MikroTik

Consolidated | Consultancy | Group

NETWORK LOAD BALANCING WORKSHOP BY ROUTEROS

BY IBRAHIM EL CHARIF

BEIRUT, LEBANON JAN 26, 2019

Knowledge Box

MikroTik
Training Partner

ABOUT ME

- Technical Operations Manager and IT Consultant at CCG Lebanon.
- Computer Communication Engineer
- Have 8+ years of experience in the IT industry
- Mikrotik Certified Trainer : MTCNA - MTCRE - MTCWE - MTCTCE
- Microsoft Certified: MCSE (Server Infrastructure Solutions Expert)
- Cisco Certified: CCNA – CCNP
- Email: Ibrahim.Cherif@ccg-lb.com / training@knowledgebox.me / ibrahimbnb@hotmail.com
- Tel: +961 70 164647

INTRODUCING OUR COMPANY

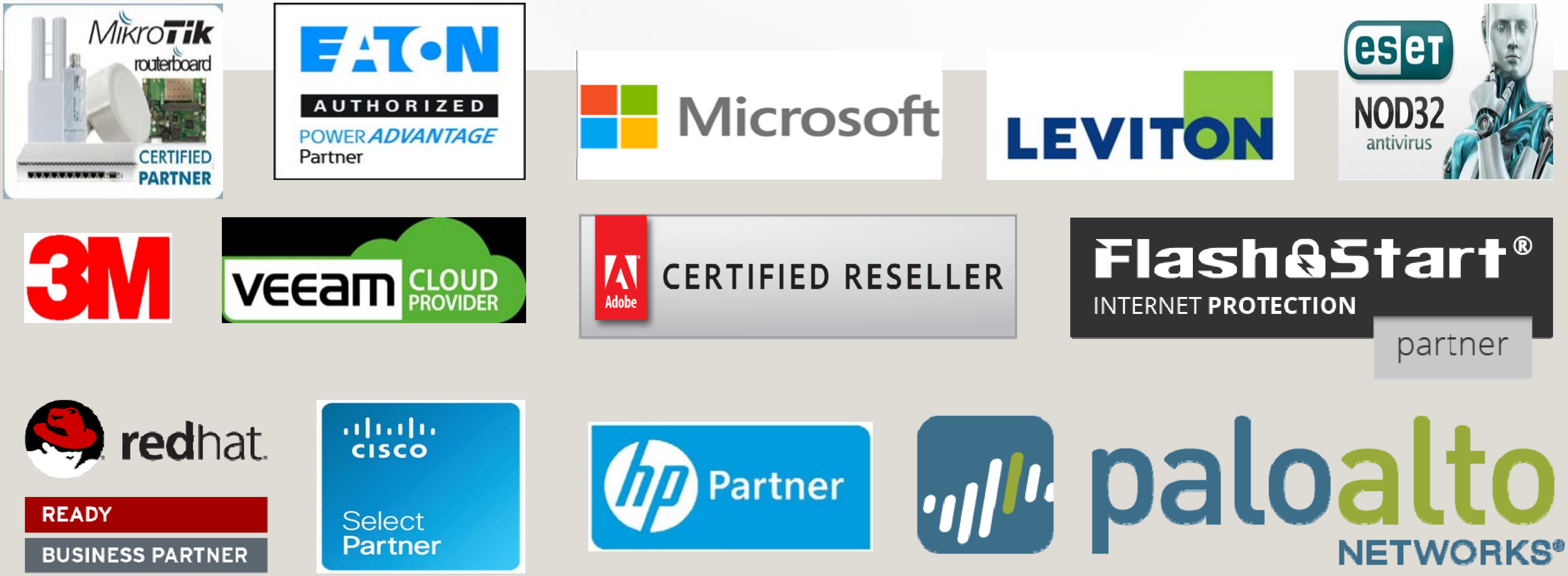
Consolidated | Consultancy | Group

- Established early 2011
- Leading Company in North Lebanon
- Full IT & Networking Solutions
- Partners with world leading companies
- Training powered by Knowledge Box Center

Knowledgebox.me
@knowledgebox.me

CCG-lb.com
CCG.leb
CCG_leb

Partners


MikroTik
routerboard
CERTIFIED
PARTNER
EATON
AUTHORIZED
POWER ADVANTAGE
Partner
Microsoft
LEVITON
eset
NOD32
antivirus
3M
veeam
CLOUD
PROVIDER
Adobe
CERTIFIED RESELLER
Flash Start®
INTERNET PROTECTION
partner
redhat.
READY
BUSINESS PARTNER
cisco
Select
Partner
hp
Partner
paloalto
NETWORKS®

Services & Support

- **CCG is a Certified MikroTik Partner, as well as having MikroTik Certified Engineers on staff. Our customer service is second to none and sets us apart from our competition. We provide Network design (LAN, WAN & WLAN), implementation, documentation, analysis, troubleshooting and training.**

- **Network Solution Design Services**
- **Installation and Configuration**
- **Management and Support**
- **VPN tunnels for multi branches company**
- **Hotspot with vouchering system for Malls, RestoCaffe, etc..**
- **Bonding, Load balance and link fail over for small to large businesses**

- **PTP and PTMP Wireless Links**
- **QOS and shaping, Queueing and Bandwidth control**
- **PPPOE server setup with online radius server for WISP companies**
- **Full wireless coverage by CAPSMAN for Universities, Malls,etc..**
- **Cloud web, content and APP filter powered by FLASHSTART for Governments, Schools, Universities, home users, companies and others**

Agenda

01 **Introduction to Load Balancing concept and advantages**

02 **RouterOS Load Balancing PCC definition and mechanism**

03 **Typical Scenario on PCC**

04 **Hints for best practices deployment & Validation**

WHAT IS NETWORK LOAD BALANCING ?

