BALANCEO DE CARGA

Alejandro Teixeira G.
ateixeira@mkx.cl
MikroTik Certified Trainer
MikroTik Trainer ID #TR0163

Topicos

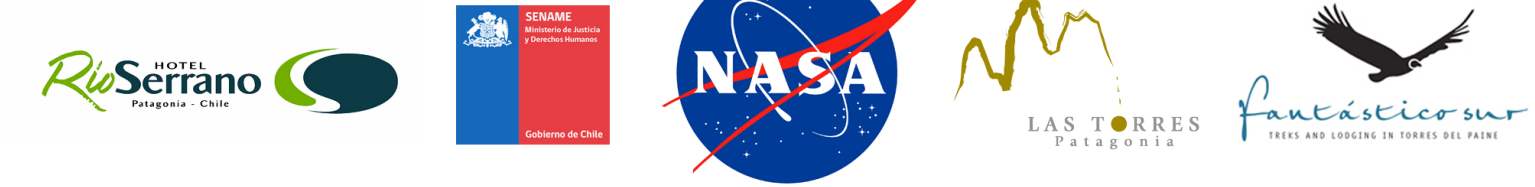
- ¿Qué es balanceo de carga?
  - Consideraciones
- Mecanismos de balanceo
  - ECMP
  - PCC
  - NTH
- Soluciones a posibles problemas
- Failover

LLEGAMOS
DONDE OTROS NO LLEGAN

Pioneros en brindar conectividad a los rincones más recónditos de la Patagonia Chilena

Nuestros clientes

NuestrosClientes



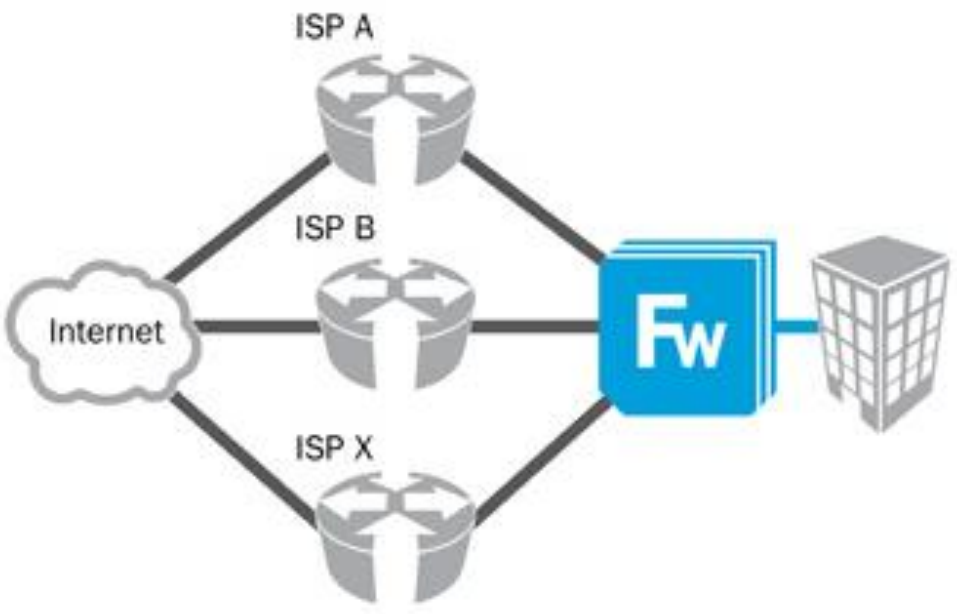
Austro proveedor oficial de NASA en Magallanes.
por segundo año consecutivo, **NASA** ha confiado en nuestros altos estándares de calidad al momento de elegir un proveedor de internet para llevar a cabo sus proyectos investigativos en el continente Antártico.

internet austro

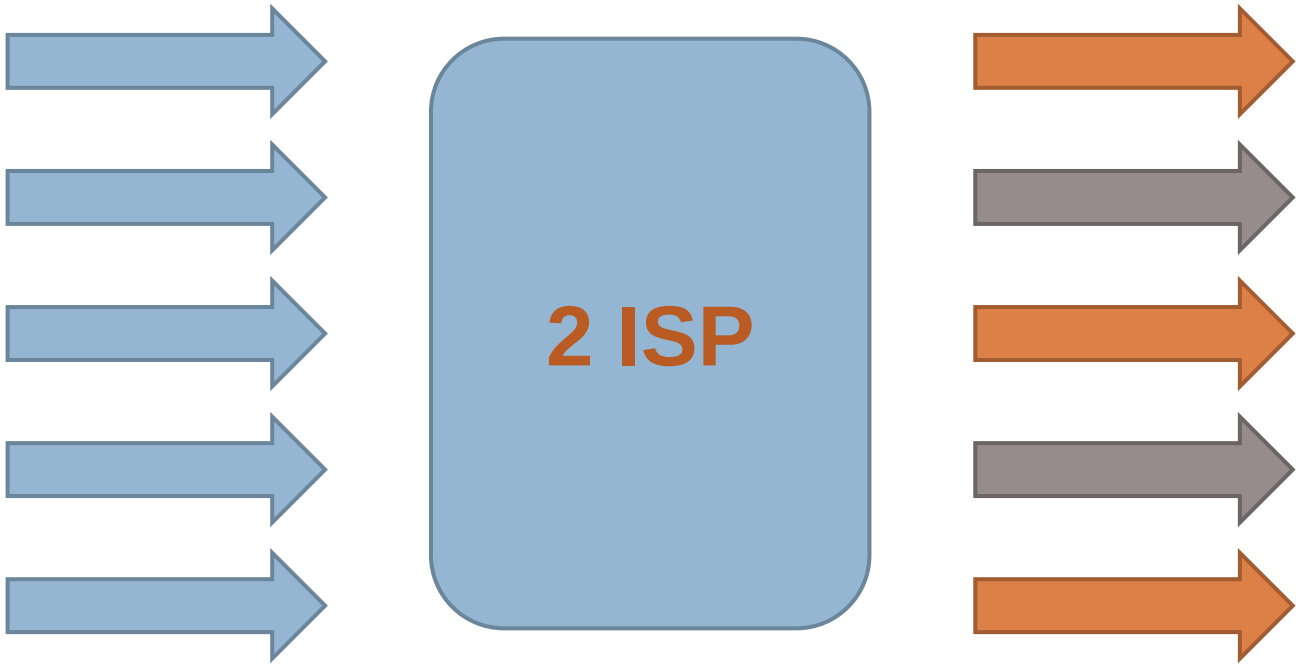
¿Qué es balanceo de carga?

¿Qué es balanceo de carga?

- Proceso a través del cual **el tráfico saliente es distribuido por múltiples enlaces**

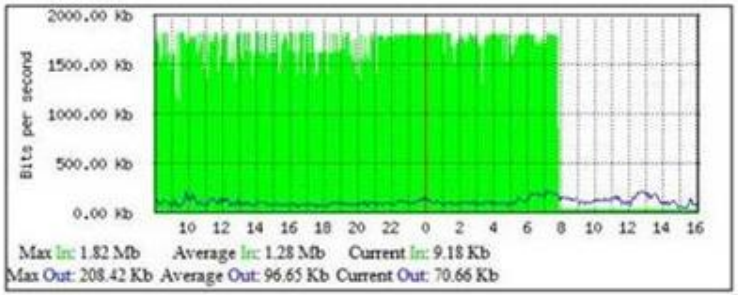


¿Qué es balanceo de carga?

