



MikroTik Certified Network Associate



Modulo 5

Administración de red

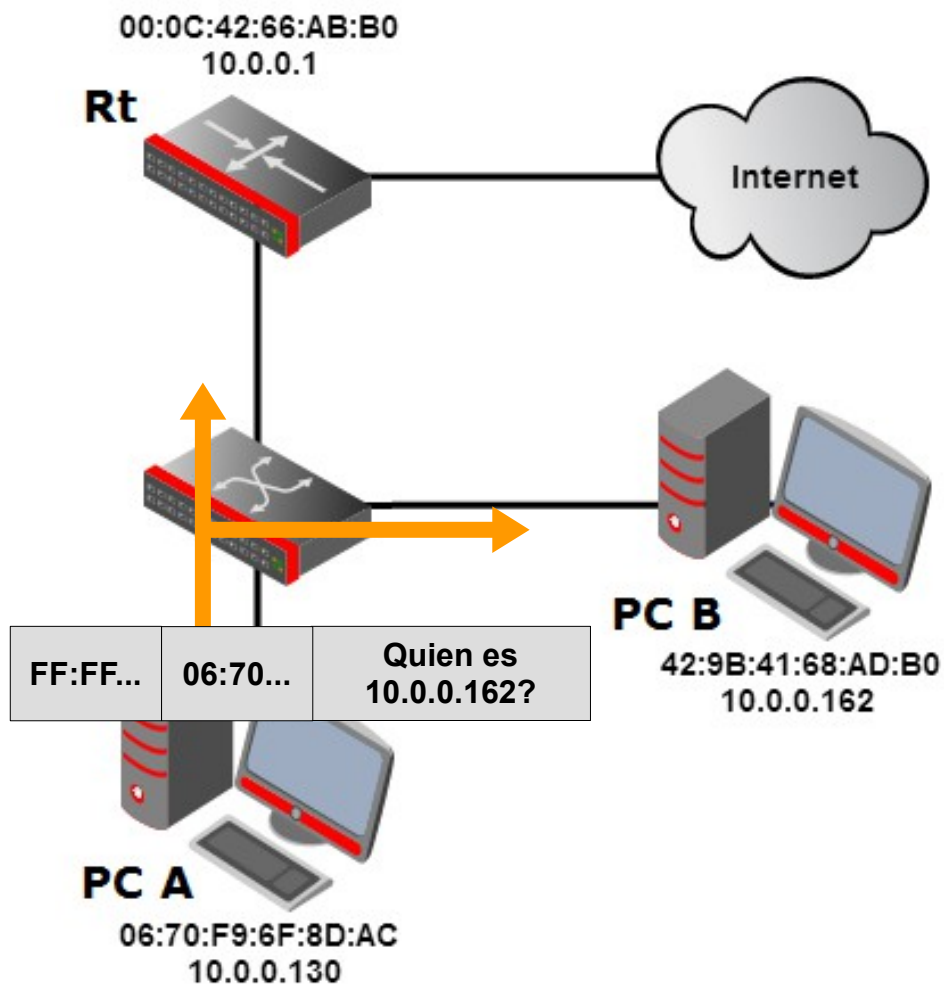


Protocolo ARP

- Address Resolution Protocol.
- ARP es un mecanismo que permite mapear direcciones IP (capa 3) con direcciones MAC (capa 2).
- Esta relación se refleja en un tabla llamada Tabla ARP.

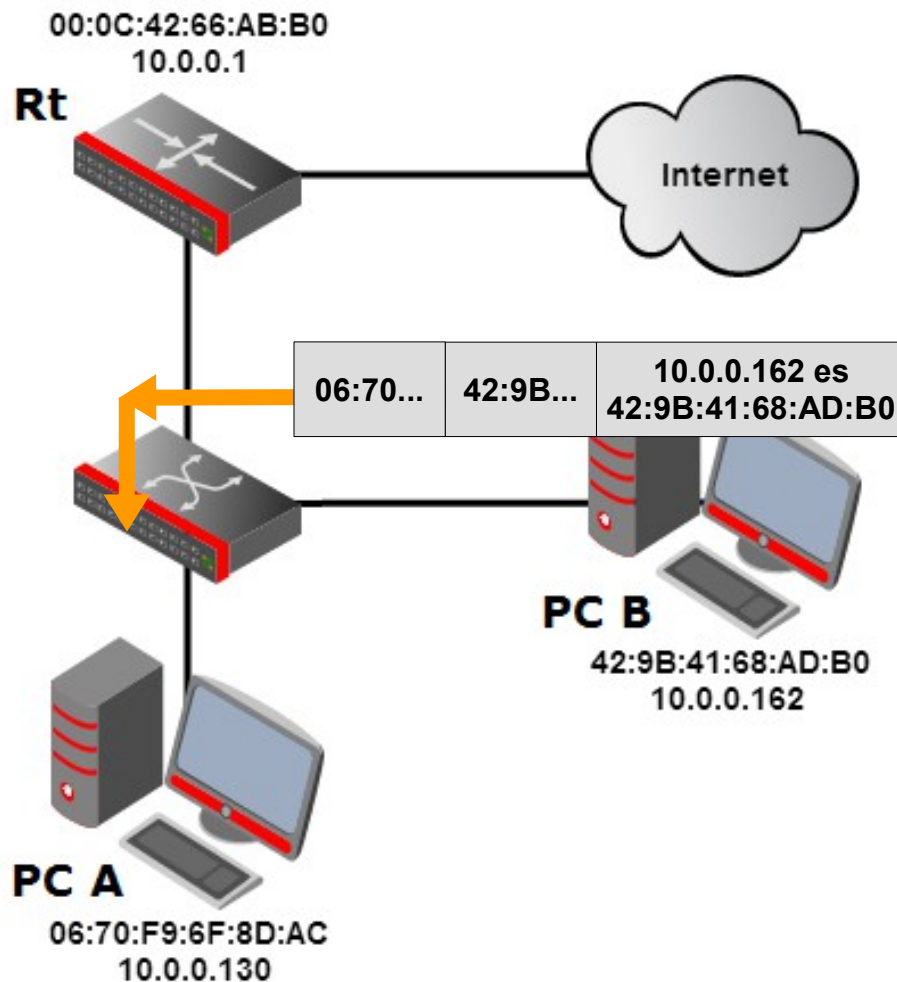
- ARP tiene dos mecanismos básicos:
 - ➔ **Consulta ARP** (ARP request)
 - ➔ **Respuesta ARP** (ARP reply)

Protocolo ARP - Consulta



- (1) Una aplicación en la PC A quiere comunicarse con otra que se encuentra en la PC B.
- (2) Arma el paquete y envia el mismo a capa 2.
- (3) Pero como desconoce la MAC de la PC destino, inicia una **Consulta ARP**, la cual es enviada por broadcast a la MAC `FF:FF:FF:FF:FF:FF`.

Protocolo ARP - Respuesta



- (1) El Rt y la PC B reciben la Consulta ARP, pero sólo PC B responde.
- (2) PC B envía una **Respuesta ARP**, esta vez dirigida directamente al dispositivo que hizo la consulta.
- (3) PC A recibe la consulta, y la almacena por un tiempo en su Tabla ARP.
- (4) Finalmente PC A envía su paquete encapsulado en una trama dirigida sólo a PC B.

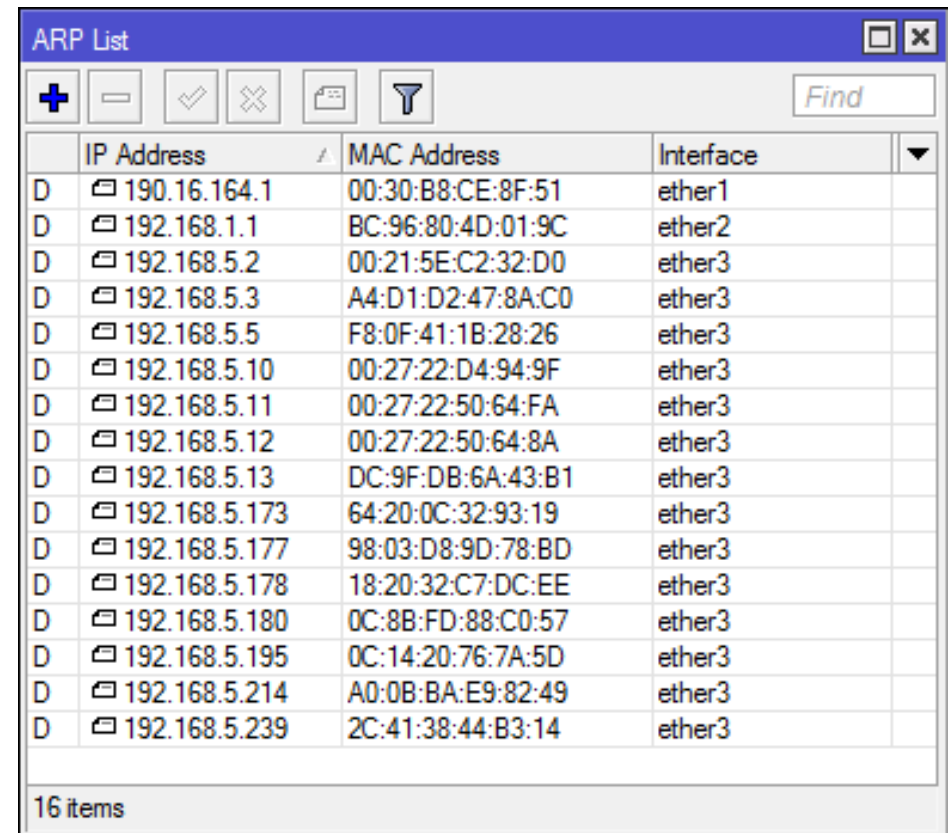


Modos de ARP

- Son 4 modos que se configuran por interfaz:
 - ➔ **Disabled:** la interfaz no hace Consultas ARP y tampoco responde Pedidos ARP.
 - ➔ **Reply Only:** sólo responde Pedidos ARP, no hace Consultas ARP.
 - ➔ **Enabled:** operación ARP completa.
 - ➔ **Proxy ARP:** la interfaz responde por todas las IPs de las redes que tenga configurada dicha interfaz.

Tabla ARP

- La tabla ARP muestra:
 - ➔ Dirección IP
 - ➔ Dirección MAC
 - ➔ Interfaz
- Esta tabla se completa dinámicamente mediante el protocolo ARP.



The screenshot shows a window titled "ARP List" with a toolbar containing icons for adding, removing, checking, unchecking, and filtering. A "Find" text box is also present. The table below lists 16 items, each with a status icon (D), an IP address, a MAC address, and an interface name.

	IP Address	MAC Address	Interface	
D	190.16.164.1	00:30:B8:CE:8F:51	ether1	
D	192.168.1.1	BC:96:80:4D:01:9C	ether2	
D	192.168.5.2	00:21:5E:C2:32:D0	ether3	
D	192.168.5.3	A4:D1:D2:47:8A:C0	ether3	
D	192.168.5.5	F8:0F:41:1B:28:26	ether3	
D	192.168.5.10	00:27:22:D4:94:9F	ether3	
D	192.168.5.11	00:27:22:50:64:FA	ether3	
D	192.168.5.12	00:27:22:50:64:8A	ether3	
D	192.168.5.13	DC:9F:DB:6A:43:B1	ether3	
D	192.168.5.173	64:20:0C:32:93:19	ether3	
D	192.168.5.177	98:03:D8:9D:78:BD	ether3	
D	192.168.5.178	18:20:32:C7:DC:EE	ether3	
D	192.168.5.180	0C:8B:FD:88:C0:57	ether3	
D	192.168.5.195	0C:14:20:76:7A:5D	ether3	
D	192.168.5.214	A0:0B:BA:E9:82:49	ether3	
D	192.168.5.239	2C:41:38:44:B3:14	ether3	

16 items



Tabla ARP estática

- ARP generalmente funciona de forma dinámica, pero por seguridad se puede configurar de forma estática.
- En este caso hay que crear las entradas de ARP (combinación IP y MAC) de forma manual.
- Los dispositivos no podrán acceder a Internet o a ciertos recursos fuera de su red local, si la entrada ARP no coincide con la configurada en el router.



Tabla ARP estática

Configuración

- Agregar una entrada estática a la tabla ARP.
- Configurar interfaz **arp=reply-only** para deshabilitar la creación ARP dinámica.

Interface <ether1>

General | Ethernet | Status | Traffic

Name: ether1

Type: Ethernet

MTU: 1500

L2 MTU:

Max L2 MTU:

MAC Address: 52:54:00:39:AE:1B

ARP:
enabled
disabled
enabled
proxy-arp
reply-only

OK
Cancel
Apply
Disable
Comment
Torch
Cable Test
Blink
Reset MAC Address

enabled | running | slave | link ok

Tabla ARP estática

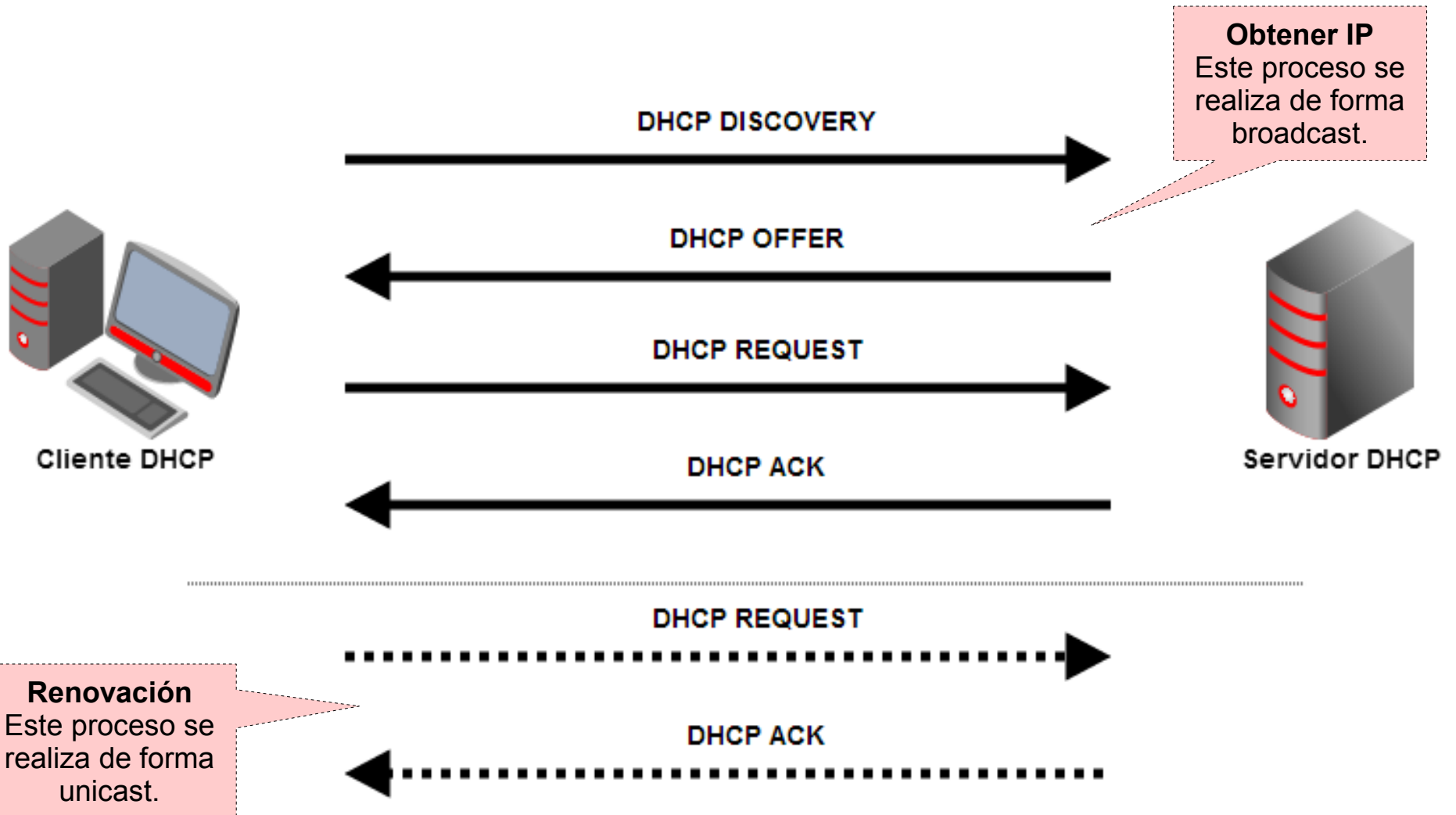
- Crear una entrada ARP estática para la notebook.
- Configurar **arp=reply-only** a la interfaz Ethernet.
- Deshabilitar / habilitar la interface o rebootear el router.
- Intentar cambiar la dirección IP de la notebook.
- Probar la conexión a internet.

Protocolo DHCP

- El Dynamic Host Configuration Protocol se usa para asignar IPs automáticamente a los dispositivos de una red.
- Además se pueden enviar otros parámetros IP y opciones personalizadas.
- Utiliza la arquitectura cliente / servidor.
- Los clientes DHCP se comunican con un servidor DHCP utilizando en un principio broadcast a nivel capa 2.



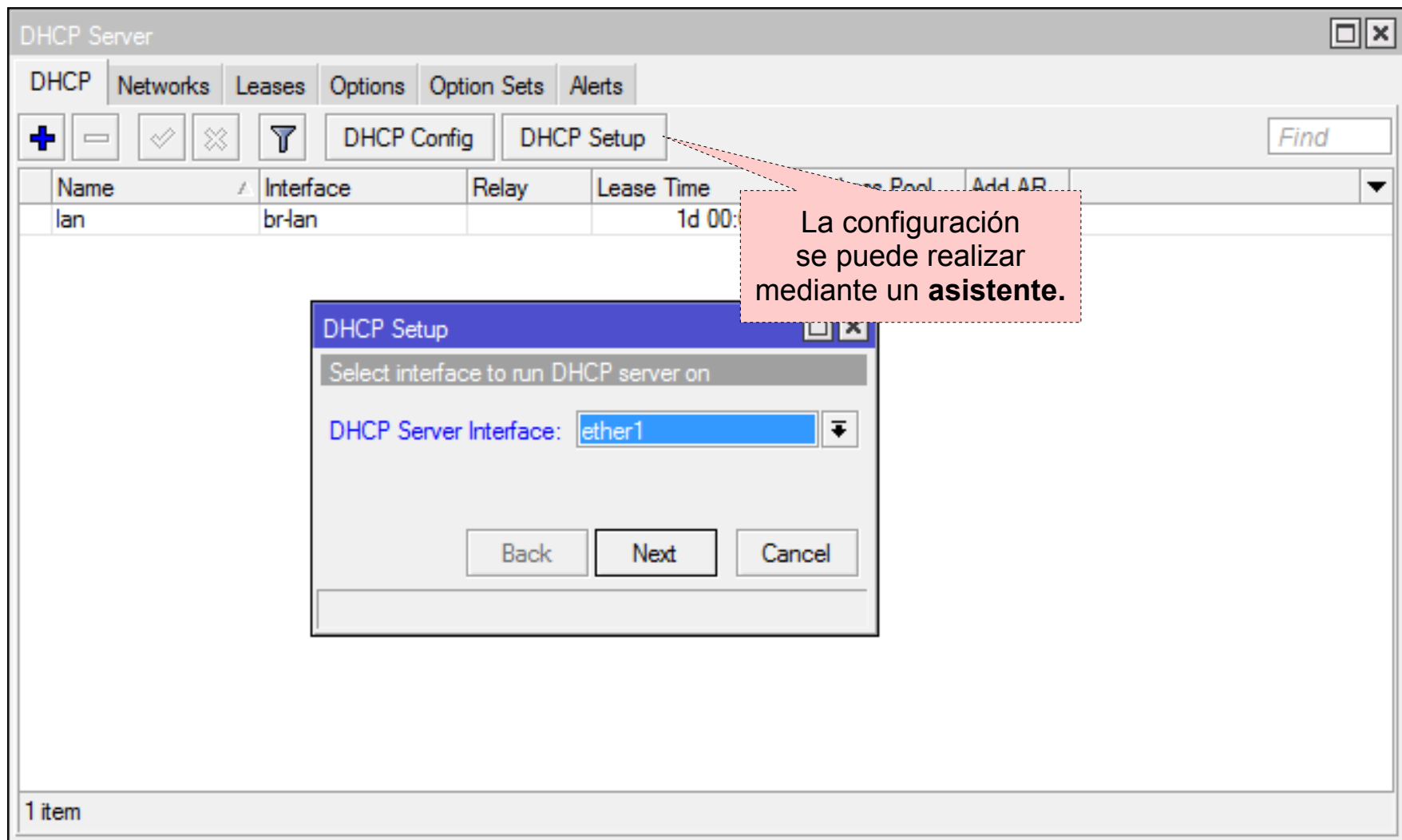
DHCP - Funcionamiento



DHCP - Configuración

- Para configurar el servidor DHCP, es requisito tener una dirección IP en la interfaz donde se va a levantar el servidor.
- Usar el botón de **DHCP Setup** para habilitar y configurar el servidor DHCP.
- Seguir las instrucciones de configuración.
- Una vez terminado el asistente, se agregan configuraciones en la solapa **DHCP, Networks** y en el menú **IP Pool**, dentro del menú principal IP.