- A technique of distributing incoming network traffic and workload across multiple internet links to increase the efficiency and reduce downtime.
- It improves the downstream bandwidth for network hosts.
- is able to keep traffic requests within the zones as much as possible, so performance increased (less latency) and the cost of the whole system is reduced (less expenses using other vendors products)

Advantages

Increased Scalability

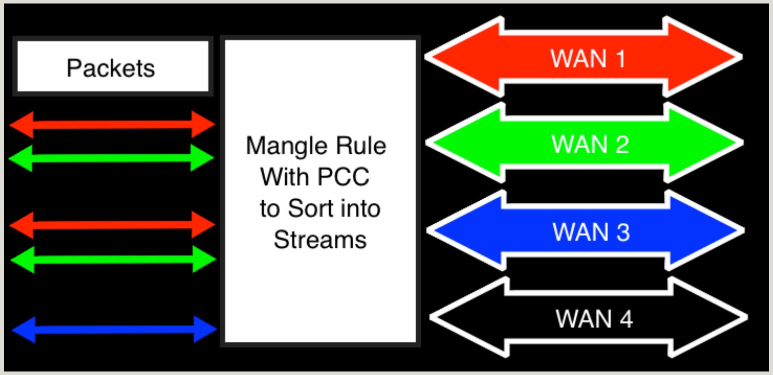
Redundancy

Reduced Downtime, Increased Performance

Increased Flexibility

PCC - PER CONNECTION CLASSIFIER INTRODUCTION

- Process can be done by sorting the packets Into streams and marked them for identification.“using Mangel Option”
- Using a hashing algorithm to first sort the traffic based on source address, source port, destination address, destination port or various combination .
- Using packet marking and routing marks and several routing tables to ensure traffic follows a specified route out the specified WAN interface.

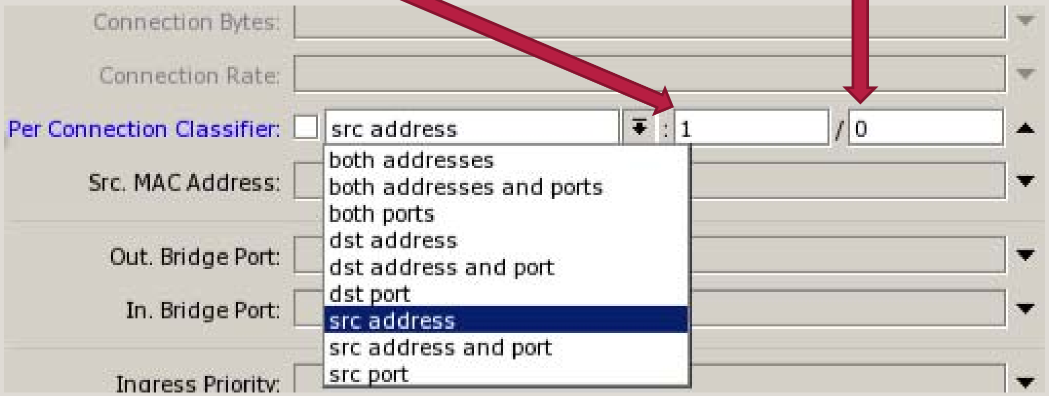


PCC - PER CONNECTION CLASSIFIER
IPV4 HEADER

<table>
<tr><th colspan="2">IPv4
Header</th></tr>
<tr><td>Source Address (sender)</td><td>Destination Address (receiver)</td></tr>
<tr><td>Port</td><td>Port</td></tr>
<tr><td colspan="2">Protocol</td></tr>
</table>

PCC - PER CONNECTION CLASSIFIER
HOW IT WORKS ?

- PCC takes selected fields from IP header, and with the help of a hashing algorithm converts selected fields into 32-bit value.
- This value then is divided by a Denominator then is compared to a specified Remainder, if equal then packet will be captured.
- You can choose from src-address, dst-address, src-port, dst-port (or various combinations) from the header to use in this operation.



Connection Bytes:

Connection Rate:

Per Connection Classifier: □ src address : 1 / 0

Src. MAC Address:

Out. Bridge Port:

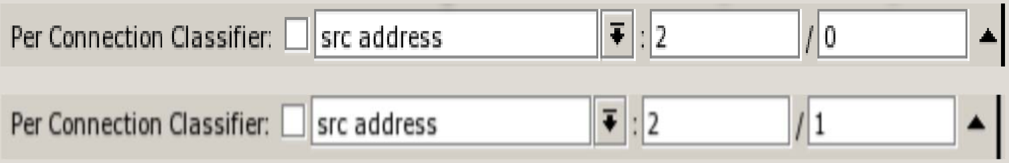
In. Bridge Port:

Ingress Priority:

PCC - PER CONNECTION CLASSIFIER
HOW TO SET PCC ?

