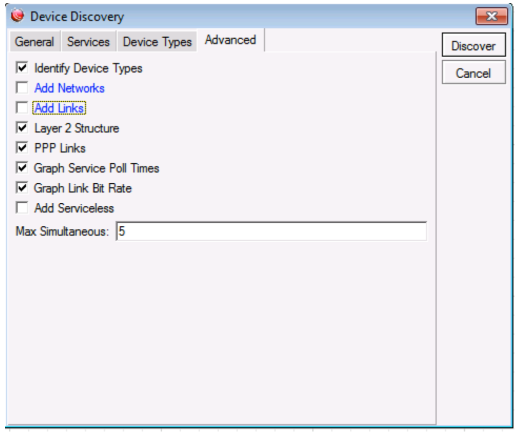


Descubriendo dispositivos

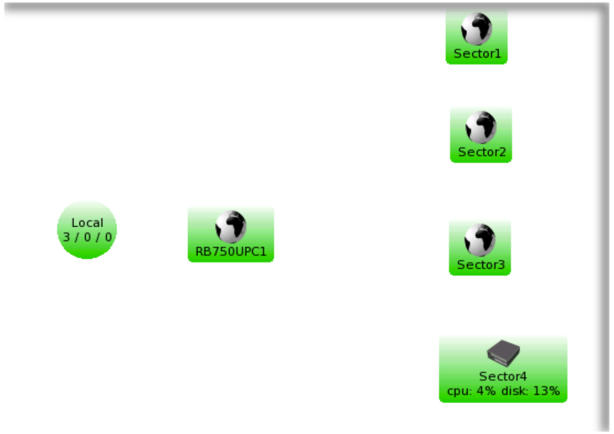


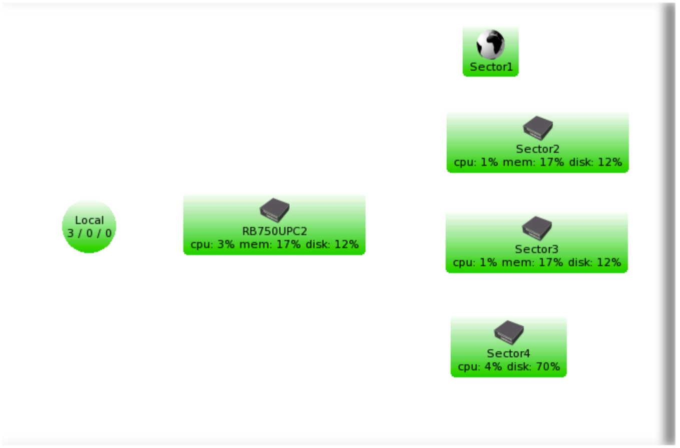






Descubriendo dispositivos

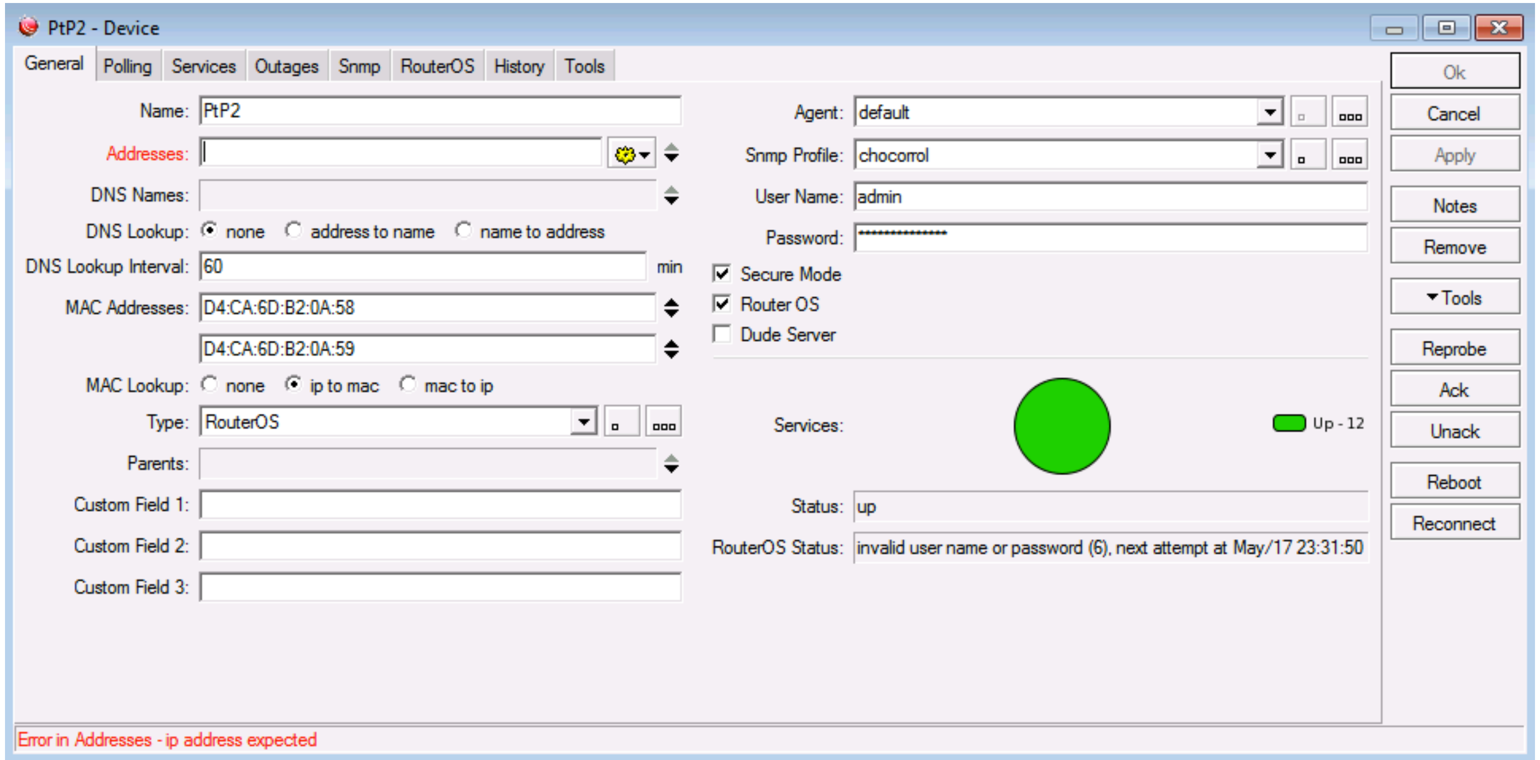


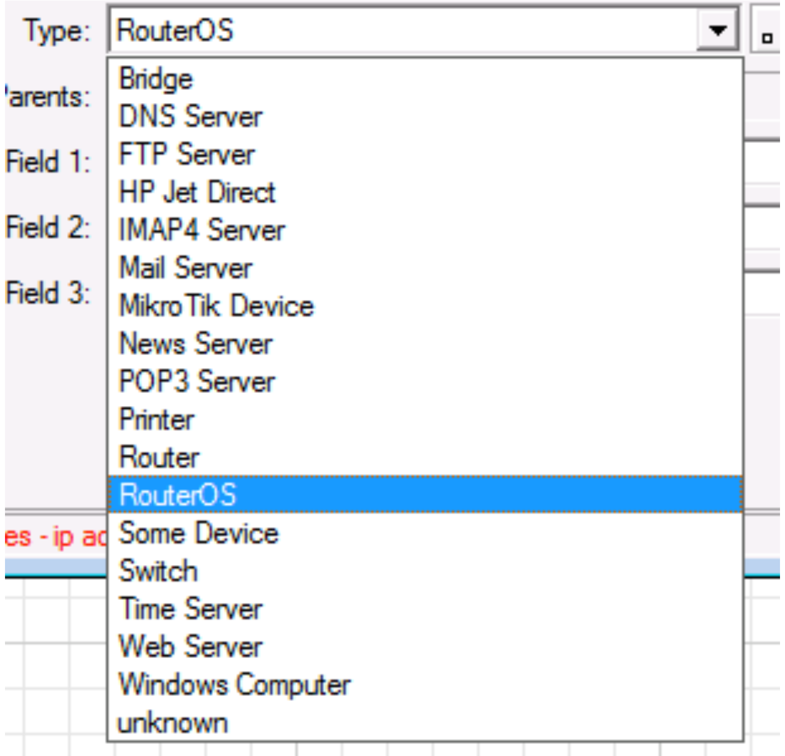


Tenemos un mapa principal y 2 submapas

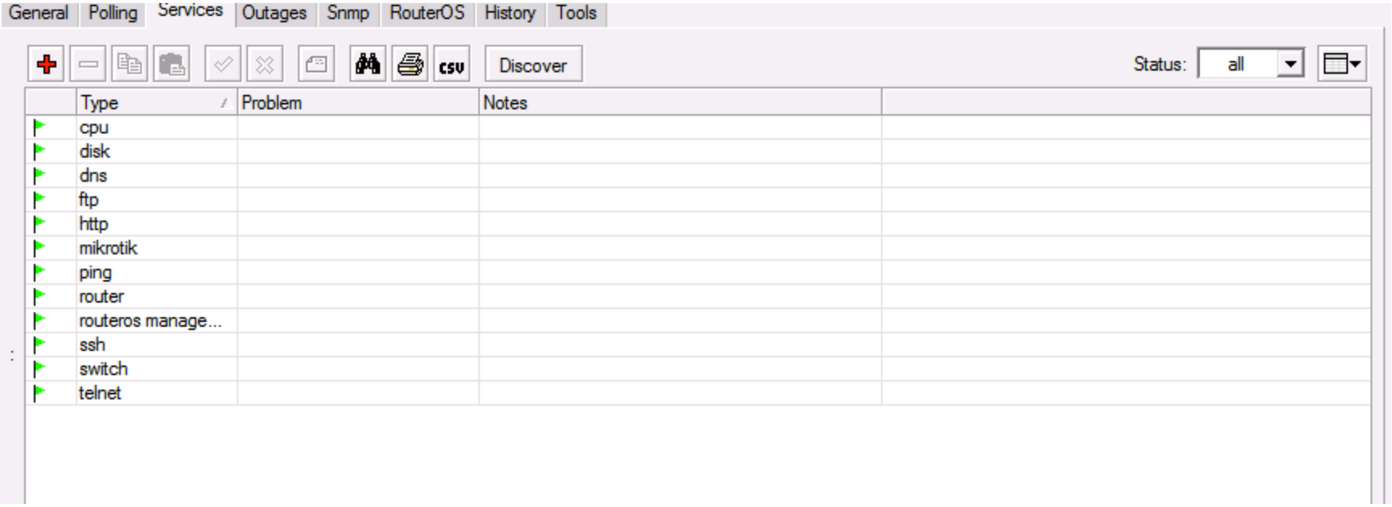
Descubriendo dispositivos

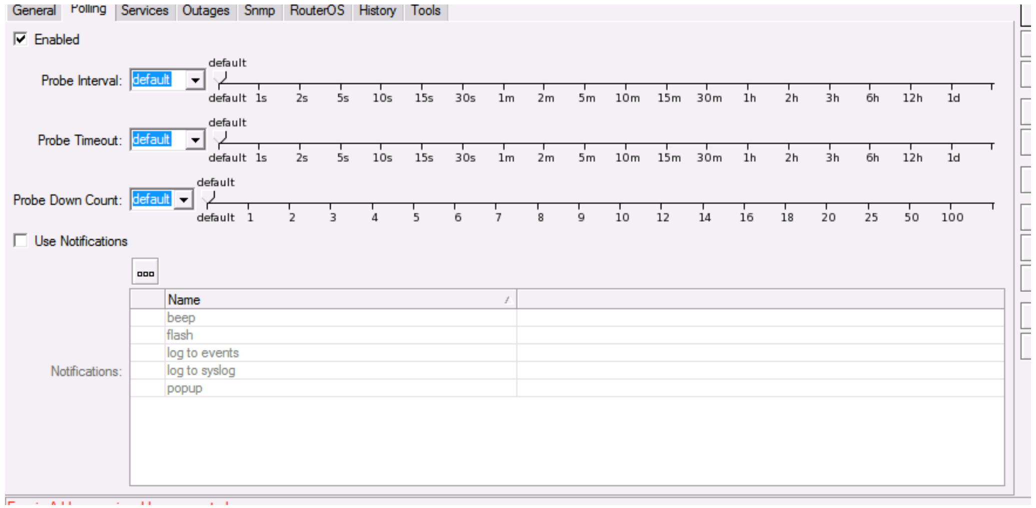
Opciones


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: chocorrol
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
Field 1:
Field 2:
Field 3:
Bridge
DNS Server
FTP Server
HP Jet Direct
IMAP4 Server
Mail Server
MikroTik Device
News Server
POP3 Server
Printer
Router
RouterOS
Some Device
Switch
Time Server
Web Server
Windows Computer
unknown

Opciones





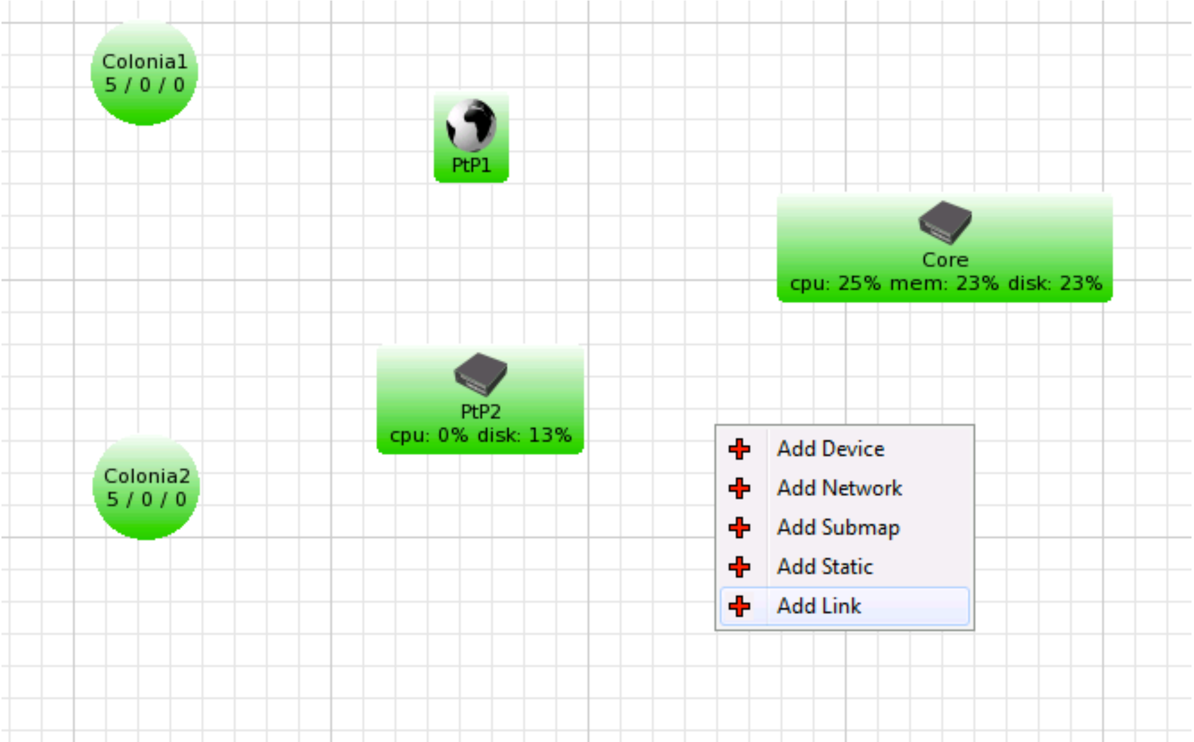
Probe interval: Cada cuánto deben ser encuestados los servicios (segundos)

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

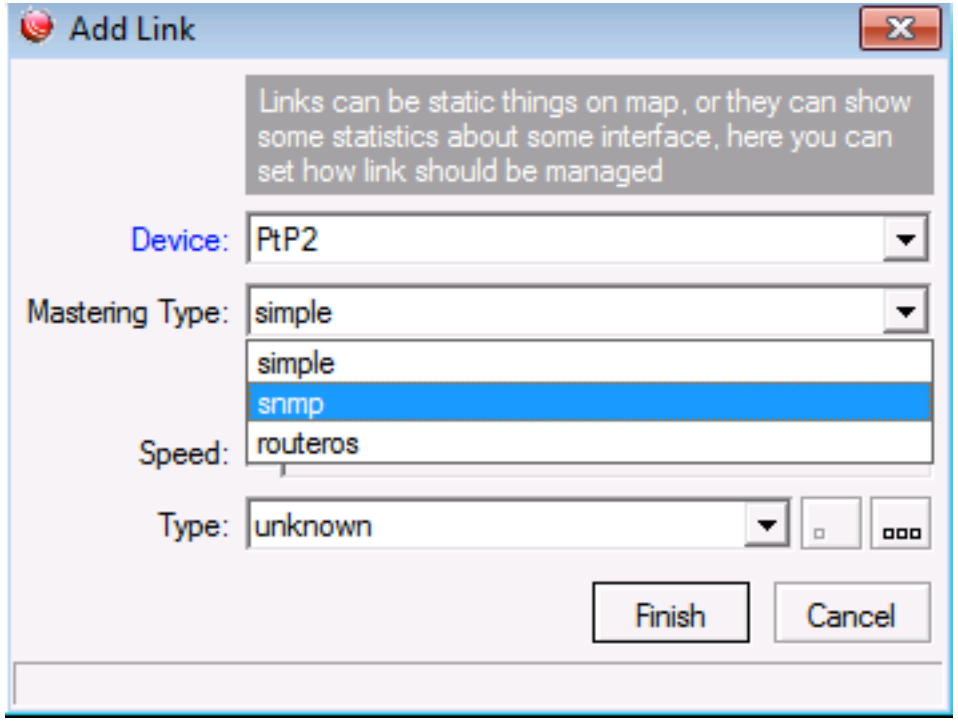
Probe down count: Cuántas veces debe fallar la ecuesta para que se considere abajo. El dispositivo se vuelve naranja pero el servicio individual pasa a rojo.