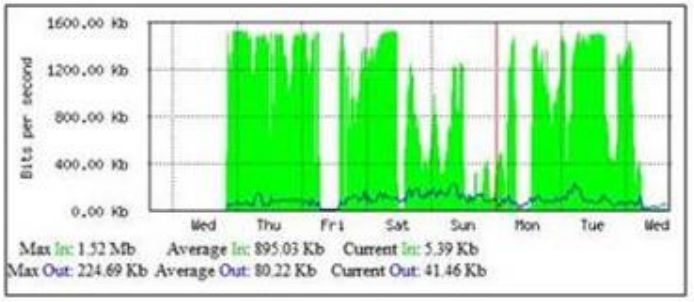


Ejemplos

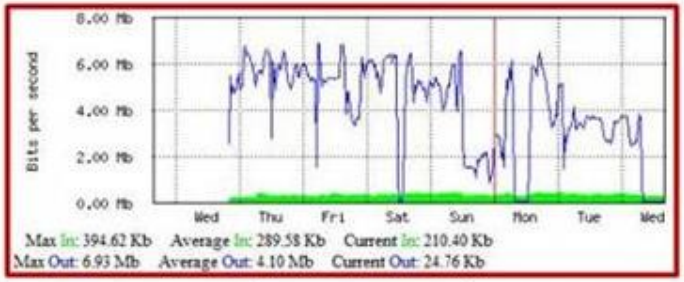
WAN1



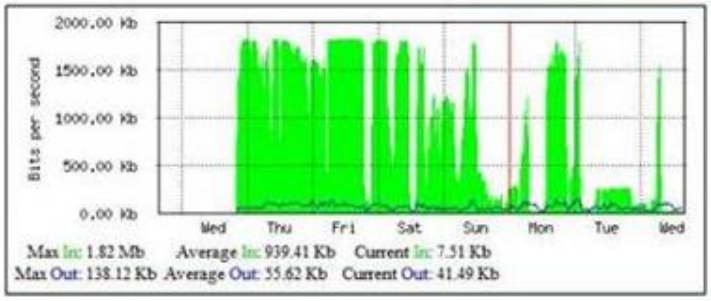
WAN2



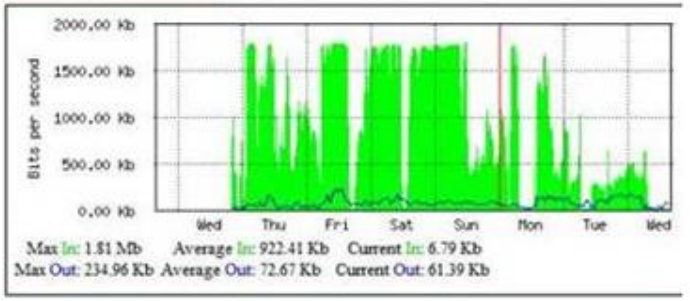
LOCAL



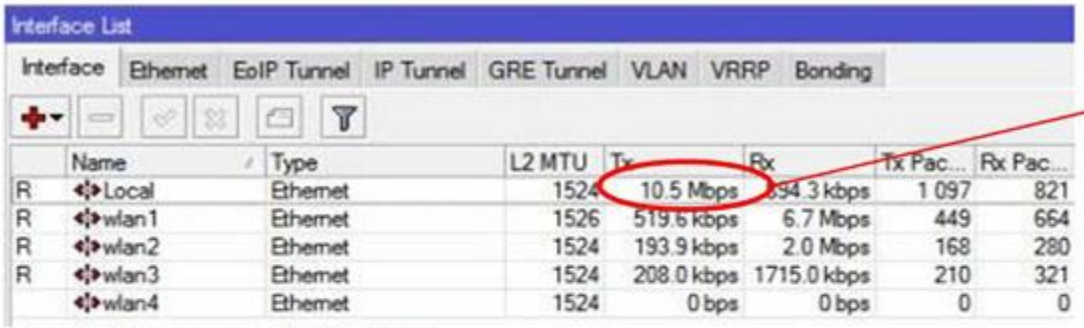
WAN3



WAN4



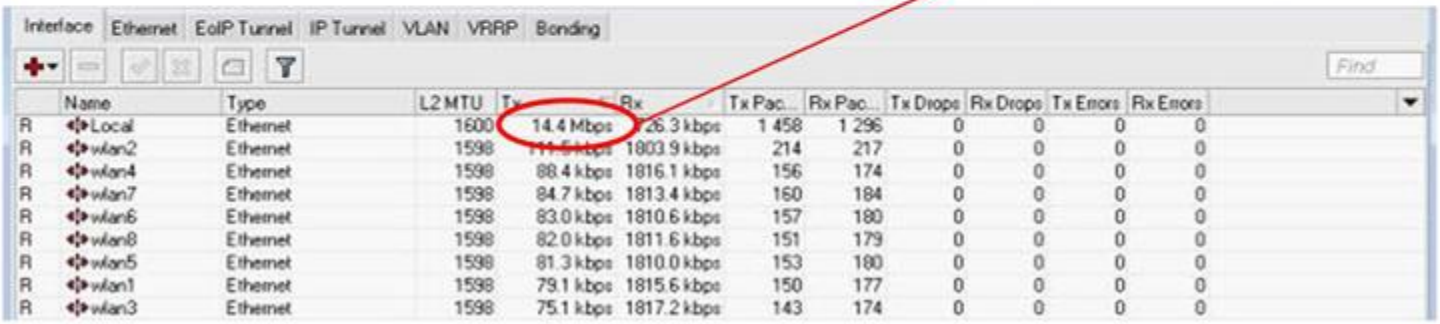
Ejemplos



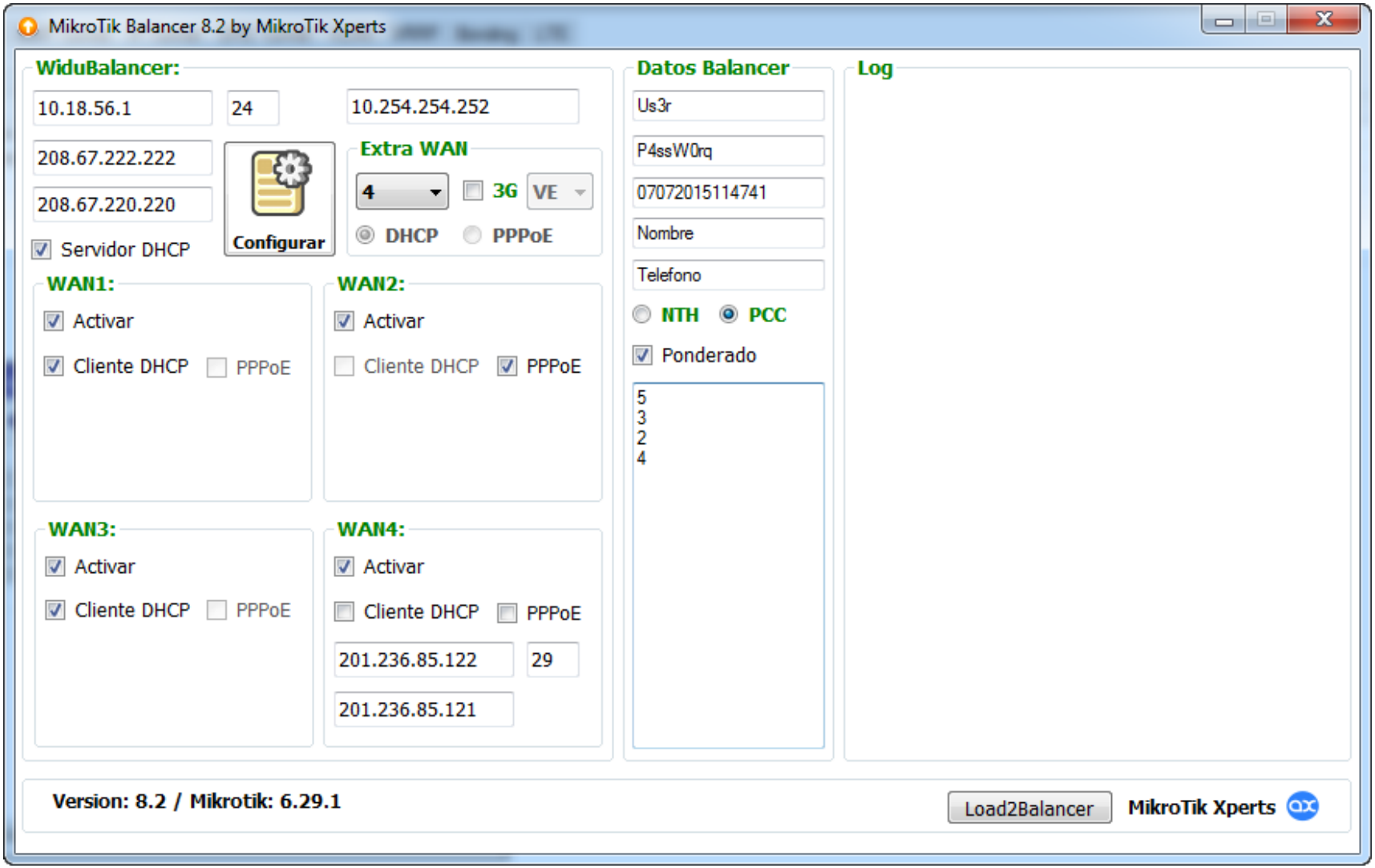
Información agregada el 07/10/2011

4 WAN
10.5 Mbps

12 WAN
14.4 Mbps



Aplicación para configuración



Consideraciones

- Cuando se emplea algún mecanismo de balanceo, **lo que realmente se balancea son el número total de conexiones** entre la cantidad de enlaces disponibles.
- **No se balancea el consumo de tráfico ni se "suma" literalmente.**

