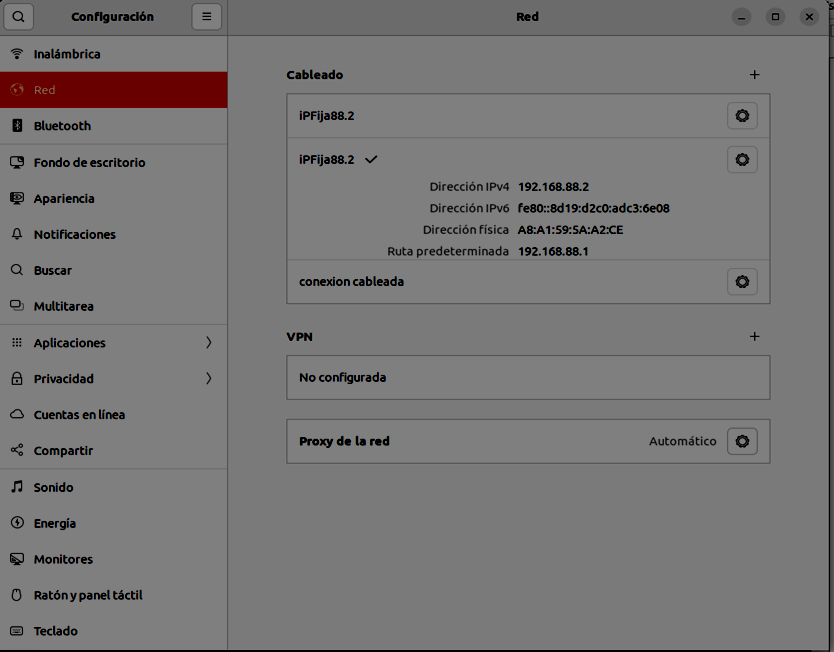
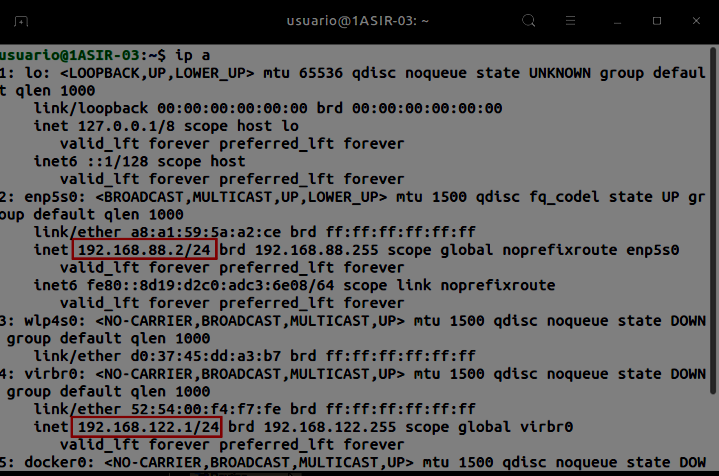
1. Pulsamos el botón reset sin el cable de alimentación, y mientras pulsamos el botón de reset insertamos el cable de alimentación y esperamos unos 10s y nos fijamos si se enciende una luz amarillo cuando se encienda dejamos de pulsar y ya estaría resteado.

1. Conectamos el cable de internet en router en la boca del puerto “internet”, y el la segunda boca del puerto metemos el otro cable que viene hacía el ordenador

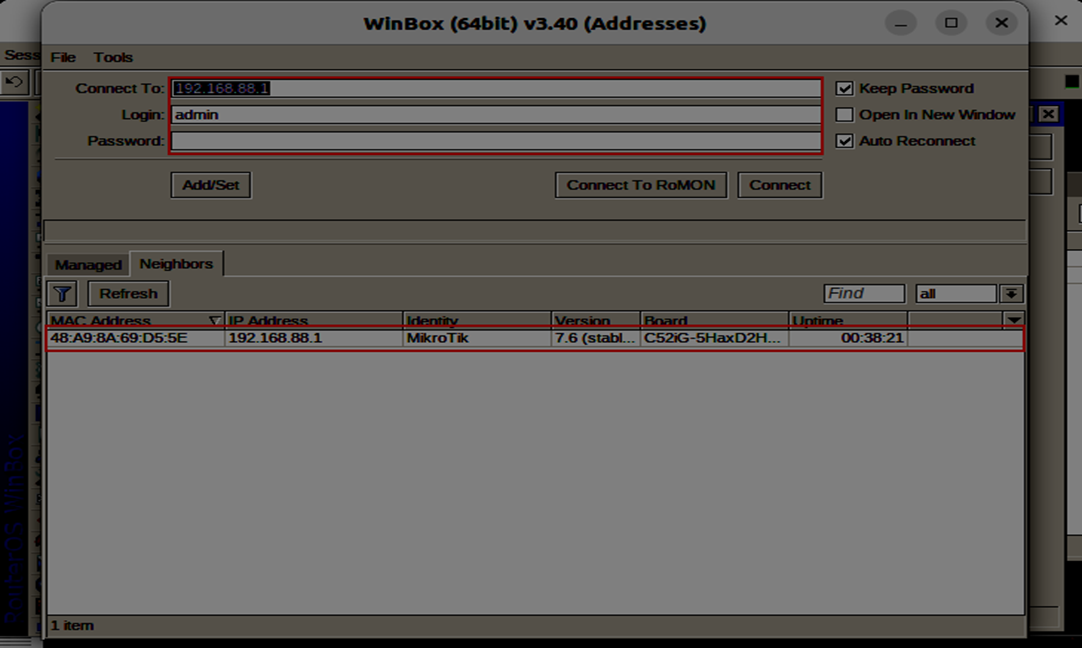
1. Añadimos una red con la siguiente dirección y dejamos la conexión cableada que tenemos por defecto



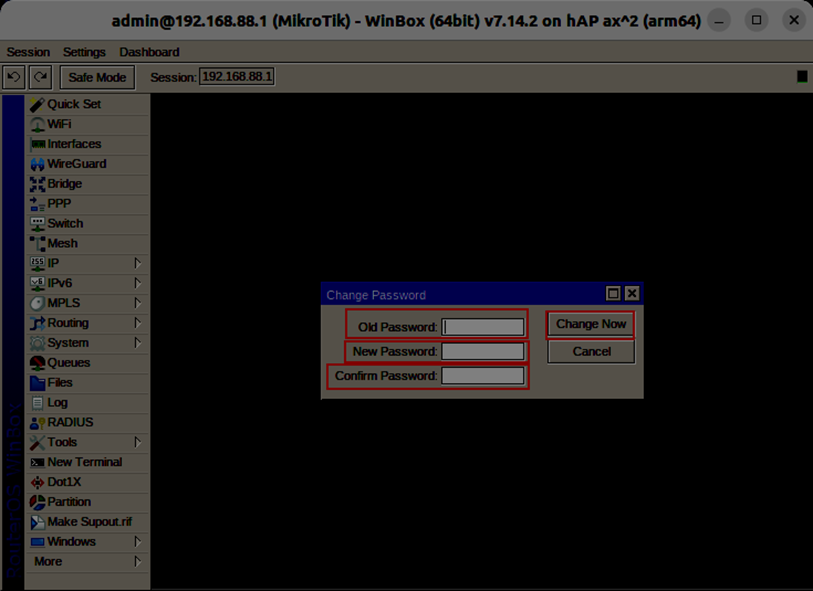
1. Una vez hagamos la red hacemos en la terminal “cmd” un “ip a” o “ifconfig” y como podemos ver tenemos la ip del router.