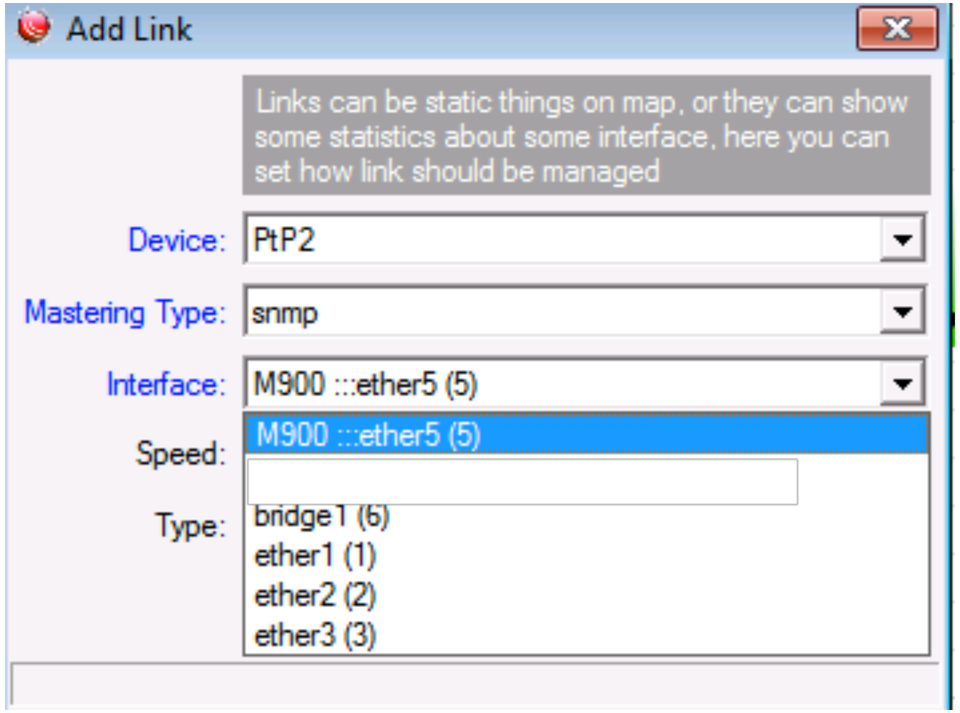
Añadimos links

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.