Mecanismos de balanceo

Herramientas involucradas

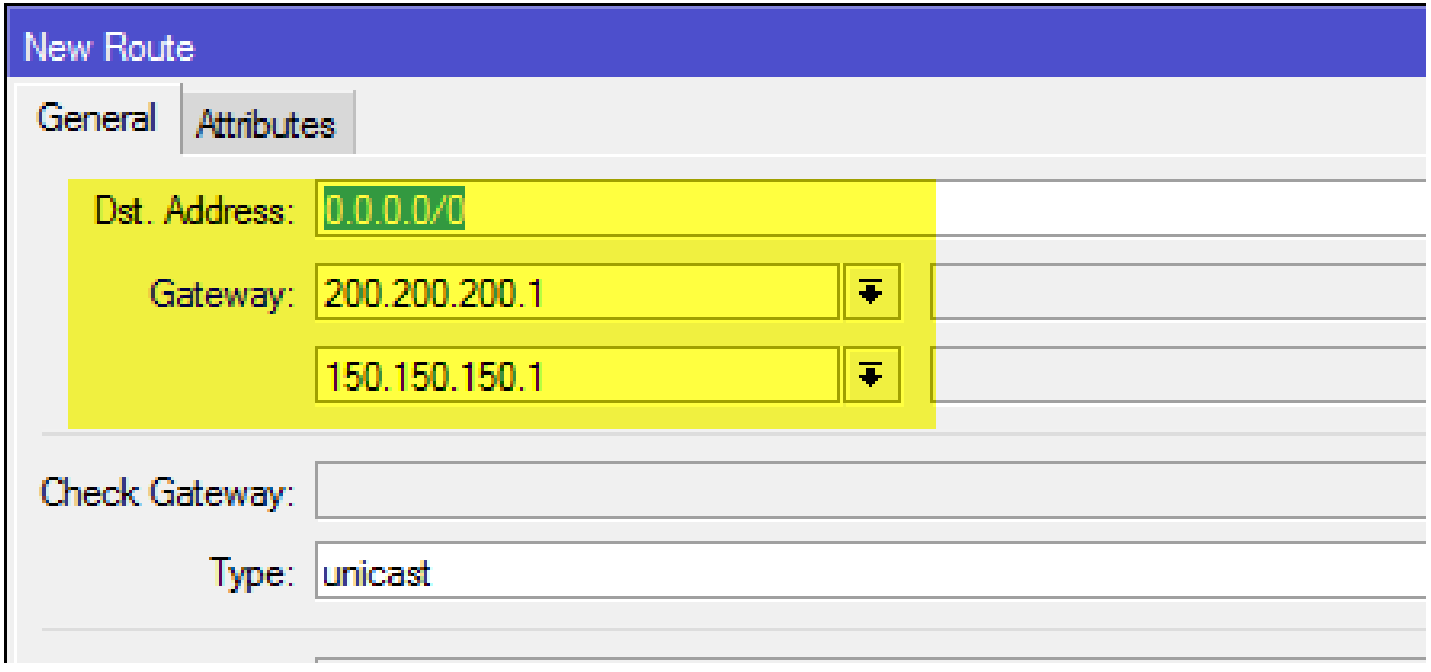
- **/ip firewall mangle**
- **/ip route**
- **/system scripts**
- **/system scheduler**
- **/ip firewall filter**

ECMP: Equal Cost Multi-Path

- Simple de implementar
- Balanceo persistente por conexión
- Se agregan todas las puertas de enlace
  - En la misma ruta
- No se puede controlar la forma de balanceo
- No funciona con puertas de enlace iguales
  - Mas de una por proveedor
- Failover automatico
  - No es práctico

ECMP: Implementación


```
/ip route add
gateway=1.1.1.1,2.2.2.1
check-gateway=ping
```



PCC: Peer Connection Classifier

- Sofisticado
- No distribuye de forma equitativa la cantidad de conexiones
- PCC toma algunos campos de la cabecera IP
  - Alguna combinación
    - IP (origen/destino) y puerto (origen/destino)
  - La cabecera se divide por el número de ISP activos
  - El resultado indica
- Clasificadores
  - src-address
  - dst-address
  - src-port
  - dst-port

PCC: ¿Cómo funciona?

- Número de enlaces wan: 3
- Posibles resultados: 0, 1 o 2

- Hash 1: 14350 / 3 = 1
- Hash 2: 3480 / 3 = 0
- Hash 3: 13468 / 3 = 1
- Hash 4: 5390 / 3 = 2
- Hash 5: 7894 / 3 = 1

- Link 0: 1
- Link 1: 3
- Link 2: 1

ALEATORIO

PCC: Implementación

/ip firewall mangle add
chain=prerouting
in-interface=lan
connection-mark=no-mark
action=mark-connection
new-connection-mark=wan1_conn
per-connection-classifier=both-addresses:2/1