1. Una vez instalado winbox, abrimos y aparece esta pestaña en la que nos conectaremos. Para ello ponemos la contraseña del router.



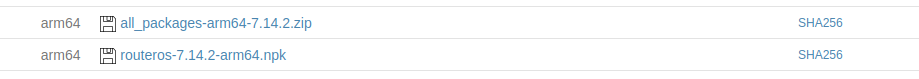
Una vez reseteada la contraseña, nos saldrá algo parecido, ponemos la contraseña por defecto del router y ponemos una contraseña adecuada.



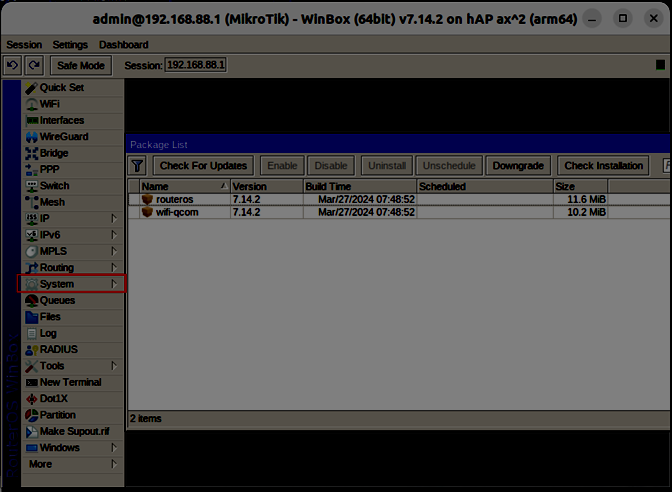
**PARA ACTUALIZAR:**

Necesitaremos descargar y añadir los paquetes necesarios de la descarga:

* wifi-qcom y arm64.npk



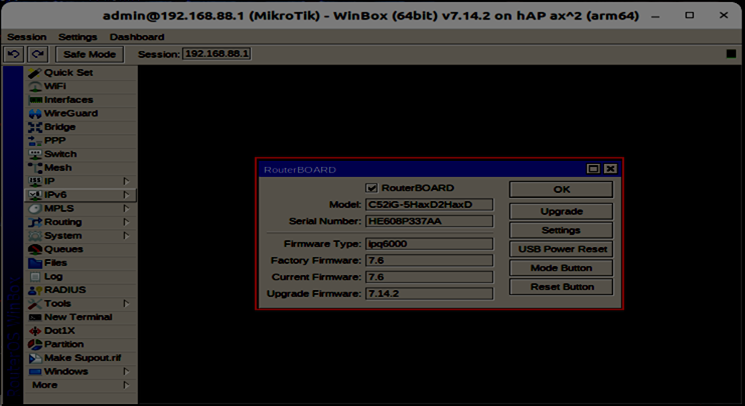
Ahora entraremos en Winbox y dentro de System > Packages y nos saldrá esta pestaña en la cual le daremos a Check For Updates cuando hayamos añadidos los paquetes

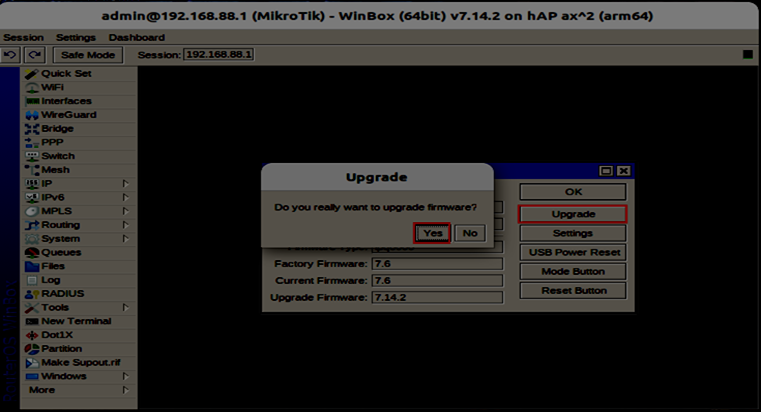


1. **ES MUY IMPORTANTE LEER los changelogs antes de actualizar** de cada versión por que puede ser que haya cambios en la versión, y eso nos puede afectar a nuestra configuración de routers.

* **stable:** Esta versión consta de 3 números de la versión, la subversión y la diversión es una versión estándar que se suele hacer cada mes probablemente.
* **long term :** Esta versión es más alargada, que queremos decir con esto, que sis tenemos una configuración que no queremos tocar y queremos dejar mucho tiempo para no tocarla puede durar muchos años porque no van a tocar muchos cambios en la versión.
* **testing :** Como el nombre mejor indica es una versión de prueba que es la 7.15, es una versión de prueba de beta se suele decir y van dando sus opiniones y los fallos.
* **development :**

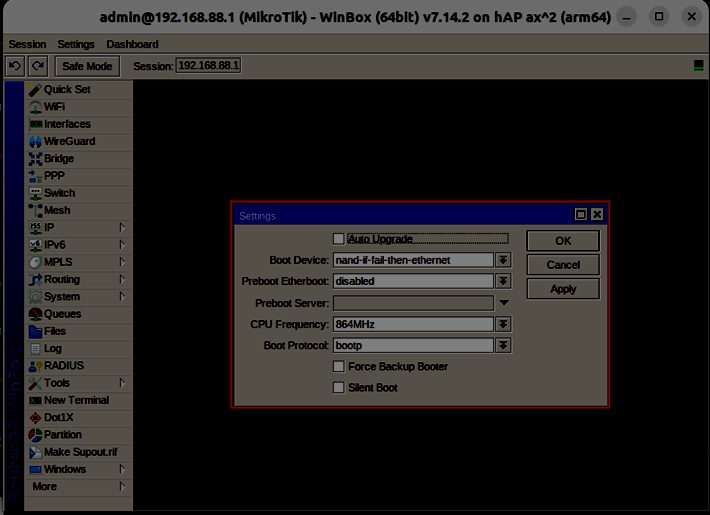
1. **Aquí vemos que de fabrica viene la 7.6 y hemos actualizado a la 7.14.2 y vamos a actualizar el firmware y reboot y vamos a forzar a apagar al router, para ponerle la versión actual del firmware**