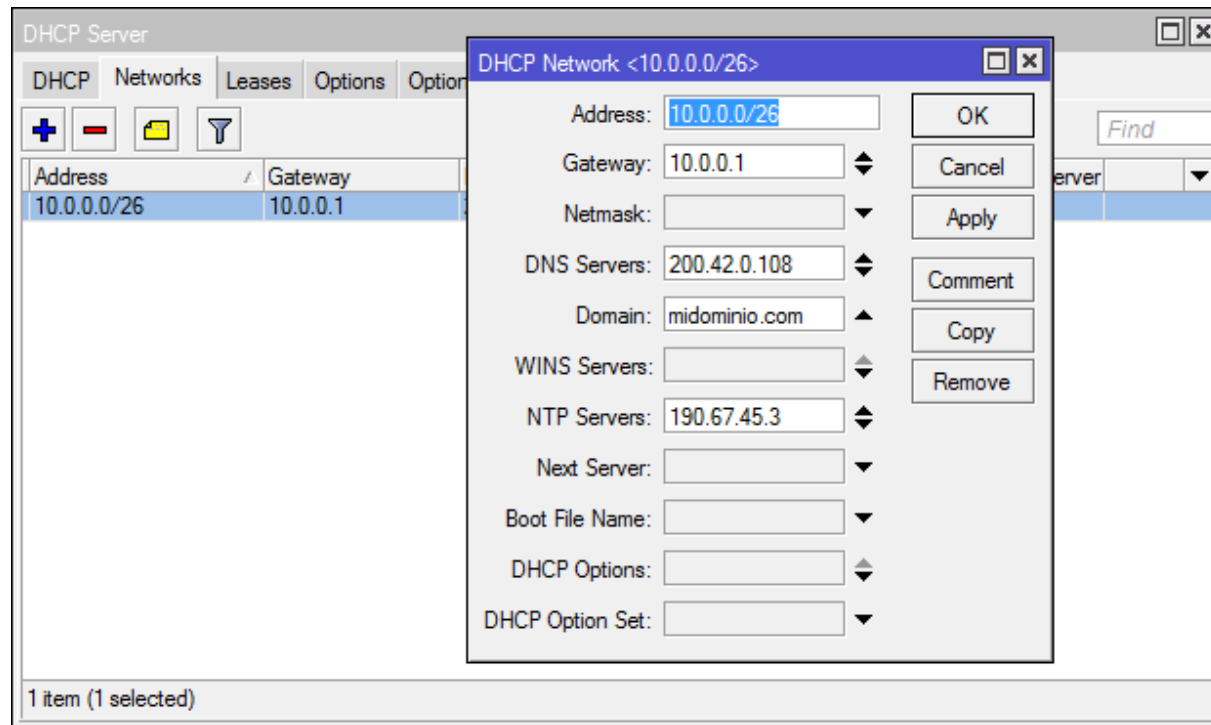
Servidor DHCP - Configuración





Servidor DHCP - Networks

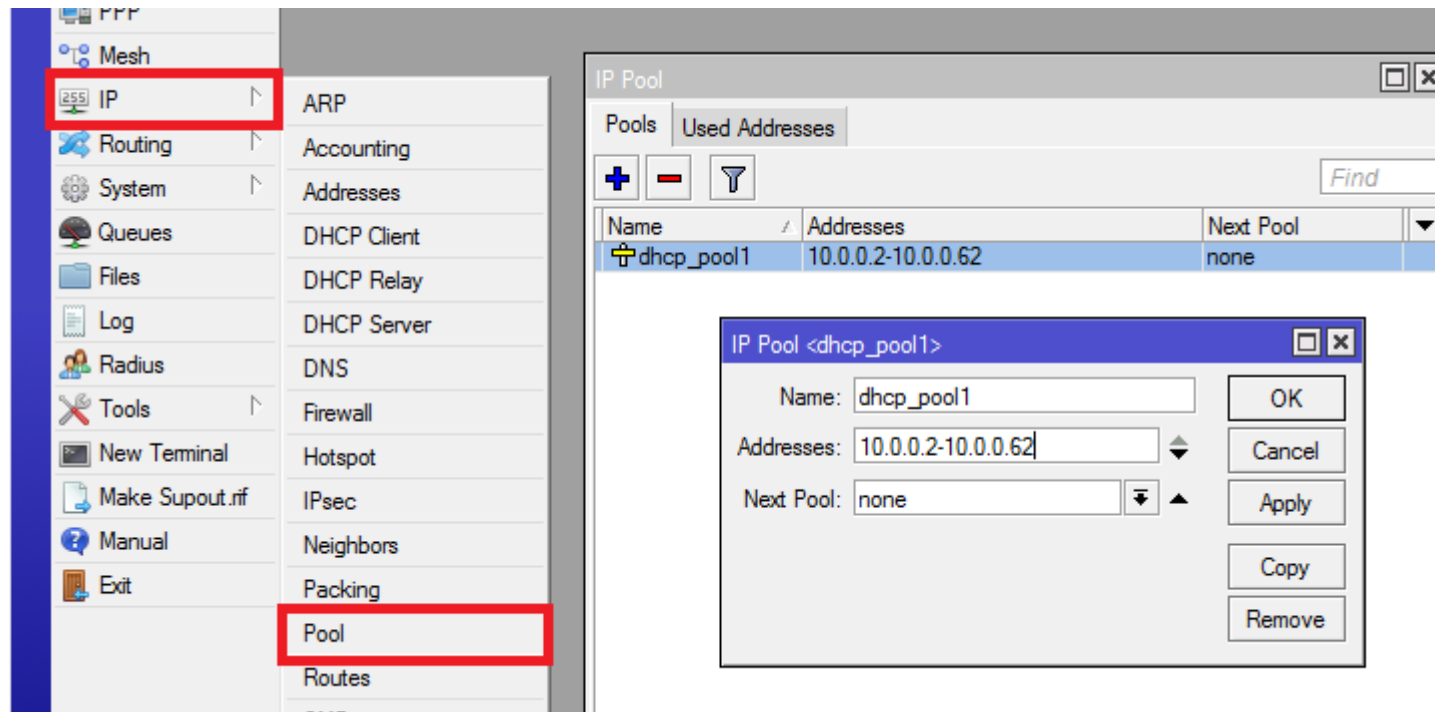
- Una vez configurado el servidor, se pueden ver los parámetros configurados en la solapa **Networks**.
- Los parámetros por defecto que se pueden configurar son: Gateway, Mascara de subred, DNS, Dominio, WINS Servers y NTP Server.





Servidor DHCP - Pool

- El rango de IPs a entregar de forma dinámica, se almacena en IP Pools.
- En caso de querer agregar o quitar IPs, se puede hacer desde este menú.





Servidor DHCP en un bridge

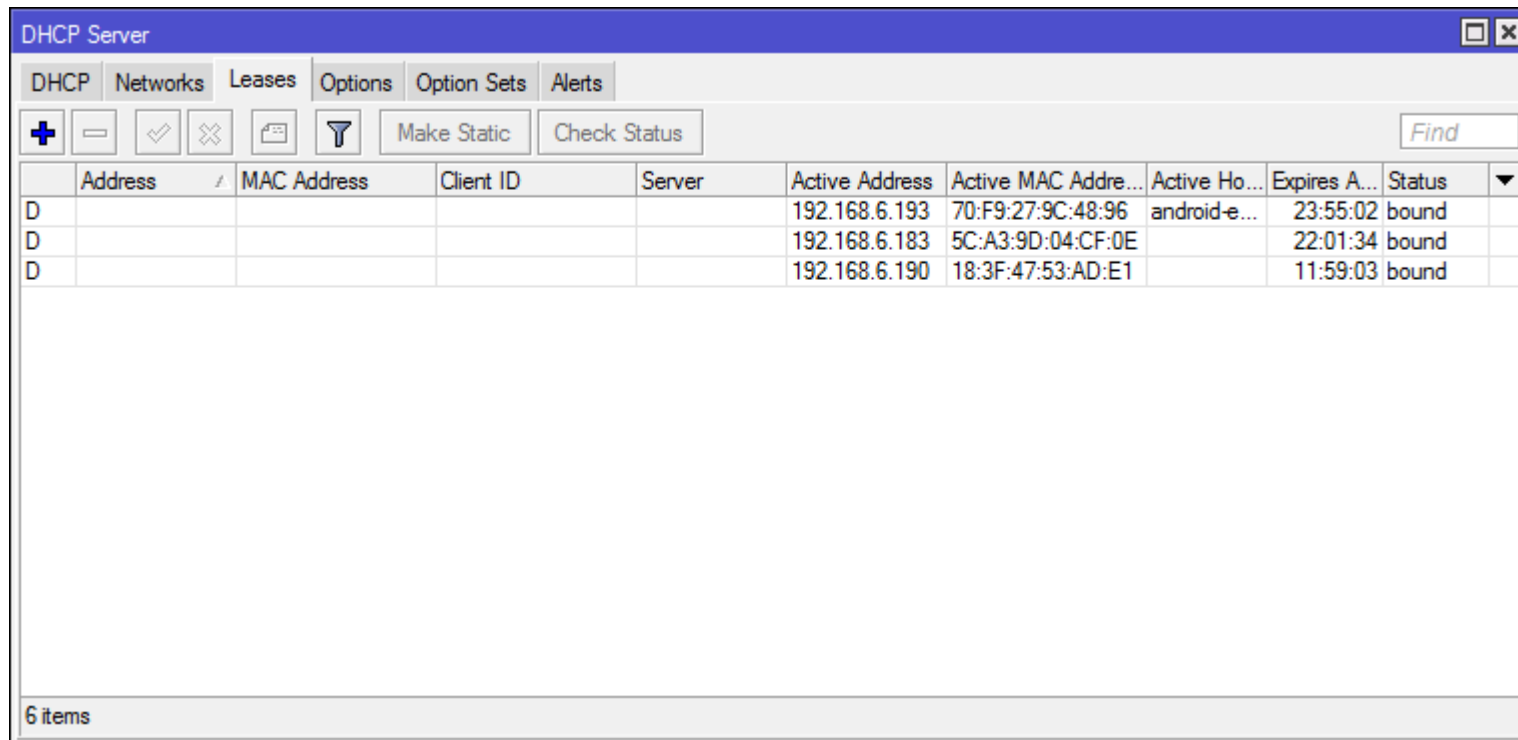
- Para configurar un servidor DHCP en un bridge, se debera crear el servidor DHCP sobre la interfaz bridge.
- La configuración de un servidor DHCP sobre una interfaz configurada como puerto de un bridge es invalida.

Servidor DHCP

- Configurar el servidor DHCP sobre la ethernet donde esta conectada la notebook.
- Cambiar la configuración de la notebook para que obtenga IP automáticamente (DHCP-Client).
- Verificar conexión a Internet.

Información del Servidor DHCP

- Se obtiene un listado de las asignaciones de IPs desde la solapa Leases dentro de la ventana **DHCP Server** que se encuentra en el menú IP.

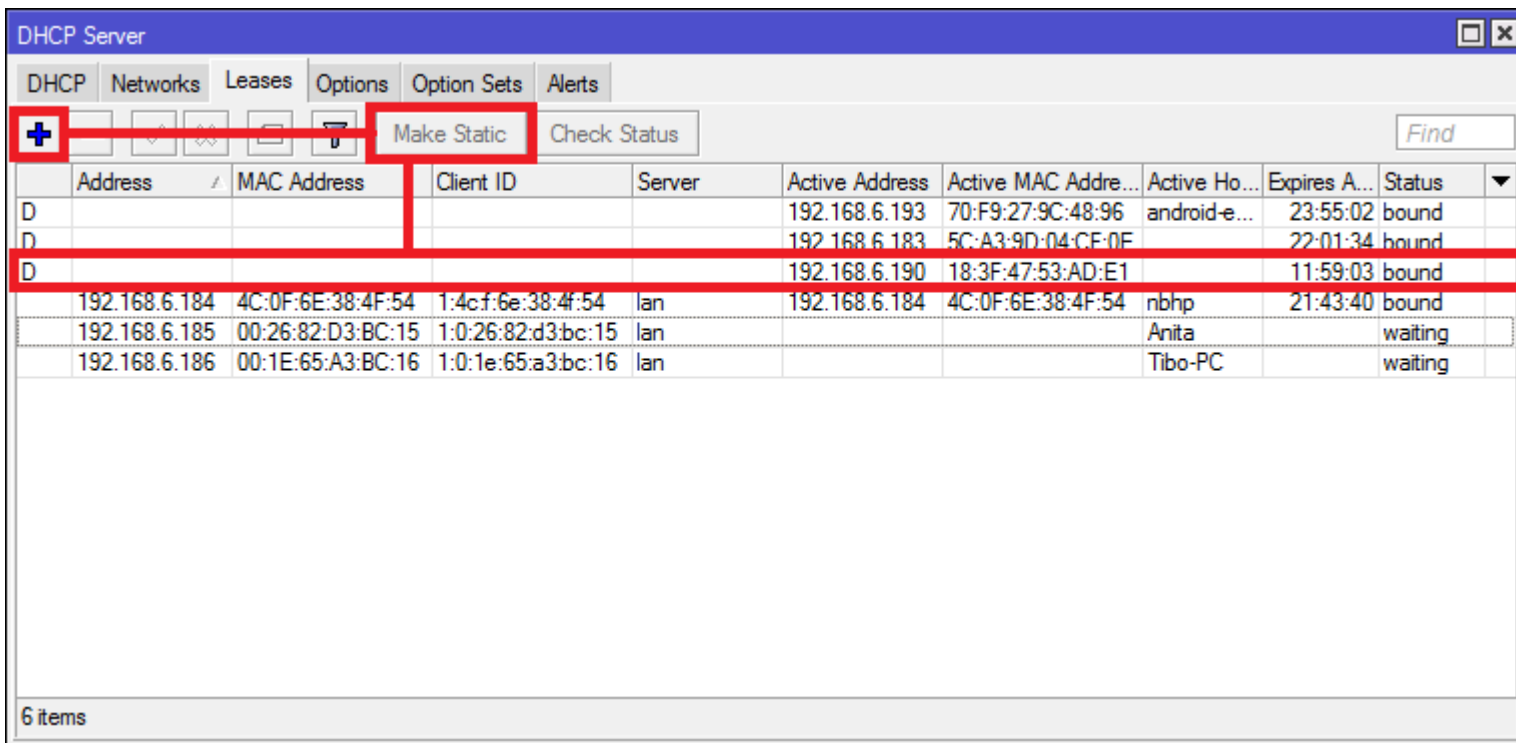


	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address...	Active Ho...	Expires A...	Status
D					192.168.6.193	70:F9:27:9C:48:96	android-e...	23:55:02	bound
D					192.168.6.183	5C:A3:9D:04:CF:0E		22:01:34	bound
D					192.168.6.190	18:3F:47:53:AD:E1		11:59:03	bound

6 items

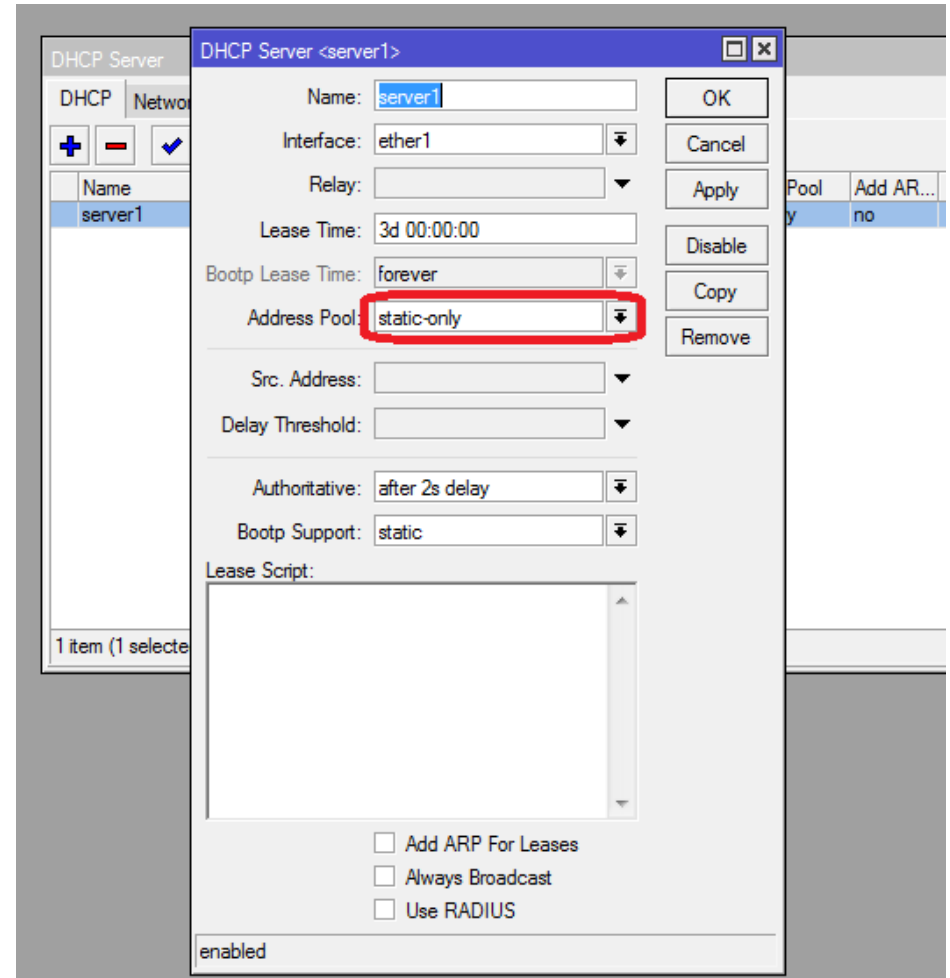
DHCP - Lease estático

- En un servidor DHCP, se pueden crear asignaciones estáticas.
- Esto se hace seleccionando una lease dinamica y convirtiendola en estática con el botón **Make Static**, o directamente agregandola con el botón "+".



DHCP - Lease estático

- El servidor DHCP podría funcionar sin los leases dinámicos.
- Los clientes recibirían IP sólo si antes se configuro una lease estática.
- Configurar **Address Pool** como **static-only**.
- **MiniLAB:** crear un lease estatico para la notebook.





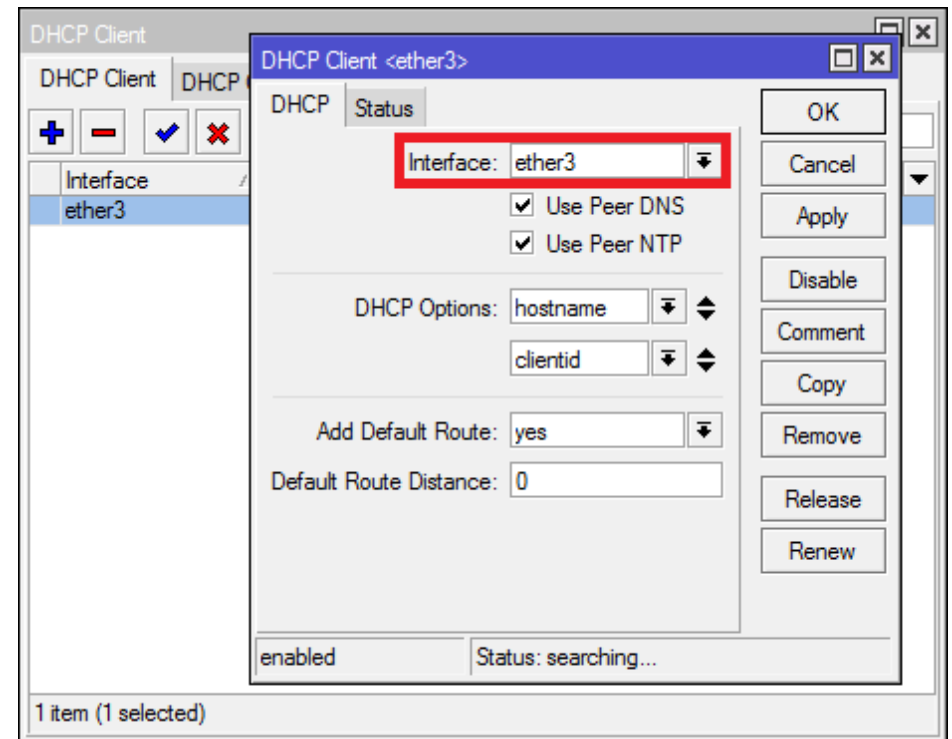
Cliente DHCP

- Se configura por interfaz y permite obtener:

- ➔ IP y máscara
- ➔ Gateway
- ➔ Servidores DNS
- ➔ Servidores NTP

- Opciones que el cliente le envía al servidor:

- ➔ Hostname
- ➔ Clientid



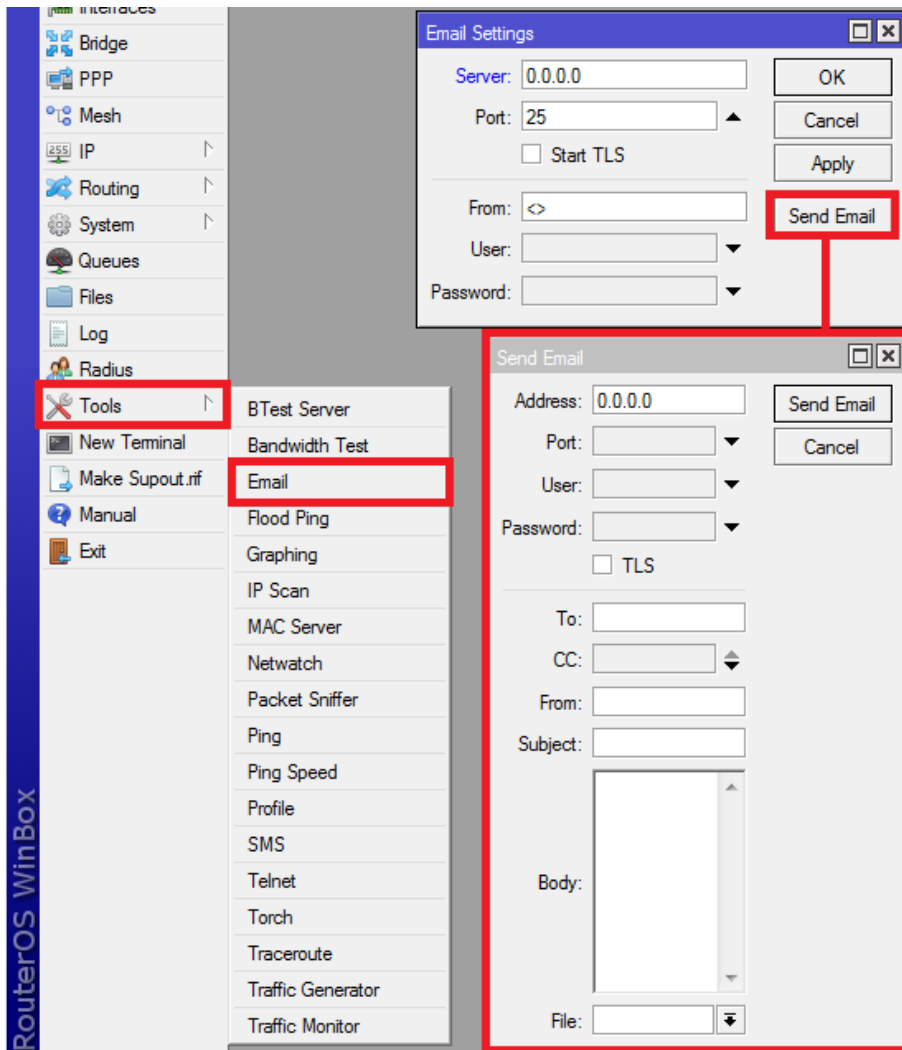


Herramientas avanzadas

- Vienen dentro del paquete **advanced-tools** y sirven como complemento de gestión y administración.
 - ➔ E-mail
 - ➔ Netwatch
 - ➔ Profiler (carga del CPU)