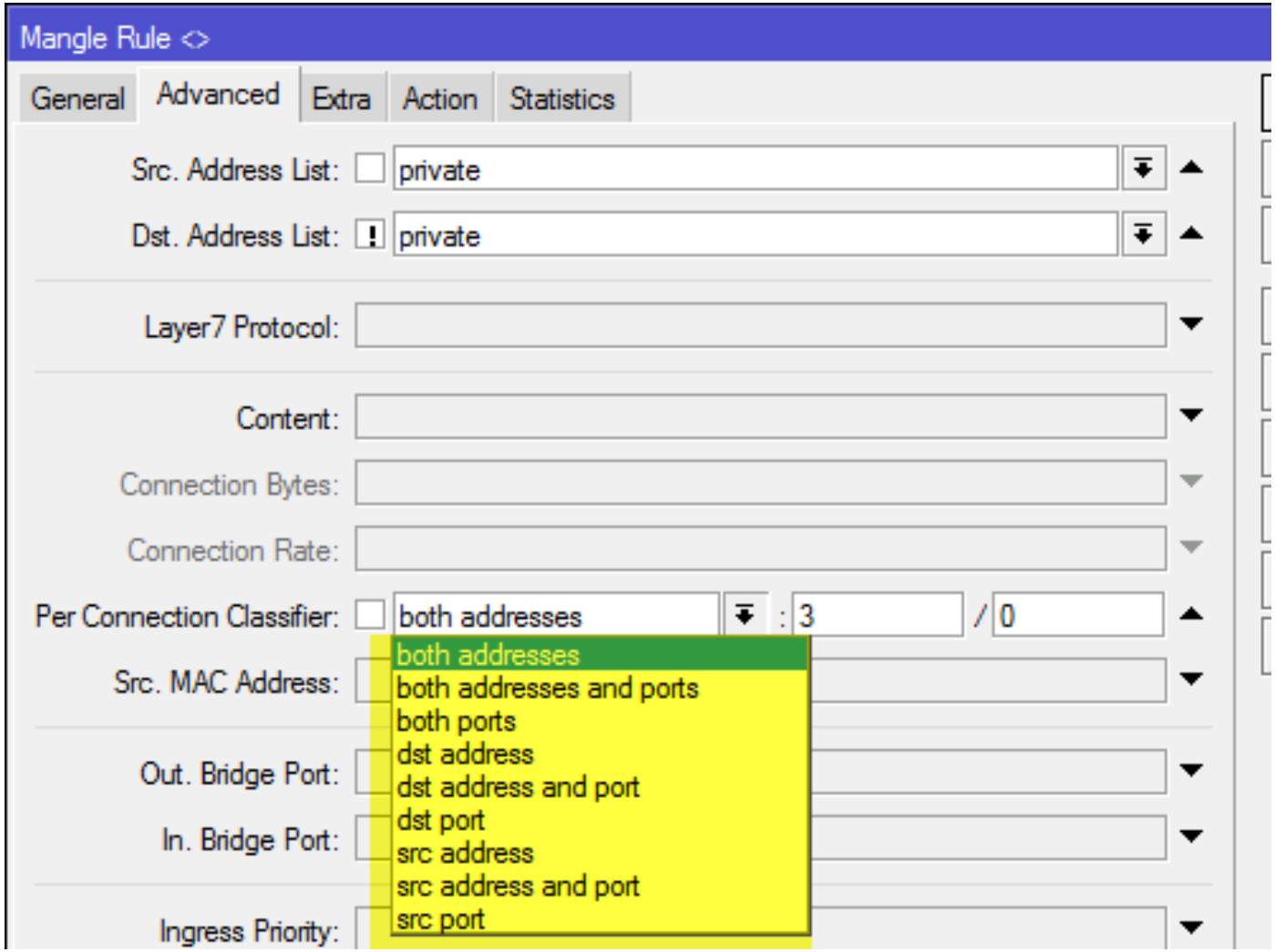
Marcas de nuevas conexiones

Repetir para cada WAN

/ip firewall mangle add
chain=prerouting
in-interface=lan
connection-mark=wan1_conn
action=mark-routing
new-routing-mark=to_wan1
passthrough=no

Marca de rutas para cada conexión marcada

PCC:MANGLE


Mangle Rule <>
General
Advanced
Extra
Action
Statistics
Src. Address List:
private
Dst. Address List:
private
Layer7 Protocol:
Content:
Connection Bytes:
Connection Rate:
Per Connection Classifier:
both addresses
3
0
Src. MAC Address:
Out. Bridge Port:
In. Bridge Port:
Ingress Priority:
both addresses
both addresses and ports
both ports
dst address
dst address and port
dst port
src address
src address and port
src port

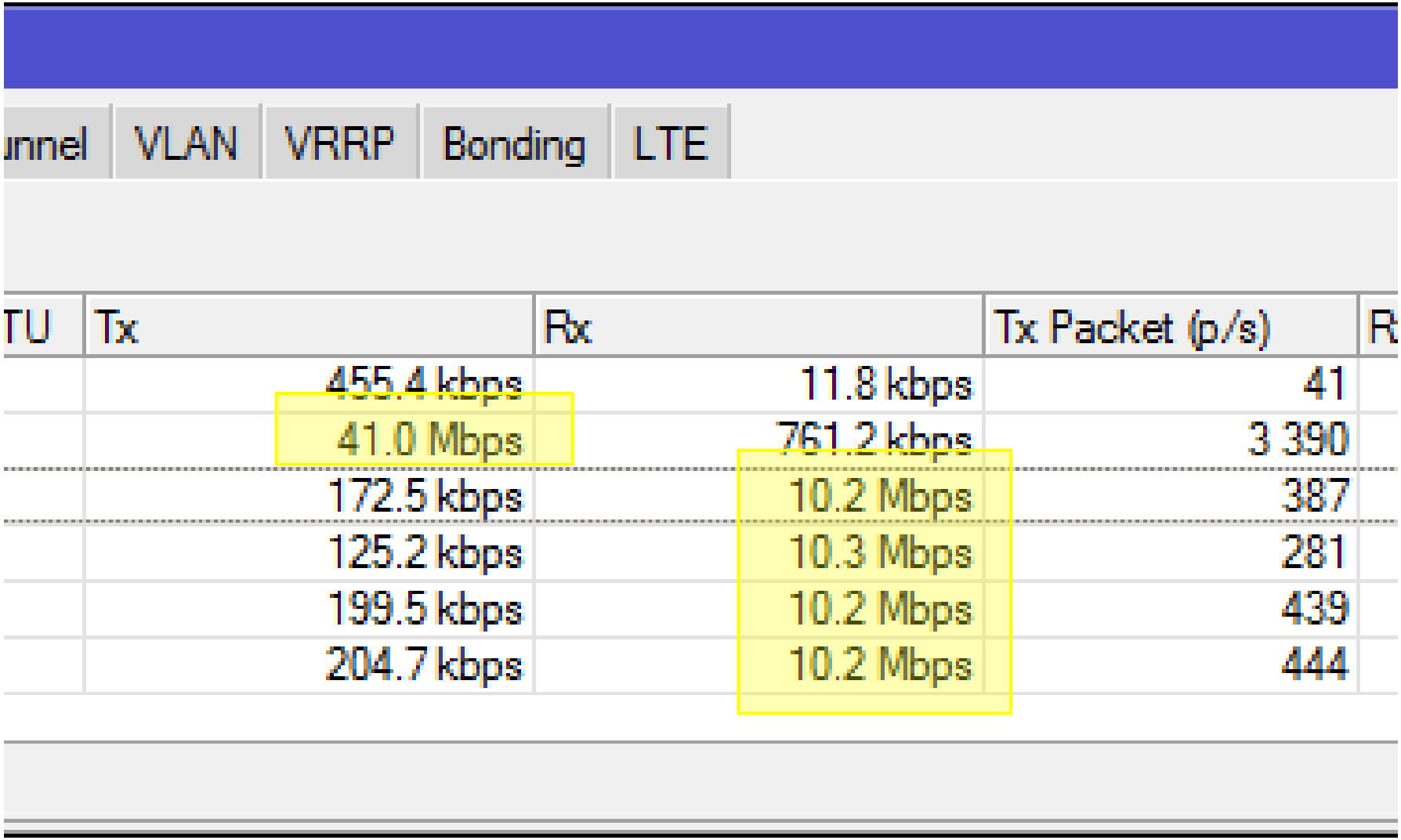
PCC: implementación

/ip route add
distance=1
gateway=1.1.1.1
routing-mark=to_wan1

/ip route add
distance=1
gateway=2.2.2.1
routing-mark=to_wan2

Rutas

Balanceo con 4 enlaces de 10M



NTH

- Permite distribuir de forma **equitativa**
- Cada regla del NTH tiene su propio **contador**
- Cuando una regla **recibe un paquete** se **incrementa el contador**
- Cuando el contador llega al máximo se reinicia

NTH: implementación

/ip firewall mangle add
chain=prerouting
in-interface=lan
connection-mark=no-mark
action=mark-connection
new-connection-mark=wan**[link number]**_conn
nth=**[link number]**,1

Nuevas marcas de conexión

Repetir para cada WAN

/ip firewall mangle add
chain=prerouting
in-interface=lan
connection-mark=wan1_conn
action=mark-routing
new-routing-mark=to_wan1
passthrough=no