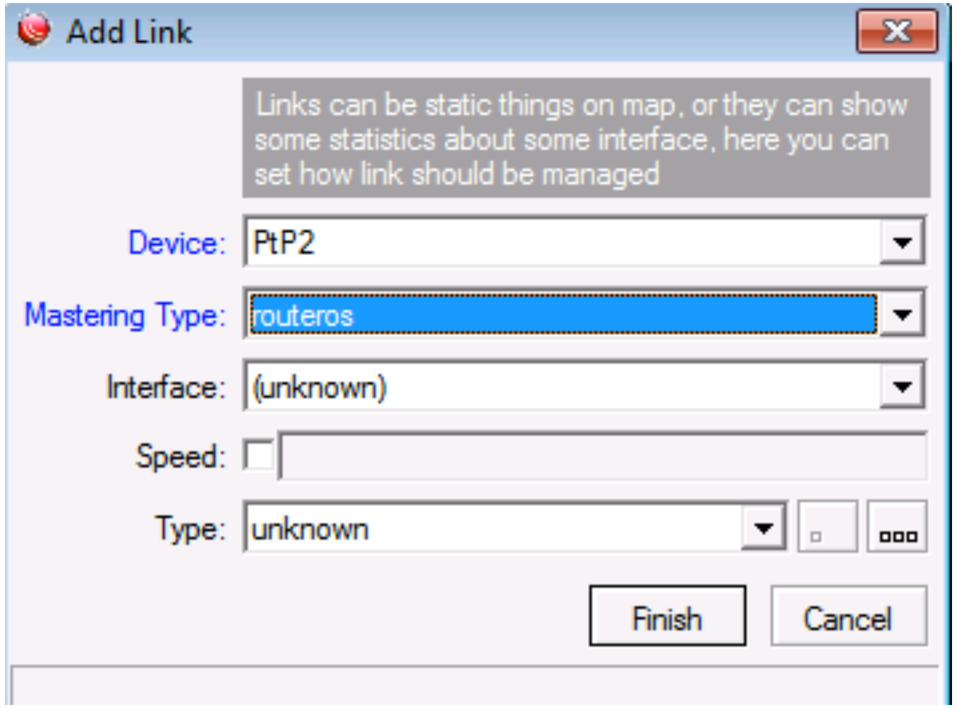


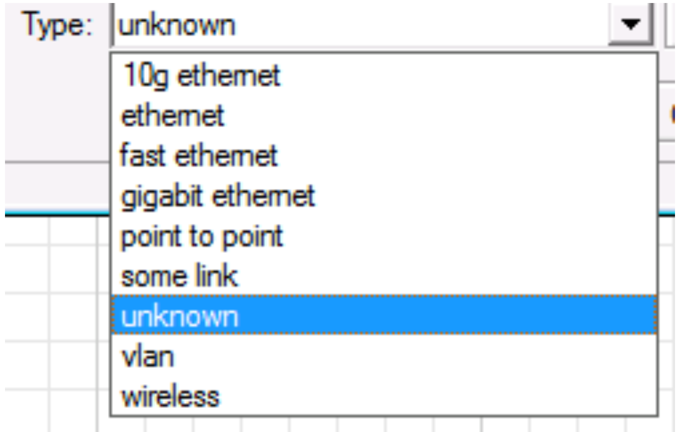
Añadimos links

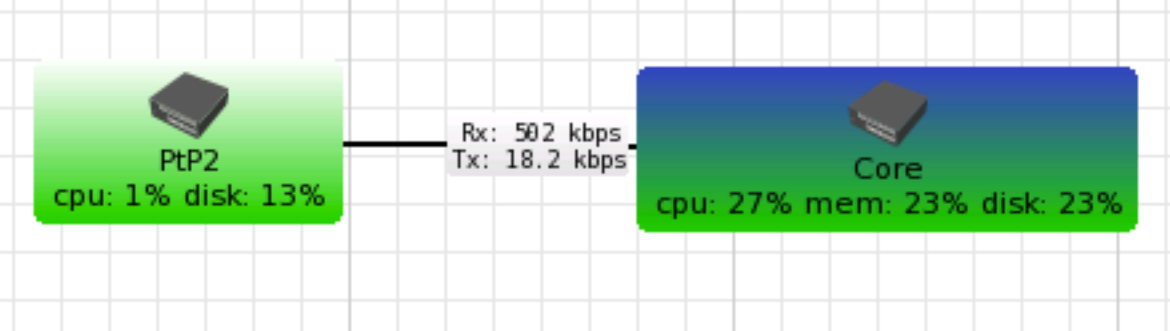




Añadimos links

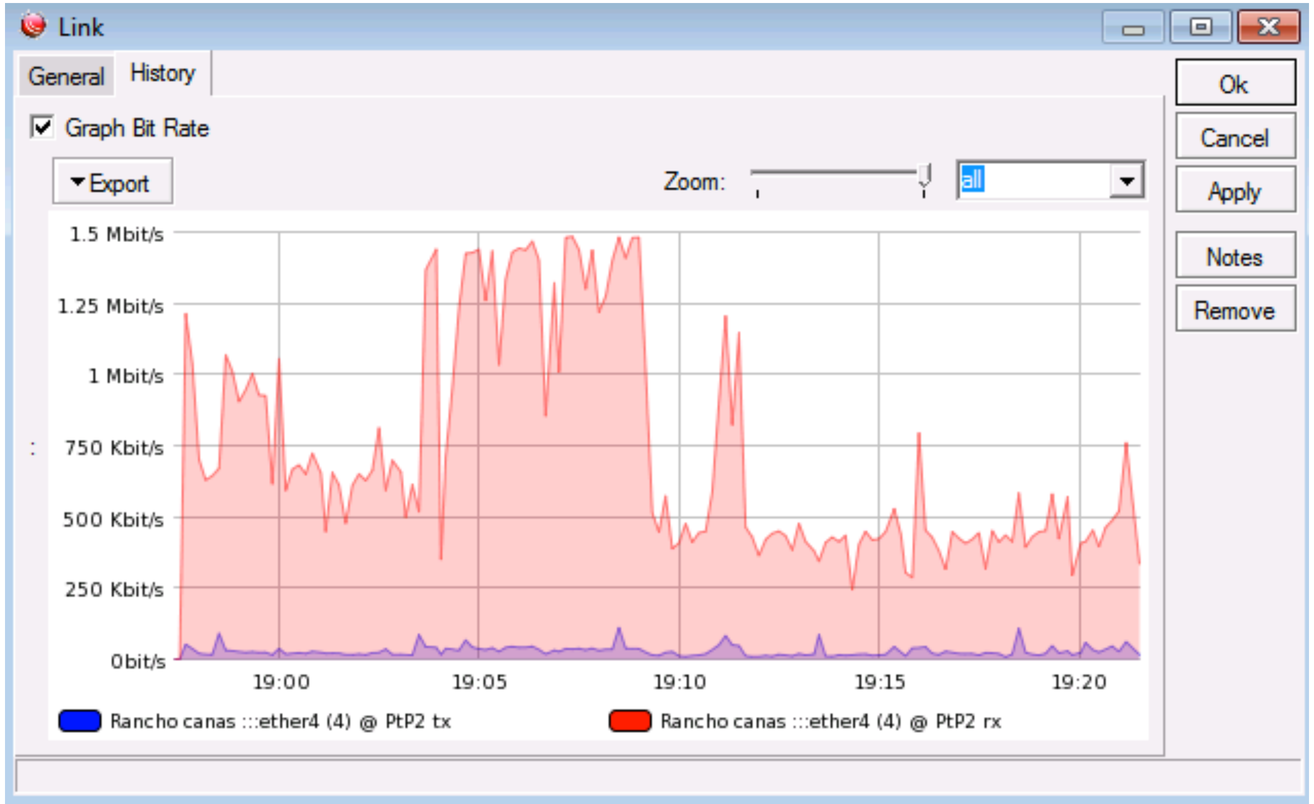




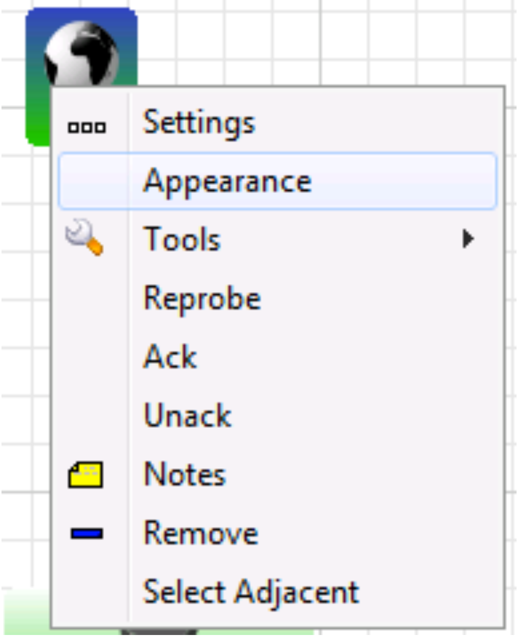


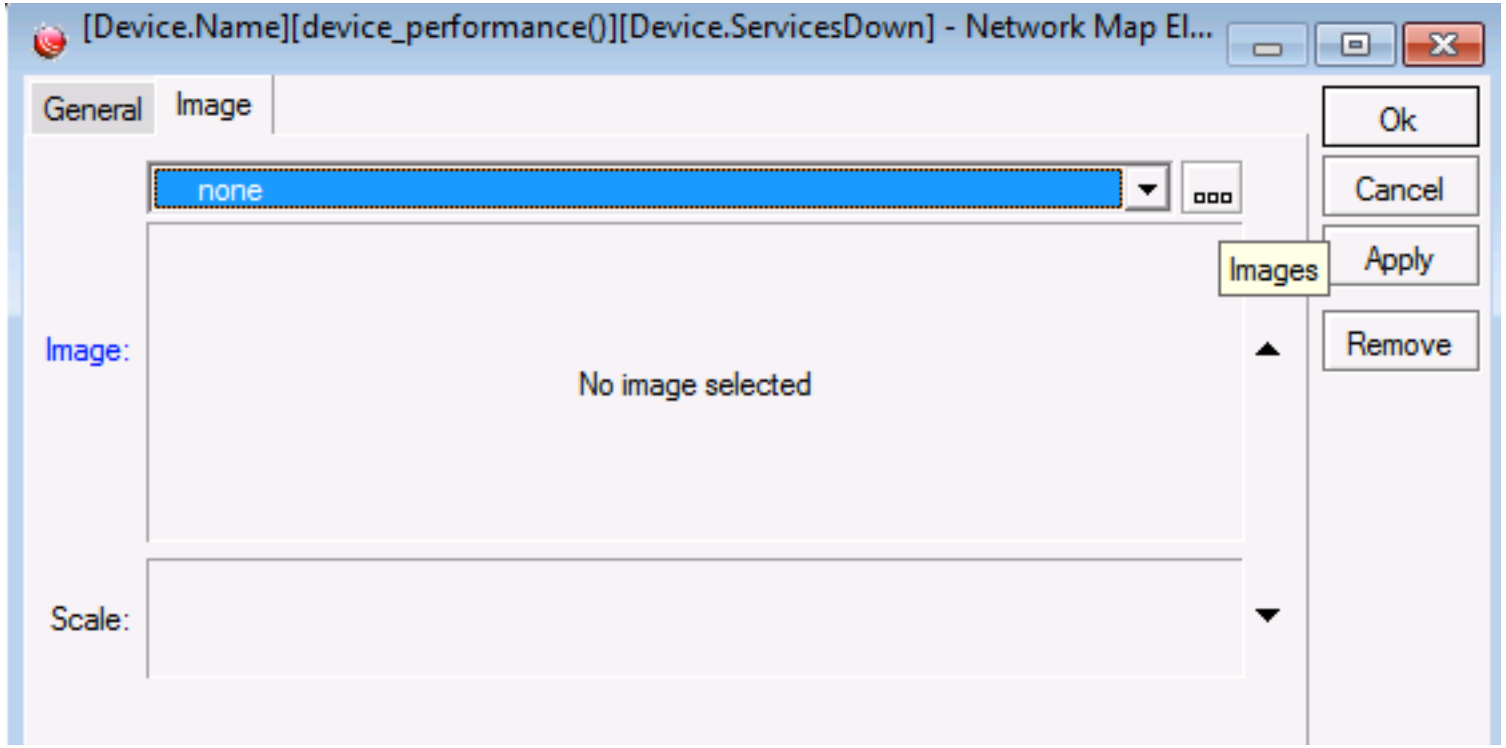
No lista nada, no es un dispositivo MikroTik

Añadimos links

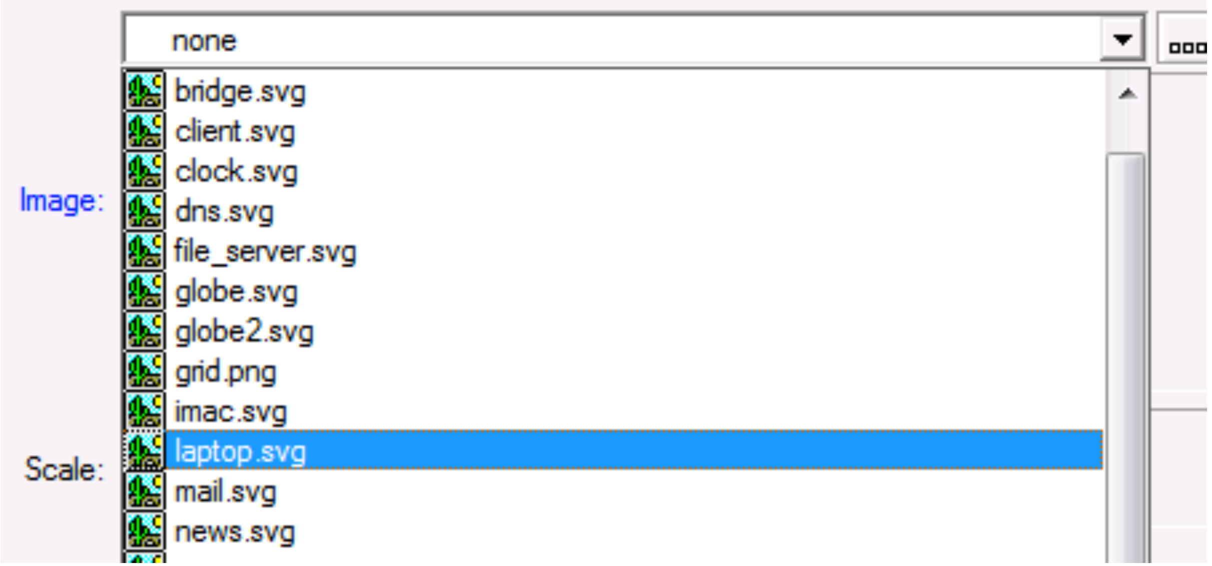


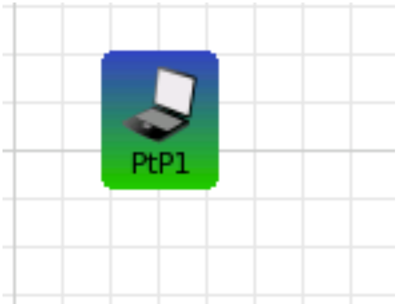
Personalizamos apariencia de dispositivos