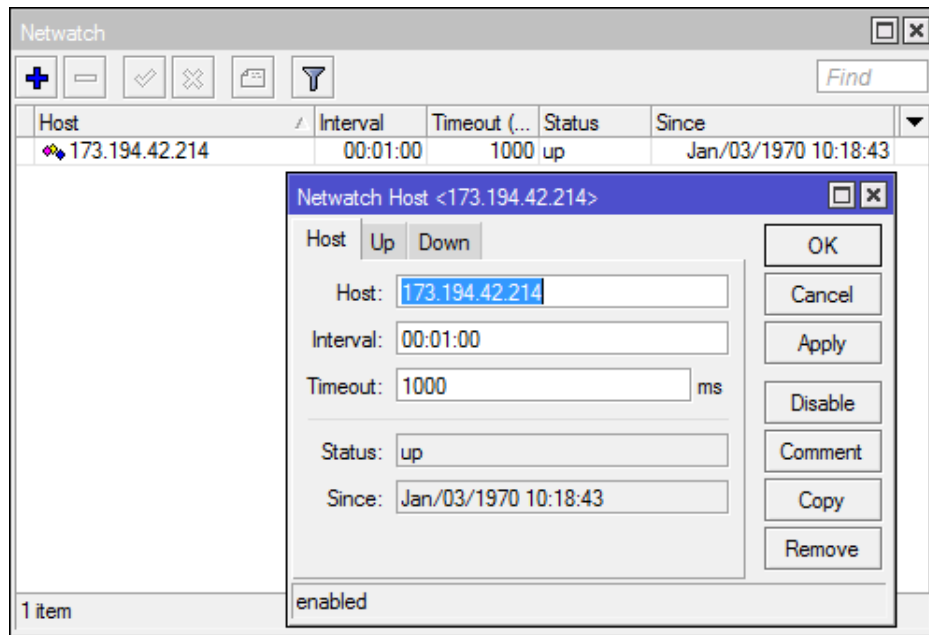
- Otras herramientas que vienen en el paquete **system** son:
 - ➔ Ping y Traceroute
 - ➔ Scheduler y Scripts

E-mail



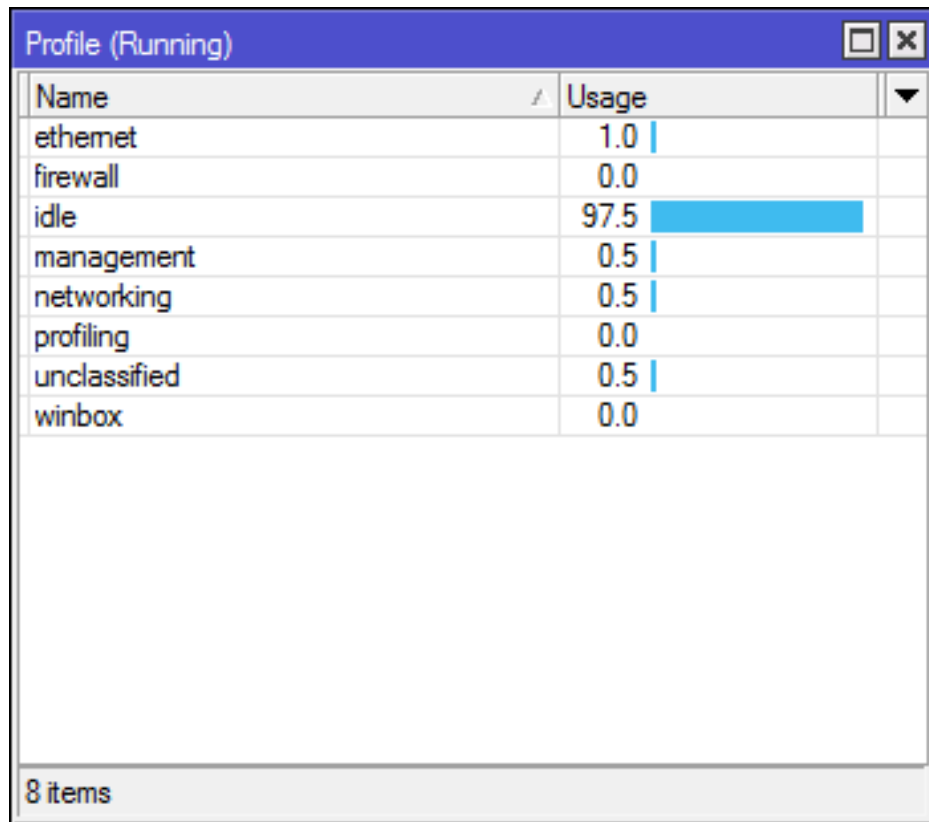
- Herramienta que se puede utilizar para enviar mails con archivos de backups o alertas.
- Parámetros importantes (dependen del SMTP server):
 - ➔ Dirección IP del servidor
 - ➔ Usuario y Password
 - ➔ From (Para)

Netwatch



- Permite monitorear dispositivos por ICMP y correr scripts.
- Parámetros a configurar:
 - ➔ Host (a monitorear)
 - ➔ Intervalo y Timeout
 - ➔ Scripts Up/Down

Profiler



Name	Usage
ethernet	1.0
firewall	0.0
idle	97.5
management	0.5
networking	0.5
profiling	0.0
unclassified	0.5
winbox	0.0

8 items

- Permite ver que funciones del router estan utilizando el CPU y en que medida.
- Idle no es un proceso, sino el CPU libre.

Diagnóstico avanzado

- Se puede hacer con dos archivos. Estos archivos .rif guardan la configuración y el estado del router en el momento que se generan.
 - ➔ **Supout.rif:** opción "Make Supout.rif", y enviarlo al soporte de MikroTik para que lo evalúen. Hay un visualizador de estos archivos dentro del área de usuarios del sitio de MikroTik.
 - ➔ **Autosupout.rif:** es un Supout.rif que se genera automáticamente en caso de fallas graves.

Modulo 6

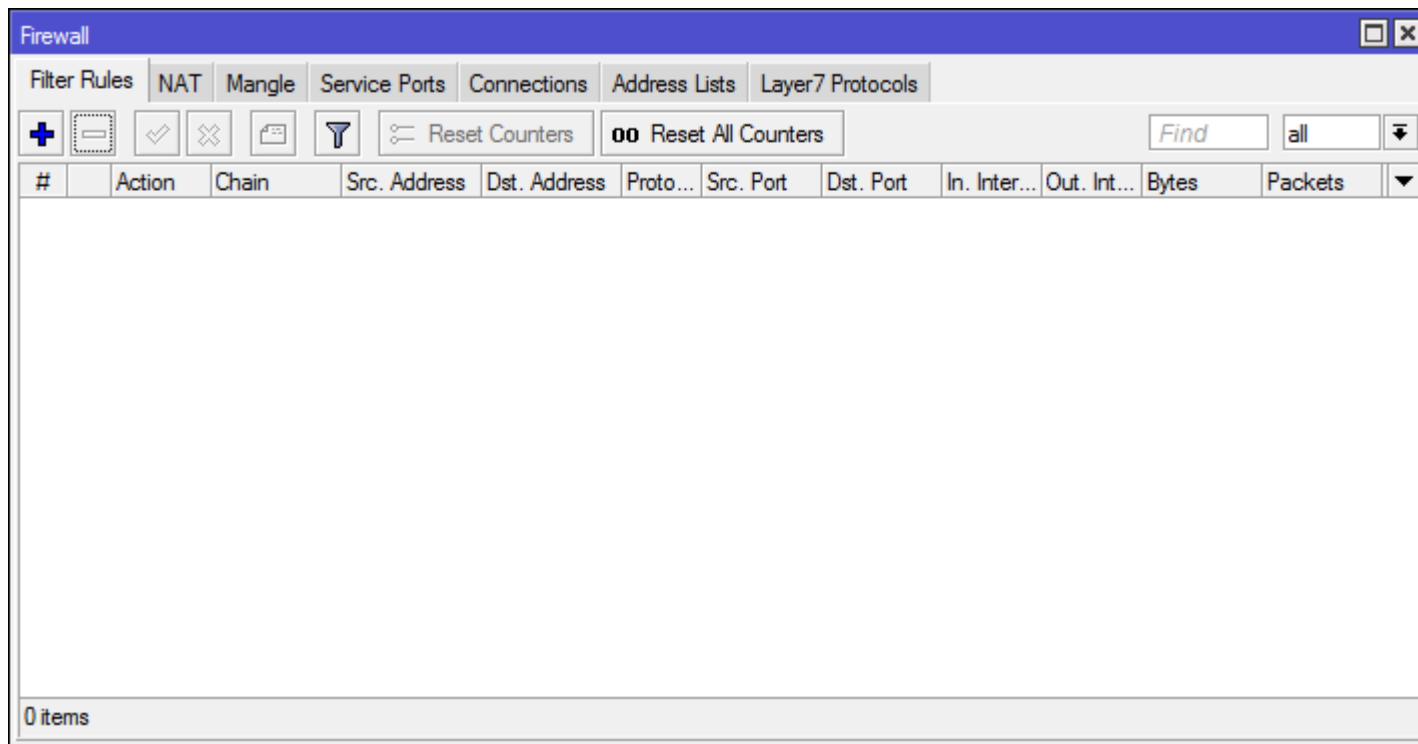
Firewall

Estructura del Firewall

- El Firewall nos permite identificar tráfico de las capas 2, 3 y 4 y ejecutar acciones. Por ejemplo:
 - ➔ Proteger al router o a los dispositivos conectados de accesos no autorizados.
 - ➔ Modificar ciertos campos de los encabezados UDP, TCP e IP.
 - ➔ Diferenciar el tráfico para su posterior control, bloqueo o modificación.

Estructura del Firewall

- El Firewall se encuentra en el menú "IP".



Estructura del Firewall

- Evalua el tráfico paquete por paquete.
- Opera con reglas que tienen dos componentes:
 - ➔ **Comparadores:** las condiciones que se deben cumplir para aplicar la regla. Algunos comparadores son: MAC origen, direccion IP origen y/o destino, protocolo, puerto origen y/o destino, interfaz de entrada o salida, etc.
 - ➔ **Acción:** la acción específica que se aplicará.
- Las reglas están ordenadas en cadenas, las cuales evaluan el tráfico en distintos puntos del router.
- Hay cadenas predefinidas (de fábrica), pero el usuario puede definir las propias.

Estructura del Firewall - Reglas

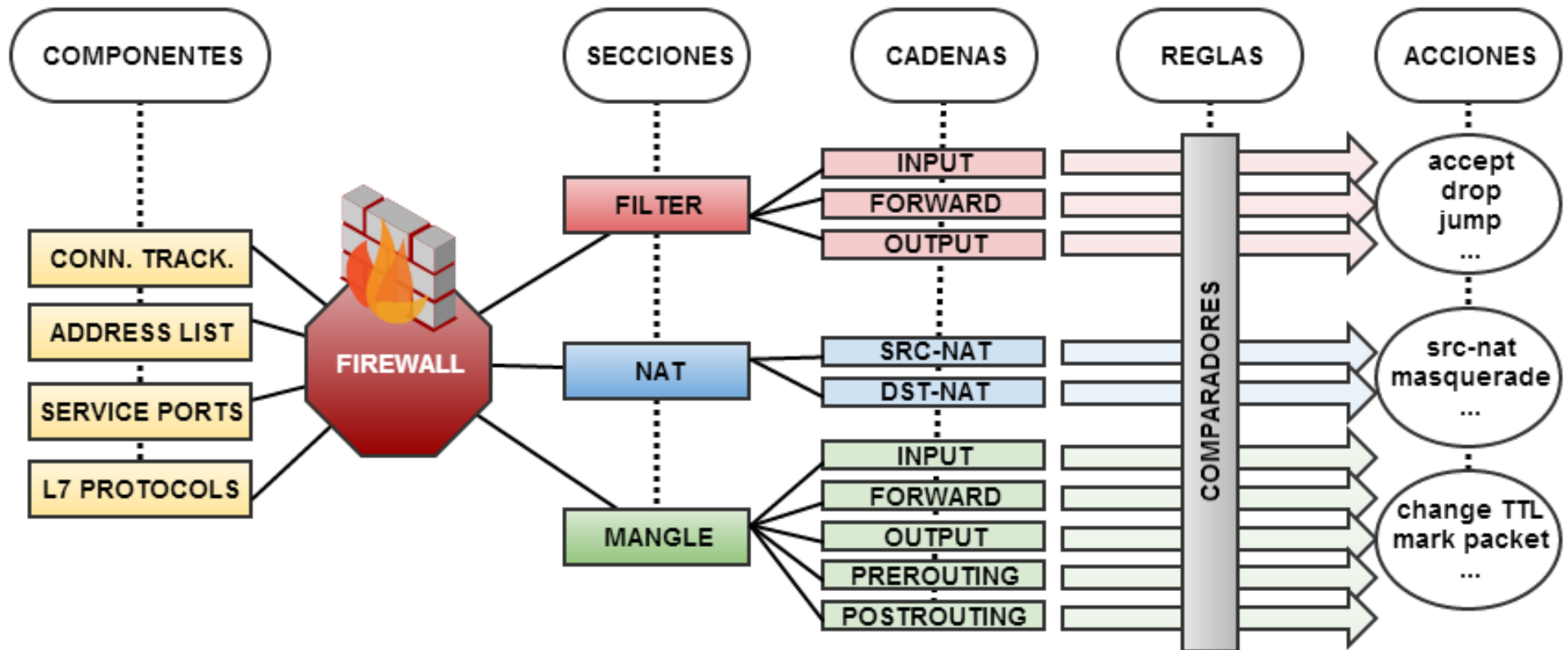
Los **comparadores** se configuran desde las solapas General, Advanced y Extra. Algunos comparadores son exclusivos de ciertas secciones.

La lista de **acciones** disponibles a a depender de la sección del Firewall donde se cree la regla.

Estructura del Firewall

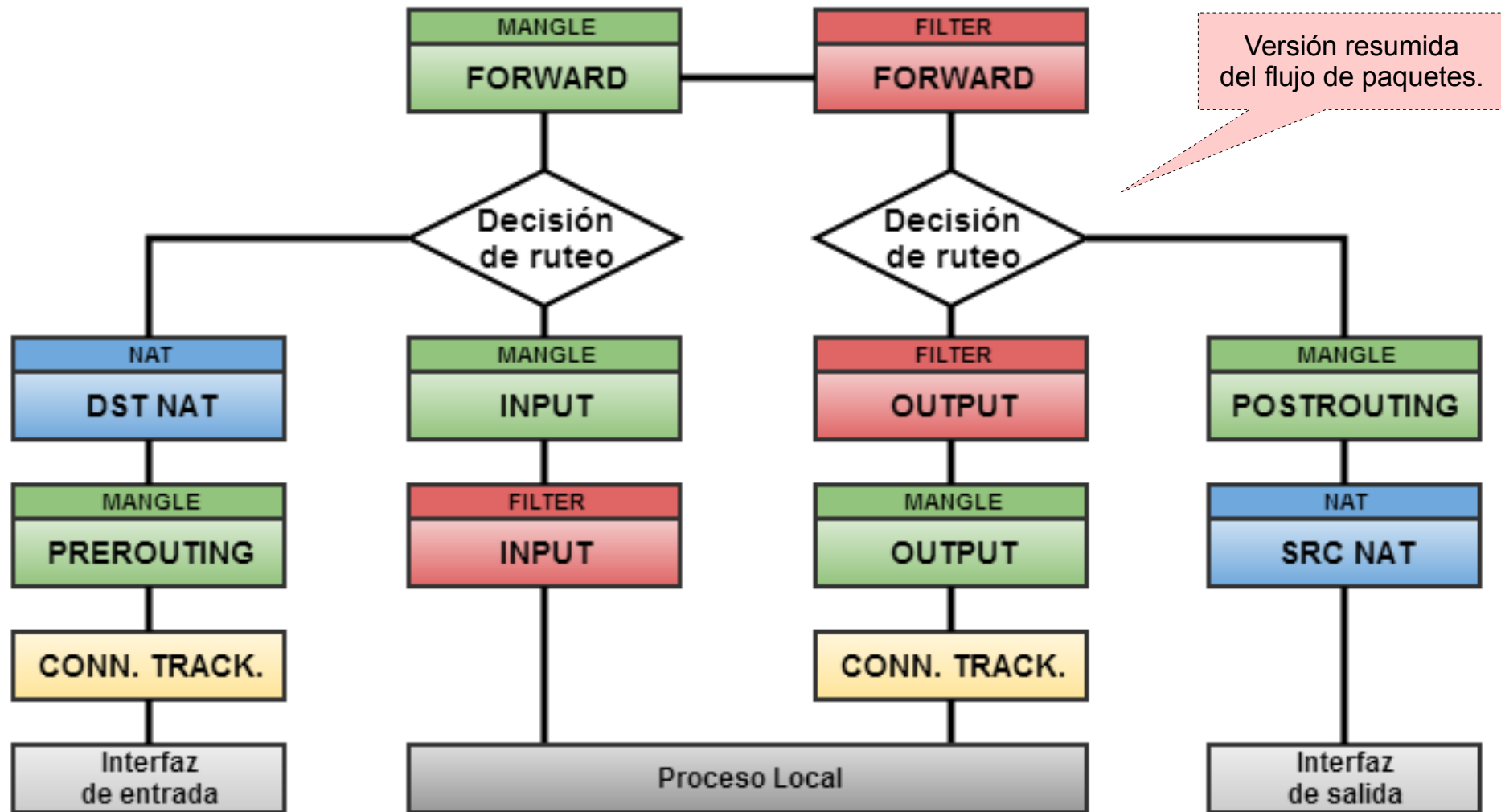
- El Firewall de RouterOS tiene 3 secciones principales que se encargan de realizar distintas funciones: **Filter**, **NAT** y **Mangle**.
- Dentro de cada sección se configuran las reglas, ordenadas en cadenas.
- Es importante conocer los siguientes esquemas:
 - ➔ **Estructura general:** para conocer de una forma gráfica los componentes y secciones del Firewall.
 - ➔ **Flujo de paquetes:** esencial para saber que esta pasando con los paquetes y en que orden. Comprender el flujo de paquetes es requisito para poder configurar reglas de manera adecuada.

Estructura general





Flujo de paquetes





Connection Tracking

- Connection Tracking (Conn. Track.), gestiona la información acerca de todas las conexiones activas.
- Crea una tabla de conexiones.
- Debe estar habilitado para que funcionen todos los comparadores del firewall dentro de Filter, NAT y Mangle.
- Por defecto viene en modo automático.

Connection Tracking

admin@malabia.psdtec.com (MiRouter) - WinBox v6.2 on RB751U-2HnD (mipsbe)

Safe Mode

Hide Passwords

RouterOS WinBox

Quick Set
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.tif
Manual
Exit

Firewall

Filter Rules NAT Mangle Service Ports Connections

Tracking

	Src. Address	Dst. Address	Proto...	Con...
A	192.168.6.184:50374	108.160.165.211:443	6 (tcp)	
A	192.168.6.184:50373	54.207.127.196:80	6 (tcp)	
A	192.168.6.184:50372	23.21.220.92:443	6 (tcp)	
A	192.168.6.184:50368	173.194.42.50:443	6 (tcp)	
A	192.168.6.184:50342	173.194.42.36:443	6 (tcp)	
A	192.168.6.184:50322	95.211.113.1:443	6 (tcp)	
A	192.168.6.184:50165	192.168.6.254:58291	6 (tcp)	
A	192.168.6.184:49614	173.194.42.54:443	6 (tcp)	
A	192.168.6.184:49613	74.125.137.125:5222	6 (tcp)	
A	192.168.6.184:49209	108.160.163.103:80	6 (tcp)	
U	192.168.6.184:17500	255.255.255.255:17...	17 (u...	
U	192.168.6.184:17500	192.168.6.255:17500	17 (u...	
U	190.191.251.1	224.0.0.1	2 (ig...	
U	190.191.250.1	224.0.0.1	2 (ig...	
U	190.191.249.1	224.0.0.1	2 (ig...	
U	190.191.248.1	224.0.0.1	2 (ig...	
U	190.191.247.1	224.0.0.1	2 (ig...	

