Políticas de ruteo con MikroTik RouterOS

Objetivos de este microcurso

1. Presentar el concepto de ruteo basado en políticas (PBR).
2. Demostrar configuraciones simples para poder implementar las políticas de ruteo típicas de los escenarios actuales.
3. Establecer criterios convenientes para cada caso.

Resumen de los temas

1. ¿Qué es una política de ruteo y para qué sirve?
2. Consideraciones previas
3. Ruteo por origen
4. Balanceo de carga PCC

¿Qué es una política de ruteo y para qué sirve?

¿Qué es una política de ruteo?

- Por definición el ruteo tradicional se realiza en base a la dirección destino de los paquetes.

- Pero el ruteo basado en políticas permite rutear paquetes en base a diversos criterios definidos por el administrador de red.

¿Para qué sirve una política de ruteo?

- Si bien su aplicación es cualquier escenario donde exista ruteo de múltiples caminos, vamos a mostrar un escenario de múltiples conexiones a Internet.

- Es decir, una política de ruteo permite a un administrador de red elegir el proveedor de Internet (ISP) por el cual enviar los datos, basándose en criterios específicos.

¿Qué es una política de ruteo y para qué sirve?

- Ruteo por protocolo.
- **Ruteo por origen** * 👉
- Balanceo de carga
  - EMCP
  - **PCC** * 👉

Diagrama de flujo

Existe 3 flujos:

- input
- output
- forward

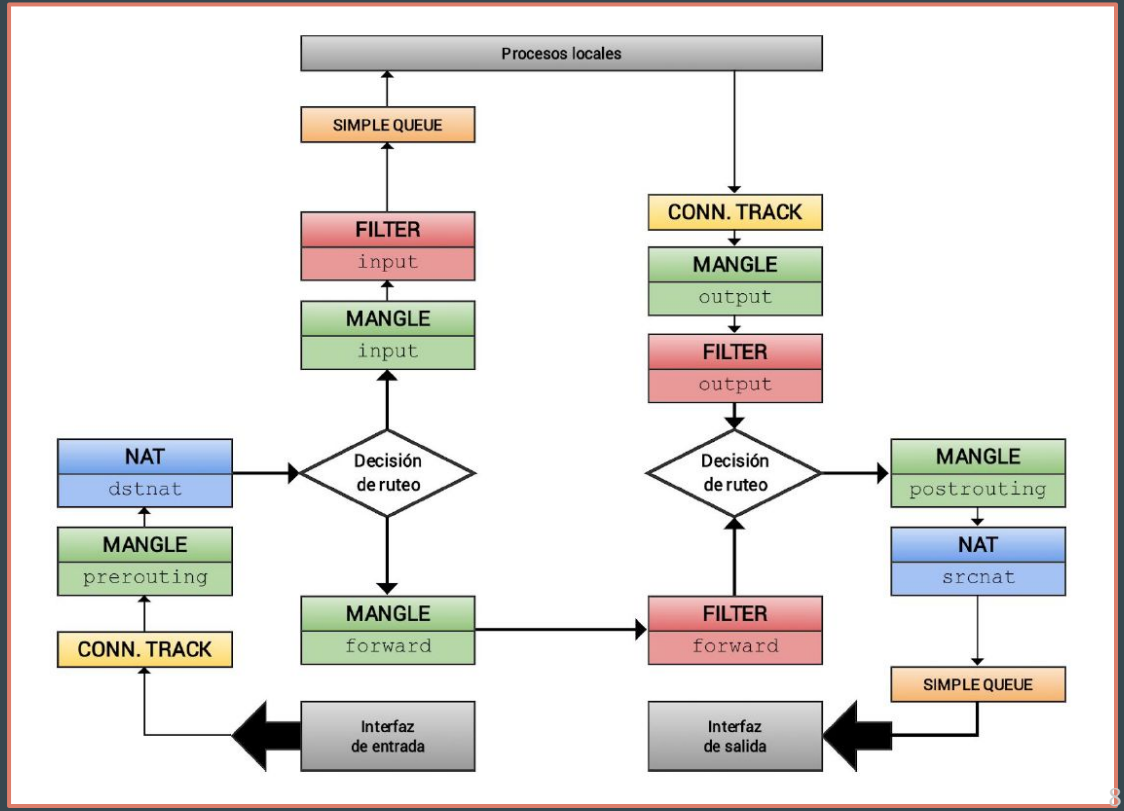


Diagrama de flujo

Existe 3 flujos:

- input
- output
- forward

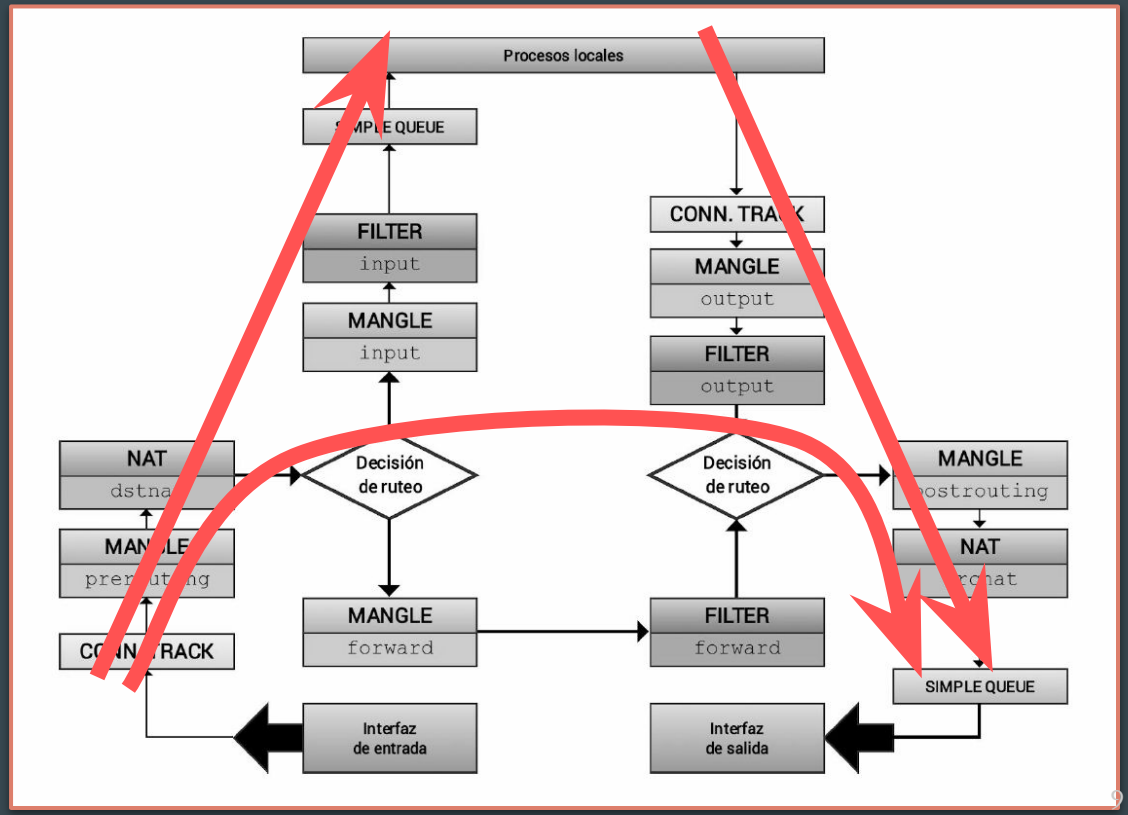