* Una vez añadidos haremos: System → Reboot

En los parámetros Settings para ver que hay una opción de configurar automáticamente las actualizaciones del firmware automáticamente con la versión



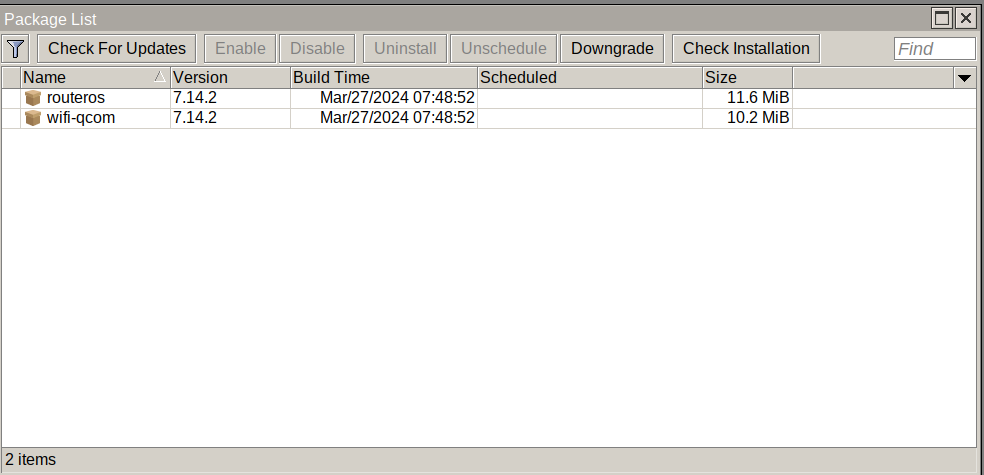
Si todo está correcto al iniciar de nuevo Winbox habremos cambiado la versión 7.14 a 7.14.2

Al actualizar a esta versión, los paquetes usados para la instalación se borrarán automáticamente

**PARA DOWNGRADEAR:**

Volveremos a descargar los mismos archivos pero de la versión inferior.

Volveremos a añadir los mismos archivos dentro de Winbox y con el botón de Downgrade podremos volver a esa versión

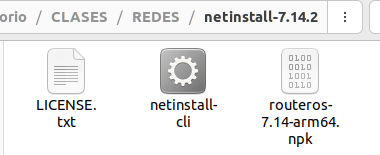


**CON NETINSTALL:**

Para instalar netinstall usaremos el siguiente archivo



Lo descomprimimos en la carpeta de REDES y dentro de ella aplicamos el archivo arm64.npk de la versión 14



**PARA INSTALAR UNA VERSIÓN ANTERIOR DESDE EL ROUTER**

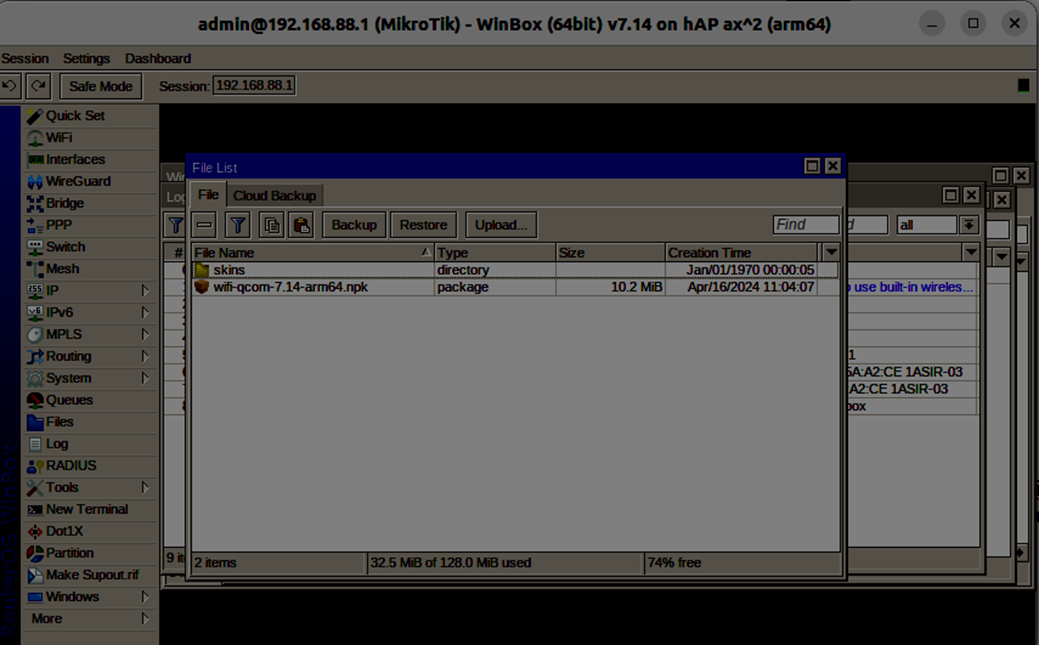
1. Poner direccion IP Fija
2. Desenchufar la corriente del router y poner el cable 2 en el 1 y este quitarlo.
3. Pulsar el botón reset
4. Usar el Comando:

sudo ./netinstall-cli -i enp5s0 routeros-7.14-arm64.npk

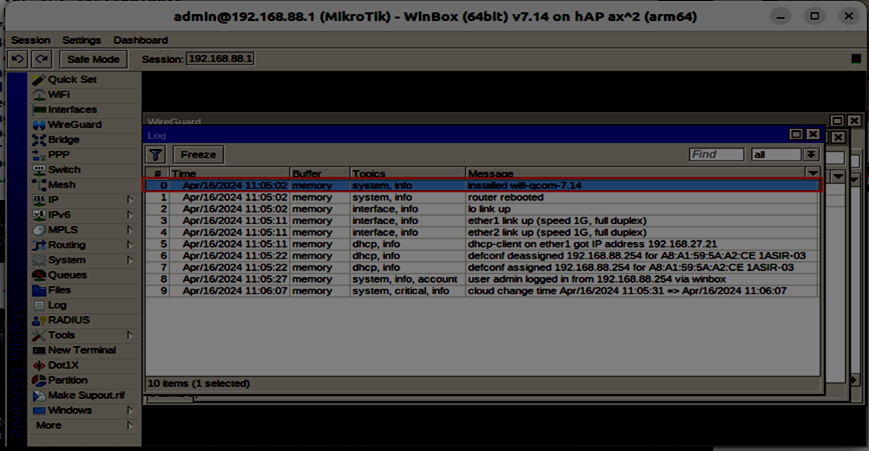
1. Esperar 30 segundo pulsando el botón de reset, y una vez terminado volver a poner el router como estaba anteriormente
2. Pulsar el botón hasta encontrar router client