65 items

Max Entries

Connection Tracking

Enabled: yes

TCP Syn Sent Timeout: auto

TCP Syn Received Timeout: yes

TCP Syn Received Timeout: 00:00:05

TCP Established Timeout: 1d 00:00:00

TCP Fin Wait Timeout: 00:00:10

TCP Close Wait Timeout: 00:00:10

TCP Last Ack Timeout: 00:00:10

TCP Time Wait: 00:00:10

TCP Close: 00:00:10

UDP Timeout: 00:00:10

UDP Stream Timeout: 00:03:00

ICMP Timeout: 00:00:10

Generic Timeout: 00:10:00

☐ TCP SynCookie

OK

Cancel

Apply

Find



Estado TCP (tcp-state)

- Parámetro que se puede consultar en cada conexión TCP que aparezca en la tabla de Connection Tracking (solapa "Connections").
- Asumiendo que PC A esta iniciando una conexión con PC B:
 - ➔ **established:** (desde PC A o B) una conexión TCP con el host remoto esta establecida de forma completa, habilitando el intercambio de datos.
 - ➔ **close:** (desde PC A o B) indica que se esta esperando para cerrar la conexión por un pedido del host remoto.
 - ➔ **time-wait:** (desde PC A o B) la conexión queda en estado de espera para asegurarse que el host remoto haya recibido la confirmación de cierre (ocurre luego de "close").
 - ➔ **syn-sent:** (desde PC A) indica que se ha enviado un segmento "syn" y la conexión queda a la espera de la respuesta del host remoto.
 - ➔ **syn-received:** (desde PC B) se ha enviado el segmento "syn+ack". La conexión queda a la espera de la confirmación del host remoto para poder establecerse de forma completa.



Estado de conexión (connection-state)

- Distintos de los estados de TCP!
- Parámetro que se puede utilizar como comparador en las reglas de firewall para todo tipo de tráfico, en las secciones Filter o Mangle.
- El Connection Tracking asigna un estado para cada paquete:
 - ➔ **invalid**: paquete que ya no forma parte de ninguna conexión conocida.
 - ➔ **new**: paquete que esta abriendo una nueva conexión. Ej.: segmento TCP "syn" o primer segmento UDP.
 - ➔ **established**: paquete que pertenece a una conexión establecida.
 - ➔ **related**: paquete que crea una nueva conexión relativa a alguna conexión ya abierta.

Estado de conexión (connection-state)

- El Connection Tracking permite el seguimiento de las "conexiones UDP", aunque UDP no establezca conexiones.
- El primer paquete será interpretado con estado **new**, el resto puede ser interpretado como **established** mientras no se alcance el valor UDP Timeout.

Filosofía de seguridad

- Antes de crear reglas, es importante elegir algún criterio para diseñar el firewall, que puede estar basado en alguno de los siguientes puntos:
 - ➔ Se confía en la red interna, las reglas afectarán a lo que viene desde la red externa.
 - ➔ Se bloquea todo por defecto, y se agregan reglas para permitir tráfico deseado.
 - ➔ Se acepta todo por defecto, y se agregan reglas para bloquear tráfico no deseado.

Sección Filter

"Proteger al router o a los dispositivos conectados de accesos no autorizados."

- Las reglas se pueden colocar en tres cadenas por defecto, para Filter las cadenas son:
 - ➔ **input:** tráfico dirigido al router.
 - ➔ **output:** tráfico generado por el router.
 - ➔ **forward:** tráfico que pasa a través del router.
- Cada cadena se encarga de procesar el tráfico en distintos puntos.



Sección Filter - Acciones

- **Comunes** (se encuentran en Filter, NAT y Mangle)
 - ➔ **accept:** acepta el paquete, el cual no pasa a la siguiente regla.
 - ➔ **add-dst-to-address-list:** agrega la dirección destino a un Address List. El paquete pasa a la siguiente regla.
 - ➔ **add-src-to-address-list:** agrega la dirección origen a un Address List. El paquete pasa a la siguiente regla.
 - ➔ **jump:** saltar una cadena personalizada. El paquete pasa a la primer regla de la cadena personalizada.
 - ➔ **return:** volver de nuevo a la cadena original en la que se encontraba el paquete antes de haber saltado. El paquete pasa a la siguiente regla a la regla con acción jump de la cadena original.



Sección Filter - Acciones

■ Comunes (se encuentran en Filter, NAT y Mangle)

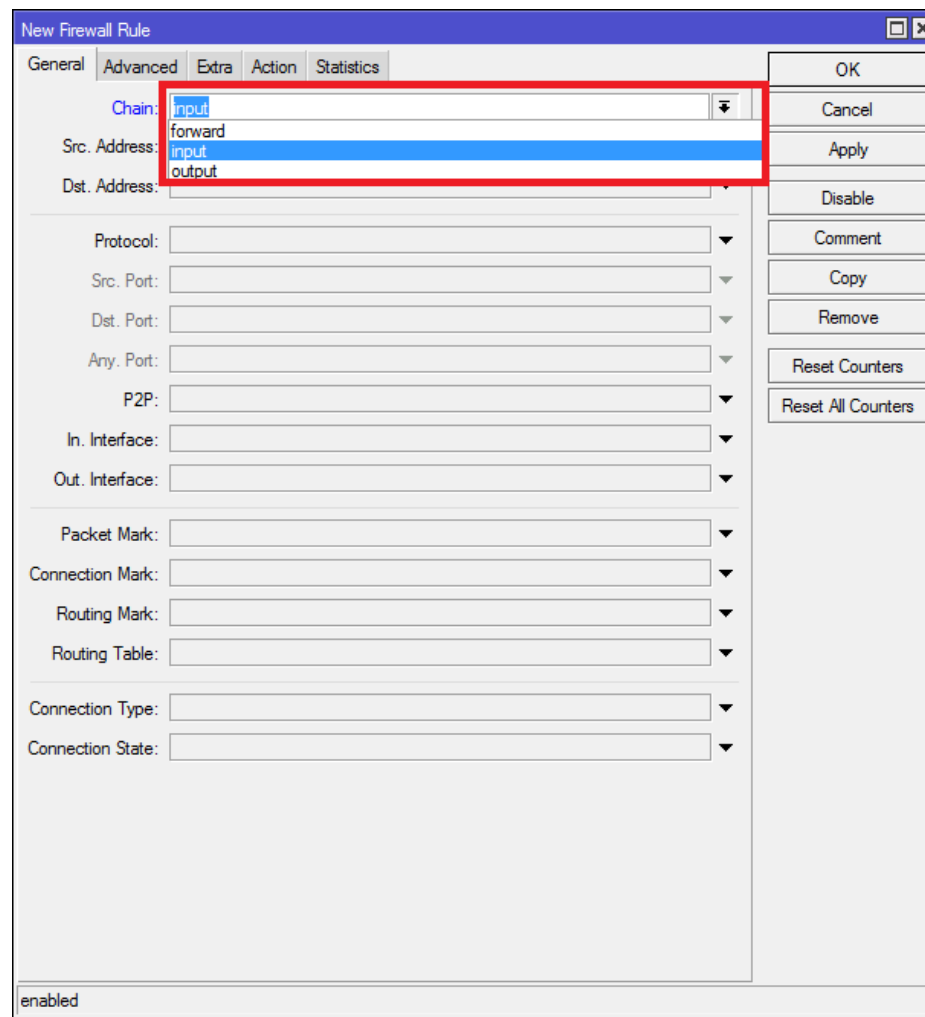
- ➔ **log:** escribe un mensaje en el log, con la siguiente información: *in-interface, out-interface, src-mac, protocol, src-ip:port->dst-ip:port* y longitud del paquete. El paquete pasa a la siguiente regla.
- ➔ **passthrough:** pasar a la siguiente regla (útil para estadísticas).

■ Exclusivas de Filter

- ➔ **drop:** descartar el paquete de forma "silenciosa". El paquete no pasa a la próxima regla.
- ➔ **reject:** descartar el paquete, devolviendo un mensaje de ICMP al remitente. El paquete no pasa a la próxima regla.
- ➔ **tarpit:** captura y retiene conexiones TCP. El paquete no pasa a la próxima regla.

Filter Input

- La cadena input analiza el tráfico dirigido al router.
- Las reglas que se agregan en la cadena input tienen como objetivo proteger al router de accesos no autorizados (hackers por ejemplo).



Filter Input

- Añadir una regla que identifique la IP de la notebook y que la acción sea "accept".
- Añadir una regla con acción "drop". Como no agregamos comparadores en esta segunda regla, estamos identificando todo el tráfico.
- Posicionar la regla de accept debajo de la de drop.
- Posicionar la regla de accept arriba de la de drop.
- Sacar conclusiones.

Filter Forward

- Procesa el tráfico que intenta atravesar el router.
- Por ejemplo, procesa el tráfico desde y hacia los clientes o usuarios conectados al router.

The screenshot shows the 'New Firewall Rule' dialog box with the 'General' tab active. The 'Chain' dropdown menu is open, displaying three options: 'forward', 'input', and 'output'. The 'forward' option is selected and highlighted in blue. A red rectangular box highlights the dropdown menu area. Below the 'Chain' dropdown, the 'Src. Address' and 'Dst. Address' fields are empty. The 'Protocol' dropdown is set to 'any'. The 'Src. Port', 'Dst. Port', and 'Any. Port' fields are empty. The 'P2P' dropdown is set to 'no'. The 'In. Interface' and 'Out. Interface' dropdowns are empty. The 'Packet Mark', 'Connection Mark', 'Routing Mark', and 'Routing Table' dropdowns are empty. The 'Connection Type' and 'Connection State' dropdowns are empty. On the right side of the dialog, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', and 'Reset All Counters'. At the bottom left, the 'enabled' checkbox is checked.

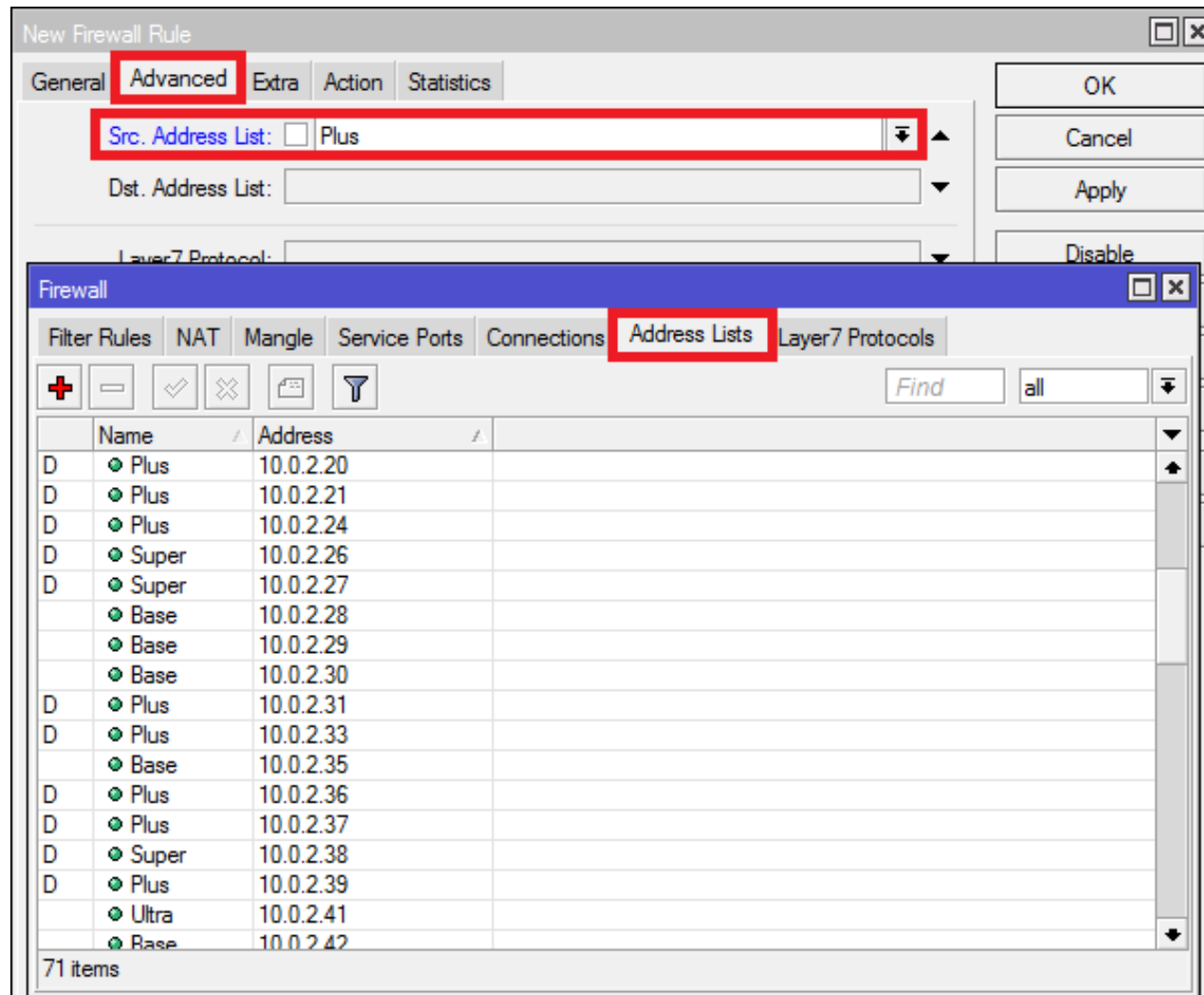
Filter Forward

- Crear una regla para bloquear el protocolo ICMP.
 - Crear una regla para bloquear el puerto TCP 80 (HTTP).
 - Tratar de abrir <http://www.mikrotik.com>.
 - Tratar de abrir <http://192.168.x.254>.
 - Por que funciona el WebFig?
-

Address List

- Address List habilita la posibilidad de filtrar varios grupos de direcciones IP en una sola regla.
- Se pueden agregar redes, rangos o una sola dirección IP.
- Se pueden agregar IPs automáticamente a una lista y luego aplicar una acción sobre la misma.
- Una vez creada la lista, se la puede usar como comparador en cualquier sección del Firewall.

Address List



Address List

- Crear una lista llamada "Bloqueos" con un par de IPs públicas: 200.42.0.108 y 8.8.4.4
- Crear una regla de forward y utilizar el Address List previamente creado para bloquear todo el tráfico ICMP a esos destinos. Elegir como acción Drop o Reject.
- Intentar hacer ping a los destinos del Address List.
- Sacar conclusiones.



Sección NAT

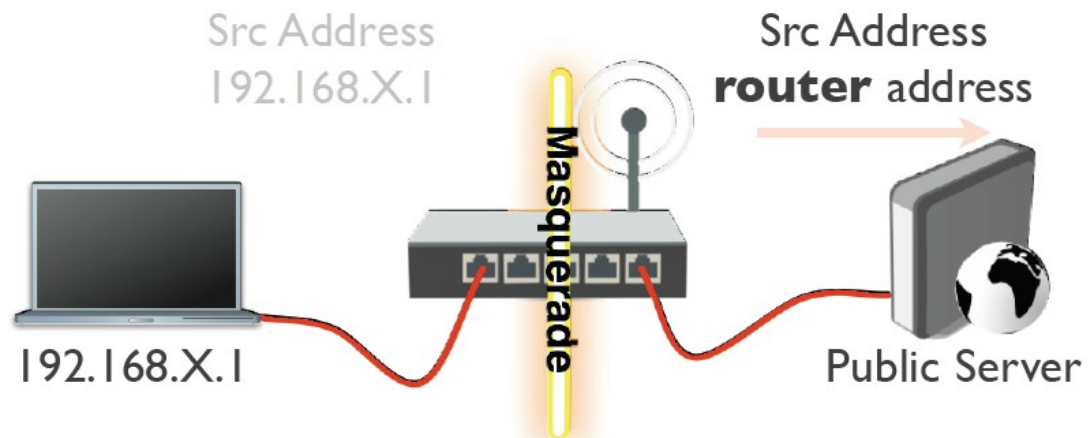
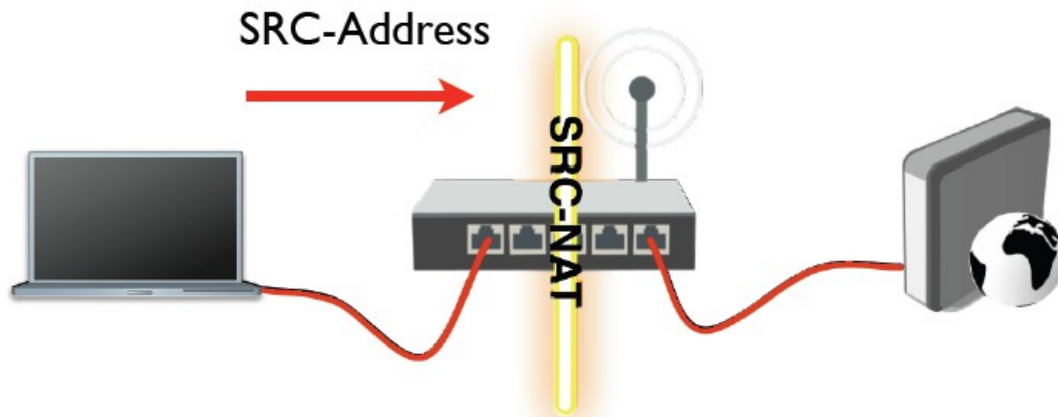
"Modificar ciertos campos de los encabezados UDP, TCP e IP".

- El router es capaz de cambiar la IP (y/o el puerto) origen o la IP (y/o el puerto) destino de los paquetes que fluyen a través de el.
- Este proceso se denomina src-nat (Source NAT) o dst-nat (Destination NAT).
- Dos cadenas de fábrica.
 - ➔ **srcnat:** hace cambios justo antes de que el paquete abandone el router.
 - ➔ **dstnat:** hace cambios a penas el paquete entra al router.

Source NAT (srcnat)

- En la cadena srcnat se puede hacer un cambio de dirección IP y/o puerto origen por otras direcciones IP y/o puerto.
- Aplicación típica es esconder IPs de redes privadas detrás de una o mas direcciones publicas.
- Acciones destacadas de la cadena srcnat:
 - ➔ **src-nat:** cambia la IP y/o puerto origen de un paquete a una IP y/o puerto local especifico.
 - ➔ **masquerade:** cambia la IP origen de un paquete por la IP de la interfaz por donde salga dicho paquete.

Source NAT (srcnat)

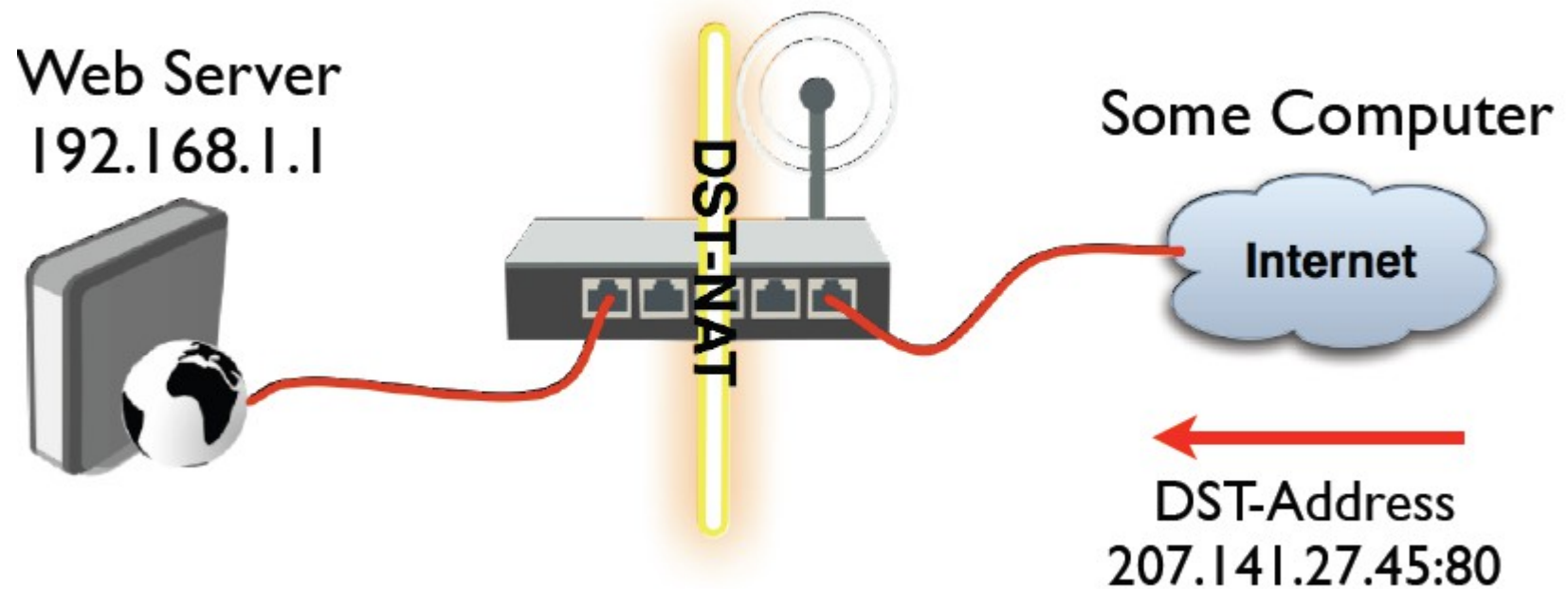




Destination NAT (dstnat)

- La cadena dstnat permite cambiar la dirección y/o el puerto del receptor a alguna otra dirección y puerto alcanzable por el router.
- Típicamente usado para acceder servicios en una red privada desde direcciones publicas accediendo las direcciones publicas que enmáscaran alguna red.
- Acciones destacadas de la cadena dstnat:
 - ➔ **dst-nat:** cambia la IP y/o puerto destino de un paquete a una IP y/o puerto especifico.
 - ➔ **redirect:** cambia el puerto destino de un paquete por un puerto perteneciente a un servicio local.