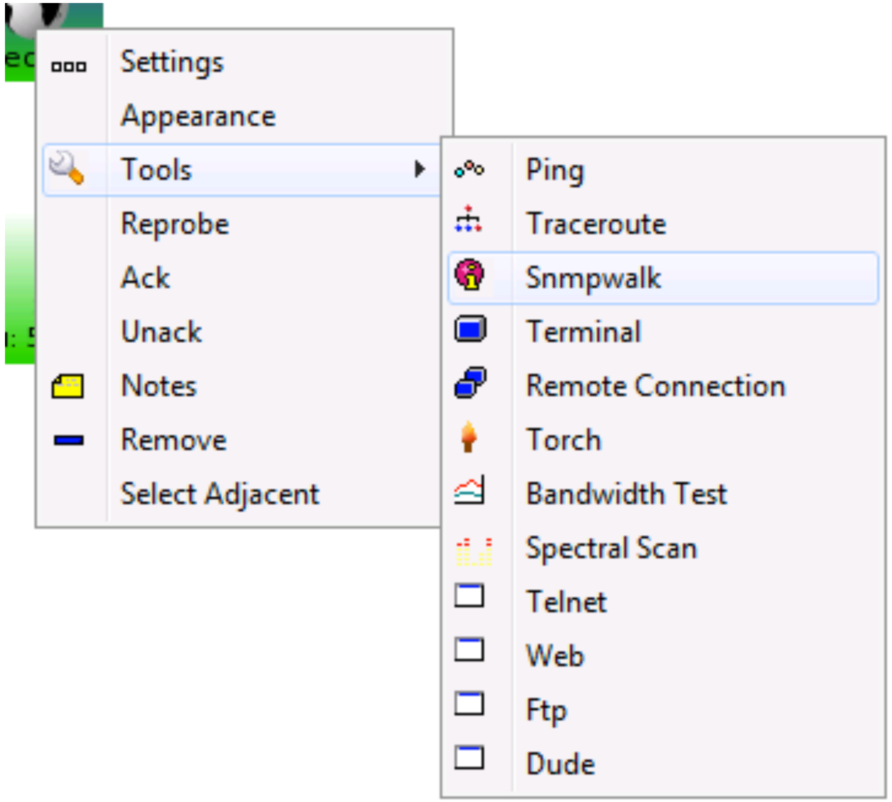


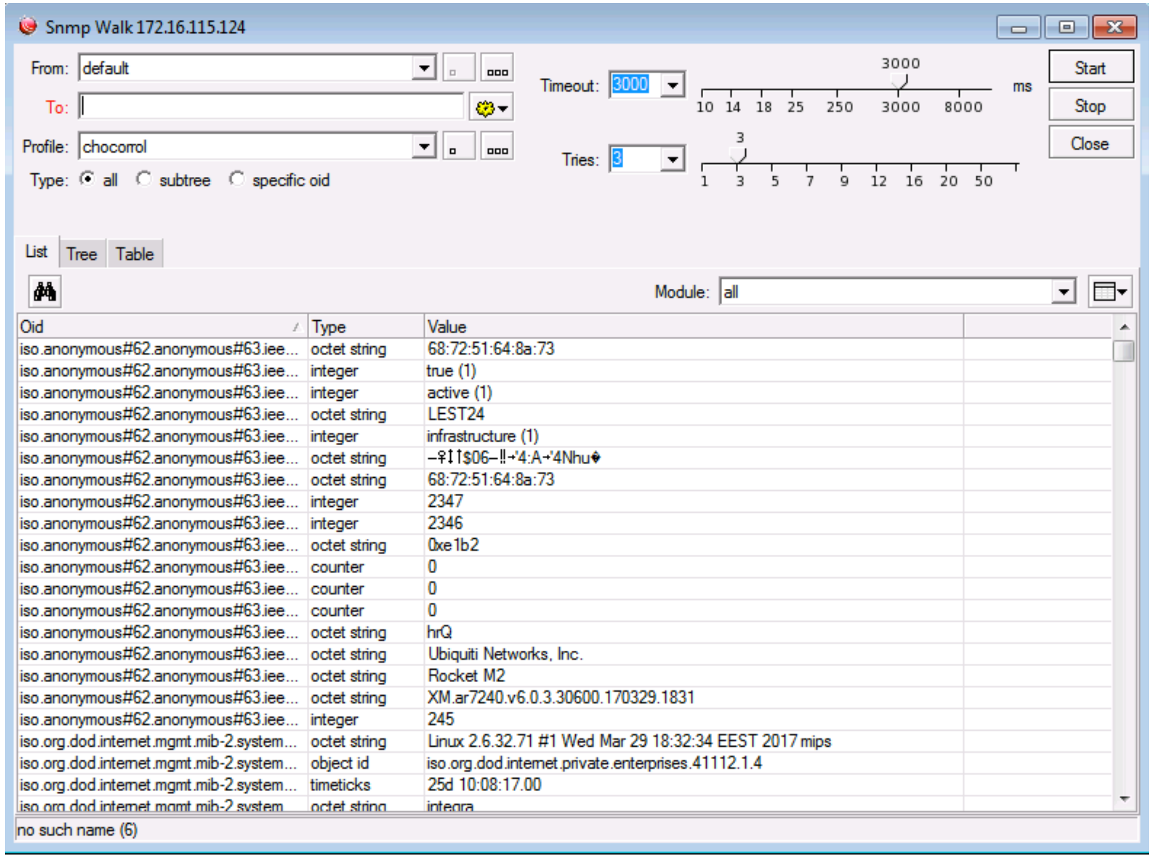
Personalizamos apariencia de dispositivos