**FICHERO WIFI-QCOM**

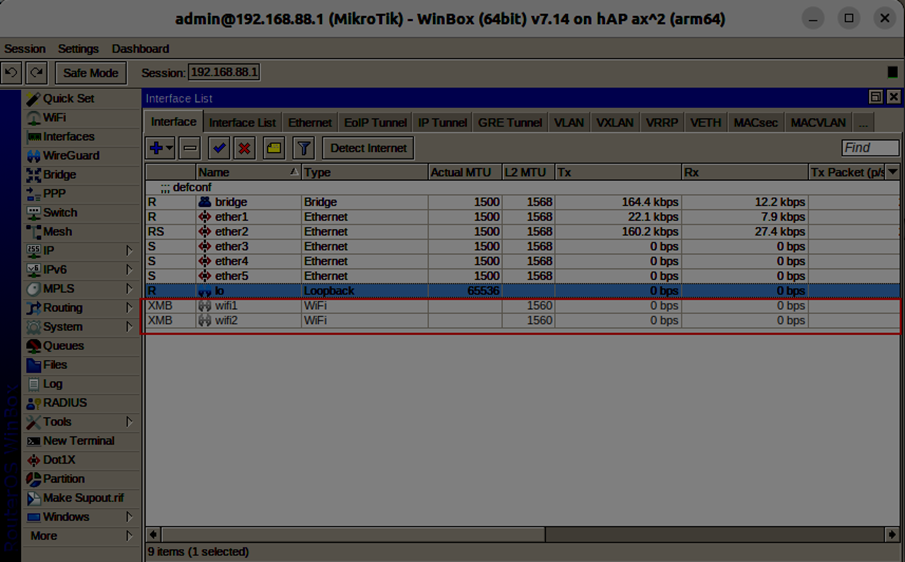
Metemos el fichero wifi-qcom con la versión correspondiente y la arquitectura arrastrado el fichero al winbox



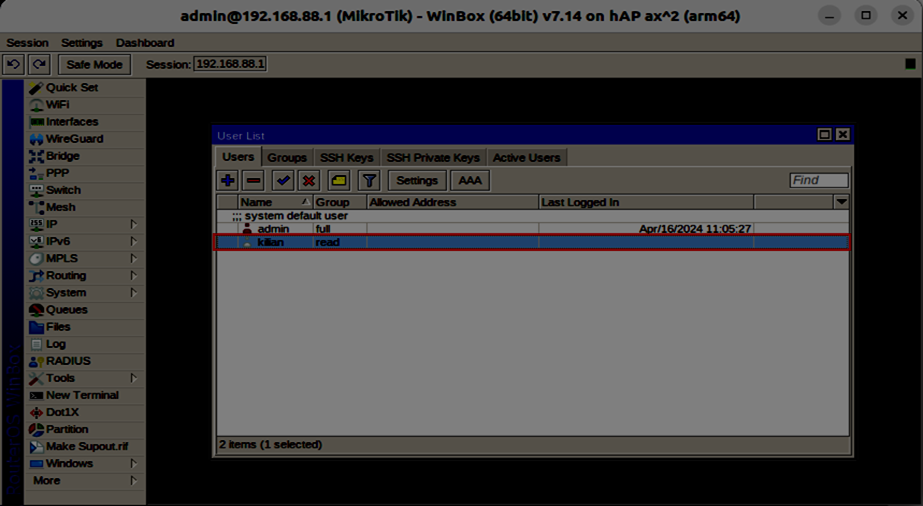
Vamos al winbox y hacemos un reboot y veremos como el paquete se ingresa automáticamente el resultado quedaría un tal que así:



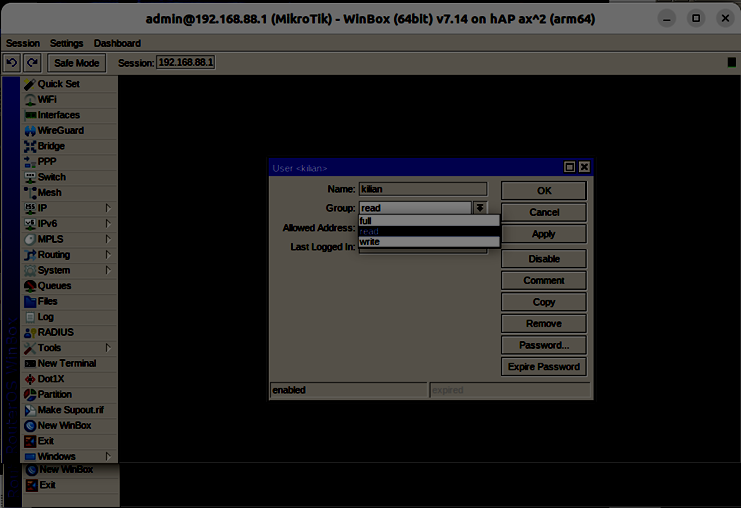
Deshabilitamos los interfaces wifi, y por defecto nos viene un interfaz de tipo loopback



Creamos un usuario para poder ver la configuracion pero no podremos cambiarla



Los permisos se pueden cambiar de esta forma el Group;



Si pulsamos Expire password. Cuando el usuario se loguee de nuevo le pedirá la contraseña antigua, y que defina una password nueva.