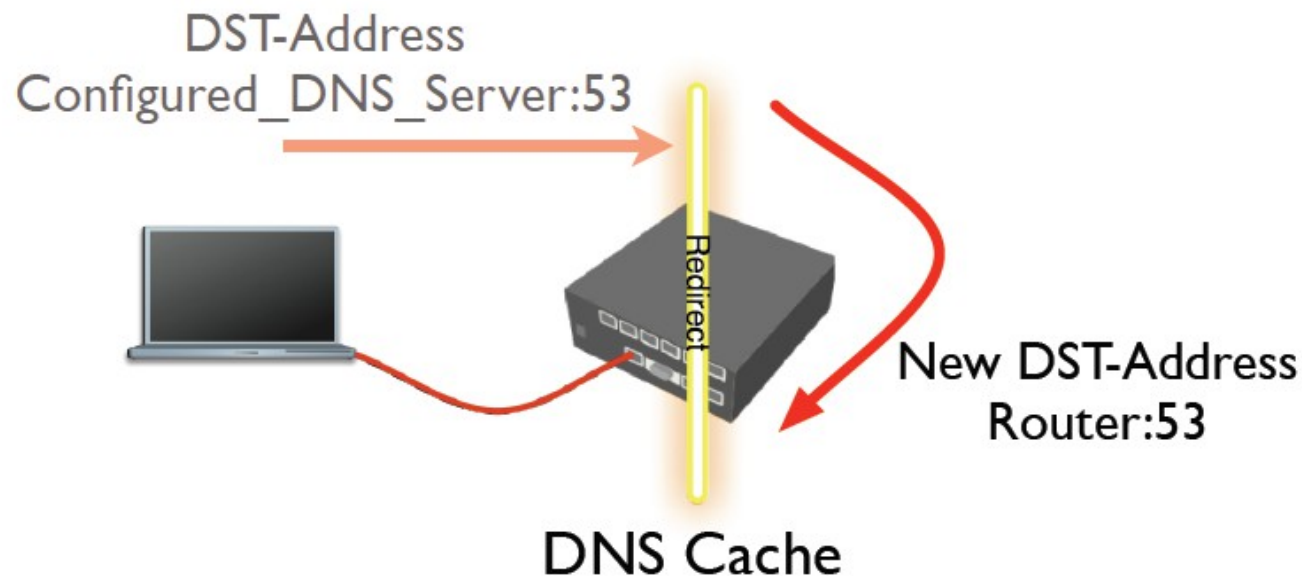
Acción dst-nat





Acción redirect

- Es un tipo especial de dstnat.
- Esta acción **sólo** redirige los paquetes al router mismo.
- Se puede utilizar para los servicios de proxy (DNS, HTTP).



Acción redirect - Configuración

NAT Rule <53>

General Advanced Extra Action Statistics

Chain: dstnat

Src. Address:

Dst. Address:

Protocol: ☐ 17 (udp)

Src. Port:

Dst. Port: ☐ 53

Any. Port:

In. Interface:

Out. Interface:

NAT Rule <53>

General Advanced Extra Action Statistics

Action: redirect

To Ports: 53

Acción **dst-nat** y **redirect**

- **dst-nat:** crear una regla para que cada vez que se inicie una conexión al puerto TCP 9080 desde la wlan1, el tráfico se termine destinando a la IP del servidor web local.
- **redirect:** crear una regla para capturar el tráfico que viene desde la ether1 al puerto 80 y reenviarlo al servidor web en la red privada.

Modulo 7

QoS

QoS - Quality of Service

- Técnica para administrar los recursos de ancho de banda, en lugar de simplemente limitar ciertos nodos o equipos.
- Con QoS podemos priorizar tráfico basándonos en ciertas métricas, lo cual es útil para:
 - ➔ Aplicaciones críticas
 - ➔ Tráfico sensible como voz y video IP.



Simple Queue

- La forma más fácil de controlar el ancho de banda, mediante reglas que limitan:
 - ➔ Bajada
 - ➔ Subida
 - ➔ Bajada + Subida
- El orden de las reglas es importante.
- La configuración se encuentra en el menu "Queue", solapa "Simple Queues".

Simple Queue

Queue List						
Simple Queues Interface Queues Queue Tree Queue Types						
<div> + - ✓ ✗ 📄 🔍 Reset Counters 00 Reset All Counters Find </div>						
#	Name	Target Address	Rx Max Limit	Tx Max Limit	Packet Marks	
3	Ibarra Laura Veronica	10.240.1.194	384k	2M		
4	Pagnini Gabriela Ana	10.240.1.193	384k	2M		
5	Mamani Damian	10.240.1.192	384k	2M		
6	Escalada Gabriela	10.240.1.191	384k	2M		
7	Benitez Diana Laura	10.240.1.34	384k	2M		
8	Coronel Yazmin	10.240.1.186	384k	2M		
9	Diaz Alfredo	10.240.1.187	384k	2M		
10	Escobar Heman	10.240.1.43	384k	2M		
11	Zenobi Alejandro	10.240.1.190	384k	2M		
12	Sosa Lorena	10.240.1.185	384k	2M		
13	Biscik Angel	10.240.1.184	384k	2M		
14	Morganti Gabriela	10.240.1.180	384k	2M		
15	Gonzalez Omar	10.240.1.178	384k	2M		
16	Blabuena Epifania	10.240.1.177	384k	2M		
17	Michia Luis Alberto	10.240.1.176	384k	2M		
18	Meliñku Beatria	10.240.1.174	384k	2M		
19	Aparicio Jonathan	10.240.1.172	384k	2M		
20	Gimenez Stella Maris	10.240.1.170	384k	2M		
21	Pereyra Analia	10.240.1.171	384k	2M		
22	Alderete Julio	10.240.1.168	384k	2M		
23	Calabrese Amaldo Enrique	10.240.1.167	384k	2M		
24	Farias Blanca	10.240.1.166	384k	2M		
25	Molini Andrea (Esc Media n 4)	10.240.1.165	384k	2M		
26	Pablo Torre Repetidora	10.240.1.164	384k	2M		
27	Echet Santiago	10.240.1.163	384k	2M		
28	Altamirano Ana	10.240.1.162	384k	2M		
<div> 165 items 13.8 KiB queued 10 packets queued </div>						



Simple Queue

Target

- Target indica en que interfaz o a que IPs será aplicada la regla de limitación.
- Target es un parámetro requerido y puede ser:
 - ➔ Dirección IP
 - ➔ Red IP
 - ➔ Interface

Simple Queue (IP)

New Simple Queue

General | Advanced | Statistics | Traffic | Total | Total Statistics

Name:

Target:

Dst.:

	Target Upload	Target Download
Max Limit:	<input type="text" value="2M"/> <input type="button" value="v"/>	<input type="text" value="5M"/> <input type="button" value="v"/> bits/s
▲ Burst		
Burst Limit:	<input type="text" value="unlimited"/> <input type="button" value="v"/>	<input type="text" value="unlimited"/> <input type="button" value="v"/> bits/s
Burst Threshold:	<input type="text" value="unlimited"/> <input type="button" value="v"/>	<input type="text" value="unlimited"/> <input type="button" value="v"/> bits/s
Burst Time:	<input type="text" value="0"/>	<input type="text" value="0"/> s
▼ Time		

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Torch

Simple Queue (Red)

New Simple Queue □ ×

General Advanced Statistics Traffic Total Total Statistics

Name:

Target: ↓ ▲

Dst.:

Target Upload Target Download

Max Limit: ↓ ↓ bits/s

▲ Burst

Burst Limit: ↓ ↓ bits/s

Burst Threshold: ↓ ↓ bits/s

Burst Time: s

▼ Time

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Torch

Simple Queue

Dst. (destino)

- Dirección IP, red IP o interfaz hacia donde va dirigido el trafico.
- No es un campo obligatorio.
- Puede ser usada para restringir la aplicación de los limites de velocidad de cierta queue.

Simple Queue

Max-limit

- El parámetro "max-limit" indica la tasa máxima que el cliente va a poder alcanzar en el "mejor escenario".
- Max-Limit es sinonimo de **MIR** (maximum information rate).

Limit-at

- El parámetro "limit-at" indica la tasa garantizada, en el "peor escenario".
- Limit-At es sinonimo de **CIR** (committed information rate).

Simple Queue (Subida+Bajada)

New Simple Queue

General Advanced Statistics Traffic Total Total Statistics

Total Limit At: ▼ bits/s

Total Max Limit: 24M ▲ bits/s

Total Priority: ▼

Total Burst Limit: ▼ bits/s

Total Burst Threshold: ▼ bits/s

Total Burst Time: ▼ s

Total Queue Type: default-small ▼

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Torch

Simple Queue

- Por WinBOX, las colas de velocidad pueden ponerse de distintos colores dependiendo de su estado:

 Verde: 0 ~ 50 % de ancho de banda usado.

 Amarillo: 51 ~ 75% de ancho de banda usado.

 Rojo: 76 ~ 100% de ancho de banda usado.

Simple Queue

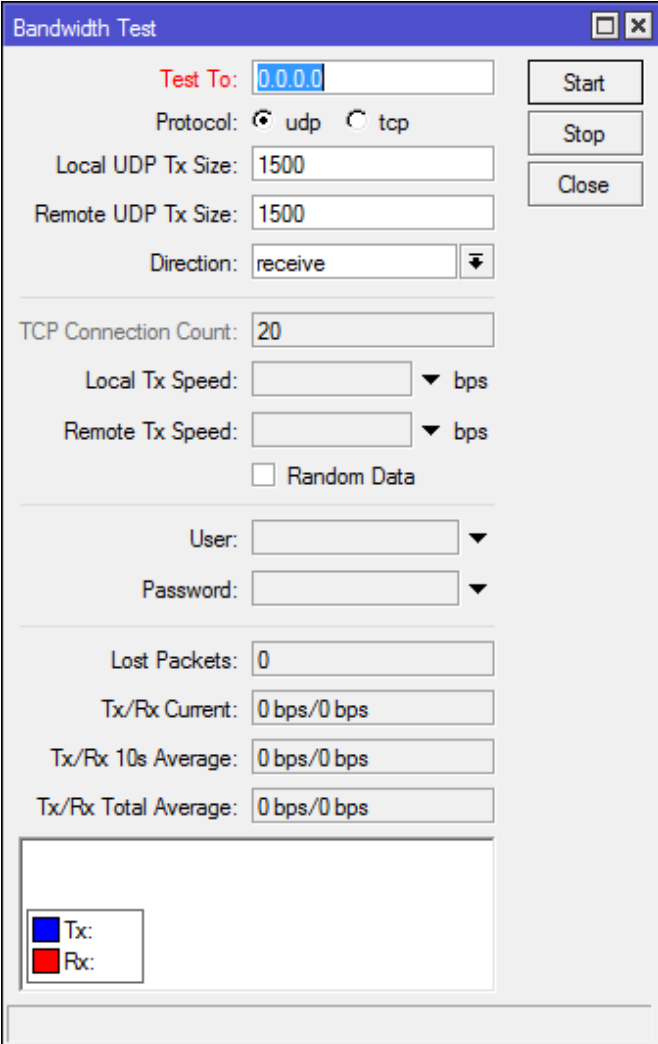
- Abrir sitio www.speedtest.net. No correr el test.
- Crear un limite de ancho de banda para su notebook (upload: 64k, download: 128k).
- Recordar que **Target** es la opción para esta configuración.
- Ahora si, hacer un test de ancho de banda.
- Verificar que ocurre con la simple queue.

Test de ancho de banda

- La herramienta se llama "**Bandwidth Test**" y se encuentra en "**Tools**".
- Es útil para monitorear el rendimiento contra un dispositivo remoto.
- Se encuentra disponible una versión para Windows que se puede obtener desde la sección Downloads de la web de MikroTik.
- **Bandwidth Test** sólo opera con equipos Mikrotik o contra la aplicación de Windows.

Test de ancho de banda

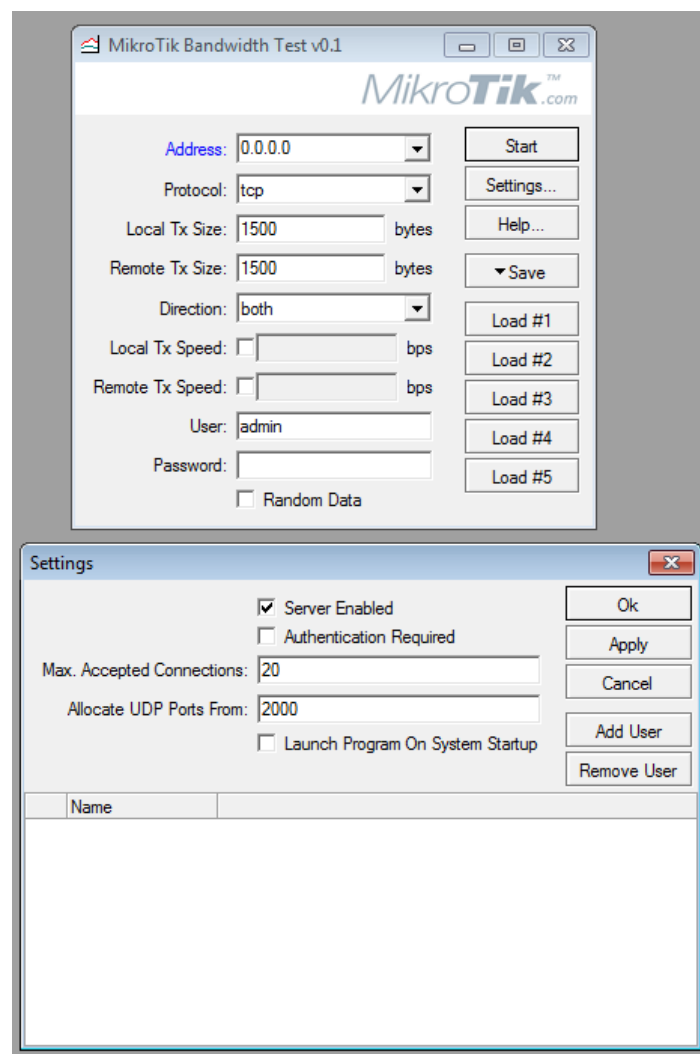
- Configurar **Test To** con la dirección destino.
- Seleccionar protocolo.
- TCP soporta múltiples conexiones.
- Autenticarse en el equipo es uno de los requisitos para su uso.



The screenshot shows the 'Bandwidth Test' application window. It features a blue title bar with standard window controls. The interface is organized into several sections. At the top, there's a 'Test To:' field with '0.0.0.0' entered, followed by 'Protocol:' with radio buttons for 'udp' (selected) and 'tcp'. Below these are 'Local UDP Tx Size:' and 'Remote UDP Tx Size:' both set to '1500'. A 'Direction:' dropdown menu is set to 'receive'. The 'TCP Connection Count:' is set to '20'. There are fields for 'Local Tx Speed:' and 'Remote Tx Speed:' with unit selectors set to 'bps'. A 'Random Data' checkbox is present. Below these are 'User:' and 'Password:' dropdown menus. The bottom section displays performance metrics: 'Lost Packets:' (0), 'Tx/Rx Current:' (0 bps/0 bps), 'Tx/Rx 10s Average:' (0 bps/0 bps), and 'Tx/Rx Total Average:' (0 bps/0 bps). At the very bottom, there's a legend with a blue square for 'Tx:' and a red square for 'Rx:', followed by a large empty rectangular area for a graph or log.

Test de ancho de banda

- Descargar Bandwidth Test desde el sitio de MikroTik.
- El servidor necesita estar habilitado en la aplicación de Windows.
- Se recomienda utilizar la autenticación.
- Hacer un test desde el router hacia la notebook.



Ráfagas

- Permite a los usuarios obtener por un corto periodo de tiempo, más ancho de banda que el permitido por el parámetro **max-limit**.
- Funciona promediando la tasa de transferencia y comparandola con ciertos valores que se definirán en la siguiente sección.
- Si bien parece complejo, hay un calculo que resuelve la complejidad de configuración.

Ráfagas

■ Definiciones:

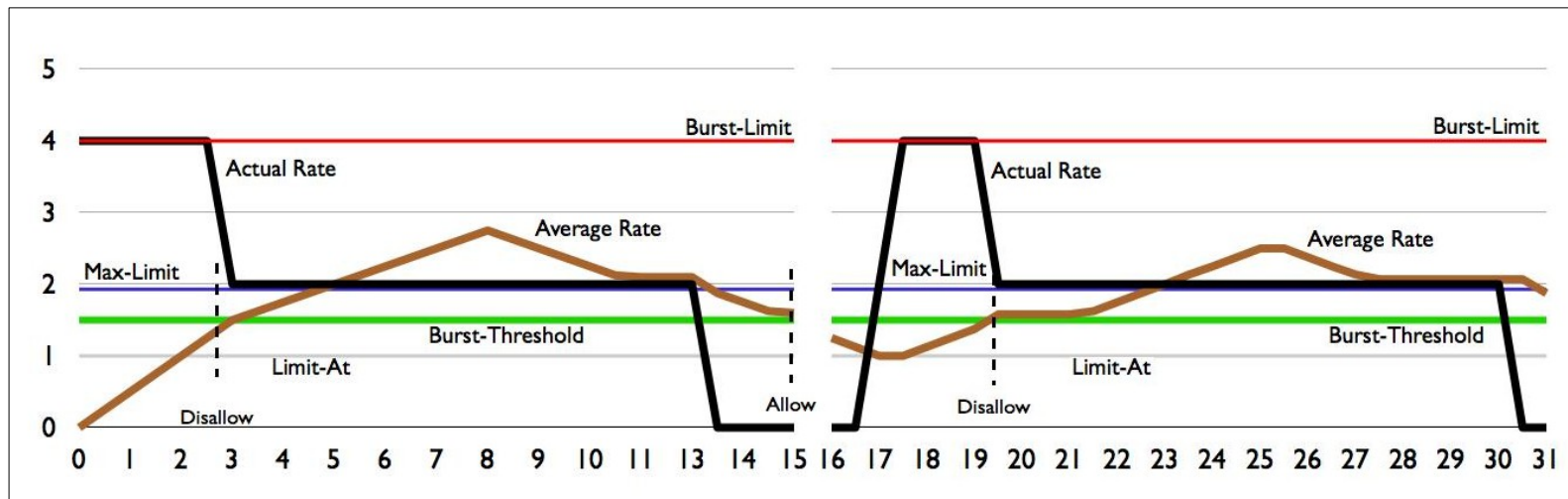
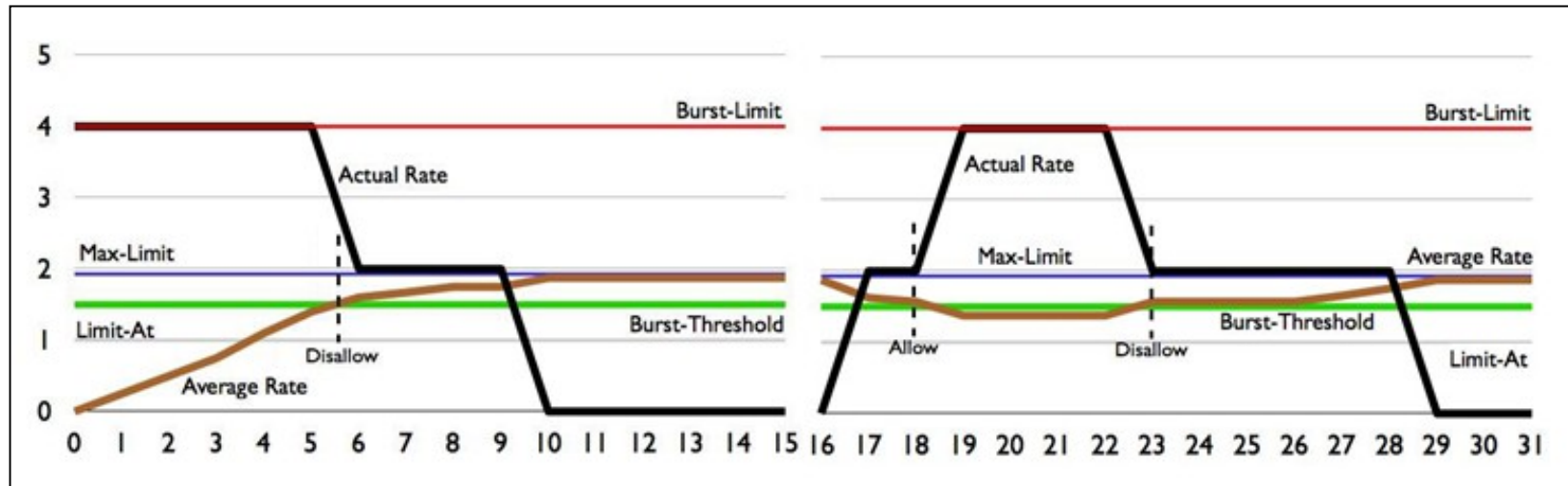
- ➔ **burst-limit:** máximo de ancho de banda permitido.
- ➔ **burst-time:** tiempo en segundos. No significa el tiempo que durará la ráfaga, sino cada cuanto tiempo se promedia.
- ➔ **burst-threshold:** este valor indica si el usuario tiene permitido acceso a la ráfaga.
- ➔ **average-rate:** el promedio de tasa de transferencia calculado en 1/16 partes del "burst-time".
- ➔ **actual-rate:** tasa de transferencia real.