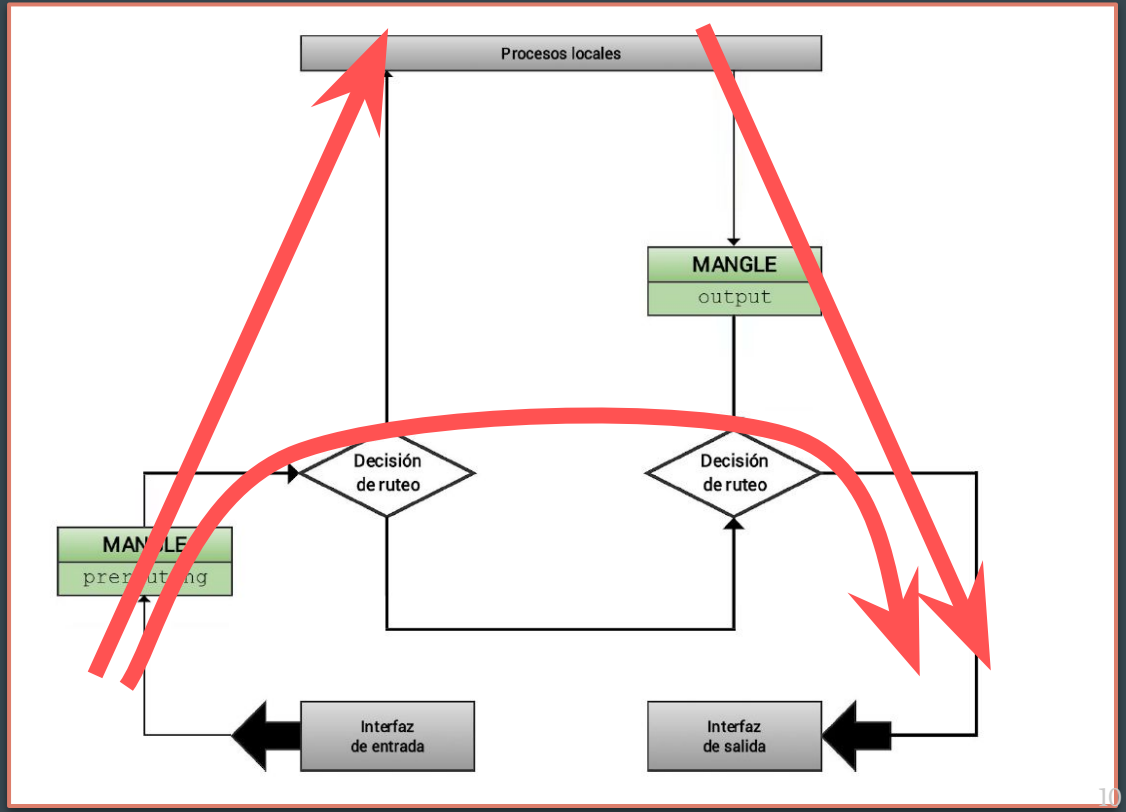