Marca de rute para cada marca de conexión

NTH: implementación

/ip route add
distance=1
gateway=1.1.1.1
routing-mark=to_wan1

/ip route add
distance=1
gateway=2.2.2.1
routing-mark=to_wan2

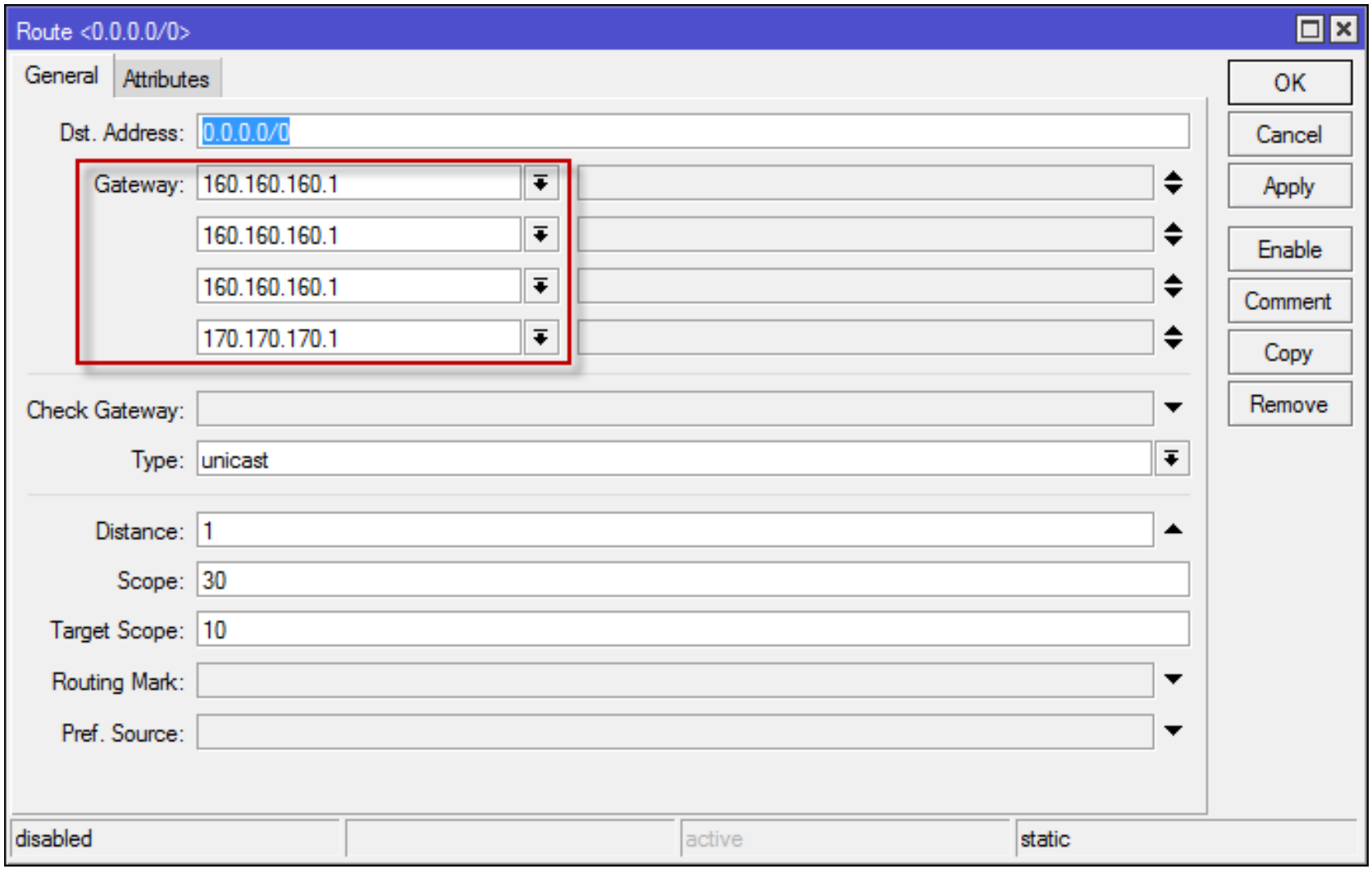
Rutas iguales que PCC

Poderación de enlaces

¿Dónde puedo aplicar ponderación?

- ECMP
  - Simple de implementar
- PCC
  - Complejo de implementar
  - Robusto y escalable
- NTH
  - No permite implementar

Ponderación: ECMP



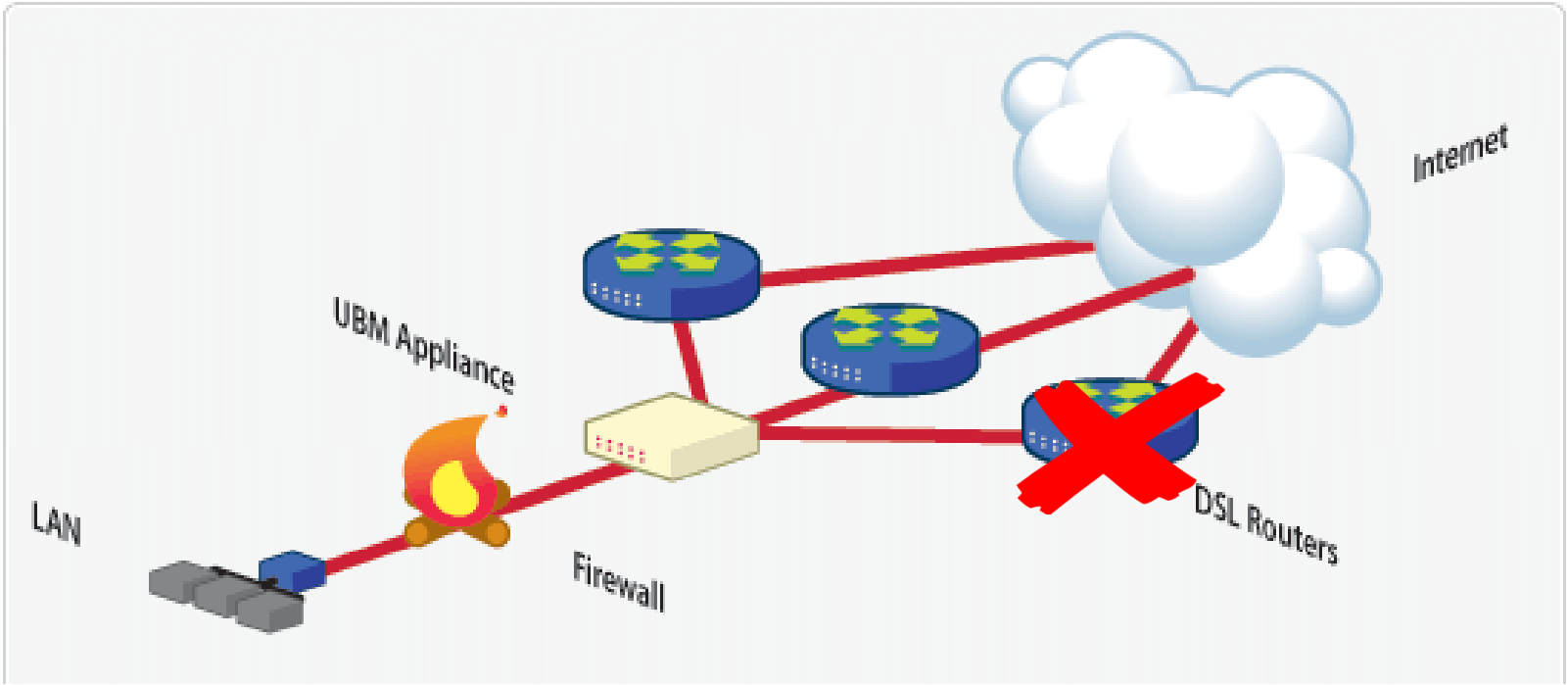
Ponderación: PCC

- add action=mark-connection chain=prerouting comment="SIN PONDERACION - 2 WAN / PCC" **connection-mark=no-mark** in-interface=ether2_laptop new-connection-**mark=mc_to-wan1 per-connection-classifier=both-addresses-and-ports:8/x**

	both addresses and ports:8/0	mc_to-wan1	0 B	0	CON PONDERAC...	
	both addresses and ports:8/1	mc_to-wan1	0 B	0	CON PONDERAC...	
	both addresses and ports:8/2	mc_to-wan1	250 B	2	CON PONDERAC...	
	both addresses and ports:8/3	mc_to-wan2	0 B	0	CON PONDERAC...	
	both addresses and ports:8/4	mc_to-wan2	0 B	0	CON PONDERAC...	
	both addresses and ports:8/5	mc_to-wan3	0 B	0	CON PONDERAC...	
	both addresses and ports:8/6	mc_to-wan3	0 B	0	CON PONDERAC...	
	both addresses and ports:8/7	mc_to-wan4	0 B	0	CON PONDERAC...	