**FORMAS PRÁCTICAS:**

**Actualizar:**

* Desde el botón Check for updates
* Manualmente
* Con netinstall

**Downgrade:**

* Manualmente
* Con netinstall

**Instalar paquetes:**

* Manualmente

**Reset de la configuración:**

* Por botón
* Desde comando/ menú winbox
* Manteniendo usuarios
* reset a no-default

**CONFIGURACIONES**

***Configuración por defecto de los router:***

* Cliente DHCP en ether1
* Bridge en ether2-ether 4
* Loopback
* IP 192.168.88.1/24 en bridge
* Servidor DHCP en bridge
* Reglas de FW que impiden configurar el router desde ether1
* NAT para que la red interna (192.168.88.1) salga a Internet usando la dirección IP pública adquirida por DHCP en ether1 (Es decir, la red 88.0/24 queda enmascarada detrás de la IP 192.168.27…. que el router coge en clase)

***No es lo mismo que Configuración en blanco***

* Necesita una IP, un Gateway y un servidor DNS
* Comprobar ping al gateway
* Comprobar ping al servidor DNS
* Comprobar ping a un dominio

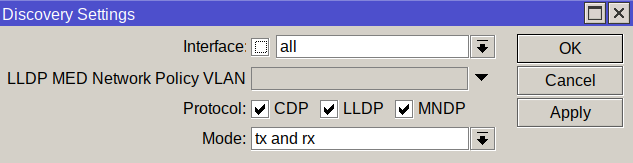
**LISTA DE INTERFACES**

En estas listas pueden excluir algunas redes o añadirlas con el nombre que tu elijas

**PROTOCOLOS DE DESCUBRIMIENTO**

* LLDP: Lime Layer Discovery Protocol
* CDP: Cisco Discovery Protocol
* MNDP: Mikrotik

Para ver todas las conexiones: IP → Neighbors → Discovery Settings →



**Cambio de IP de nuestra red interna:**

Antes: 192.168.88.1/24

Despues: 10.0.11.1/24

Para ello: Borramos la pool

**Con terminal**

* ***Primero Borramos***

ip address/print → borrar configuración del address 1

ip pool/print → borramos todos los pool

ip/dhcp-server/print → borramos todos

ip/dhcp-server/network/print → borramos todos

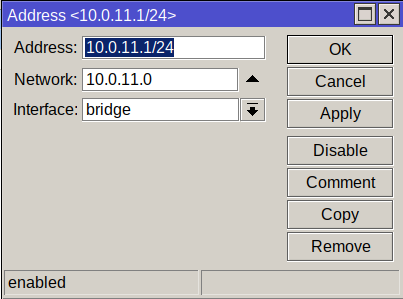
* ***Segundo Aplicamos***

ip/address/add address 10.0.11.1/24 interface=bridge

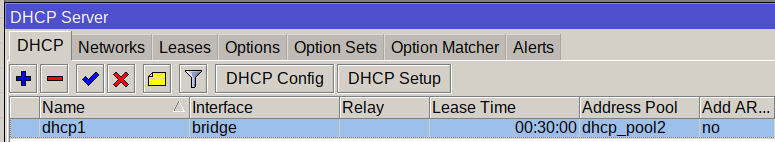
ip/dhcp-server/setup

**Con GUI**

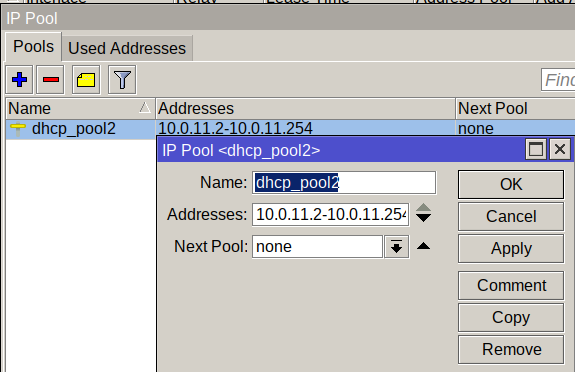
Entramos en IP → Addresses → Cambiamos la configuración



Vamos a IP → Dhcp-Server → Borramos la configuración y aplicamos la nueva



Vamos a IP → Pool → Borramos la configuración y aplicamos una nueva



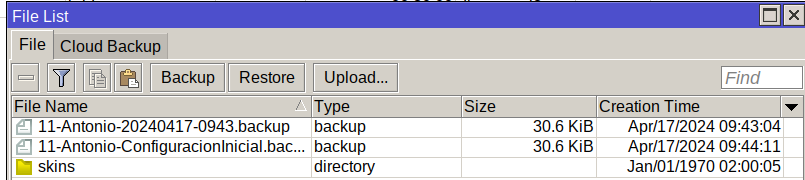
A veces tenemos que cambiar o borrar la IP del router… por lo que podemos quedarnos ‘fuera’

!!!Usar la conexión MAC puede ayudar¡¡¡

**BACKUP**

Es un fichero binario, que solo sirve en el mismo router, pero no en otro igual ya que no sirve

Para entrar al backup, pulsaremos en Files y a continuación en el botón de Backup, en este crearemos un backup con nuestro nombre, con el botón derecho lo descargamos y lo guardaremos en nuestro equipo





**SERVIDOR DHCP:**

Para cambiar un servidor DHCP hay que:

* Borrar el servidor DHCP: /ip/dhcp-server/remove
* Borar la network: /ip/dhcp-server/network/remove
* Borrar el pool: ip/pool/remove

**CRITERIO DE RUTAS**

Una ruta es un destino con un gateway y una distancia.

Un router tiene configuradas muchas rutas.

* Si un router tiene varias rutas al mismo destino, se elige la menor distancia
* Si hay varias rutas a un mismo destino con igual distancia. ECMP

**DNS**

En DNS la configuración manual siempre tiene prioridad con la configuración dinámica

**¿Qué servidores DNS proporciona el servidor DHCP?**

**0.** ¿En la configuración de la red aparece NO DNS? SI es asi, no va NINGÚN SERVIDOR DNS

1. ¿En la configuración de la red hay servidores DNS? Si es asi: solo se ofrecen esos

***En caso de que no esté marcado No-dns y que no haya servidores en la red:***

1. ¿El router permite peticiones DNS? Si es así, se ofrece
2. ¿El router tiene DNS dinámicos?
   1. Si, se ponen en el orden
   2. NO, ¿El router tiene servidores DNS configurados?
      1. Se ofrecen en el orden que tenga

**CONCEPTOS:**

* **ARP:** Address Resolution Protocol
* **DHCP:** Dynamic Host Configuration Protocol
* **DNS:** Domain Name Server

**DNS**

Nos permite manejar nombres de dominio en lugar de direcciones IP. Asi, cuando en el navegador escribimos [www.google.es](http://www.google.es), pues el navegador DNS es quien hace la busqueda ww.google.es <-> 142.169.1.243

Si yo se que tengo que comunicar con ww.goggle.es y no conozco su IP

* Envio una consulta DNS al servidor DNS: ¿quién es [www.google.es](http://www.google.es)?
* El servidor DNS me responde: [www.google.es](http://www.google.es) es 142.169.1.243

**ARP**

Permite encontrar la dirección MAC de un equipo del que conocemos su IP.