Diagrama de flujo

Simplificado para explicar políticas de ruteo utilizando una sección del Firewall llamada **Mangle**.



Consideraciones previas

Consideraciones previas

- Cuando hablamos de un escenario de múltiples ISPs, es importante mantener la coherencia en la comunicación.

- Puesto de otro modo, si me comunico con un router que tiene 3 ISPs, y lo hago por la ISP2, la respuesta debería venir de ISP2.

- Para que esto ocurra, hay que hacer 2 reglas “obligatorias” por cada ISP que se agregue.

Consideraciones previas

- En primer lugar, hay que identificar las conexiones entrantes y vincularlas con cada ISP, cosa que se logra con marcando las conexiones.

```
/ip firewall mangle add chain=prerouting \
in-interface=ether1_isp1 connection-state=new \
action=mark-connection new-connection-mark=mc_isp1
```

```
/ip firewall mangle add chain=prerouting \
in-interface=ether2_isp2 connection-state=new \
action=mark-connection new-connection-mark=mc_isp2
```

Consideraciones previas

- Y como segundo paso, hay que hacer que el router responda las solicitudes por el ISP que corresponde, basándose en la marca de conexión.

```
/ip firewall mangle add chain=output \
connection-mark=mc_isp1 \
action=mark-routing new-routing-mark=tabla_isp1 passthrough=no

/ip firewall mangle add chain=output \
connection-mark=mc_isp2 \
action=mark-routing new-routing-mark=tabla_isp2 passthrough=no
```

Ruteo por origen

Ruteo por origen

- En este caso sencillo se utiliza una lista para rutear paquetes por un gateway en base a la dirección IP origen.

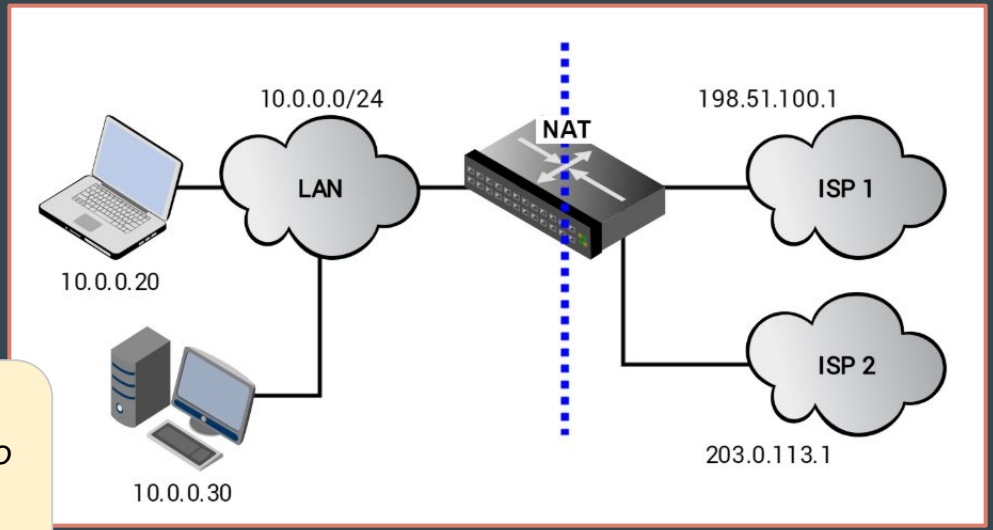
- Este método es muy similar si optamos rutear por protocolo.

- En RouterOS existen varias formas de hacerlo, aquí se presentan dos de ellas.

Ruteo por origen

Escenario inicial:

- 2 ISP
- 1 LAN
- NAT



Objetivo:
Que cada dispositivo alcance Internet por un ISP en particular.

Ruteo por origen (utilizando action=routing-mark)

Parte 1/2

```
/ip firewall mangle
add chain=prerouting \
src-address-list=lista_salida-isp1 \
action=mark-routing \
new-routing-mark=tabla_isp1
passthrough=no

/ip firewall address-list
add action=10.0.0.30 \
list=lista_salida-isp1
```

Definición de una lista de direcciones IP.

Se realiza la búsqueda del próxima salto en una tabla paralela, llamada “tabla_isp1”.

Completar la lista con IPs, redes o rangos.

Ruteo por origen (utilizando action=routing-mark)

Parte 2/2

Tablas adicionales (una por ISP)

```
/ip route
add dst-address=0.0.0.0/0 \
gateway=198.51.100.1 \
routing-mark=tabla_isp1
```

Definición de una tabla de ruteo paralela.

```
/ip route
add dst-address=0.0.0.0/0 \
gateway=203.0.113.1 \
routing-mark=tabla_isp2
```

Ruteo por origen (utilizando action=route)

```
/ip firewall mangle
add chain=prerouting \
src-address-list=lista_salida-isp1 \
action=route \
route-dst=198.51.100.1 \
passthrough=no

/ip firewall address-list
add action=10.0.0.30 \
list=lista_salida-isp1
```

Definición de una lista de direcciones IP.