Failover

Failover



Cómo manejar Failover

- Formas comúmes
  - Scripts
    - Haciendo ping a links externos.
  - Netwatch
    - Haciendo ping a links externos.
- Sin scripts ni Netwatch
  - Routes Nexthop Lookup
    - Rutas recursivas
    - Usando scope=10
    - check-gateway=ping

Failover: scripts


```
:local pingip
:set pingip [/ping 1.1.1.1 count=10]
:if ($pingip = 0) do={
        /ip dhcp-client disable [find interface=ether1_wan1]
        :delay 1s
        /ip dhcp-client enable [find interface=ether1_wan1]
}
:global gateway1a [/ip dhcp-client get [find interface=wan1] gateway]
:global gateway1b [/ip route get [find routing-mark=mr_to-wan1 comment=mr_to-wan1] gateway]
:if ($gateway1a != $gateway1b) do={
        /ip route set [find comment=mr_to-wan1] gateway=$gateway1a
}
```

Failover: consideraciones

- Debe existir **una o mas rutas por defecto**
  - Se usa como desborde cuando una tabla de enrutamiento no está disponible
- Se puede aplicar la opción **check-gateway=ping** para revisar estado de la puerta de enlace
  - Esto no garantiza que el servicio esté caído dado que solo revisa la conexión con la puerta de enlace
- **Se debe hacer chequeo externo**

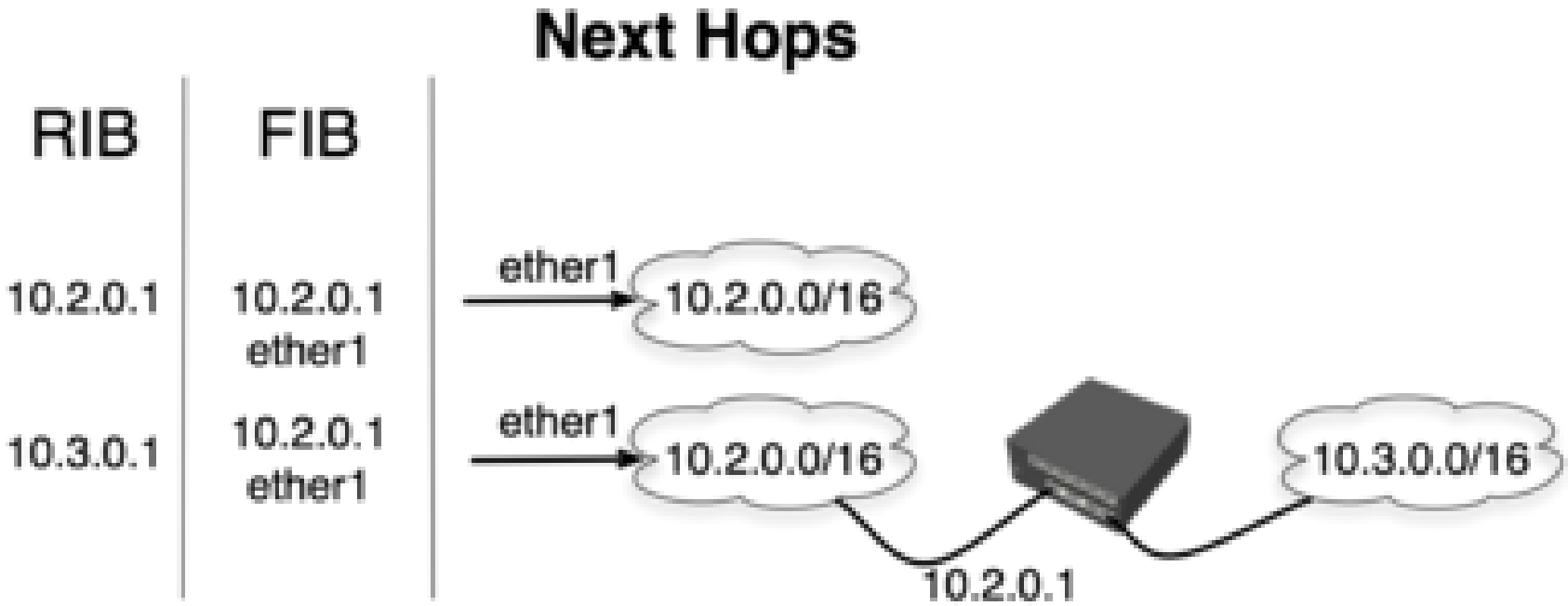
Resolviendo el Next-Hop Recursivo

- Es posible especificar el gateway a una red incluso si el gateway no se puede alcanzar directamente. Esto se puede lograr usando **Resolución de Next-Hop Recursivo** desde cualquier ruta existente

- **Una ruta debe estar en el scope** (al alcance) de otra ruta para que la Resolución de Next-Hop Recursivo funcione.

Nexthop Lookup: scope

- Nexthop 10.2.0.1 es resuelta por una ruta conectada, su estado es alcanzable
- Nexthop 10.3.0.1 es resuelto a través de la ruta 10.3.0.0/16, su estado es recursivo, y utiliza 10.2.0.1 como valor de próximo salto instalado en el FIB.



Failover

Failover usando scope y check-gateway by ping

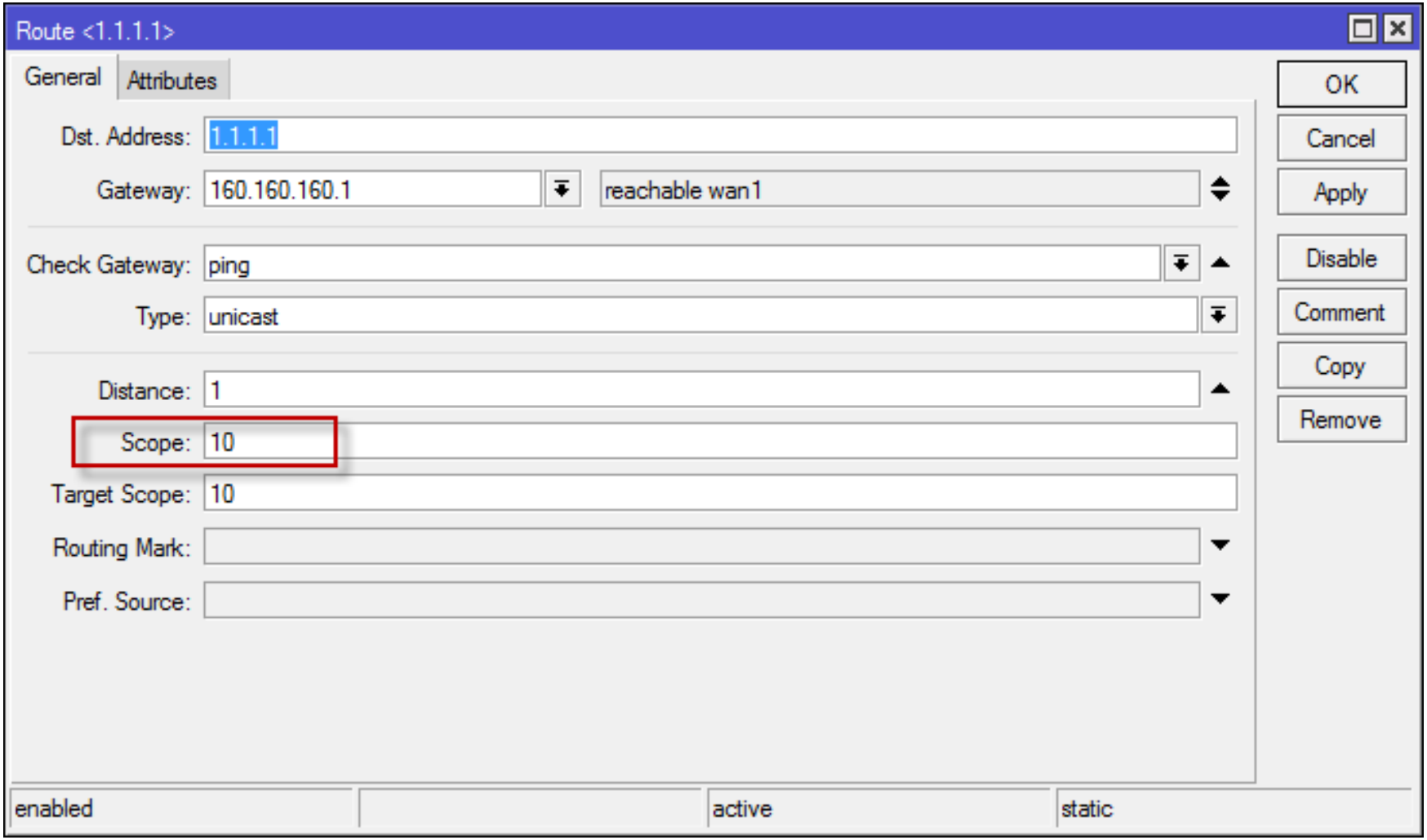
/ip route

add **dst-address**=8.8.8.8 **gateway**=1.1.1.1 **scope=10**
add **dst-address**=8.8.4.4 **gateway**=2.2.2.1 **scope=10**