- Using Mangle Rule Advanced Tab to specify the field from IP header, Denominator and the Remainder

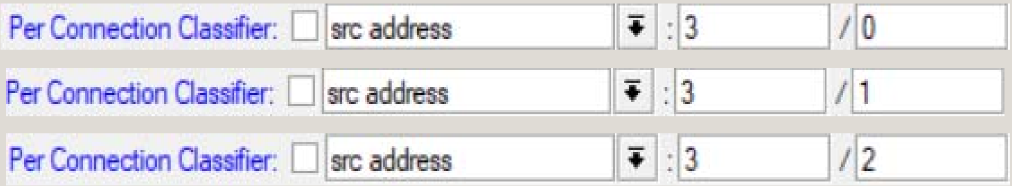
- **2 WAN connections:**
  2 / 0 First WAN
  2 / 1 Second WAN



Per Connection Classifier: □ src address : 2 / 0

Per Connection Classifier: □ src address : 2 / 1

- **3 WAN connections:**
  3 / 0 First WAN
  3 / 1 Second WAN
  3 / 2 Third WAN and so on...



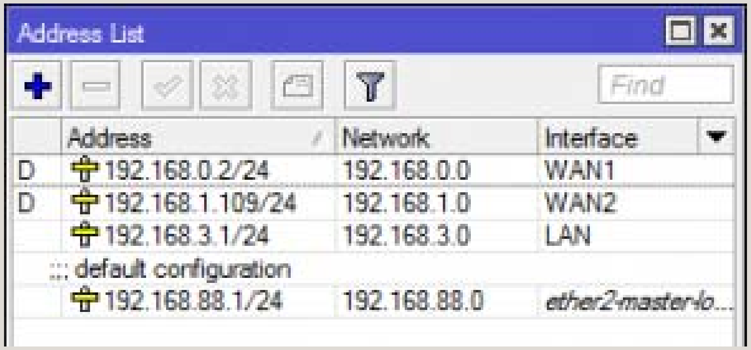
Per Connection Classifier: □ src address : 3 / 0

Per Connection Classifier: □ src address : 3 / 1

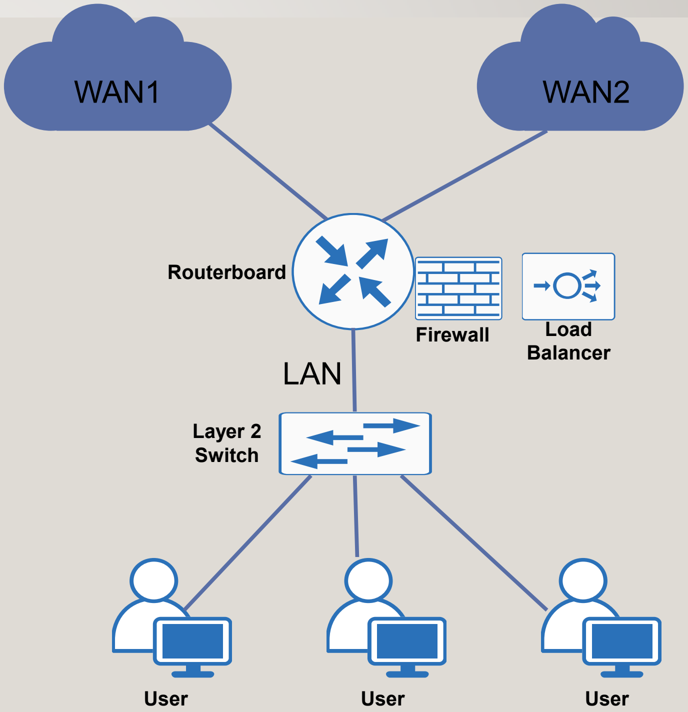
Per Connection Classifier: □ src address : 3 / 2

TYPICAL SCENARIO (DUAL WAN)

- Go to interfaces and name the interfaces as LAN ,WAN1 and WAN2.
- Assign IP to your interfaces. In this tutorial we are using DHCP for both of WAN connections.