No se realiza búsqueda en la tabla de ruteo, de utiliza directamente “route-dst”.

Completar la lista con IPs, redes o rangos.

Balanceo de carga PCC

Balanceo de carga PCC

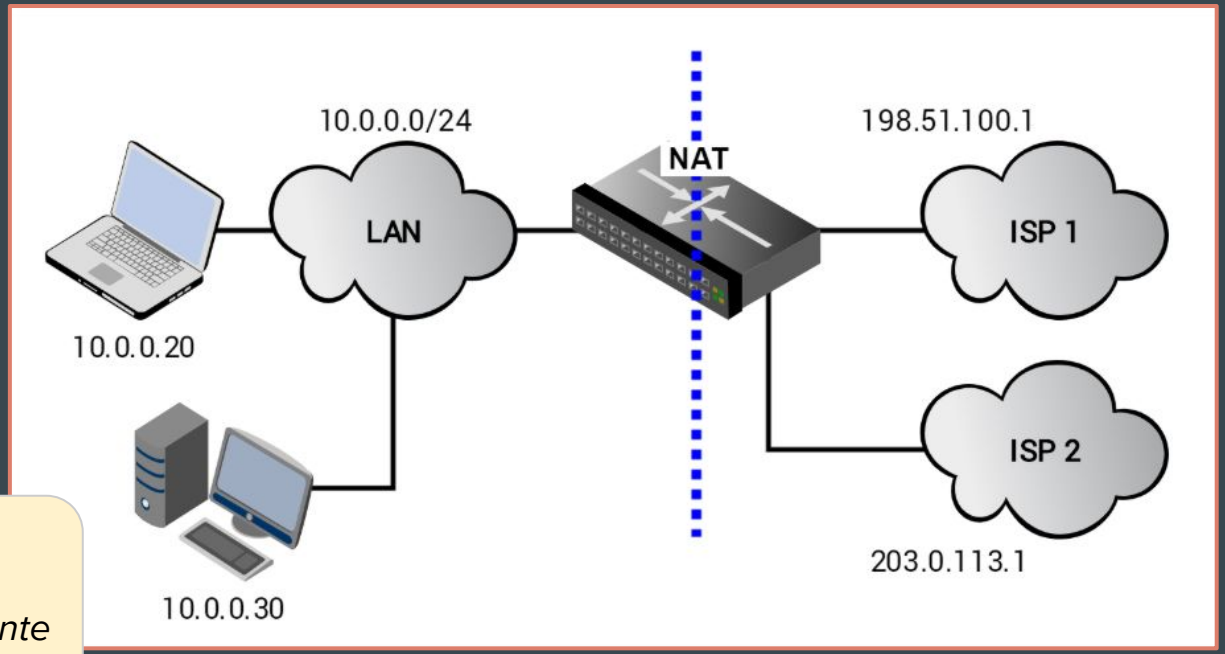
- En este caso sencillo se utiliza un conjunto de reglas con el comparador **PCC** para dividir el tráfico en múltiples “flujos”.

- Luego cada flujo se rutea por un gateway en particular.

Balanceo de carga PCC

Escenario inicial:

- 2 ISP
- 1 LAN
- NAT



Objetivo:
*Que el tráfico total se divida proporcionalmente por conexión***.*

Balanceo de carga PCC

Parte 1 - Crear tabla de ruteo para cada ISP.

Parte 2 - Asegurar que las conexiones iniciadas por un determinado ISP, sean respondidas por el mismo ISP.

Parte 3 - Establecer la política de ruteo para dividir el tráfico en “flujos”.