Ráfagas - Funcionamiento

- La ráfaga es permitida mientras **average-rate** este por debajo de **burst-threshold**.
- La ráfaga tendrá un límite definido por el parámetro **burst-limit**.
- La variable **average-rate** sera calculada promediando 16 muestras del **actual-rate**, dividido el parametro **burst-time**.
 - ➔ Ej.: Si burst-time es 16 segundos, entonces se toma una muestra cada 16 segundos.
 - ➔ Ej.: Si burst-time es 8 segundos, entonces se toma una muestra cada 0,5 segundos.
- La duración real de la ráfaga se calcula como:
 - ➔ $(\text{burst-threshold} \times \text{burst-time}) / \text{burst-limit} = \text{rafaga en segs.}$

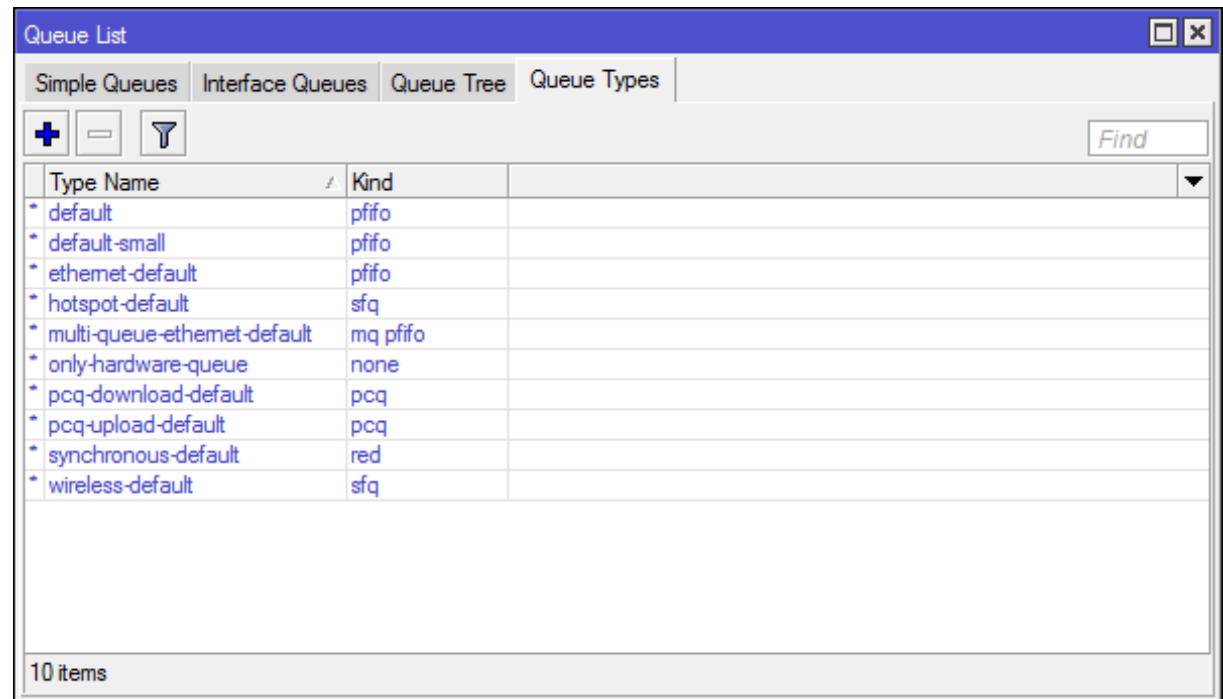
Ráfagas - Ejemplos



Algoritmos de encolado

■ RouterOS soporta:

- ➔ PFIFO
- ➔ BFIFO
- ➔ RED
- ➔ SFQ
- ➔ PCQ



Type Name	Kind
* default	pfifo
* default-small	pfifo
* ethernet-default	pfifo
* hotspot-default	sfq
* multi-queue-ethernet-default	mq pfifo
* only-hardware-queue	none
* pcq-download-default	pcq
* pcq-upload-default	pcq
* synchronous-default	red
* wireless-default	sfq

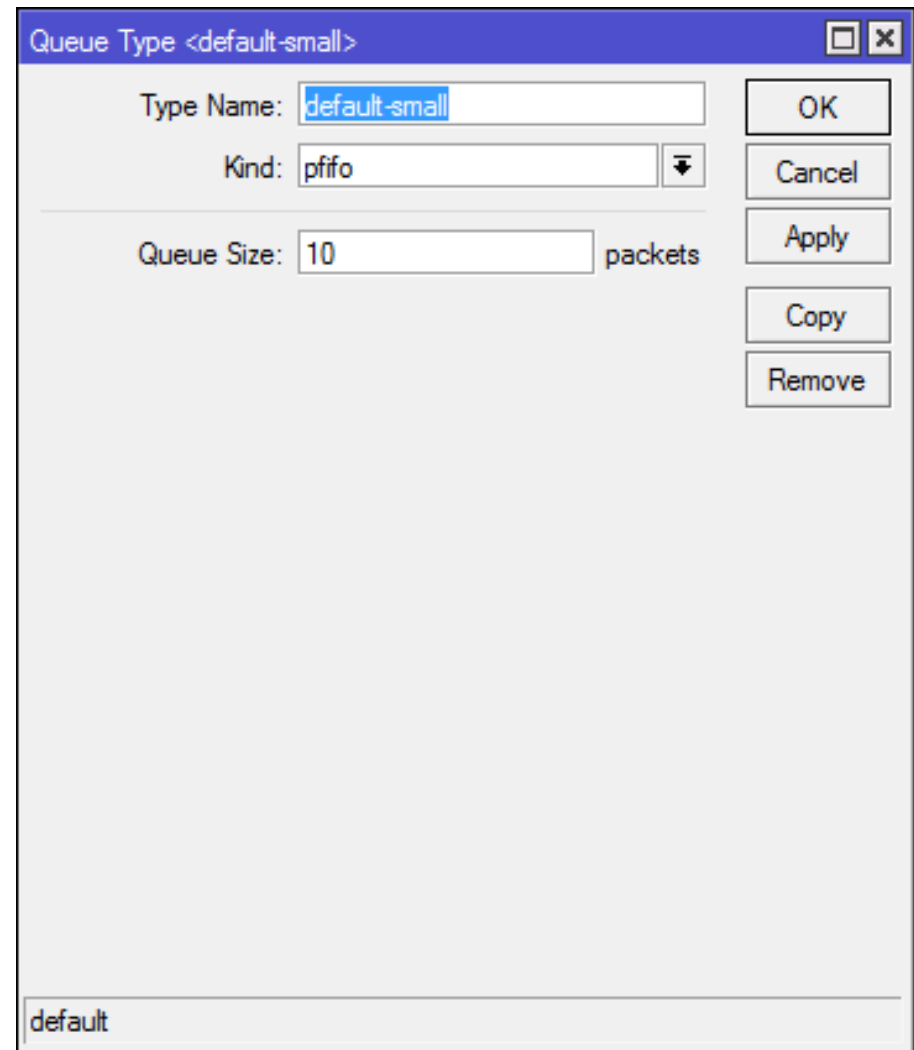
10 items

Queue Types

- Los algoritmos de encolado se configuran como Queue Types (tipos de cola).
- Las queues se pueden configurar para que encolen el tráfico de una forma u otra dependiendo de que Queue Type se configure.
- La configuración de Queue Type se encuentra en la solapa "Advanced" de cualquier Simple Queue.

Queue Types

- La configuración de cada Queue Type se encuentra en una solapa con el mismo nombre dentro de la ventana Queues.
- Por defecto, todas las queues son **default-small**, un tipo de cola que tiene PFIFO como algoritmo de encolado.



Per Connection Queue (PCQ)

- Per Connection Queue (PCQ) es un tipo de mecanismo de encolado dinámico que permite ecualizar el tráfico de varios usuarios.
- Su configuración se encuentra en la solapa "Queue Types" dentro de "Queues".

Queue Type <pcq-download-default>

Type Name: pcq-download-default

Kind: pcq

Rate: 0

Limit: 50

Total Limit: 2000

Burst Rate:

Burst Threshold:

Burst Time: 00:00:10

Classifier: ☐ Src. Address ☒ Dst. Address
☐ Src. Port ☐ Dst. Port

Src. Address Mask: 32

Dst. Address Mask: 32

Src. Address6 Mask: 128

Dst. Address6 Mask: 128

default

OK Cancel Apply Copy Remove

PCQ - **pcq-rate**

- El parámetro **pcq-rate** limita la tasa de transferencia máxima permitida.
- El parámetro **classifier**, indica que datos va a tener el router para aplicar una limitación. Puede ser dirección IP/puerto origen y/o destino. De modo que PCQ se puede utilizar para ecualizar tráfico de usuarios o de aplicaciones.

PCQ - pcq-limit

- El parámetro pcq-limit se mide en paquetes.
- Un número alto de paquetes:
 - ➔ Incrementa el tamaño del buffer, reduciendo la probabilidad de descartes
 - ➔ Aumenta la latencia.
- Un número bajo de paquetes:
 - ➔ La probabilidad de descartes aumente y hay más reenvios con lo cual la latencia disminuye.

PCQ - Definir Simple Queue

Simple Queue <Clientes>

General Advanced Statistics Traffic Total Total Statistics

Name: Clientes

Target: br-lan

Dst.:

Target Upload Target Download

Max Limit: 1M 5M bits/s

Burst

Burst Limit: unlimited unlimited bits/s

Burst Threshold: unlimited unlimited bits/s

Burst Time: 0 0 s

Time

enabled

Simple Queue <Clientes>

General Advanced Statistics Traffic Total Total Statistics

Packet Marks:

Target Upload Target Download

Limit At: unlimited unlimited bits/s

Priority: 8 8

Queue Type: pcq-upload-default pcq-download-default

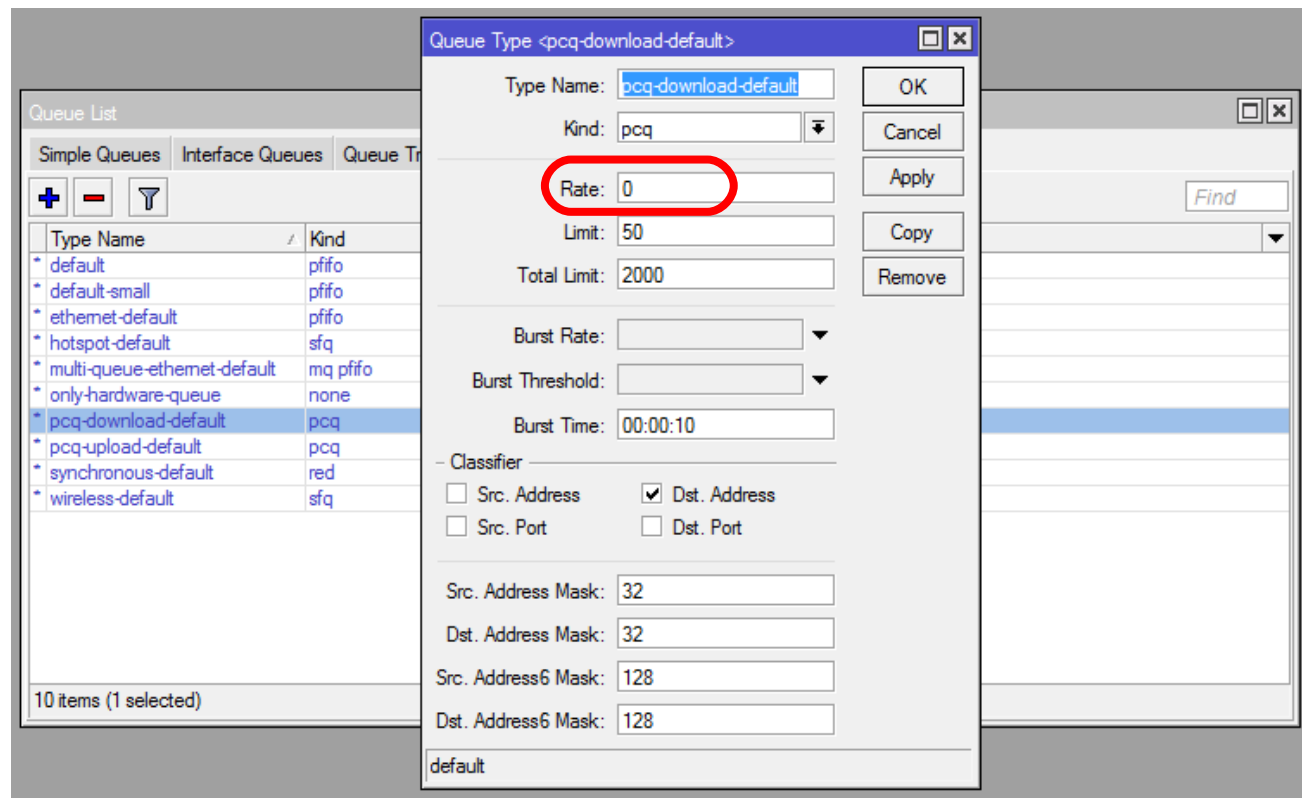
Parent: none

enabled

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters Torch

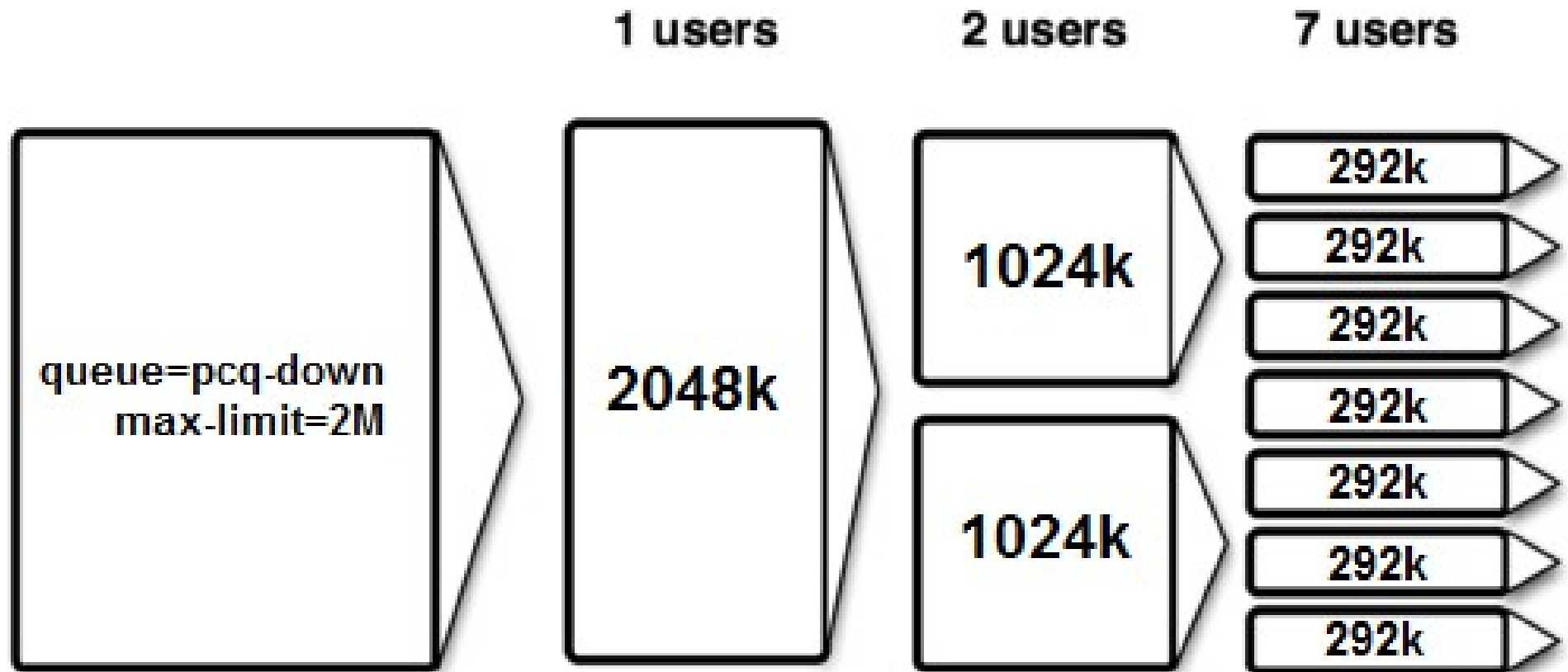
PCQ - Configurar Queue Type

Tipo de cola PCQ configurada para equalizar el tráfico entre todos los usuarios alcanzados por la simple queue que la tengan como tipo de cola.



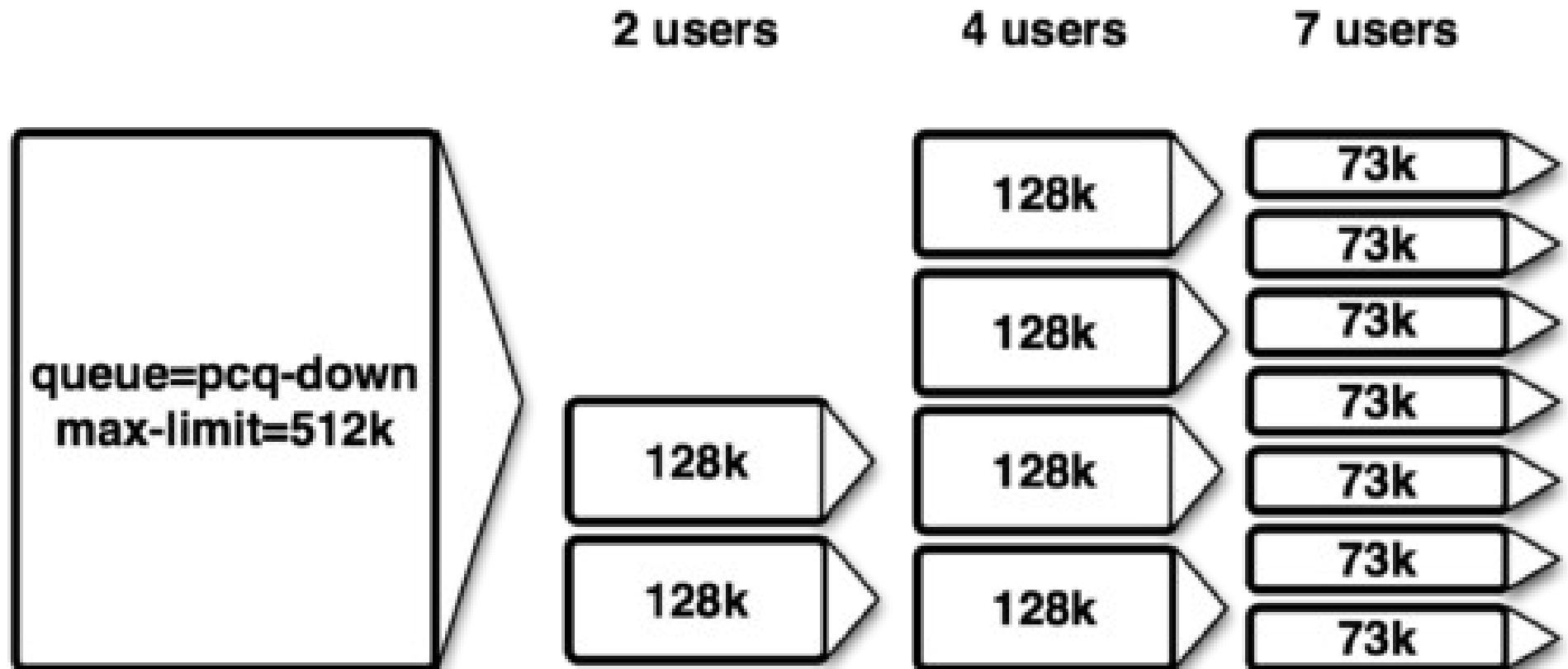
PCQ - Ecualizar ancho de banda

pcq-rate=0



PCQ - Ancho de banda fijo

pcq-rate=128000



PCQ

- Configurar una red entre router propio y al menos 1 vecino, para lo que se va a necesitar un bridge.
- Poner un rango de IPs nuevo a elección.
- Crear una cola simple con límite de 1Mbit/s utilizando PCQ como tipo de cola.
- Verificar con Bandwidth Test que la cola PCQ cumpla su función de ecualización.

Monitoreo de Ancho de Banda

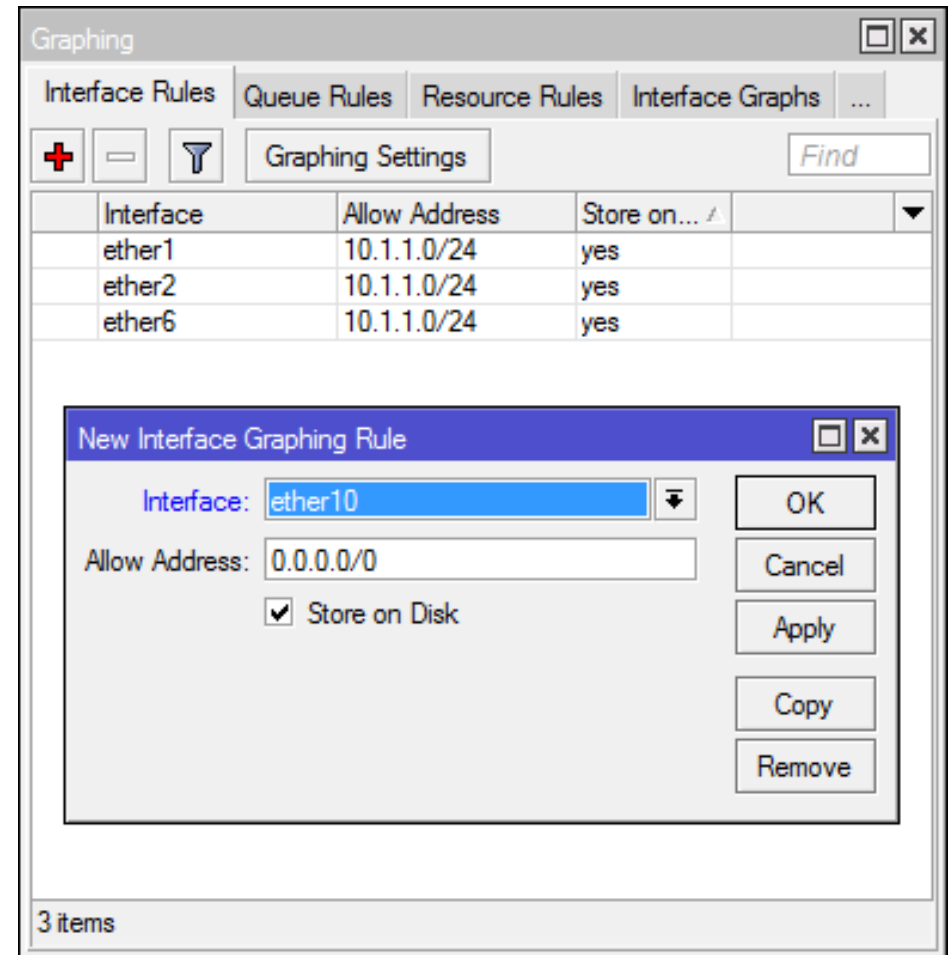
- “Torch” se encuentra en el menú “Tools” y es una herramienta de monitoreo ancho de banda.
- Seleccionar la interfaz en la que se quiera monitorear.
- Establecer los clasificadores.
- Dependiendo de los clasificadores, se puede ver el tráfico por conexión.