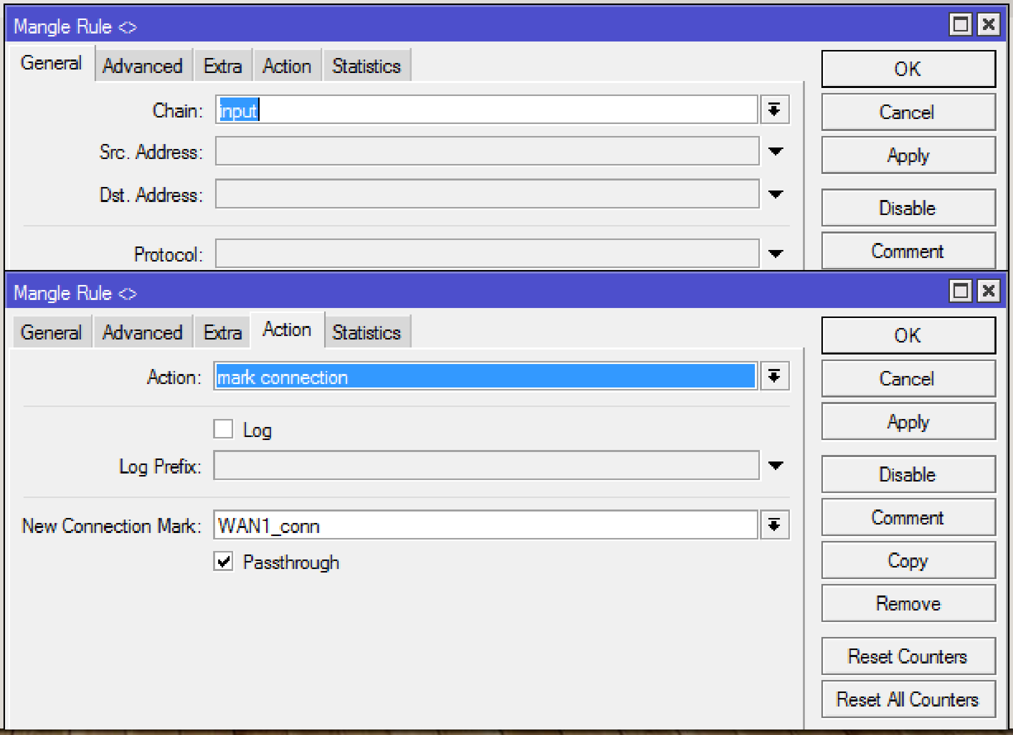


	Address	Network	Interface
D	192.168.0.2/24	192.168.0.0	WAN1
D	192.168.1.109/24	192.168.1.0	WAN2
	192.168.3.1/24	192.168.3.0	LAN
	::: default configuration		
	192.168.88.1/24	192.168.88.0	ether2-master-lo...



TYPICAL SCENARIO (DUAL WAN)
STEP1

- Click on IP > Firewall > Mangle
- Add a new mangle rule for WAN1
  Chain=input
  In.interface=WAN1
- Click on action tab
  Action=mark connection
  New Connection Mark=WAN1_conn
  Check the pass through.
- Repeat the same process for WAN2

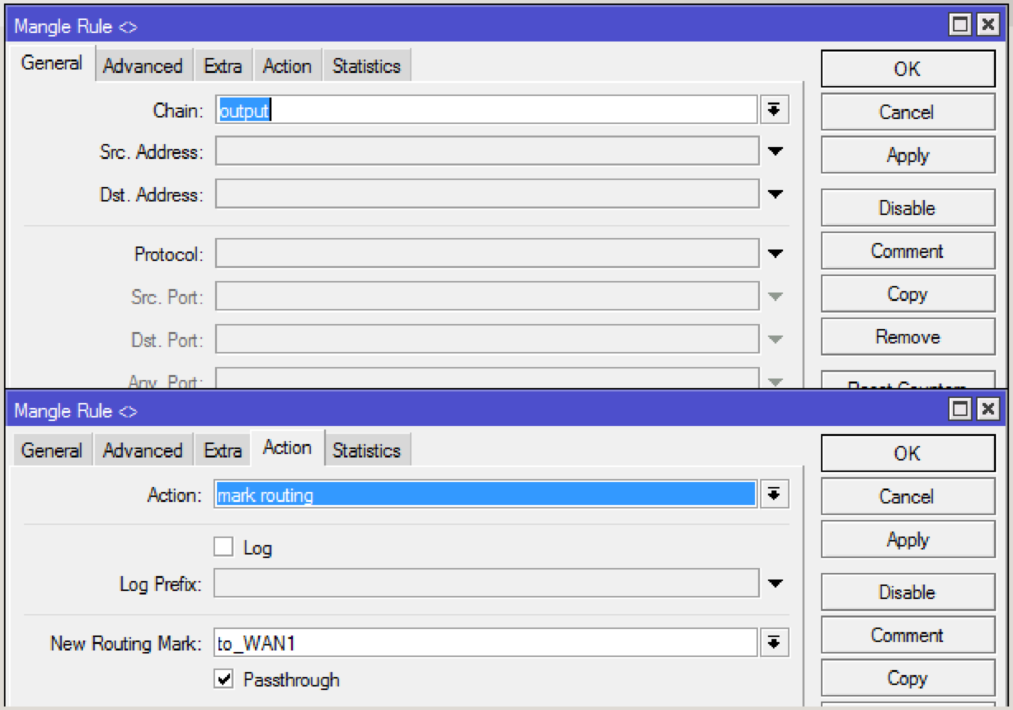


Chain: input
Src. Address:
Dst. Address:
Protocol:

Action: mark connection
☐ Log
Log Prefix:
New Connection Mark: WAN1_conn
☑ Passthrough

