Manual de Configuración del Balanceador de Carga Mikrotik RB750Gr3

Dr. Óscar Olvera Neria
Consultor certificado en **MTCNA**, **MTCRE**, **MTCTCE**, **MTCSE** y **MTCINE**
Versión 1.0, 24/12/2022

Cuando se tienen dos o más proveedores de servicio de internet (ISP, por sus siglas en inglés) y se desea aprovechar el ancho de banda disponible, entonces es necesario balancear el tráfico entre todos los proveedores.

Balanceo de carga a través del método PCC

En este manual se detalla la configuración para el balanceo de carga usando el método Per Classifier Connection (PCC). Este método es propietario de Mikrotik, es eficiente y permite tener control sobre el marcado de las conexiones en Mangle. PCC trabaja en capa 3 (L3) pues requiere información del encabezado de los paquetes IP de las conexiones.

a) b)

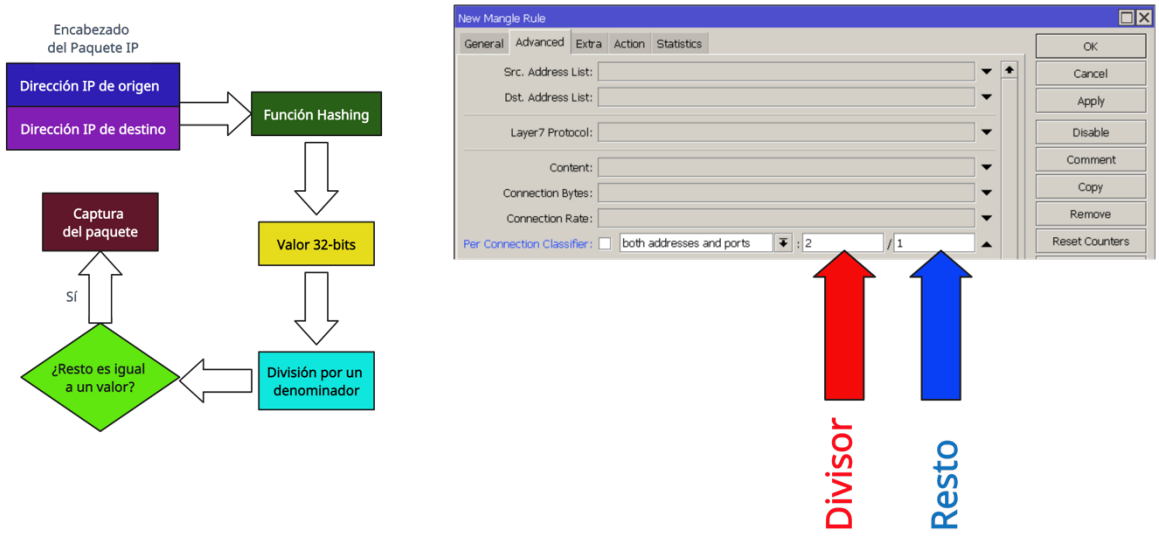


Figura 1. a) Proceso de captura de paquetes mediante el método PCC que emplea valores seleccionados del encabezado para aplicar reglas de selección y descarte de paquetes. b) Especificación de PCC en Mangle.

PCC toma los campos seleccionados (direcciones IP) del encabezado del paquete y con la ayuda de un algoritmo Hashing convierte los campos elegidos en un valor de 32-bits. Este valor es dividido por un denominador y el resto es comparado con un valor específico, entonces si son iguales el paquete será capturado. Se puede elegir la dirección IP origen o destino, el puerto

origen o destino (o combinaciones de estos valores) del encabezado para usarse en la operación Hashing, tal como se muestra en la Figura 1a.

Los detalles de PCC se declaran en Firewall → Mangle → Advanced → Per Connection Classifier, como se muestra en la Figura 1b. Divisor (*D*) corresponde al número de proveedores de servicio de internet cuando los anchos de banda son simétricos, en nuestro caso *D* = 2. Mientras que debemos definir una regla en Mangle para cada uno de los valores de resto, *R* = 0, 1. En general, *R* = *0*, 1,..., *D* –1.