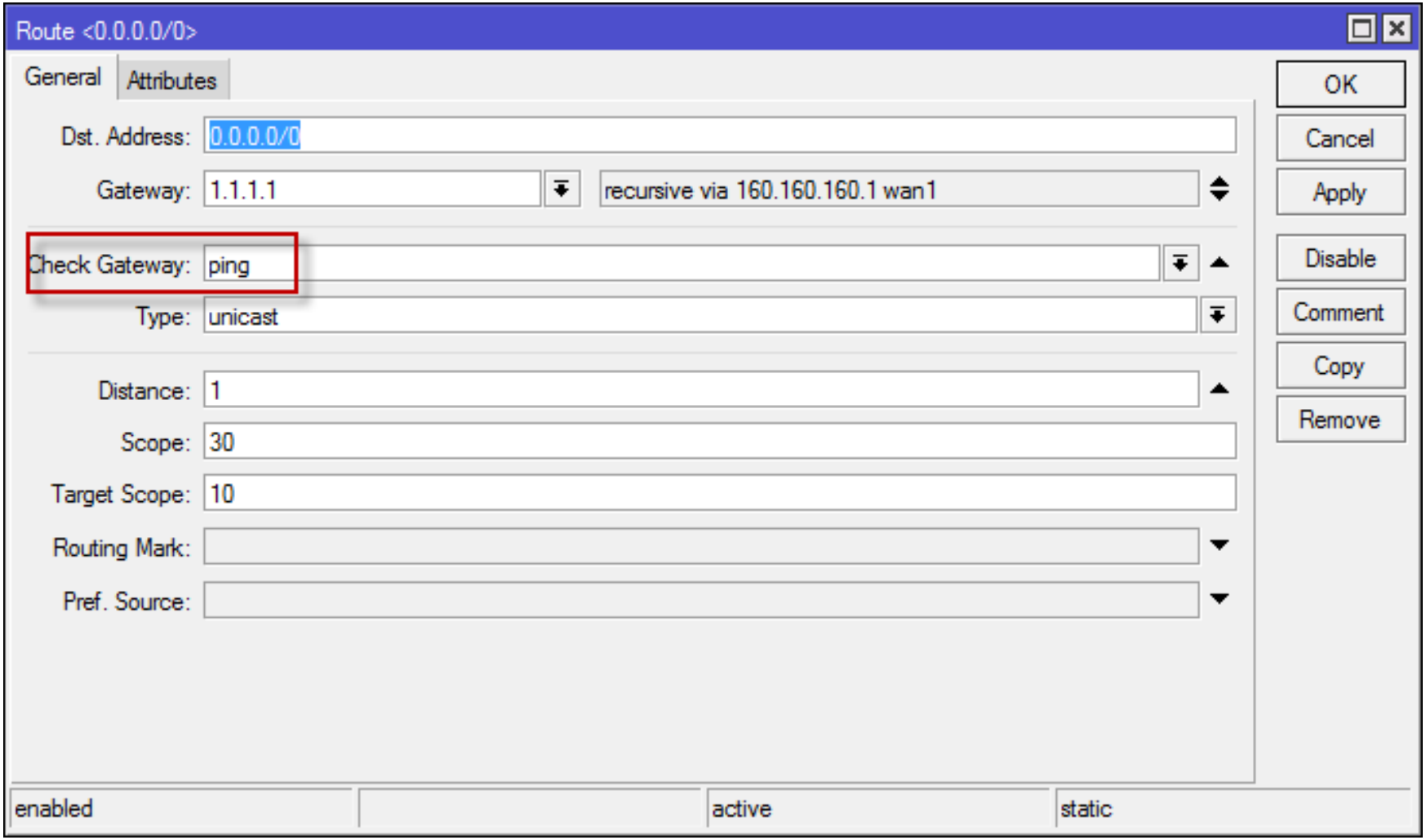
add **distance**=1 dst-adress=0.0.0.0/0 **gateway**=8.8.8.8 **routing-mark**=to_wan1 **check-gateway=ping**

add **distance**=2 **gateway**=8.8.4.4 **routing-mark**=to_wan2 **check-gateway=ping**

Failover: chequeo ping recursivo



Failover: chequeo ping recursivo



Failover: chequeo ping recursivo

Route List

Routes | Nexthops | Rules | VRF

Find | all

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source	Comment
XS	0.0.0.0/0	3.3.3.3	1	mr_to-wan3		recursive - x
XS	0.0.0.0/0	4.4.4.4	1	mr_to-wan4		recursive - x
AS	0.0.0.0/0	2.2.2.2 recursive via 170.170.170.1 wan2	1	mr_to-wan2		recursive - wan2
AS	0.0.0.0/0	1.1.1.1 recursive via 160.160.160.1 wan1	1	mr_to-wan1		recursive - wan1
AS	2.2.2.2	170.170.170.1 reachable wan2	1			recursive - mr_to-wan2
AS	1.1.1.1	160.160.160.1 reachable wan1	1			recursive - mr_to-wan1
AS	0.0.0.0/0	1.1.1.1 recursive via 160.160.160.1 wan1	1			recursive - default
S	0.0.0.0/0	2.2.2.2 recursive via 170.170.170.1 wan2	2			recursive - default
XS	4.4.4.4	179.179.179.1%wan4	1			mr_to-wan4 - recursive
XS	0.0.0.0/0	179.179.179.1%wan4	1	mr_to-wan4		mr_to-wan4
XS	0.0.0.0/0	179.179.179.1%wan4	4			mr_to-wan4
XS	3.3.3.3	179.179.179.1%wan3	1			mr_to-wan3 - recursive
XS	0.0.0.0/0	179.179.179.1%wan3	1	mr_to-wan3		mr_to-wan3
XS	0.0.0.0/0	179.179.179.1%wan3	3			mr_to-wan3
XS	0.0.0.0/0	170.170.170.1	1	mr_to-wan2		mr_to-wan2
XS	0.0.0.0/0	170.170.170.1	2			mr_to-wan2
XS	0.0.0.0/0	160.160.160.1	1	mr_to-wan1		mr_to-wan1
XS	0.0.0.0/0	160.160.160.1	1			mr_to-wan1
XS	0.0.0.0/0	160.160.160.1 , 160.160.160.1 , 160.160.160.1 , 170.170....	1			ECMP PONDERADO
XS	0.0.0.0/0	170.170.170.1 , 160.160.160.1	1			ECMP
AS	10.253.253.0/...	100.100.100.1 reachable ether1_admin	1			
DAC	100.100.100.0...	ether1_admin reachable	0		100.100.100....	
DAC	160.160.160.0...	wan1 reachable	0		160.160.160....	
DAC	170.170.170.0...	wan2 reachable	0		170.170.170....	
DAC	179.179.179.0...	wan3 reachable, wan4 reachable	0		179.179.179....	
DAC	192.168.255.0...	ether2_laptop reachable	0		192.168.255.1	

26 items (6 selected)

Failover recursivo

- **Importante:** Éste método de implementar failover no funciona cuando se tienen múltiples links con el mismo gateway. En éste caso es necesario scripts o netwatch chequeando enlaces externos.
- Si el enlace no tiene IP y gateway fijo también son necesarios scripts.

Failover con desborde

Failover con desborde

- **Redistribuye** las conexiones correspondientes a la wan sin servicio por el resto de las wan.
- La redistribución se puede llevar a cabo usando diferentes lógicas. Depende directamente del criterio del administrador
  - Redistribución **en base a ponderaciones**
  - Redistribución **en base a cantidad de wan**
- Técnica complicada y compleja de desarrollar
  - Se recomienda emplear herramientas API

Ejercicio: failover con desborde

		1	2	3	2,3	1,3	1,2
	1,2,3	2,3	1,3	1,2	1	2	3
6/0	1	2	1	1	1	2	3
6/1	1	2	1	1	1	2	3
6/2	1	3	1	1	1	2	3
6/3	2	2	1	2	1	2	3
6/4	2	2	1	2	1	2	3
6/5	3	3	3	1	1	2	3