TYPICAL SCENARIO (DUAL WAN) STEP2

- Add new mangle rules
  Click on red + sign.
  Chain=output
  Connection mark=WAN1_conn
- Click on action tab
  Action=mark routing
  New Connection Mark=to_WAN1
  Check the pass through.
- Repeat the same process for WAN2

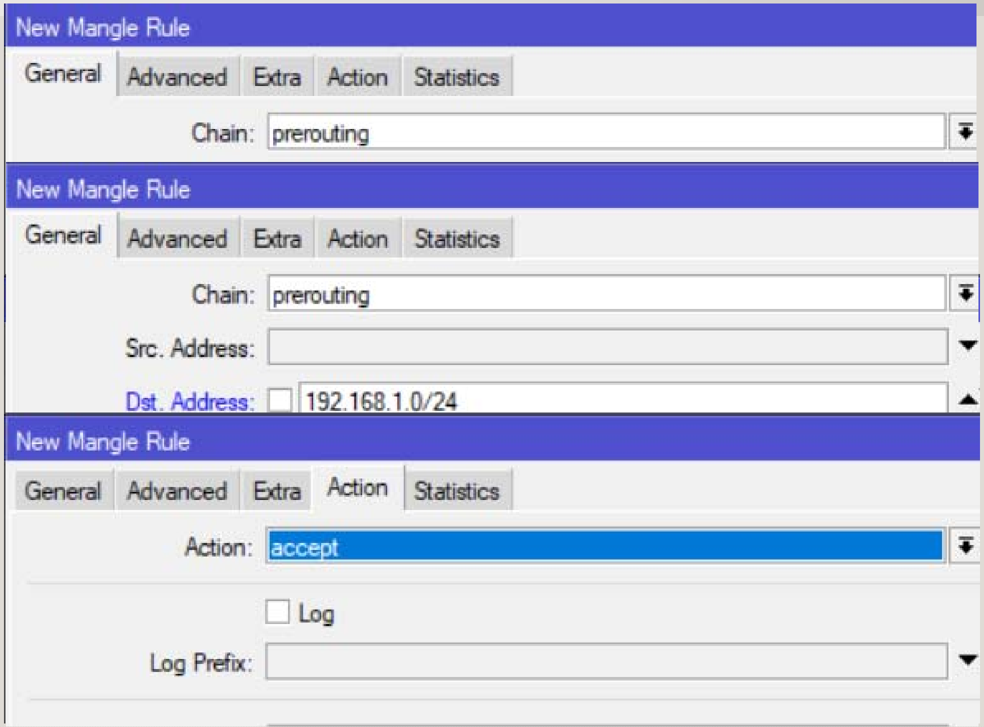


Chain: output
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:

Action: mark routing
□ Log
Log Prefix:
New Routing Mark: to_WAN1
☑ Passthrough

TYPICAL SCENARIO (DUAL WAN) STEP3

- Add 1st mangle rule for PCC
  Chain=Prerouting
  In.interface=LAN
  Dst.Address 192.168.0.0/24
- Click on action tab.
  Action=accept
- Add 2nd mangle rule for PCC
  Chain=Prerouting
  In.interface=LAN
  Dst.Address 192.168.1.0/24
- Click on action tab.
  Action=accept



Chain: prerouting

Chain: prerouting

Src. Address:

Dst. Address: □ 192.168.1.0/24

Action: accept

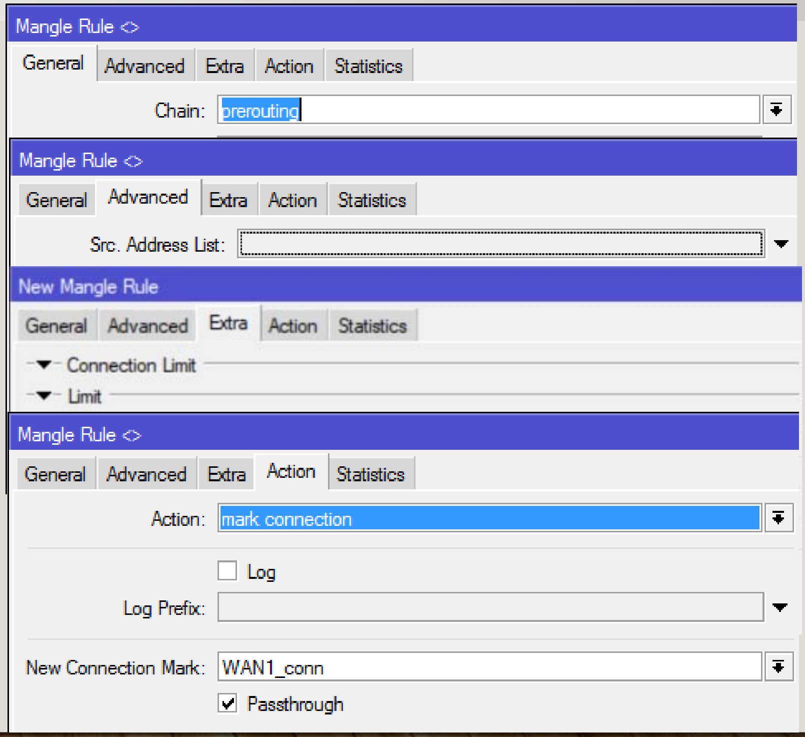
□ Log

Log Prefix:

TYPICAL SCENARIO (DUAL WAN)

Add PCC (Per connection Classifier) Rules to SORT the traffic into STREAMS

- Add a new mangle rule for PCC
  Chain=Prerouting
  In.interface=LAN
- Click on Advanced tab.
  Per connection Classifier=both addresses and ports 2/0
  (we have two WAN's so we will use 2 over 0).
- Click on extra tab.
  DST.address type ,Address type=Local, Click on invert
- Click on action tab.
  Action=mark connection, New connection mark=WAN1_Conn
- Same process for WAN2 but this time we change
  Per Connection Classifier=both addresses and ports 2/1



Chain: prerouting

Src. Address List:

Action: mark connection

☐ Log

Log Prefix:

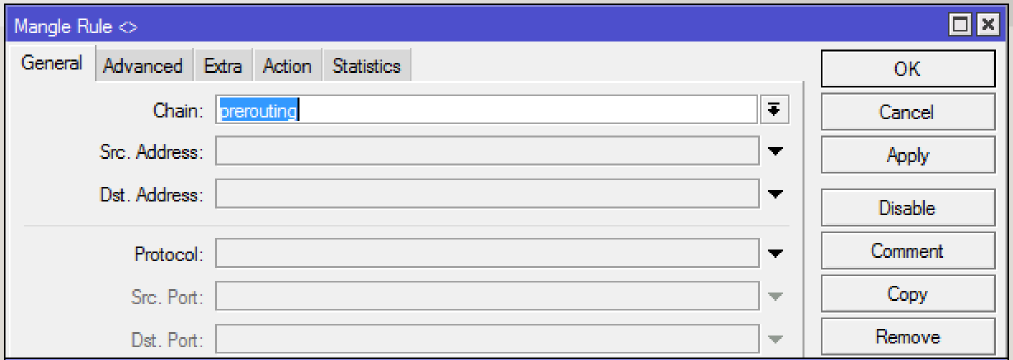
New Connection Mark: WAN1_conn

☑ Passthrough

TYPICAL SCENARIO (DUAL WAN)

Add final mangle rules

- Click on red + sign
- Chain=prerouting
  In.interface=LAN
  Connection mark=WAN1_conn
- Action=mark routing
  New routing mark=to-WAN1
  Check pass through
- Add the same rule for WAN2.



Mangle Rule <>

Chain: prerouting

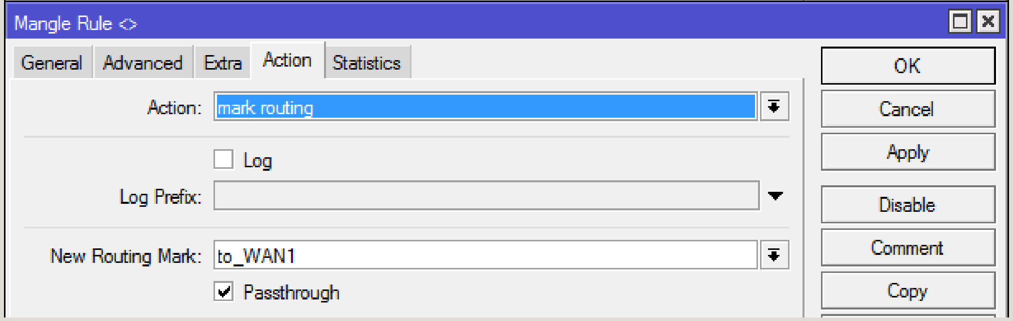
Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:



Mangle Rule <>

Action: mark routing

□ Log

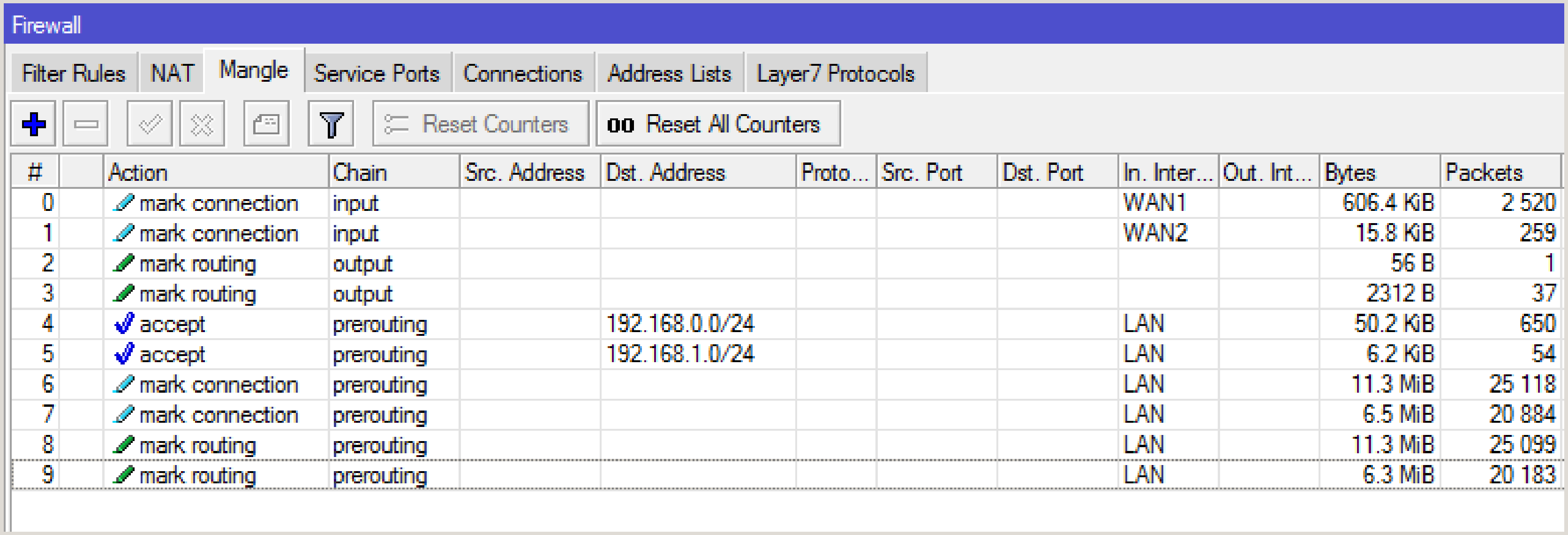
Log Prefix:

New Routing Mark: to_WAN1

☑ Passthrough

TYPICAL SCENARIO (DUAL WAN)

- Your mangle rules should look like this.

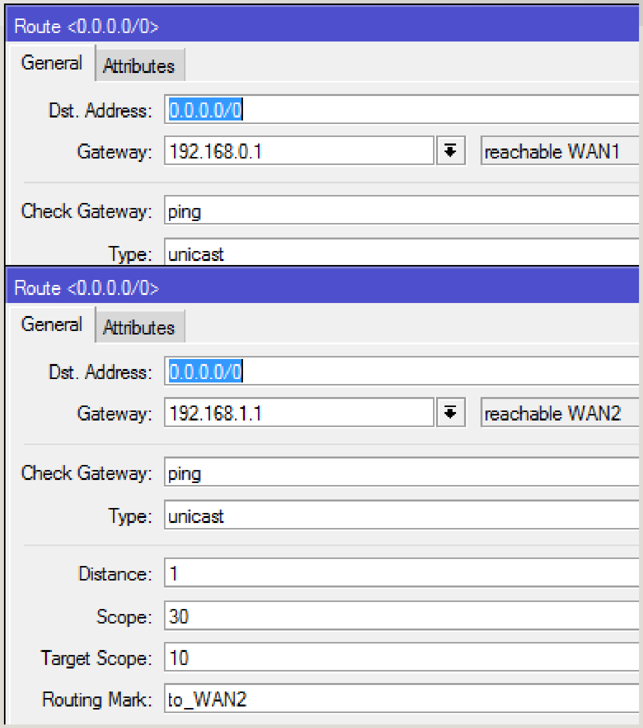


#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0		mark connection	input						WAN1		606.4 KiB	2 520
1		mark connection	input						WAN2		15.8 KiB	259
2		mark routing	output								56 B	1
3		mark routing	output								2312 B	37
4		accept	prerouting		192.168.0.0/24				LAN		50.2 KiB	650
5		accept	prerouting		192.168.1.0/24				LAN		6.2 KiB	54
6		mark connection	prerouting						LAN		11.3 MiB	25 118
7		mark connection	prerouting						LAN		6.5 MiB	20 884
8		mark routing	prerouting						LAN		11.3 MiB	25 099
9		mark routing	prerouting						LAN		6.3 MiB	20 183

TYPICAL SCENARIO (DUAL WAN)

Add the gateways

- Click on IP> Routes and Click on red + sign.
- Gateway= 192.168.0.1
  Check gateway=ping (This is a fail over entry which
  will ping the gateway continuously, if the gateway does not responds,
  It will disconnect that Line and put the load on the rest of the lines.)
  Routing Mark=to_WAN1
- Now add second route
  Gateway= 192.168.1.1
  Check gateway=ping (This is a fail over entry which
  will ping the gateway continuously ,if the gateway does not responds,
  it will disconnect that Line and put the load on the rest of the lines.)
  Routing Mark=to_WAN2