***NOTA:***

En la red local, los envios se hacen en “CAPA 2”, usando tramas ETHERNET que usan DIRECCIONES MAC de ORIGEN y DESTINO y esas tramas, en su interior, llevan los PAQUETES IP con DIRECCIONES IP SRC y DST

**DHCP-SERVER**

**POOL**

Conjunto de direcciones IP disponibles para asignar dinámicamente y que además lleva el seguimiento de las direcciones asignadas (para no asignar varias veces la misma IP)

Si configuramos DHCP-Server con STATIC-ONLY (en lugar de un pool) solo ofreceremos direcciones IP a los equipos que tenga una asignación estática en DHCP-SERVER - LEASES

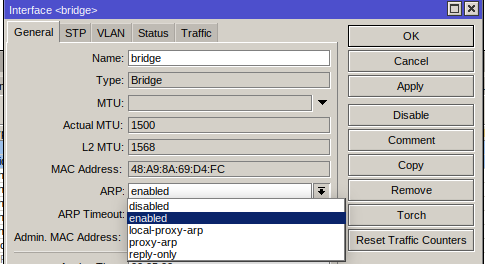
**¡¡¡¡ Es una medida de protección de acceso a la red !!!!**

Si el equipo se conecta, que no tiene asignación de IP, se configura una dirección IP adecuada, con su GW y su DNS…

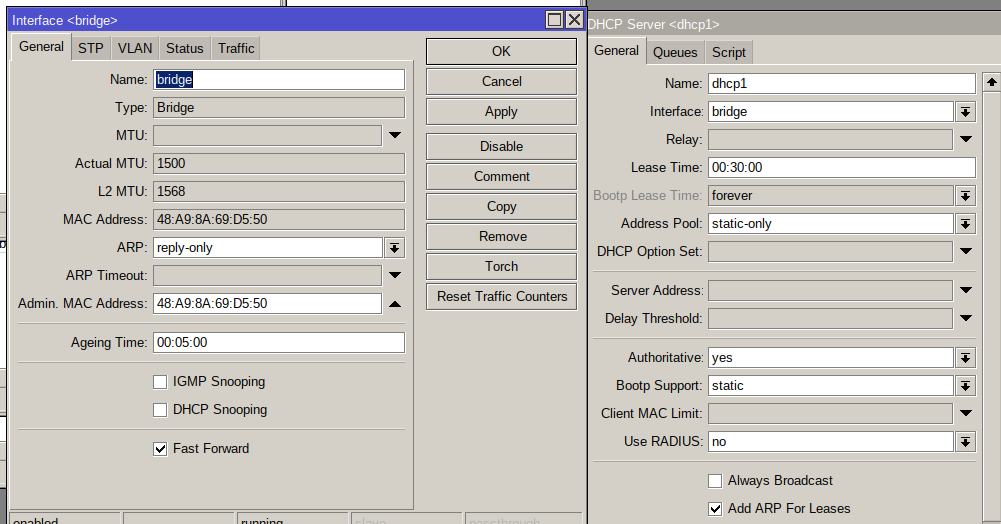
**¡¡¡ La medida de seguridad es una MIERDA !!!!**

**EJERCICIO DHCP-SERVER:**

1. Asigna un STATIC-LEASE a tu equipo: 10.0.x.123
2. Asegurate de que solo hay una LEASE
3. Cambia el DHCP-Server y ponlo en STATIC-ONLY
4. Tu compañero se conecta a tu router: no obtiene IP
5. Tu compañero asigna a su ordenador una IP adecuada a tu red: tiene acceso a Internet
6. Acordarme del ARP



1. En el DHCP - Server marcamos ADD ARP FOR LEASES
2. En el interfaz BRIDGE configuramos ARP: Reply - Only



1. Comprobamos que al listillo ta no tiene acceso a internet
2. Luego de comprobar esto, volvemos a dejar todo casi como estaba:
   1. Nos aseguramos de que el bridge tiene ARP: enabled
   2. En DHCP-Server desactivamos ADD ARP FOR LEASES y volvemos a poner el POOL
   3. Eso si: Mantenemos el STATIC-LEASE 10.0.x.123 a nuestro equipo

**BRIDGE**

* Si desmarcamos HW Offload: la función de bridge la hace la CPU siempre (software)
* Si marcamos HW Offload:
  + La función del bridge la hará el hardware SIEMPRE QUE SE DEN LAS CONDICIONES NECESARIAS

*Cuales son las condiciones para poder usarlo:*

* El dispositivo tiene un switch-chip integrado con los puertos directamente conectados
* Solo puede haber creado un bridge por cada switch-chip

**FIREWALL DE BRIDGE:**

El firewall se aplica a paquetes que pasan de una red a otra. Por defecto, las reglas de FW no se aplican a paquetes en la mism RED

Podemos forzar a que el FW se aplique también a los paquetes que pasan por un bridge.

***CHAINS:***

* Input → Paquetes que van dirigidos al router
* Output → Paquetes enviados por el propio router
* Forward → Paquetes que atraviesan el router

**EJERCICIO FIREWALL:**

1. Tu compañero se conecta a tu router. Haz ping a su dirección. Comprueba que OK
2. En tu router desactiva todas las reglas de IP Firewall-filter
3. Crea una regla de FW:
   1. chain=forward Protocol=ICMP action=drop dst-address=10.0.x.123
4. Comprueba que tu compi puede hacerte PING aunque la regla FW lo impida
5. Ene bridge, en el botón de SETTINGS, activa la opción “Use Firewall”
   1. Comprobamos que ahora no puede hacerte PING
6. *¿Puedo enviar paquetes a Internet?*

Desde el PC si que hago ping 8.8.8.8

1. *Tengo resolución de nombres en dominio*

Desde el PC no hago ping google.es

**EMPEZAMOS POR ROUTER:**

**¿Tenemos IP en ether1? ¿Tenemos ruta por defecto? ¿Tenemos DNS?**

*¿El router puede hacer ping 8.8.8.8?*

Si no puede, el error está en la IP de ether1, shcp-client de ether1 o gw por defecto

*¿El router puede hacer ping a google.es?*

Si no resuelve el nombre del dominio, comprobar 1º DNS y si está activo use-dns en dhcp-client

El ROUTER tiene bloqueado en input las consultas DNS

1. En ese caso: crea una regla de FW que permita consultas DNS (udp 53)

**PORT KNOCKING**

De modo que solo accedan al WINBOX del router (ttcp 8291) los equipos que hagan la llamada mágica: 3508-....