En este manual se presenta la configuración cuando se tienen dos proveedores de servicios de internet y una red local, usando un Bridge con los puertos restantes. Se agrega un servidor DHCP en la red local, tal como se muestra en el diagrama de red en la Figura 2.

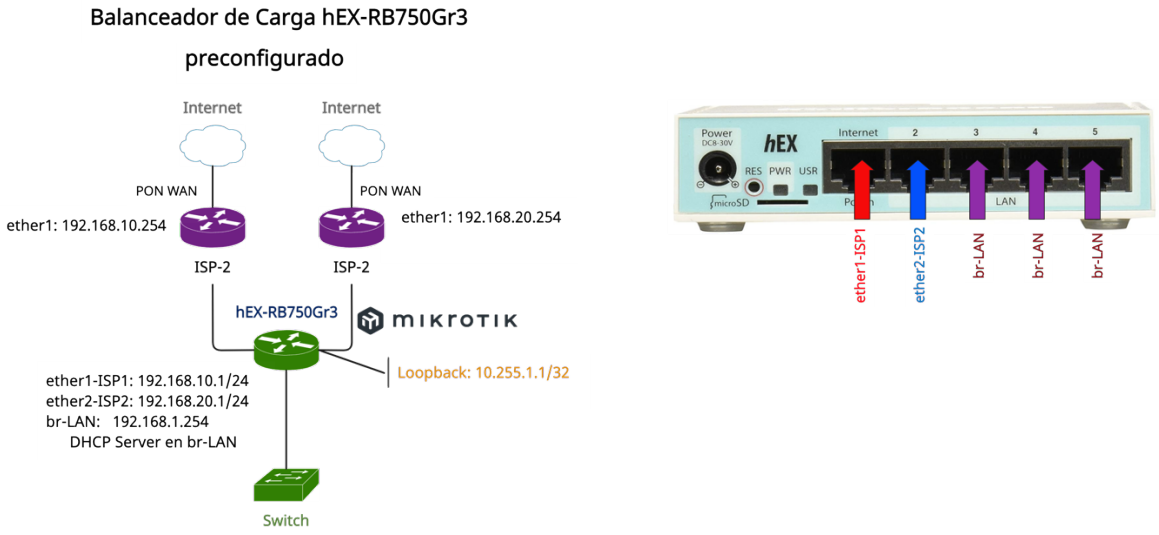


Figura 2. Diagrama de red para un Balanceo de carga usando un router Mikrotik RB750Gr3 con cinco puertos Gbps y dos proveedores de internet (ISP).

La configuración del router puede entenderse en tres sencillos pasos. El primero de ellos es asignar las IPs de cada uno de los proveedores de internet y de la red LAN. Se debe garantizar que se realiza el enmascaramiento para que la red local pueda navegar en internet. Posteriormente se debe realizar el marcado de conexiones, y con estas marcas introducir las marcas de enrutamiento. Finalmente, con las marcas de enrutamiento, en la Tabla de ruteo se agregan los Gateways que deben usarse según la marca específica de enrutamiento. También se debe activar el failover en caso de que falle algún ISP. No debe olvidarse tener rutas por defecto en caso de que el paquete no tenga marca de enrutamiento, para ello debe habilitarse la Tabla main sin marcas.

El marcado de conexiones y de enrutamiento se lleva a cabo en Mangle, es decir, el router debe tener habilitado el **Connection Tracking**, por lo que el consumo de CPU es un factor para considerar, por ello, entre más reglas se agreguen mayor será el consumo de CPU. Es importante

recordar que un paquete solo puede tener una marca, por lo que en este router no puede configurarse simultáneamente un árbol de colas que también requiere marcas de conexión. Como regla, el router utilizado como balanceador no debe usarse como Firewall, como servidor VPN, o para administrar las colas simples. El tráfico que llegue al encolador debe estar ya acotado, de manera que este equipo solo se utilice para enrutar tráfico hacia los proveedores de internet.

a) Configuración inicial del Router

En esta sección se genera la configuración inicial del router, es decir, se quita la configuración por defecto; se cambia el nombre del router y de las interfaces; se declaran los DNS; se asignan las direcciones IPs a los puertos y se configura un DHCP server para los clientes locales.