Monitoreo de Ancho de Banda

Torch (Running)									
- Basic					- Filters				
Interface: ether6					Src. Address: 0.0.0.0/0				Start
Entry Timeout: 00:00:03 s					Dst. Address: 0.0.0.0/0				Stop
- Collect					Src. Address6: ::/0				Close
<input checked="" type="checkbox"/> Src. Address					Dst. Address6: ::/0				New Window
<input checked="" type="checkbox"/> Dst. Address					MAC Protocol: all				
<input type="checkbox"/> MAC Protocol					Protocol: any				
<input type="checkbox"/> Protocol					Port: any				
<input type="checkbox"/> Src. Address6					VLAN Id: any				
<input type="checkbox"/> Dst. Address6									
<input type="checkbox"/> Port									
<input type="checkbox"/> VLAN Id									
Et...	Prot...	Src.	Dst.	VLAN Id	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...	
800 (ip)		10.240.1.92	190.230.141.29		193.8 k...	10.9 kbps	18	12	
800 (ip)		10.240.1.102	181.30.240.76		985.6 k...	23.9 kbps	81	48	
800 (ip)		10.240.1.120	78.140.165.6		427.9 k...	9.4 kbps	35	19	
800 (ip)		10.240.1.113	74.125.215.147		1269.7 ...	30.5 kbps	105	57	
800 (ip)		10.240.1.120	50.7.69.186		1017.4 ...	24.0 kbps	84	48	
800 (ip)		10.240.1.111	181.30.241.17		1753.6 ...	61.5 kbps	146	82	
800 (ip)		10.240.1.175	208.167.236.35		47.2 kbps	5.9 kbps	17	7	
800 (ip)		10.240.1.92	190.231.57.250		127.2 k...	8.2 kbps	12	9	
800 (ip)		10.240.1.92	190.51.181.245		238.0 k...	12.7 kbps	23	15	
800 (ip)		10.240.1.47	200.73.71.128		63.9 kbps	22.2 kbps	43	43	
800 (ip)		10.240.1.91	157.55.1.215		230.2 k...	7.9 kbps	21	13	
800 (ip)		10.240.1.92	2.237.154.228		45.9 kbps	4.9 kbps	9	6	
800 (ip)		10.240.1.90	151.63.74.239		0 bps	3.6 kbps	0	0	
800 (ip)		10.240.1.92	151.33.173.195		86.1 kbps	4.2 kbps	7	8	
800 (ip)		10.240.1.92	179.24.10.177		118.4 k...	5.6 kbps	10	10	
800 (ip)		10.240.1.92	190.137.83.147		80.6 kbps	3.4 kbps	7	6	
800 (ip)		10.240.1.92	190.152.189.56		54.8 kbps	2.5 kbps	5	5	
800 (ip)		10.240.1.78	31.13.85.16		36.9 kbps	7.6 kbps	7	6	
800 (ip)		10.240.1.92	81.64.175.48		130.0 k...	6.9 kbps	12	12	
800 (ip)		10.240.1.89	190.44.186.205		10.9 kbps	149.2 k...	19	32	
800 (ip)		10.240.1.71	177.155.66.125		160 bps	869 bps	0	0	
800 (ip)		10.240.1.92	2.232.162.254		8.3 kbps	965 bps	2	1	
384 items		Total Tx: 12.0 Mbps		Total Rx: 1211.9 kbps		Total Tx Packet: 1 178		Total Rx Packet: 818	

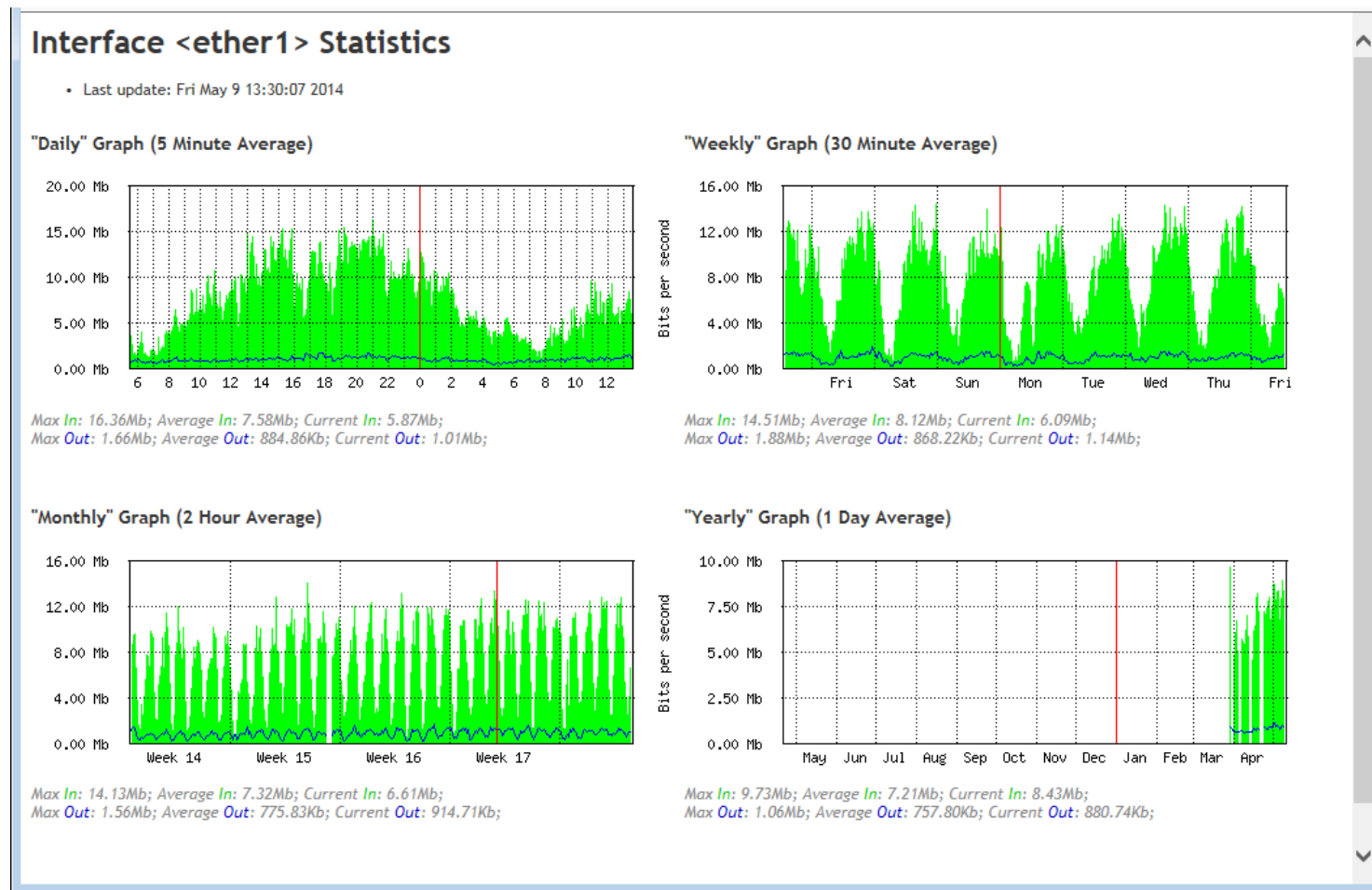
Gráficos de Simple Queue

- Es posible obtener el gráfico para cada regla de cola simple.
- Los gráficos muestran la cantidad de tráfico que pasa a través de la cola.
- **MiniLAB:** Habilitar los gráficos para las colas.



Gráficos de Simple Queue

Los gráficos están disponibles vía WebFig. Para verlos: <http://192.168.x.254/graphs>



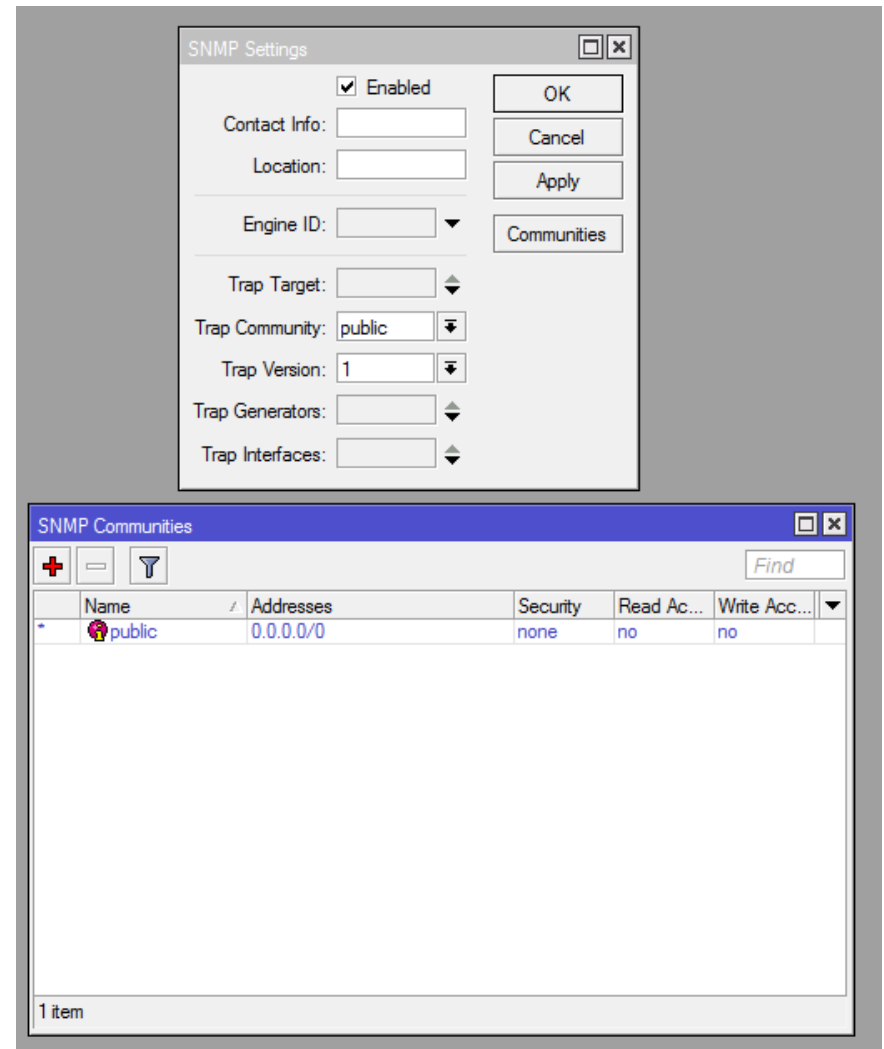
SNMP

- SNMP (Simple Network Management Protocol) es un protocolo estandar utilizado para administrar dispositivos en una red IP.
- Un router con SNMP habilitado, puede ser accedido para leer o escribir datos (estadísticas o configuraciones) utilizando clientes SNMP (por ejemplo el MikroTik Dude Server).
- SNMP tiene 3 versiones: v1, v2c y v3, siendo la última la mas segura y performante.



SNMP

- El SNMP corre sobre los puertos UDP 161 y 162.
- Se configura desde el menú "IP", submenu "SNMP".



Módulo 8

Túneles

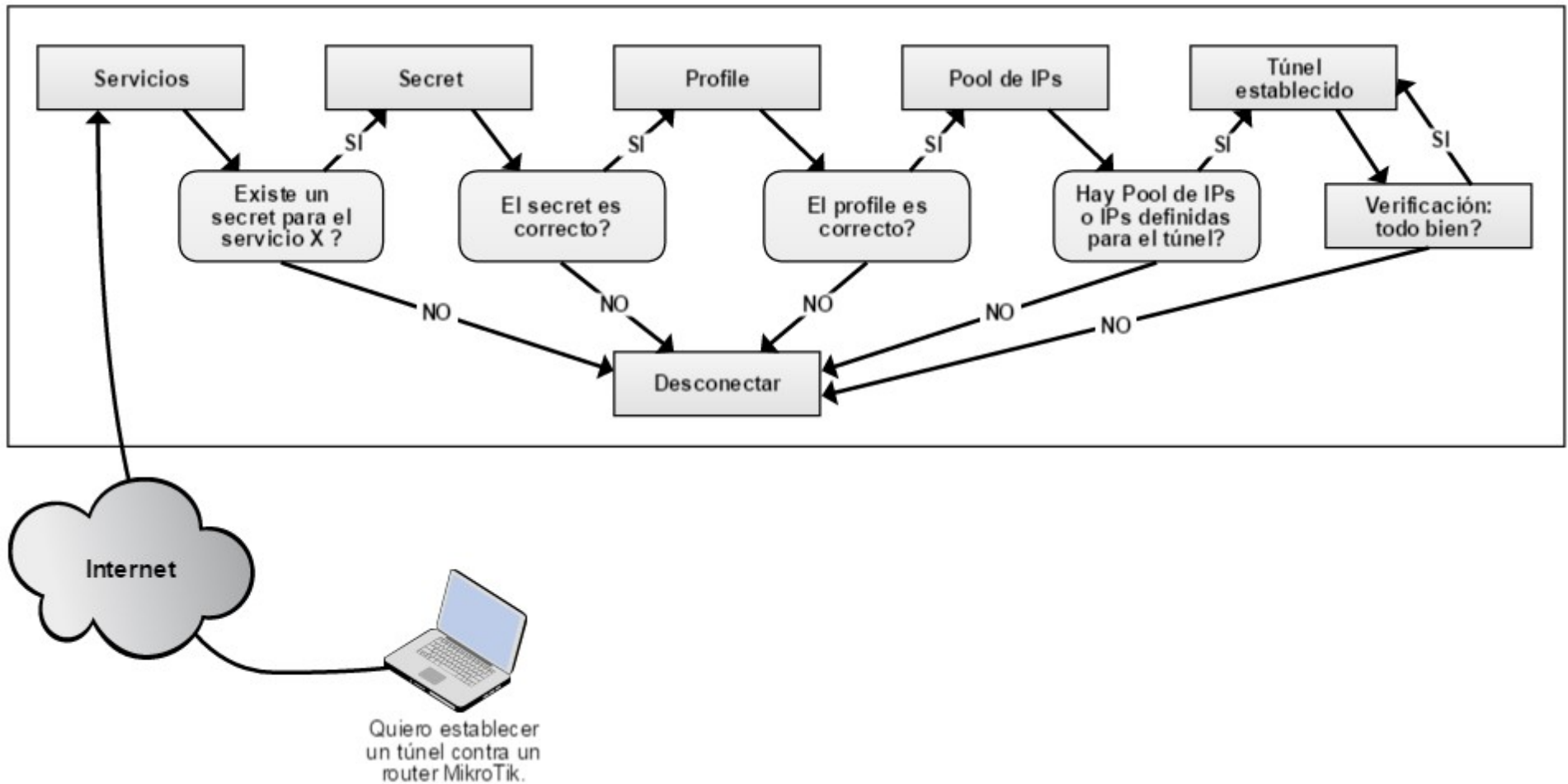
Túneles

- RouterOS soporta varios tipos de túneles punto a punto y punto multi punto.
- Forma de expandir redes privadas de forma segura a traves de Internet.
- Ejemplos y usos prácticos:
 - ➔ **Túneles PtP:** se utilizan para unir dos sitios remotos a traves de Internet. La *mayoría* se crean desde el menú principal "Interfaces".
 - ➔ **Túneles PtMP:** se utilizan para unir varios sitios remotos a uno central o concentrador. Se crean desde el menú principal "PPP".
 - ➔ Más allá de la topología utilizada, los túneles pueden o no tener seguridad.

Estructura del menú PPP

- Cuatro componenetes:
 - ➔ **Pool de IPs:** que se utilizaran para cada extremo del túnel.
 - ➔ **Profile:** perfil con configuraciones generales, acá se carga el Pool a utilizar.
 - ➔ **Secret:** es el usuario o cuenta que debe pertenecer a un profile. En caso de no querer utilizar un pool, en el secret se pueden configurar IPs fijas.
 - ➔ **Servicio:** se debe configurar al menos un servicio para poner "armar" un túnel con el MikroTik. Pude haber más de un servicio activo a la vez. Cada servicio lleva su configuración en particular.

Estructura del menú PPP





Menú PPP

The screenshot shows the PPP menu interface with the following sections and callouts:

- Interface**: The main menu bar.
- PPPoE Servers**: A sub-menu option.
- Secrets**: A sub-menu option with a callout: **Secrets**
Donde se crean las cuentas de usuario.
- Profiles**: A sub-menu option with a callout: **Profiles**
Donde se crean los perfiles para los usuarios, con opciones comunes como por ejemplo Pool, DNS, Encriptación, etc.
- Active Connections**: A sub-menu option with a callout: **Active Connections**
Donde se ve un registro de los usuarios conectados.
- IP → Pool**: A callout pointing to the bottom left: **IP → Pool**
Esta sección se encuentra fuera de PPP y es desde donde se crean los pools de direcciones IP para entregar a los potenciales clientes que se conecten por algun servicio de PPP.

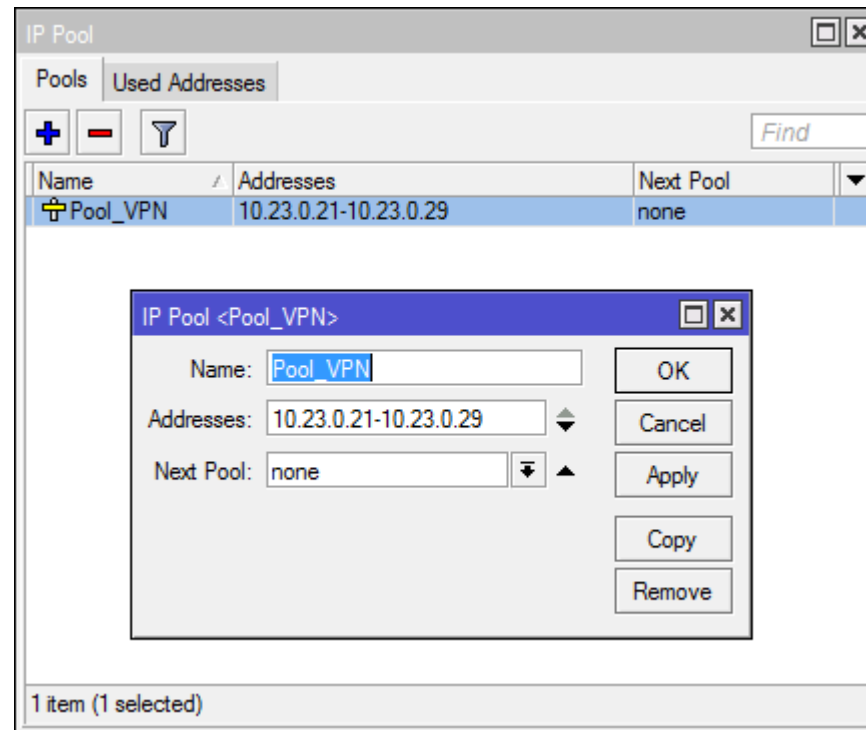
The interface also includes a toolbar with icons for adding, removing, and filtering, and a table with columns: Name, Type, L2 MTU, Rx, Tx Packet (p/s), and Rx Packet (p/s).

Servicios

- MikroTik soporta los siguiente servicios dentro de la sección **PPP**:
 - ➔ **async** (Asynchronous)
 - ➔ **L2TP** (requiere visibilidad capa 3)
 - ➔ **OVPN** (open VPN)
 - ➔ **PPPoE** (requiere visibilidad capa 2)
 - ➔ **PPTP** (requiere visibilidad capa 3)
 - ➔ **SSTP** (requiere visibilidad capa 3)

IP Pool

- Define el rango de direcciones IP para **PPP**, DHCP y los clientes HotSpot.
- Se utiliza un pool, cuando hay más de un cliente (PPP, DHCP o HotSpot).





PPP Profiles

- Los perfiles definen parámetros aplicables tanto a un servidor como a un cliente:
- **Local Address:** es la IP gateway de la red publicada.
- **Remote Address:** es la IP (o el pool), que tendrá el/los cliente/s PPP.
- **Solapa Limits:** bytes totales consumibles, y tasas de transferencia

The screenshot shows the 'PPP Profile <default-encryption>' window with the 'General' tab selected. The window contains the following fields and controls:

- Name:** default-encryption
- Local Address:** 10.23.0.254 (with up/down arrows)
- Remote Address:** Pool_VPN (with up/down arrows)
- Bridge:** (empty dropdown)
- Bridge Port Priority:** (empty dropdown)
- Bridge Path Cost:** (empty dropdown)
- Incoming Filter:** (empty dropdown)
- Outgoing Filter:** (empty dropdown)
- Address List:** (empty dropdown)
- DNS Server:** 8.8.4.4 (with up/down arrows)
- WINS Server:** (empty dropdown)
- Change TCP MSS:** radio buttons for ☐ default, ☐ no, and ☒ yes

On the right side of the window, there are buttons for **OK**, **Cancel**, **Apply** (dashed border), **Comment**, **Copy**, and **Remove**. At the bottom left, the text 'default' is visible.

PPP Secrets

- Es la Base de Datos de usuarios.
- Define los Nombres de Usuario y Contraseñas en el router.
- En el CallerID puede especificarse la MAC con que se espera a ese usuario.
- Permite definir en qué servicio PPP es aplicable dicha cuenta de usuario.