**EJERCICIO PORT KNOCKING:**

/ip firewall filter add action=drop chain=input dst-port=8291 protocol=tcp src-address-list=\ !PERMITIDOS

add action=add-src-to-address-list address-list=TOQUE1 address-list-timeout=\5s

chain=input dst-port=38 protocol=tcp

add action=add-src-to-address-list address-list=TOQUE2 address-list-timeout=\5s chain=input dst-port=455 protocol=tcp src-address-list=TOQUE1

add action=add-src-to-address-list address-list=PERMITIDOS chain=input \dst-port=99

protocol=tcp src-address-list=TOQUE2

Con los puertos correspondientes

**NAT**

Es un proceso de firewall que permite modificar las direcciones de los paquetes

1. **Source NAT:** Se modifica la dirección/puerto de origen del paquete
2. **Destinatarios NAT:** Se modifica la dirección/puerto de destino del paquete

***Cómo funciona:***

18.19.20.21 (Direccion publica) → R1 → 192.168.1.1 (direccion que llega a mi casa)

**Paquete original → Origen → 192.168.1.2:4567 → 8.8.8.8:53**

*Cuando el paquete pasa por el R1, se hace el cambio de dirección de origen:*

**Paquete ‘enmascarado’ → 18.19.20.21:4567 → 8.8.8.8:53**

**Paquete de respuesta: 8.8.8.8:53 → 18.19.20.21:4567**

**Desenmascarar :** 8.8.8.8:53 → 18.19.20.21:4567

8.8.8.8:53 → 192.168.1.2:4567

Para poder hacer NAT el router necesita llevar un seguimiento de las comunicaciones

| **IP: origen** | **IP: puerto destino** | **IP: puerto nuevo origen** | **IP: puerto nuevo destino** |
| --- | --- | --- | --- |
| 192.168.1.2:4567 | 8.8.8.8:53 | 18.19.20.21:4567 | 8.8.8.8:53 |

**NAT EN MIKROTIK:**

1. **Chains de NAT:**

* **srcnat:** permite cambiar la dirección IP y puerto de origen
* **dstnat:** permite cambiar la dirección IP y puerto de destino

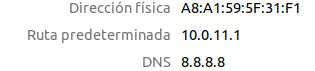
1. **Actions de NAT:**

* **accept:** acepta el paquete y no se hacen cambios ni se sigue evaluando NAT
* **src-nat:** cambio la IP/puerto origen por los indicados. Debo indicar nueva dirección/puerto
* **dst-nat:** cambio la IP/puerto destino por los indicados. Debo indicar nueva dirección/puerto
* **masquerade**: es como src-nat pero utiliza la dirección del interfaz de salida. NO es necesario indicar nueva dirección/puerto
* **redirect**: acción especial para el dst-nat

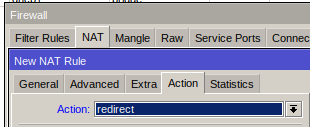
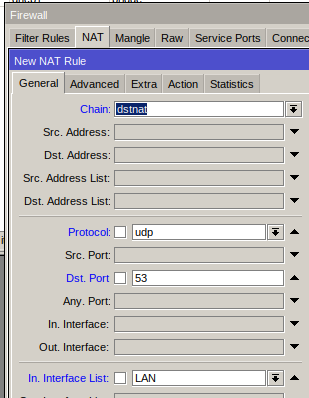
**EJERCICIO REDIRECT:**

* Nos aseguramos de que nuestra IP sea: 10.0.x.123
* Nuestro primer servidor dns es: 10.0.x.1

1. Comprobaremos que nuestro DNS sea 8.8.8.8



1. Haremos la siguiente configuración desde Ip → Firewall → NAT → Nueva regla



Con esto podremos conectarnos a nuestro router a traves de router.lan

**DNS es un servicio ESENCIAL en INTERNET**

* Resuelve los nombres de dominio o direcciones IP
* NO ES UN PROTOCOLO CIFRADO
* TAMPOCO ES UN PROTOCOLO AUTENTICADO
* Es muy fácil interceptar peticiones DNS y alterar las respuestas
* Podemos hacer que los incautos vayan a páginas PELIGROSAS en lugar de las reales

**DoH:** DNS over HTTPS

**TÚNELES**

La tecnología de túneles va a permitir que los paquetes que se envían, son a su vez, tramas. Es decir va a meter paquetes dentro de paquetes

* **PPP:** Point to Point Protocol
* **PPPoE:** PPP over Ethernet
* **L2TP:** Layer 2 Tunnel Protocol

*HTML → TCP → IP → Trama Ethernet*

**Página Web: 5200 Bytes**

**Trama:** 1500 Bytes: MAC Origen → MAC Destino → Datos\_trama

**Paquete:** 1400 Bytes: IP Origen → IP Destino → Datos\_Paquete

**TCP:** 1460 Bytes: Puerto Origen → Puerto Destino → Datos\_tcp

**¿Cuántos paquetes tengo que enviar si quiero llegar a la página web de 5200 Bytes?**

[aa:bb:cc:dd:ee:ff - 11:dd:33:ff:22:ee [192.168.1.100 - 192.168.1.2 [80-3456 W1] ] ]

[aa:bb:cc:dd:ee:ff - 11:dd:33:ff:22:ee [192.168.1.100 - 192.168.1.2 [80-3456 W2] ] ]

[aa:bb:cc:dd:ee:ff - 11:dd:33:ff:22:ee [192.168.1.100 - 192.168.1.2 [80-3456 W3] ] ]

[aa:bb:cc:dd:ee:ff - 11:dd:33:ff:22:ee [192.168.1.100 - 192.168.1.2 [80-3456 W4] ] ]

**DIRECCIONES PPPoE**

* Cifrado
* Comprensión de datos

**Paquete ‘normal’:** Trama ethernet → Paquete IP → TCP → HTML

**Encapsulado ‘pppoe’:** Trama ethernet → Trama PPPoE → Paquete IP → TCP → HTML

**EJERCICIO PPPoE:**

**SERVIDOR:**

* Desactiva el cliente PPPoE
* Activa el cliente DHCP y se asegura de tener internet
* Crea un POOL de direcciones para los clientes PPPoE
* Crea un PPP-Profile con remote-address-pool local-addresses=1.2.3.4 y el profile creado
* Crea un PPP Secret para los usuarios, indicando el perfil creado
* Crea un PPP-PPPoE-Server en ether1 con un service name unico

**CLIENTE**

* Modifica el cliente PPPoE para conectarse al SERVICIO del compañero
* Comprueba que se conectan al servidor y que hay internet
* Si no hay internet, busca el problema

**TÚNEL L2TP:**

Con este túnel puedes conectarte a la misma red desde cualquier parte del mundo.