1. Eliminar la configuración por defecto del router. Conectar al puerto **ether2**, el cual tiene una dirección 192.168.88.1. Ingresar por MAC Address desde winbox:
    a. usuario: admin
    b. password:

```
> system reset-configuration no-defaults=yes skip-backup=yes
```

2. Una vez que se reinicie, ingresar nuevamente al router desde winbox usando la MAC Address. Cambiar la identidad del router

```
> system identity set name=Balanceador
```

3. Cambiar el nombre de las interfaces, dependiendo cuántos IPS se tengan. Máximo se pueden tener cuatro IPS porque el Router RB750Gr3 solo tiene cinco puertos ethernet Gbps. Un puerto se ocupa para la LAN o Bridge.

```
/interface ethernet
set [ find default-name=ether1 ] name=ether1-ISP1
set [ find default-name=ether2 ] name=ether2-ISP2
```

4. Crear un bridge llamado **br-LAN** con los puertos restantes **ether3**, **ether4** y **ether5**. En caso de que se tengan más de dos proveedores de internet se debe dejar al menos un puerto disponible para conectar un equipo switch para la red LAN.

```
/interface bridge
add name=br-LAN

/interface bridge port
add bridge=br-LAN interface=ether3
add bridge=br-LAN interface=ether4
add bridge=br-LAN interface=ether5
```

5. Asignar las direcciones IP a las interfaces que se nombraron en los pasos anteriores. Ver el diagrama de red en la Figura 2.

br-LAN: 192.168.1.254/24,
ether1-ISP1: 192.168.10.1/24
ether2-ISP2: 192.168.20.1/24

```
/ip address
add address=192.168.1.254/24 interface=br-LAN network=192.168.1.0
add address=192.168.10.1/24 interface=ether1-ISP1 network=192.168.10.0
add address=192.168.20.1/24 interface=ether2-ISP2 network=192.168.20.0
```

6. Probar que las IPs asignadas responden a través de un ping

```
> ping 192.168.1.254
> ping 192.168.10.1
> ping 192.168.20.1
```

7. Agregar un servidor DNS al router. Pueden usarse de manera temporal los servidores de google, en caso de que se tengan los DNS del proveedor ISP usarlos aquí. Permitir solicitudes remotas.

```
/ip dns
set allow-remote-requests=yes servers=8.8.8.8,8.8.4.4
```

8. Agregar un servidor DHCP a la interface **br-LAN** para que los usuarios de la red local adquieran una dirección IP de manera automática.
    a. Pool: 192.168.1.10-192.168.1.253
    b. Lease time: 24:00:00

```
/ip pool
add name=dhcp_pool0 ranges=192.168.1.10-192.168.1.253
/ip dhcp-server
add  address-pool=dhcp_pool0  disabled=no  interface=br-LAN  lease-time=1d
name=dhcp1
/ip dhcp-server network
add address=192.168.1.0/24 dns-server=8.8.8.8 gateway=192.168.1.254
```

9. Mover el cable a cualquiera de los puertos del **br-LAN** para verificar que el servidor DHCP proporciona IP al cliente. La primera dirección que asignará será la 192.168.1.253, de acuerdo con la configuración usada en este manual.

b) Agregar las rutas por defecto y enmascaramiento

En esta sección agregamos las dos rutas por defecto para cada uno de los proveedores. Esta ruta será usada para todos aquellos paquetes que no tengan marca de conexión y corresponden a la tabla de enrutamiento principal. En el diagrama de red de la Figura 2a, se muestran los Gateway para cada uno de los ISP.

1. Agregar el default Gateway para el ISP1 e ISP2

```
/ip route
add check-gateway=ping distance=1 gateway=192.168.10.254
add check-gateway=ping distance=2 gateway=192.168.20.254
```

El ISP2 se configuró como respaldo del ISP1. Todos los paquetes que no tengan marca de enrutamiento usarán estos gatways.