Ejercicio: failover con desborde

ether2_laptop		both addresses and ports:6/0	0 B	0	mc_to-wan1
ether2_laptop		both addresses and ports:6/1	0 B	0	mc_to-wan1
ether2_laptop		both addresses and ports:6/2	0 B	0	mc_to-wan1
ether2_laptop		both addresses and ports:6/3	0 B	0	mc_to-wan2
ether2_laptop		both addresses and ports:6/4	0 B	0	mc_to-wan2
ether2_laptop		both addresses and ports:6/5	0 B	0	mc_to-wan3
ether2_laptop		both addresses and ports:6/0	0 B	0	mc_to-wan2
ether2_laptop		both addresses and ports:6/1	0 B	0	mc_to-wan2
ether2_laptop		both addresses and ports:6/2	0 B	0	mc_to-wan3
ether2_laptop		both addresses and ports:6/3	0 B	0	mc_to-wan1
ether2_laptop		both addresses and ports:6/4	0 B	0	mc_to-wan1
ether2_laptop		both addresses and ports:6/5	0 B	0	mc_to-wan1
ether2_laptop		both addresses and ports:6/2	0 B	0	mc_to-wan2
ether2_laptop		both addresses and ports:6/5	0 B	0	mc_to-wan2
ether2_laptop		both addresses and ports:6/0	0 B	0	mc_to-wan3
ether2_laptop		both addresses and ports:6/1	0 B	0	mc_to-wan3
ether2_laptop		both addresses and ports:6/3	0 B	0	mc_to-wan3
ether2_laptop		both addresses and ports:6/4	0 B	0	mc_to-wan3

Posibles problemas

Posibles problemas balanceando

- Problemas con páginas HTTPS
- Problemas con conexiones al mismo router
- Permitir acceso a servidores internos por una WAN específica (DST-NAT)
- Forzar un host por una wan específica.
- Varios links con el mismo gateway

Problema con SSL páginas HTTPS

- Sitios como Gmail y bancos no permiten establecer múltiples conexiones provenientes de diferentes enlaces simultáneamente.
  - Phishing
- Comunmente se usa el 443

Problema con SSL páginas HTTPS

/ ip firewall mangle

Colocar de primera en el mangle

add action=accept chain=prerouting dst-port=443 in-interface=lan passthrough=no protocol=tcp

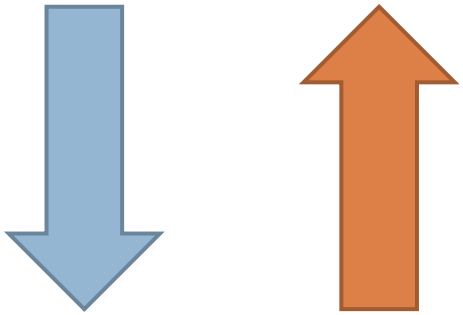
/ip route

Ruta por defecto para conexiones delmismo router o no marcadas.

add distance=1 gateway=1.1.1.1
add distance=1 gateway=2.2.2.1

Problema con conexiones dirigidas al router

- Paquetes salientes utilizan la misma decisión de ruteo que los paquetes que atraviesan el router.
- Las respuestas de un paquete que fue recibida por wan1 podría ser enviada de vuelta y enmascarada por wan2



Problema con conexiones dirigidas al router

/ip firewall mangle add
action=mark-connection
chain=input
connection-mark=no-mark
in-interface=wan1
new-connection-mark=wan1_conn

Marcamos conexiones de entrada

Repetim os para cada wan

/ip firewall mangle add
action=mark-routing
chain=output
connection-mark=wan1_conn
new-routing-mark=to_wan1
passthrough=no

Forzamos que la conexión sea ruteada por una wan específica.

Permitir acceso a servidores internos desde una wan específica

- add action=mark-connection **chain=forward** connection-mark=no-mark **in-interface=wan1 new-connection-mark=mc_to-wan1 out-interface=ether2_laptop passthrough=no**

- add action=mark-routing **chain=prerouting connection-mark=mc_to-wan1** in-interface=ether2_laptop **new-routing-mark=mr_to-wan1** passthrough=no

Forzar acceso a internet por una wan específica

- add **action=mark-routing chain=prerouting** comment=EXCEPCION **dst-address=54.165.129.249 new-routing-mark=mr_to-wan2**

Múltiples enlaces con el mismo Gateway

Forza el tráfico respetando cada routing-mark

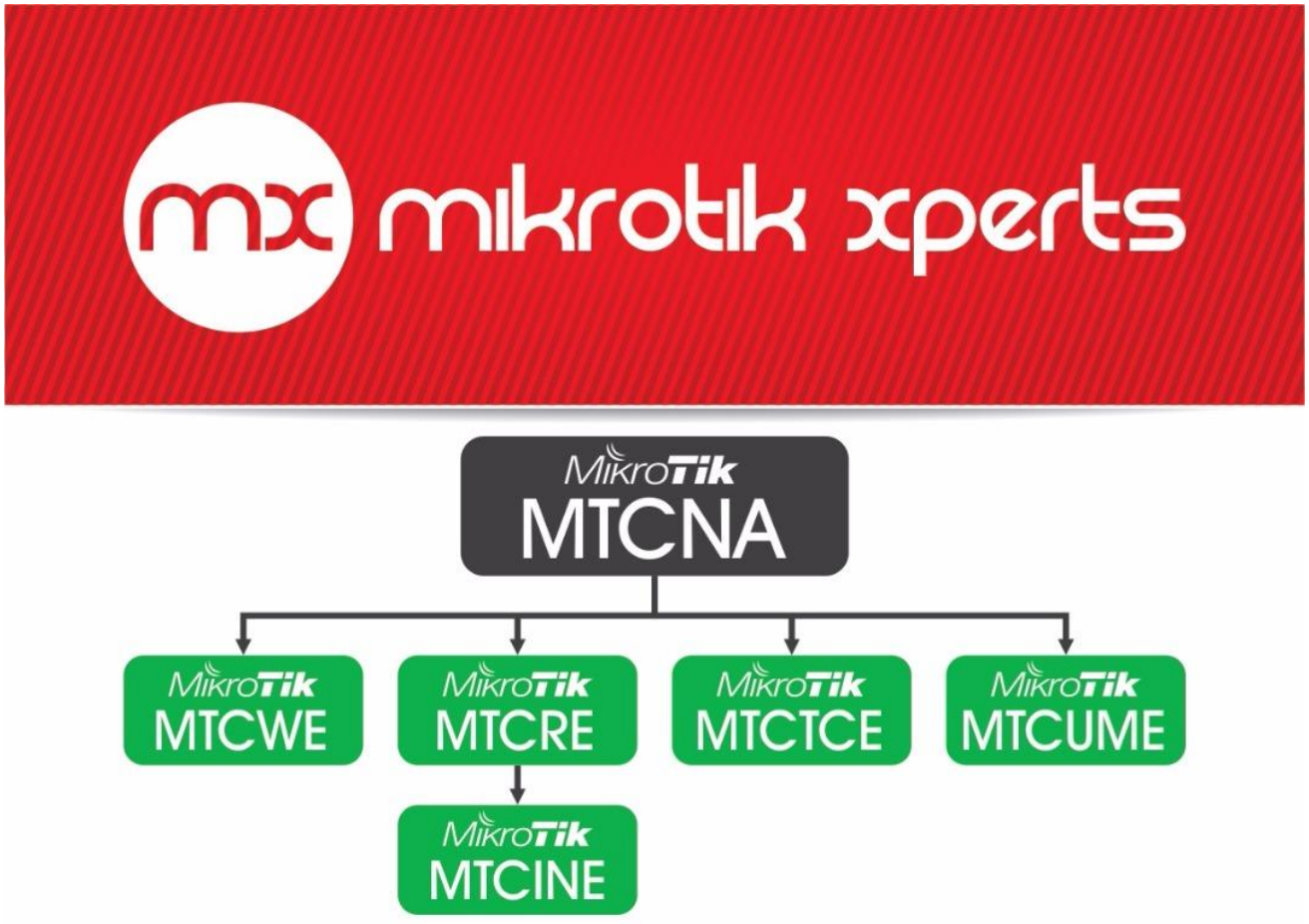
/ip route

add **gateway**=10.10.1.1**%wan1** **routing-mark**=to_wan1

add **gateway**=10.10.1.1**%wan2** **routing-mark**=to_wan2

Invitación

- Cursos de certificación oficial MikroTik



Invitación


Certificaciones Oficiales
MikroTik
WhatsApp: +56-9-9017-1908, Fijo: 2-2583-5522
www.mkx.cl / cursos@mkx.cl
Las Condes, Santiago - Chile
AcademyXpertsChile

¿Preguntas?

Gracias por su atención