**SSTP**: Secure Socket Tunnel Protocol

**SDN**:Software Defined Networks

**Configuracion SSTP entre routers Mikrotik:**

* **Servidor:**
  + Activar servidor SSTP
  + Crear Pool
  + Crear Secret y poner local-addresses and remote
  + Crear ruta estática usando la IP cliente
* **Cliente:**
  + Crear interfaz cliente
  + Crear ruta estática usando la IP del servidor
* **Checks:**
  + Ping entre PC conectado al servidor con PC conectado al cliente

**ACTIVIDAD SSTP:**

**SERVIDOR**

/interface/sstp-server/server set enabled=true

/ppp/secret add name=u1 password=u1

local-address=10.255.255.1

remote-address=10.255.255.2

/ip/route/add dst-address=10.0.y.0/24

gateway=10.255.255.1

**CLIENTE**

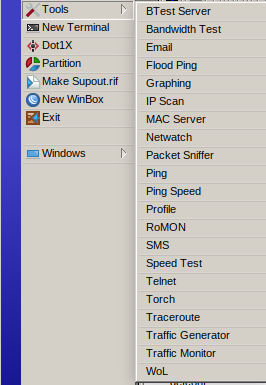
/interface/sstp-client/add connect-to=192.168.27.x

user=u1 password=u1 disabled=no

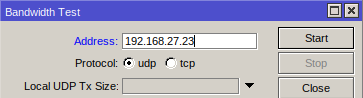
/ip/route/add dst-address=10.0.x.0/24

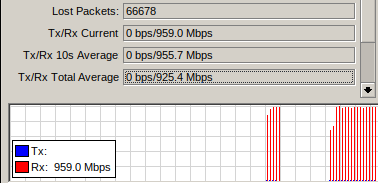
gateway=10.255.255.1

**TOOLS:**



* **BTest Server:** Nos permite realizar pruebas de ancho de banda. En ella desactivaremos la autenticación. Si dejamos deshabilitada la autenticación, cualquier persona que se conecte puede hacer que nos baje la velocidad del ordenador
* **Bandwidth Test:** Permite realizar pruebas de ancho de banda aplicando la dirección IP del compañero

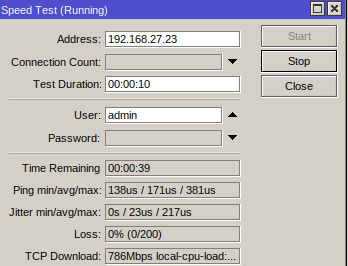




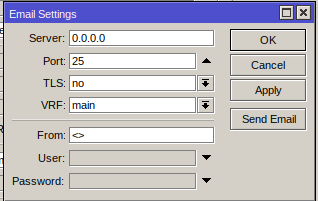
**UDP:** Se envía mucha información pero se pierden paquetes

**TCP:** Cuando se envían los paquetes va aumentando la capacidad respectivamente

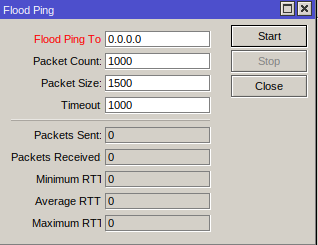
* **Speed Test:** Otra herramienta para medir el ancho de banda, funciona igual que bandwidth test



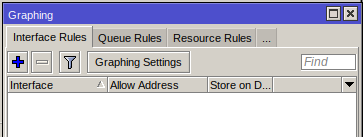
* **Email:** Podemos conectarnos al servidor, podemos crear un script para saber cada cuanto se conecta el usuario



* **Flood ping:** Estadística para ver si se pierden paquetes por el camino y cuantos se envian.



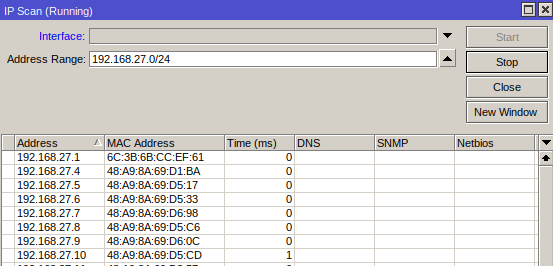
* **Graphing:** Guarda información y presenta gráficos sobre el uso de recursos (RAM, memoria…) estos gráficos no son en tiempo real, se hacen cada 5 minutos



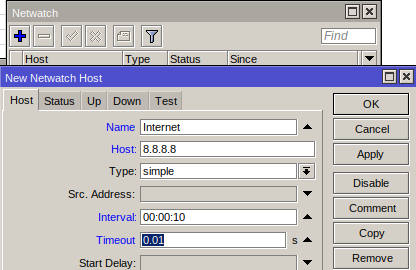
**¿Puedo en un interfaz ver los gráficos en tiempo real?**

Si, desde interfaces → Traffic (por ejemplo)

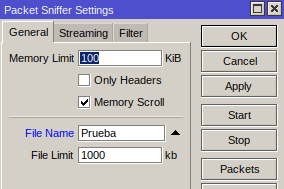
* **IP Scan:** Permite ver los equipos que responde a la red aplicada

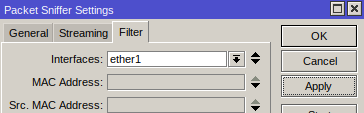


* **MAC Server:** El router permite que se conecten al propio router
* **Netwatch:** Permite monitorizar el estado de un dispositivo



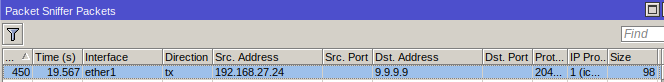
* **Packet Sniffer:** Permite crear un fichero con los filtros que quiera guardar



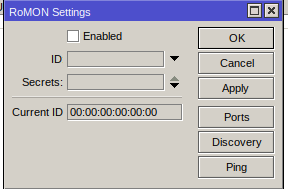


Para realizar la prueba del paquete, haremos un ping en la maquina al 9.9.9.9

Una vez llegue a 10 paquete paramos el ping y en Packets vemos todos los paquetes enviados y el archivo de prueba en Files



* **Profile:** Podemos ver que es lo que está haciendo nuestro router
* **RoMON:** Es un protocolo propio de mikrotik que nos va a ayudar a configurar los dispositivos y conectarnos a ellos los cuales tenga RoMON activo



**WIRELESS:**

**BANDAS**

* 2.4 GHz
* 5 GHz
* 60 GHz

De forma general, a mayor frecuencia

* Mayor capacidad (es decir, mas Mbps)

**WIFI EN MIKROTIK**

* **CAPs:** Controlled Access Point
* **CAPs\MAN:** CAPs Manager