2. Enmascaramos el tráfico que sale por las interfaces ether1-ISP1 y ether2-ISP2 para que la red br-LAN pueda navegar en internet

```
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1-ISP1
add action=masquerade chain=srcnat out-interface=ether2-ISP2
```

c) Es necesario cambiar la contraseña y el usuario por defecto.

El usuario por defecto es admin, y la contraseña está en blanco, por lo cual será necesario cambiar la contraseña, tal como se muestra en la Figura 3. System → Password

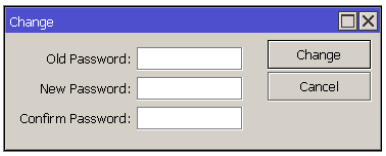


Figura 3. Ventana para cambiar contraseña del router

d) Balanceo de carga PCC

En esta sección se realizará la configuración PCC. Primero aceptamos todo el tráfico que venga de la red **br-LAN** y del ISP1 y ISP2, de esta manera no marcamos estas conexiones.

1. Creamos una regla Mangle **prerouting** con dirección destino 192.168.10.0/24 y acción **accept**.
2. Creamos una regla Mangle **prerouting** con dirección destino 192.168.20.0/24 y acción **accept**.
3. Creamos una regla Mangle **prerouting** con dirección destino 192.168.1.0/24 y acción **accept**.

Posteriormente marcamos los paquetes que entren por la interface local **br-LAN**. Esta marcación permitirá balancear las conexiones.
4. Crear una regla Mangle **prerouting** con In-Interface=**br-LAN**, PCC classifier **both addresses**, denominador 2, resto 0 con una **action**=**mark-connection** ISP1-Conn

5. Crear una regla Mangle prerouting con In-Interface=**br-LAN**, PCC classifier **both addresses**, denominador 2, resto 1 con una **action**=**mark-connection** ISP1-Conn

```
/ip firewall mangle
add action=accept chain=prerouting dst-address=192.168.10.0/24
```

```
add action=accept chain=prerouting dst-address=192.168.20.0/24
add action=accept chain=prerouting dst-address=192.168.1.0/24
add action=mark-connection chain=prerouting in-interface=br-LAN new-
connection-mark=ISP1-Conn passthrough=yes per-connection-classifier=\
    both-addresses:2/0
add action=mark-connection chain=prerouting in-interface=br-LAN new-
connection-mark=ISP2-Conn passthrough=yes per-connection-classifier=\
    both-addresses:2/1
```

6. Crear una regla Mangle **prerouting** con In-Interface=**ether1-ISP1**, **action=mark-connection** ISP1-Conn
7. Crear una regla Mangle **prerouting** con In-Interface=**ether2-ISP2**, **action=mark-connection** ISP2-Conn

```
/ip firewall mangle
add action=mark-connection chain=prerouting in-interface=ether1-ISP1 new-
connection-mark=ISP1-Conn passthrough=yes
add action=mark-connection chain=prerouting in-interface=ether2-ISP2 new-
connection-mark=ISP2-Conn passthrough=yes
```

8. Crear una regla Mangle **output** con **connection-mark=ISP1-Conn**, con una **action=mark-routing** ISP1

Creamos una regla para cuando la conexión venga desde internet a través de un proveedor de servicios de internet, la respuesta salga por el mismo proveedor.