Balanceo de carga PCC

Parte 1 - Crear tabla de ruteo para cada ISP.

```
/ip route
add dst-address=0.0.0.0/0 \
gateway=198.51.100.1 \
routing-mark=tabla_isp1
```

Definición de una tabla de ruteo paralela.

```
/ip route
add dst-address=0.0.0.0/0 \
gateway=203.0.113.1 \
routing-mark=tabla_isp2
```

Balanceo de carga PCC

Parte 1 - En la tabla “main” mencionar cada ISP diferencia por “distance”.

```
/ip route
add dst-address=0.0.0.0/0 \
gateway=198.51.100.1 \
distance=11
```

Parámetro distance para permitir failover entre ISPs.

```
/ip route
add dst-address=0.0.0.0/0 \
gateway=203.0.113.1 \
distance=12
```

Balanceo de carga PCC

Parte 2 - Asegurar que las conexiones iniciadas por un determinado ISP, sean respondidas por el mismo ISP. Identificar conexiones nuevas:

```
/ip firewall mangle
add chain=prerouting \
in-interface=ether1_isp1 \
connection-state=new \
action=mark-connection \
new-connection-mark=mc_isp1
```

Toda conexión nueva que ingrese por ether1_isp1...

Marcar conexión como “mc_isp1”.

Balanceo de carga PCC

Parte 2 - Asegurar que las conexiones iniciadas por un determinado ISP, sean respondidas por el mismo ISP. Responder por el ISP correspondiente:

```
/ip firewall mangle
add chain=output \
connection-mark=mc_isp1 \
action=mark-routing \
new-routing-mark=tabla_isp1
passthrough=no
```

Toda conexión marcada como “mc_isp1”...

Realizar la búsqueda del próxima salto en una tabla paralela, llamada “tabla_isp1”.

Balanceo de carga PCC

Parte 3 - Establecer la política de ruteo para dividir el tráfico en “flujos”.

```
/ip firewall mangle
add chain=prerouting \
connection-state=new \
in-interface=ether5_lan \
dst-address-type=!local \
per-connection-classifier=both-addresses:2/0 \
action=mark-connection \
new-connection-mark=mc_isp1
```

Toda conexión nueva que venga desde la LAN y que no vaya destinada al router...

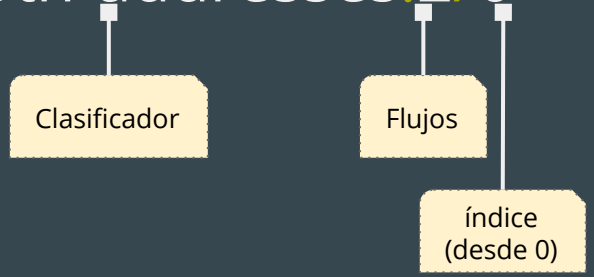
Política PCC!

Marcar conexión como “mc_isp1”.

Balanceo de carga PCC

Detalle del comparador PCC

per-connection-classifier=both-addresses:2/0



both-addresses: significa que el router va a clasificar los paquetes en base a dirección origen y destino.

2/0: significa que de la totalidad de las conexiones caigan en esta regla, sólo se tomará el 50%. Se debe crear otra regla igual, pero con 2/1 para que se tome el otro 50% de los paquetes.

Balanceo de carga PCC

Ejemplos:

per-connection-classifier=src-addresses:10/x

Divide el tráfico en 10 partes, basándose en la IP origen de los paquetes.

per-connection-classifier=both-addresses-and-ports:4/x

Divide el tráfico en 4 partes, basándose en la IP y puerto origen e IP origen y destino de los paquetes.