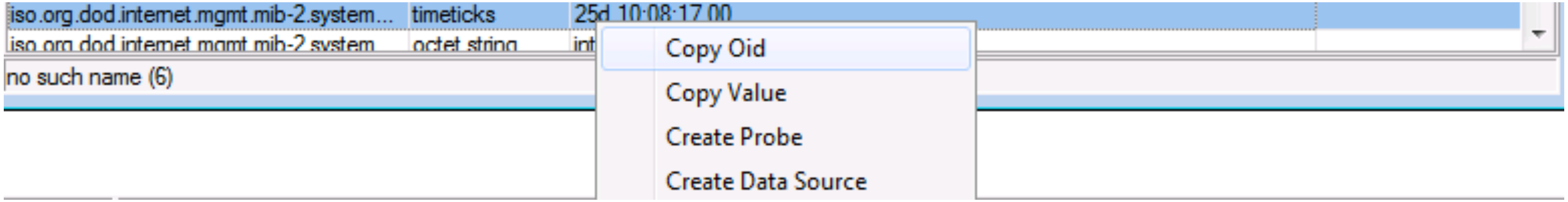


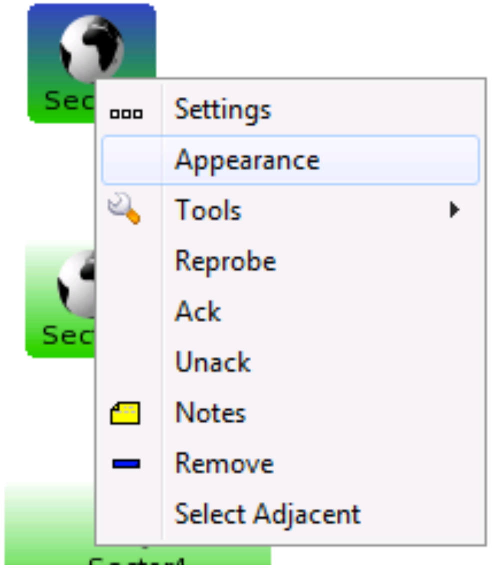
Informamos por OIDS

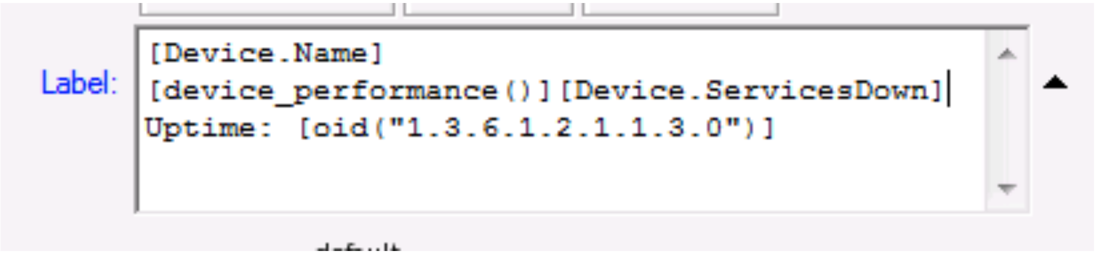




Informamos por OIDS



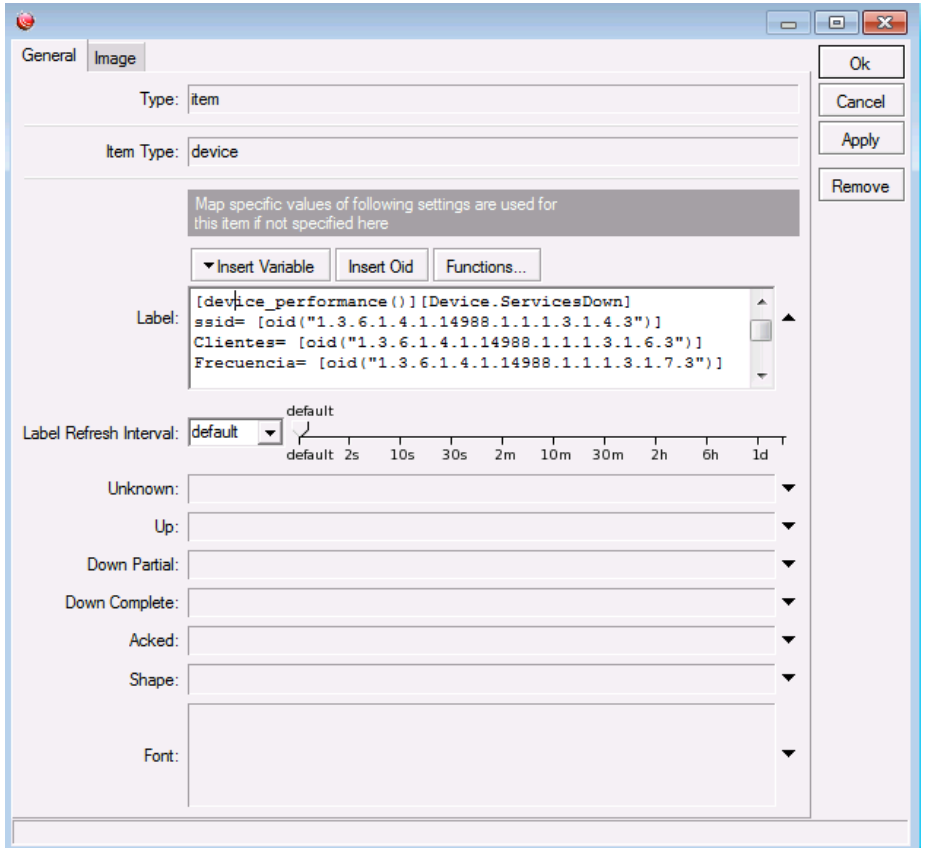


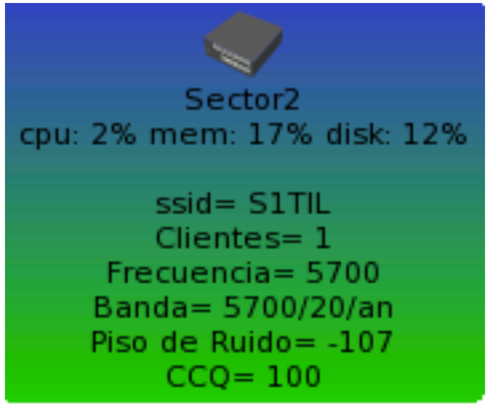


Informamos por OIDS

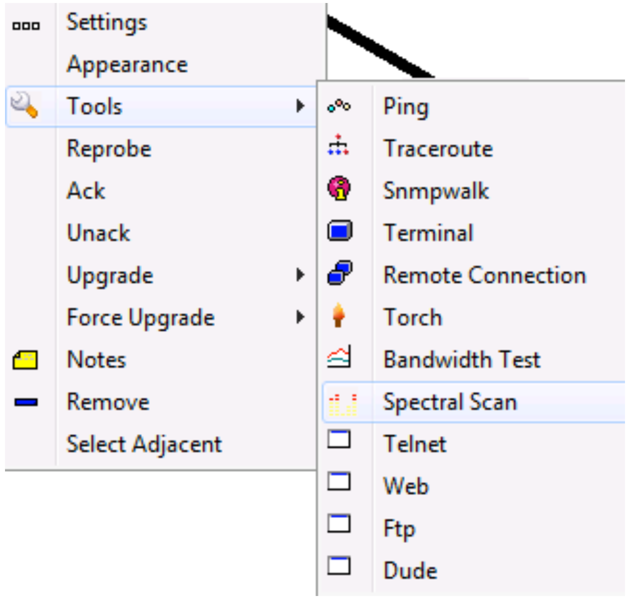
```
[admin@ASILO S3] > int wire
[admin@ASILO S3] /interface wireless> print oid
 0 tx-rate=.1.3.6.1.4.1.14988.1.1.1.3.1.2.5
   rx-rate=.1.3.6.1.4.1.14988.1.1.1.3.1.3.5
   ssid=.1.3.6.1.4.1.14988.1.1.1.3.1.4.5 bssid=.1.3.6.1.4.1.14988.1.1.1.3.1.5.5
   client-count=.1.3.6.1.4.1.14988.1.1.1.3.1.6.5
   frequency=.1.3.6.1.4.1.14988.1.1.1.3.1.7.5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