9. Crear una regla Mangle **output** con **connection-mark=ISP2-Conn**, con una **action=mark-routing** ISP2

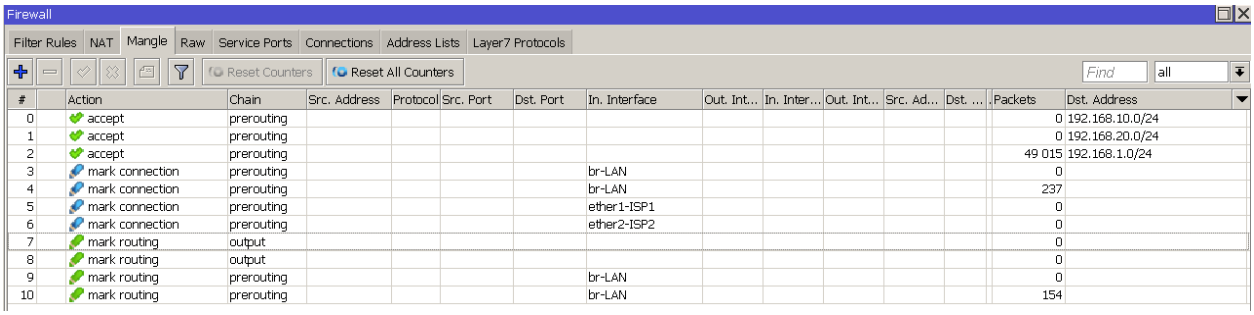
```
/ip firewall mangle
add action=mark-routing chain=output connection-mark=ISP1-Conn new-routing-
mark=ISP1 passthrough=no
add action=mark-routing chain=output connection-mark=ISP2-Conn new-routing-
mark=ISP2 passthrough=no
```

Ahora creamos las marcas de enrutamiento para las marcas de conexiones.

10. Crear una regla Mangle **prerouting** con In-Interface=**br-LAN**, **connection-mark=ISP1-Conn**, con una **action=mark-routing** ISP1

11. Crear una regla Mangle **prerouting** con In-Interface=**br-LAN**, **connection-mark=ISP2-Conn**, con una **action=mark-routing** ISP2

```
/ip firewall mangle
add action=mark-routing chain=prerouting connection-mark=ISP1-Conn in-
interface=br-LAN new-routing-mark=ISP1 passthrough=no
add action=mark-routing chain=prerouting connection-mark=ISP2-Conn in-
interface=br-LAN new-routing-mark=ISP2 passthrough=no
```



#	Action	Chain	Src. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. ...	Packets	Dst. Address
0	accept	prerouting											0	192.168.10.0/24
1	accept	prerouting											0	192.168.20.0/24
2	accept	prerouting											49 015	192.168.1.0/24
3	mark connection	prerouting					br-LAN						0	
4	mark connection	prerouting					br-LAN						237	
5	mark connection	prerouting					ether1-ISP1						0	
6	mark connection	prerouting					ether2-ISP2						0	
7	mark routing	output											0	
8	mark routing	output											0	
9	mark routing	prerouting					br-LAN						0	
10	mark routing	prerouting					br-LAN						154	

Figura 4. Orden de las reglas en Mangle. Primero aceptamos el tráfico local, luego creamos marcas de conexión, con estas marcas generamos marcas de enrutamiento.

A continuación, se muestra los comandos en Mangle en el orden correcto.

```
/ip firewall mangle
add action=accept chain=prerouting dst-address=192.168.10.0/24
add action=accept chain=prerouting dst-address=192.168.20.0/24
add action=accept chain=prerouting dst-address=192.168.1.0/24
add action=mark-connection chain=prerouting in-interface=br-LAN new-
connection-mark=ISP1-Conn passthrough=yes per-connection-classifier=\
    both-addresses:2/0
add action=mark-connection chain=prerouting in-interface=br-LAN new-
connection-mark=ISP2-Conn passthrough=yes per-connection-classifier=\
    both-addresses:2/1
add action=mark-connection chain=prerouting in-interface=ether1-ISP1 new-
connection-mark=ISP1-Conn passthrough=yes
add action=mark-connection chain=prerouting in-interface=ether2-ISP2 new-
connection-mark=ISP2-Conn passthrough=yes
add action=mark-routing chain=output connection-mark=ISP1-Conn new-routing-
mark=ISP1 passthrough=no
add action=mark-routing chain=output connection-mark=ISP2-Conn new-routing-
mark=ISP2 passthrough=no
add action=mark-routing chain=prerouting connection-mark=ISP1-Conn in-
interface=br-LAN new-routing-mark=ISP1 passthrough=no
add action=mark-routing chain=prerouting connection-mark=ISP2-Conn in-
interface=br-LAN new-routing-mark=ISP2 passthrough=no
```

d) Enrutamiento con las marcas de ruteo

Crear dos rutas hacia ISP1 y ISP2 con las marcas de enrutamiento que se han creado