Balanceo de carga PCC

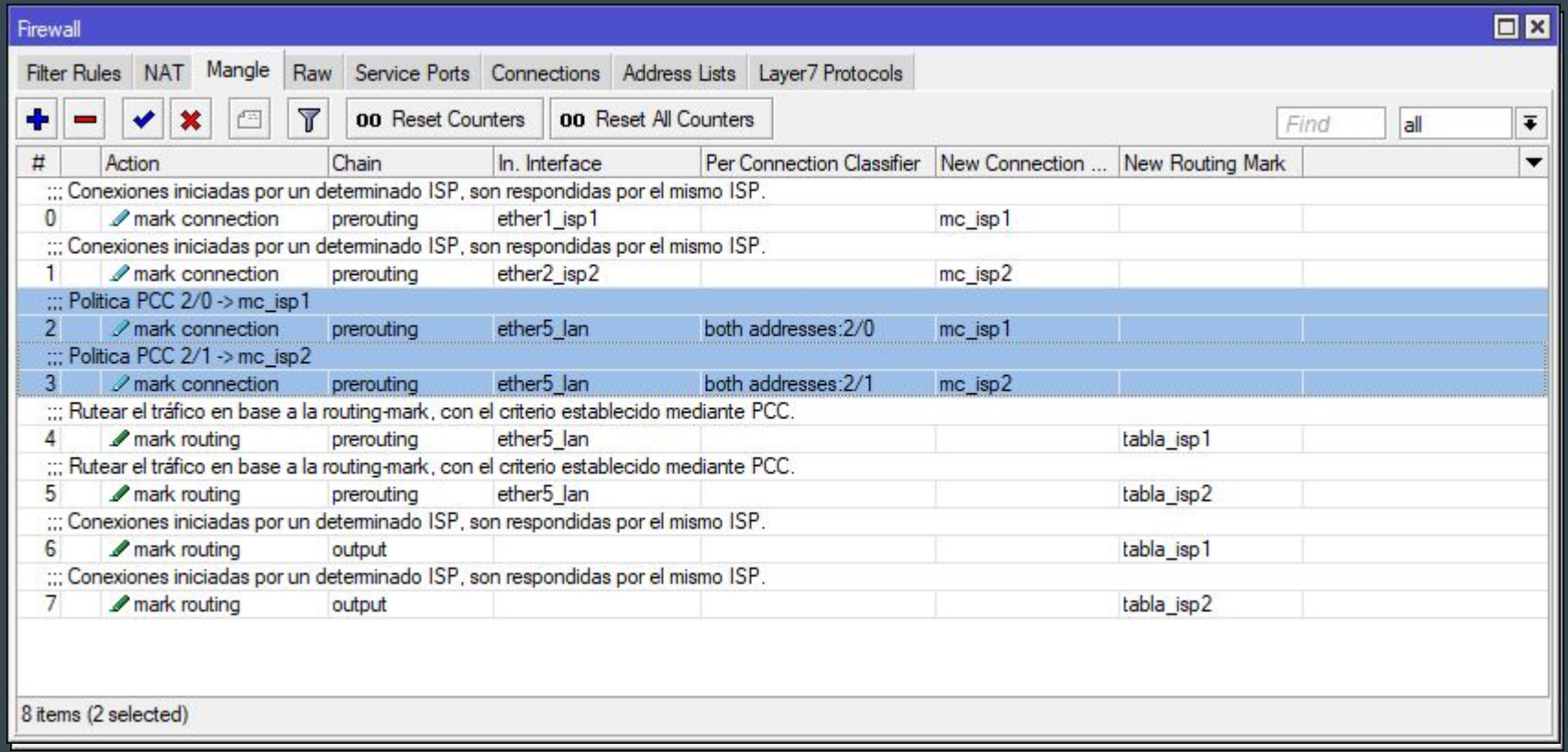
Finalmente, rutear el tráfico en base a la routing-mark establecida en las reglas anteriores con el criterio establecido mediante PCC.

```
/ip firewall mangle
add chain=prerouting \
in-interface=ether5_lan \
connection-mark=mc_isp1 \
action=mark-routing \
new-routing-mark=tabla_isp1 \
passthrough=no
```

Todo paquete perteneciente a una conexión marcada como “mc_isp1” que venga desde la LAN...

Se realiza la búsqueda del próxima salto en una tabla paralela, llamada “tabla_isp1”.

Balanceo de carga PCC



Políticas de ruteo con MikroTik RouterOS