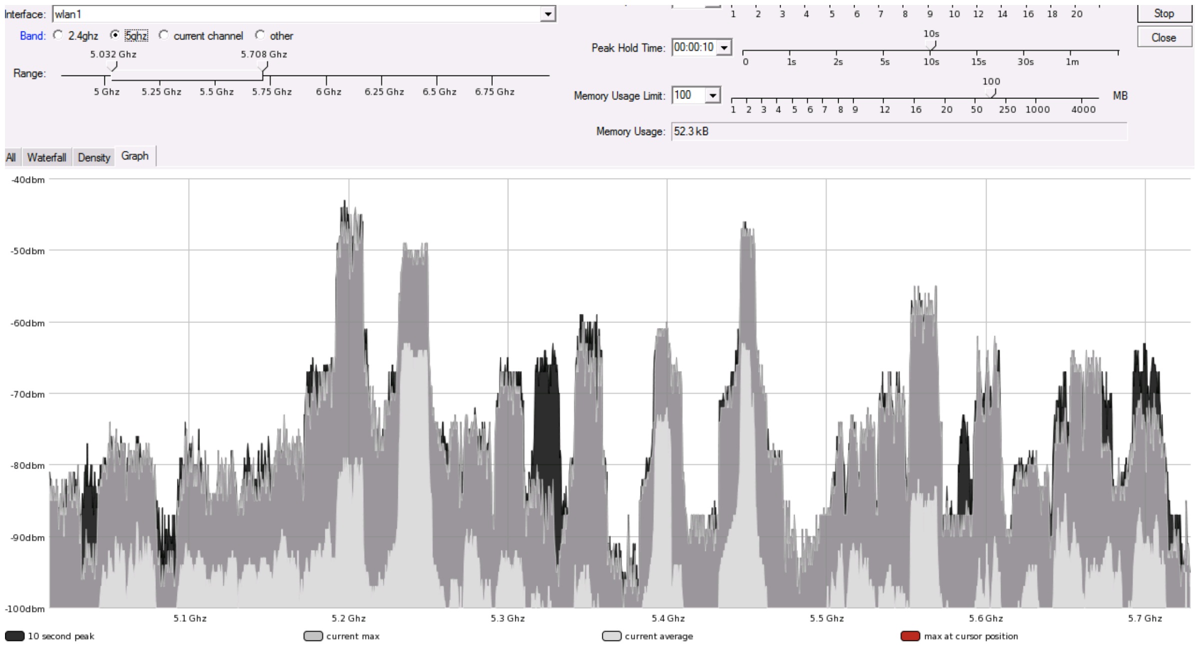


Otras herramientas (Spectral scan)

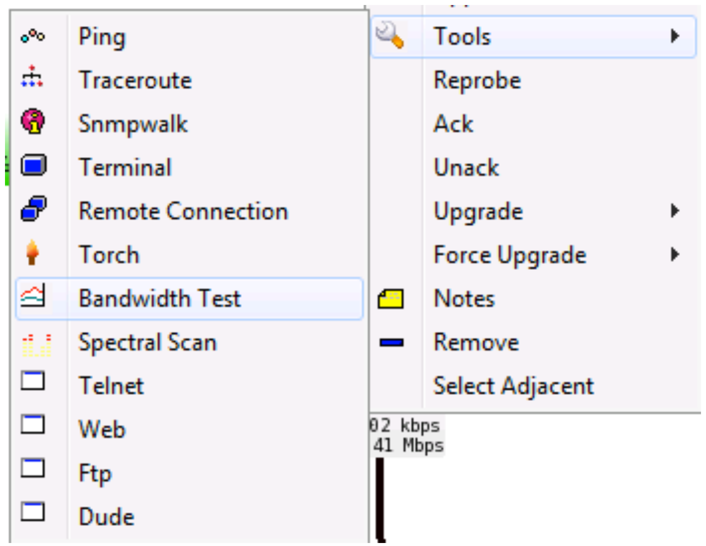


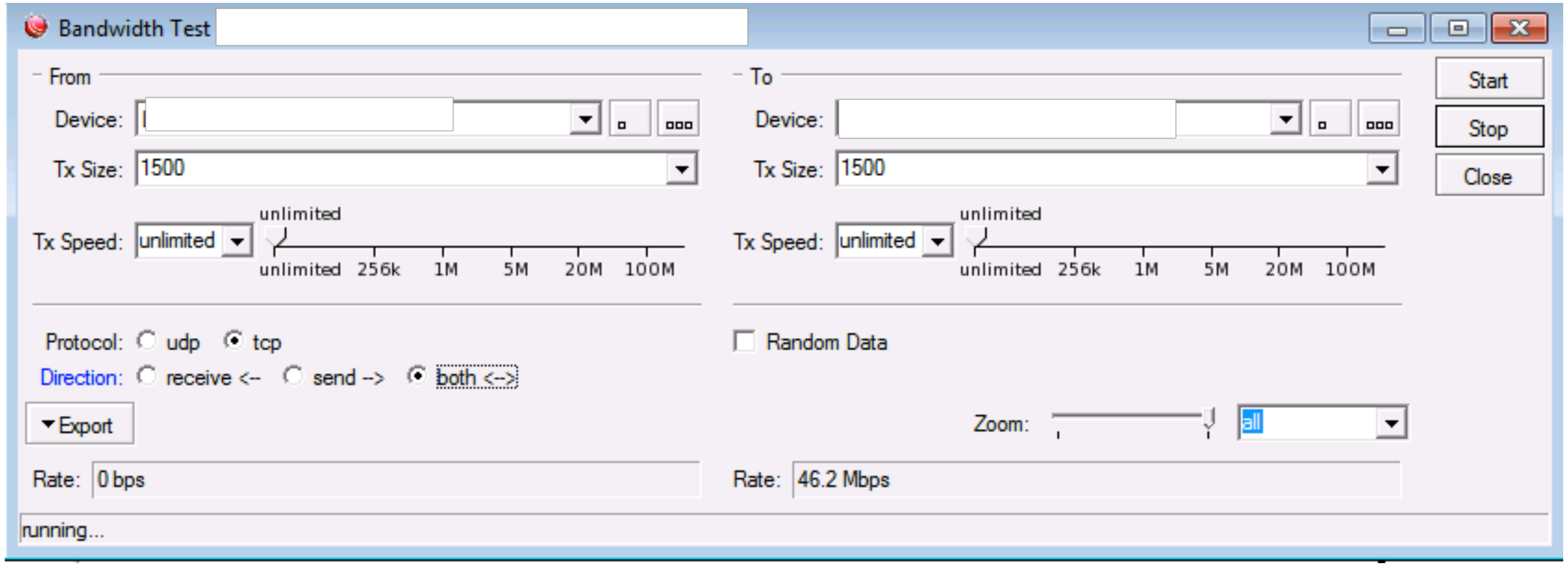
No todos los chipsets de MikroTik son soportados

Otras herramientas (Spectral scan)

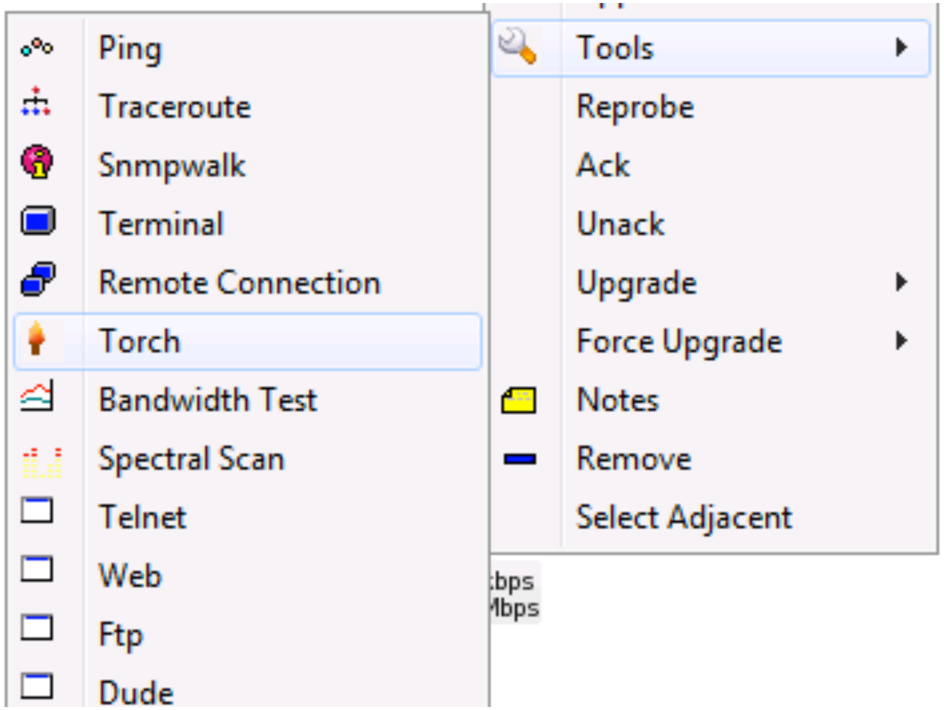


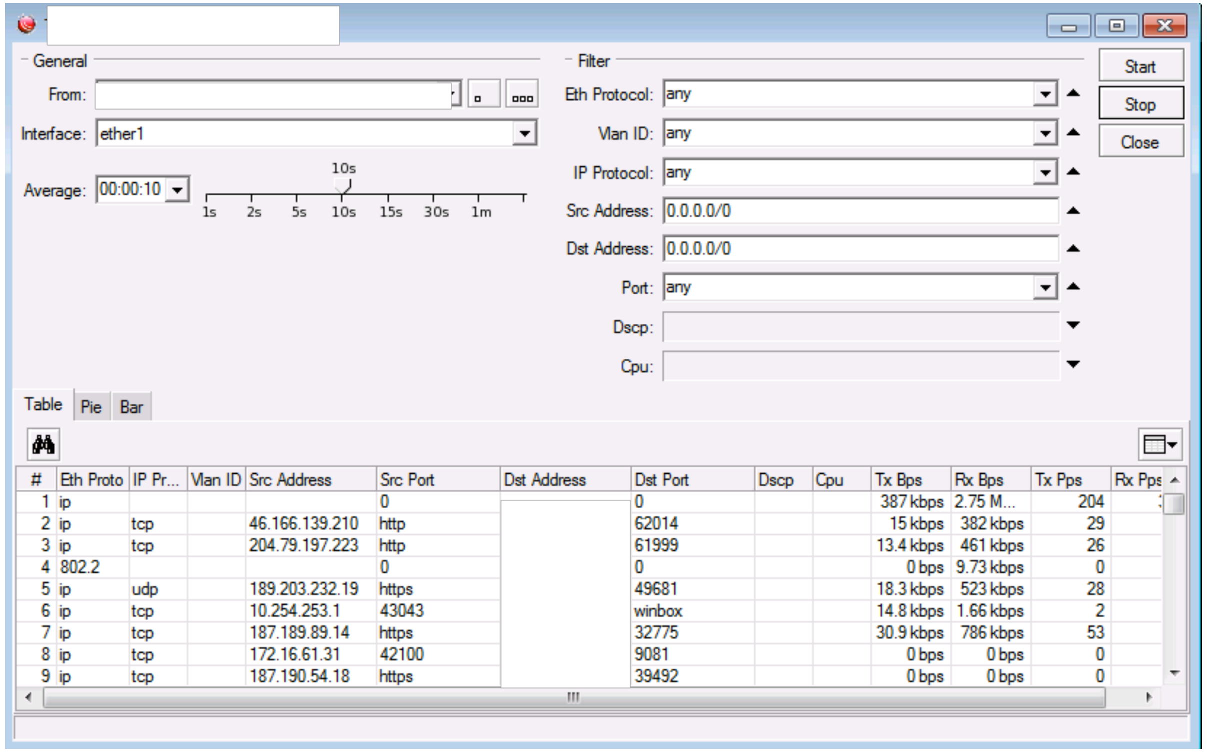
Otras herramientas (Bandwidth test)



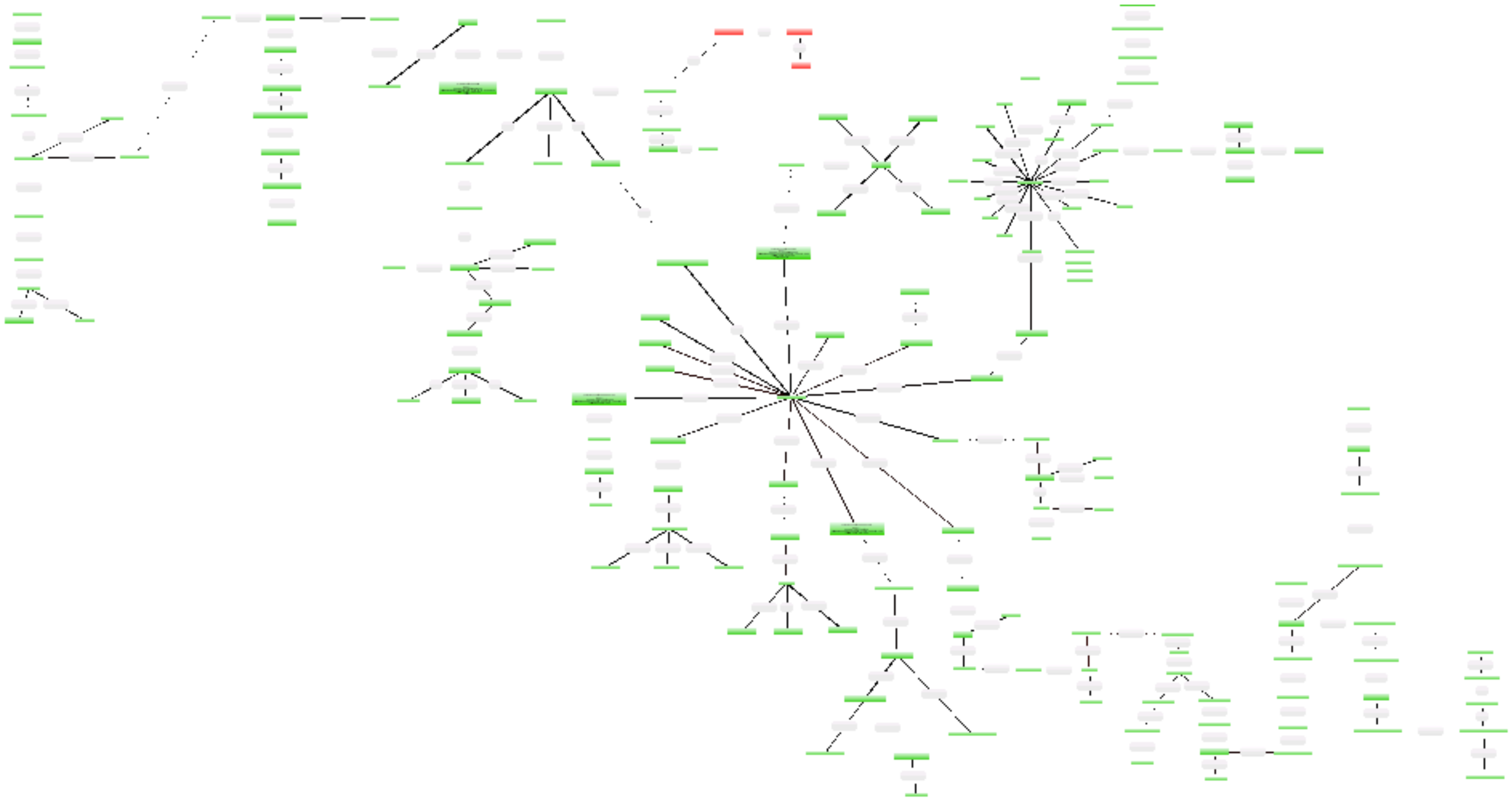


Otras herramientas (Torch)

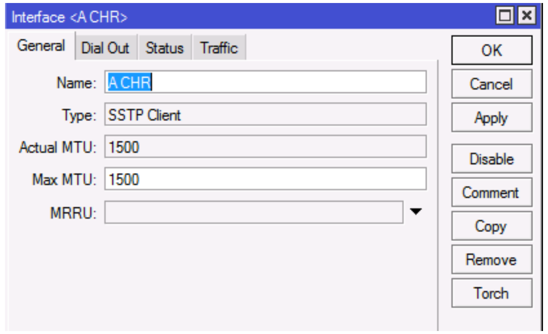




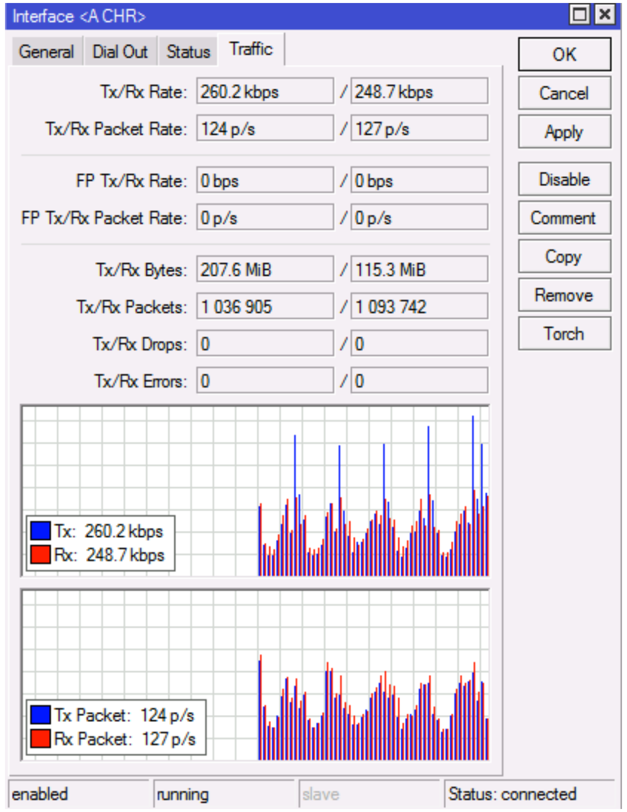
Mi dude ;)



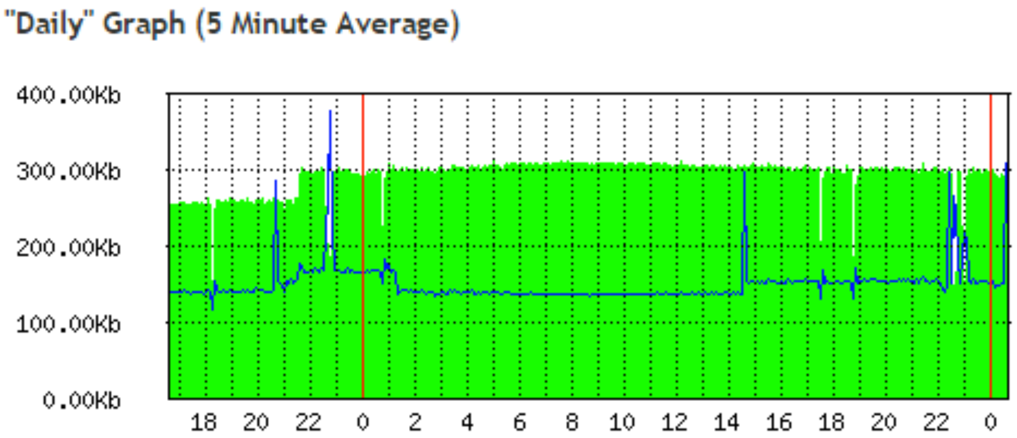
Mi dude ;)



Interface <A CHR>
General
Dial Out
Status
Traffic
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch
Name: A CHR
Type: SSTP Client
Actual MTU: 1500
Max MTU: 1500
MRRU:



Interface <A CHR>
General
Dial Out
Status
Traffic
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch
Tx/Rx Rate: 260.2 kbps / 248.7 kbps
Tx/Rx Packet Rate: 124 p/s / 127 p/s
FP Tx/Rx Rate: 0 bps / 0 bps
FP Tx/Rx Packet Rate: 0 p/s / 0 p/s
Tx/Rx Bytes: 207.6 MiB / 115.3 MiB
Tx/Rx Packets: 1 036 905 / 1 093 742
Tx/Rx Drops: 0 / 0
Tx/Rx Errors: 0 / 0
Tx: 260.2 kbps
Rx: 248.7 kbps
Tx Packet: 124 p/s
Rx Packet: 127 p/s
enabled
running
slave
Status: connected



"Daily" Graph (5 Minute Average)
400.00Kb
300.00Kb
200.00Kb
100.00Kb
0.00Kb
18 20 22 0 2 4 6 8 10 12 14 16 18 20 22 0

Saludos banda!
Whatsapp Wisp México
Whatsapp Wisp Oaxaca

Gracias

INTEGRA
Redes y telecomunicaciones