1. Agregar el Gateway para cada ISP, ver diagrama de red, y agregar el failover. Es necesario que cuando no esté funcionando el marcado de conexiones, también esté habilitado un default Gateway para la tabla de enrutamiento main.

```
/ip route
add check-gateway=ping distance=1 gateway=192.168.10.254 routing-mark=ISP1
add distance=2 gateway=192.168.20.254 routing-mark=ISP1
add check-gateway=ping distance=1 gateway=192.168.20.254 routing-mark=ISP2
```

add distance=2 gateway=192.168.10.254 routing-mark=ISP2

Anexo. Configuración de balanceo Mikrotik RB750Gr3

```
# serial number = HCX081TMAXG
/interface bridge
add name=br-LAN
/interface ethernet
set [ find default-name=ether1 ] name=ether1-ISP1
set [ find default-name=ether2 ] name=ether2-ISP2
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=dhcp_pool0 ranges=192.168.1.10-192.168.1.253
/ip dhcp-server
add address-pool=dhcp_pool0 disabled=no interface=br-LAN lease-time=1d
name=dhcp1
/interface bridge port
add bridge=br-LAN interface=ether3
add bridge=br-LAN interface=ether4
add bridge=br-LAN interface=ether5
/ip address
add address=192.168.1.254/24 interface=br-LAN network=192.168.1.0
add address=192.168.10.1/24 interface=ether1-ISP1 network=192.168.10.0
add address=192.168.20.1/24 interface=ether2-ISP2 network=192.168.20.0
/ip dhcp-server network
add address=192.168.1.0/24 dns-server=8.8.8.8 gateway=192.168.1.254
/ip dns
set allow-remote-requests=yes servers=8.8.8.8,8.8.4.4
/ip firewall mangle
add action=accept chain=prerouting dst-address=192.168.10.0/24
add action=accept chain=prerouting dst-address=192.168.20.0/24
add action=accept chain=prerouting dst-address=192.168.1.0/24
add action=mark-connection chain=prerouting in-interface=br-LAN new-
connection-mark=ISP1-Conn passthrough=yes per-connection-classifier=\
    both-addresses:2/0
add action=mark-connection chain=prerouting in-interface=br-LAN new-
connection-mark=ISP2-Conn passthrough=yes per-connection-classifier=\
    both-addresses:2/1
add action=mark-connection chain=prerouting in-interface=ether1-ISP1 new-
connection-mark=ISP1-Conn passthrough=yes
add action=mark-connection chain=prerouting in-interface=ether2-ISP2 new-
connection-mark=ISP2-Conn passthrough=yes
add action=mark-routing chain=output connection-mark=ISP1-Conn new-routing-
mark=ISP1 passthrough=no
add action=mark-routing chain=output connection-mark=ISP2-Conn new-routing-
mark=ISP2 passthrough=no
add action=mark-routing chain=prerouting connection-mark=ISP1-Conn in-
interface=br-LAN new-routing-mark=ISP1 passthrough=no
add action=mark-routing chain=prerouting connection-mark=ISP2-Conn in-
interface=br-LAN new-routing-mark=ISP2 passthrough=no
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1-ISP1
add action=masquerade chain=srcnat out-interface=ether2-ISP2
/ip route
add check-gateway=ping distance=1 gateway=192.168.10.254 routing-mark=ISP1
```

```
add distance=2 gateway=192.168.20.254 routing-mark=ISP1
add check-gateway=ping distance=1 gateway=192.168.20.254 routing-mark=ISP2
add distance=2 gateway=192.168.10.254 routing-mark=ISP2
add check-gateway=ping distance=1 gateway=192.168.10.254
add check-gateway=ping distance=2 gateway=192.168.20.254
/system clock
set time-zone-name=America/Mexico_City
/system identity
set name=Balanceador
/system package update
set channel=long-term
```