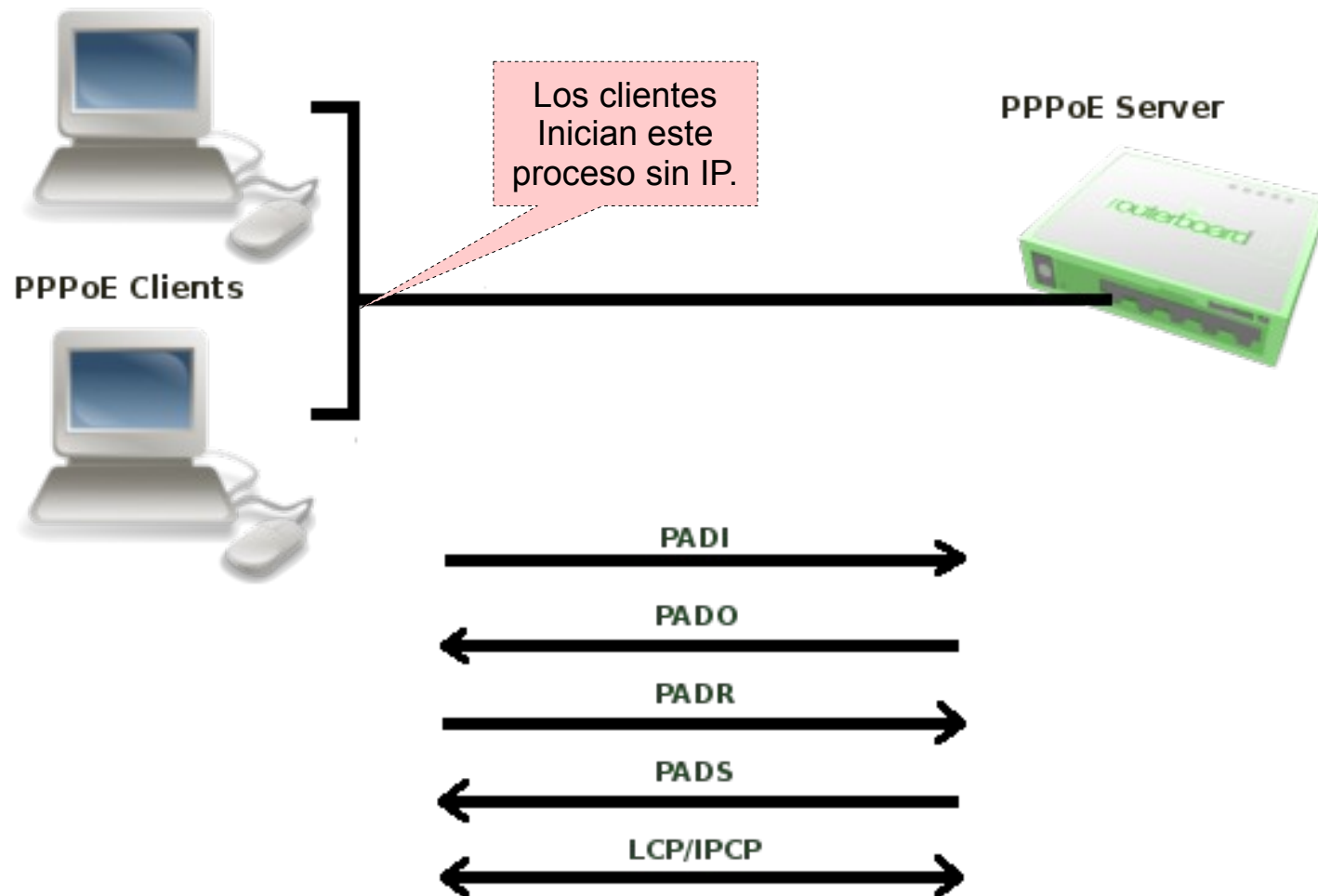
The screenshot shows a web-based configuration window titled "PPP Secret <usuario>". The window contains several input fields and a list of buttons on the right side. The fields are: "Name" with the value "usuario", "Password" with the value "wY3akCZB", "Service" with the value "any", "Caller ID" (empty), "Profile" with the value "default-encryption", "Local Address" (empty), "Remote Address" (empty), "Routes" (empty), "Limit Bytes In" (empty), "Limit Bytes Out" (empty), and "Last Logged Out" (empty). The buttons on the right are: "OK", "Cancel", "Apply" (highlighted with a dashed border), "Disable", "Comment", "Copy", and "Remove". At the bottom of the window, the status "enabled" is displayed.

Protocolo PPPoE

- Protocolo punto a punto sobre Ethernet, se utiliza a menudo para controlar las conexiones de cliente para DSL o redes inalámbricas bridgeadas.
- MikroTik RouterOS soporta cliente PPPoE y el servidor PPPoE.
- En escenarios WISP, es la forma ideal de entregar IPs públicas a los usuarios.



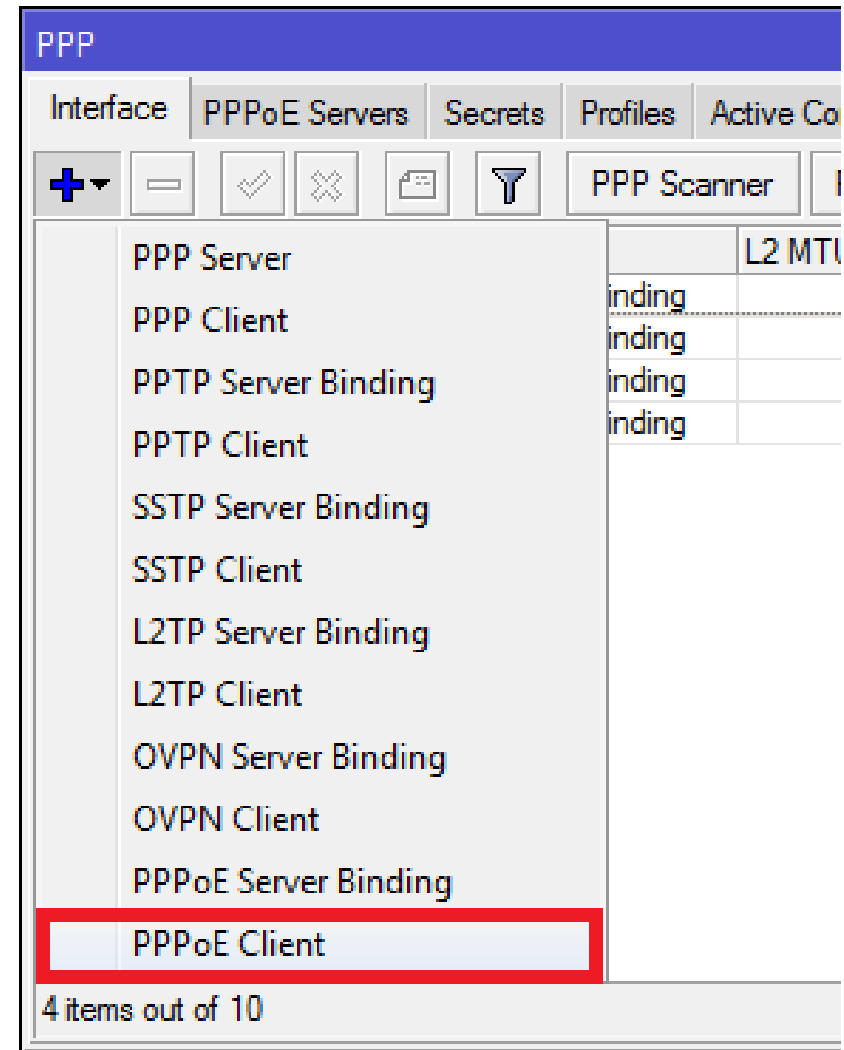
Protocolo PPPoE





PPPoE - Cliente

- Requiere la creación de una interface virtual PPPoE Client, sobre una interface maestra física real.
- De ahí en más, básicamente solo considera el servicio, las credenciales y el perfil de red.





PPPoE - Servidor

- Crear la interfaz PPPoE Server sobre una interfaz real particular.
- Especificar un Default Profile, donde se parametricen las características de red del servicio.
- Se pueden crear varios servidores por interfaz diferenciados por "Service Name".

New PPPoE Service

Service Name:

Interface: ▼

Max MTU:

Max MRU:

MRRU: ▲

Keepalive Timeout: ▲

Default Profile: ▼

☐ One Session Per Host

Max Sessions: ▼

- Authentication -

☒ pap ☒ chap

☒ mschap1 ☒ mschap2

enabled

OK Cancel Apply Disable Copy Remove

Protocolo PPPoE

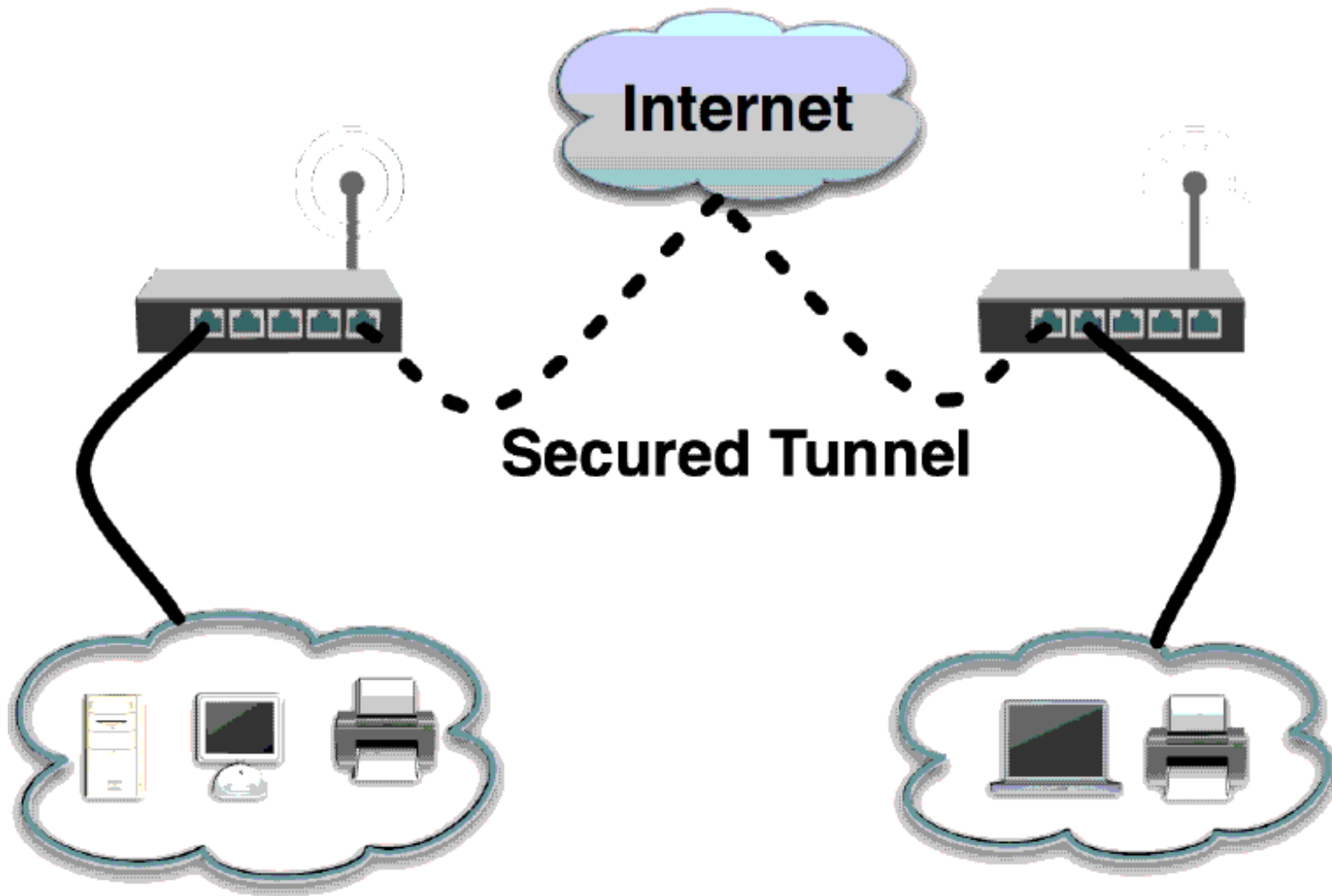
- Cada alumno va a crear un server y el compañero el cliente.
- Elegir un rango de IP.
- Verificar conectividad.



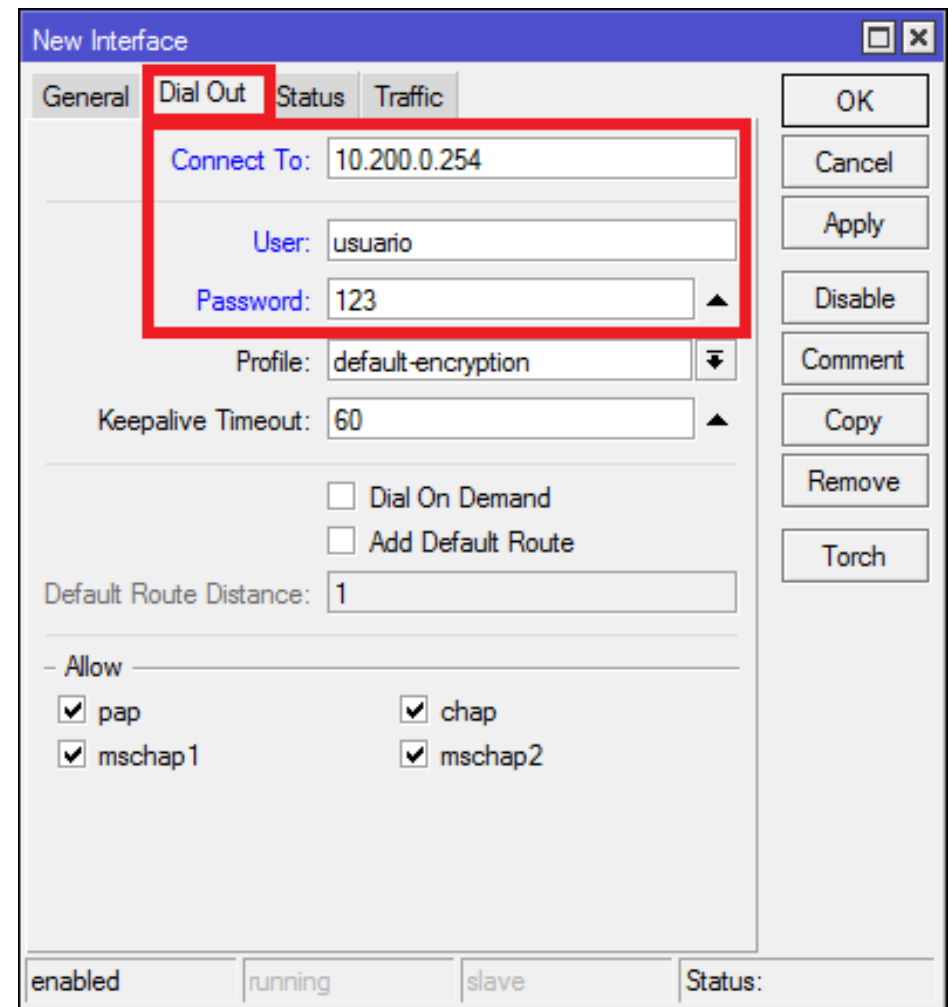
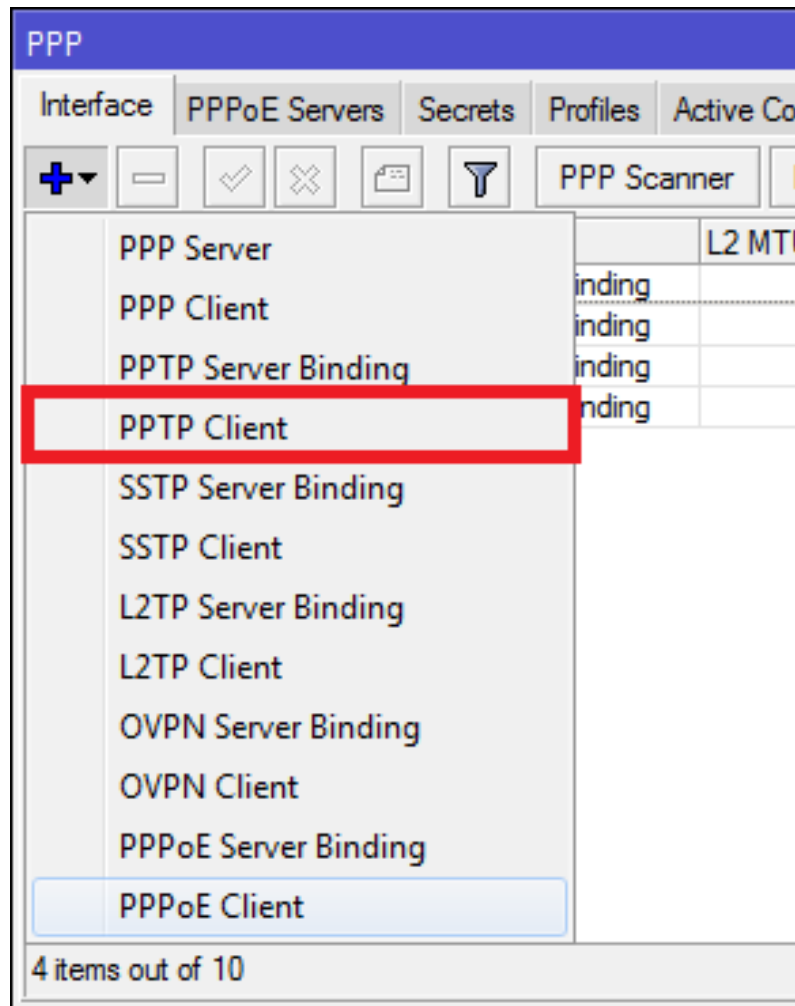
Protocolo PPTP

- El PPTP es un protocolo que establece túneles encriptados a través de IP.
- Utiliza el standard GRE, que hace uso del protocolo IP número 47 (igual que los túneles EoIP).
- MikroTik RouterOS incluye soporte para tanto para el cliente, como para el servidor PPTP.
- Se utiliza comunmente para:
 - ➔ Fijar vínculo entre locales a través de Internet.
 - ➔ Para los clientes móviles o remotos, a fin de poder acceder a recursos de la empresa.

PPTP



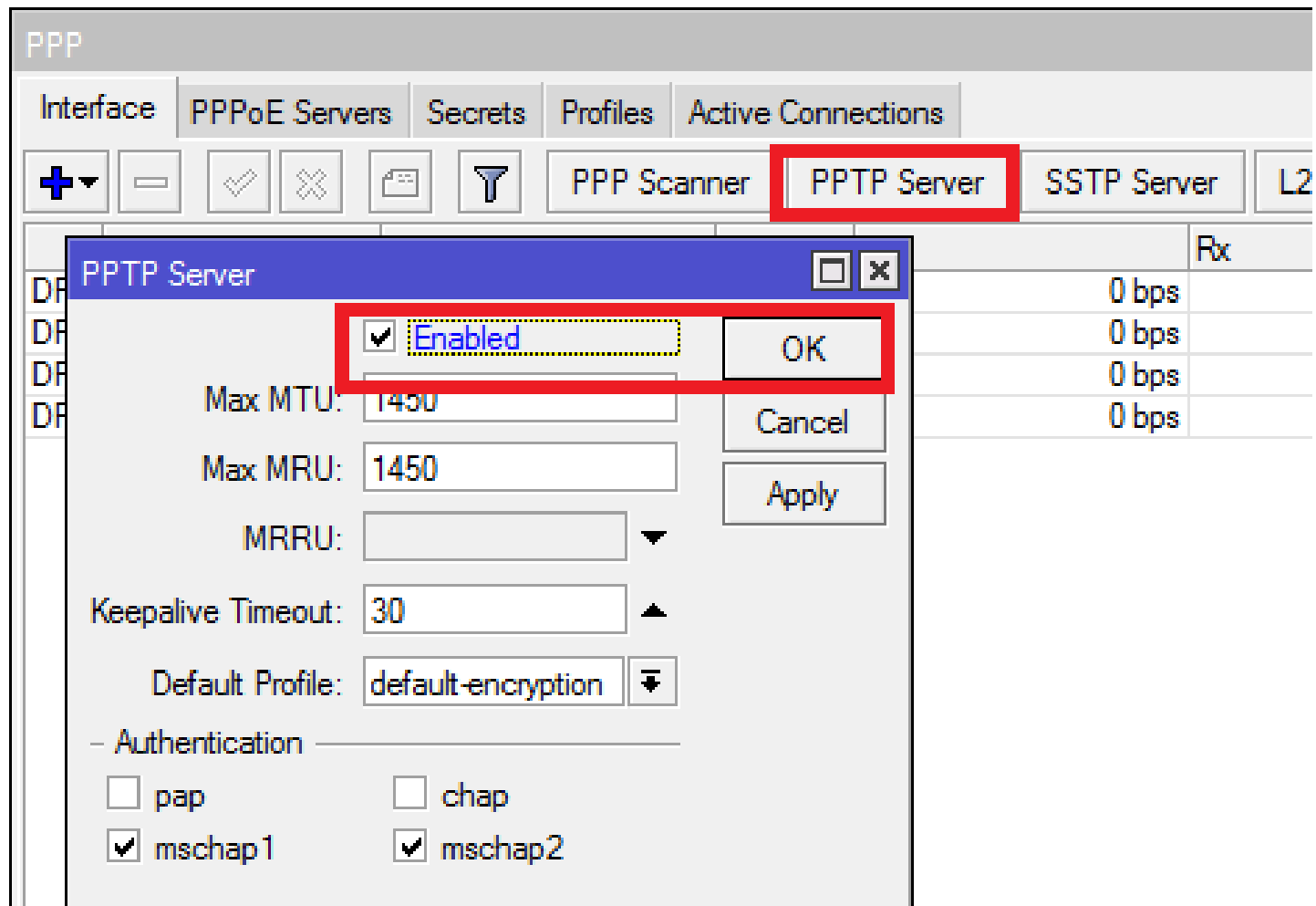
PPTP Cliente



PPTP - Cliente

- Eso es todo para la configuración del cliente PPTP.
- Utilizar "Add Default Route" para agregar al servidor PPTP como puerta de enlace predeterminada.
- Utilizar las rutas estáticas para enviar el tráfico específico para el Túnel PPTP.

PPTP - Servidor





Usuarios de un PPTP Server

- La configuración de los clientes PPTP se almacena en los ppp secrets.
- Los ppp secrets se utilizan para los clientes PPTP, L2TP y PPPoE.
- La base de datos de ppp secrets está configurada en el mismo router servidor.
- Tanto para los clientes PPTP, PPPoE, L2TP como PPP, se puede usar el mismo Profile de clientes.

Protocolo PPTP

- Cada alumno va a crear un server y el compañero el cliente.
- Elegir un rango de IP.
- Verificar conectividad.

www.prozcenter.com/entrenamientos/mtcna