Route <0.0.0.0/0>

Dst. Address: 0.0.0.0/0

Gateway: 192.168.0.1 reachable WAN1

Check Gateway: ping

Type: unicast

Route <0.0.0.0/0>

Dst. Address: 0.0.0.0/0

Gateway: 192.168.1.1 reachable WAN2

Check Gateway: ping

Type: unicast

Distance: 1

Scope: 30

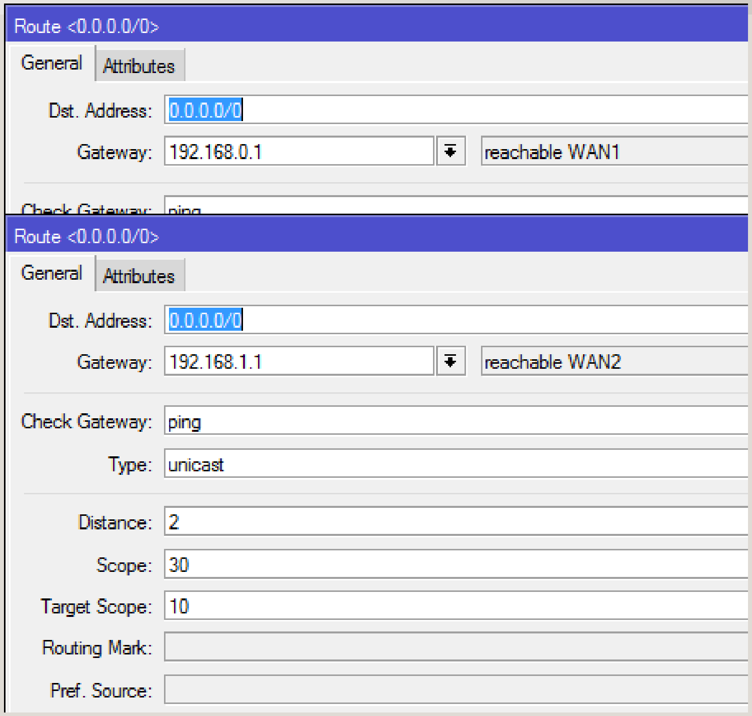
Target Scope: 10

Routing Mark: to_WAN2

TYPICAL SCENARIO (DUAL WAN)

Add the routes with distance

- Again click on red + sign
  Gateway= 192.168.0.1
  Check gateway=ping
  Distance=1 (It tells the router which gateway to ping first)
- Again for the second one.
  Gateway= 192.168.1.1
  Check gateway=ping
  Distance=2



Route <0.0.0.0/0>

Dst. Address: 0.0.0.0/0
Gateway: 192.168.0.1 reachable WAN1
Check Gateway: ping

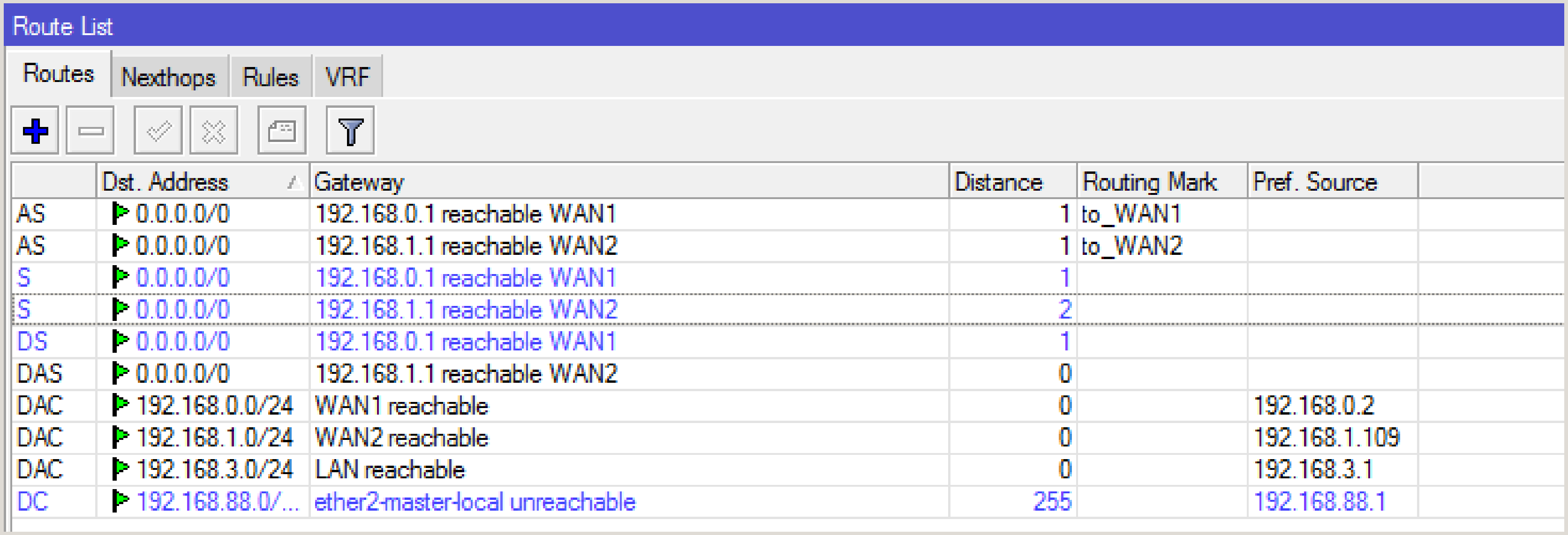
Route <0.0.0.0/0>

Dst. Address: 0.0.0.0/0
Gateway: 192.168.1.1 reachable WAN2
Check Gateway: ping
Type: unicast
Distance: 2
Scope: 30
Target Scope: 10
Routing Mark:
Pref. Source:

TYPICAL SCENARIO (DUAL WAN)

Routes Table

- Your route rules should look like this.

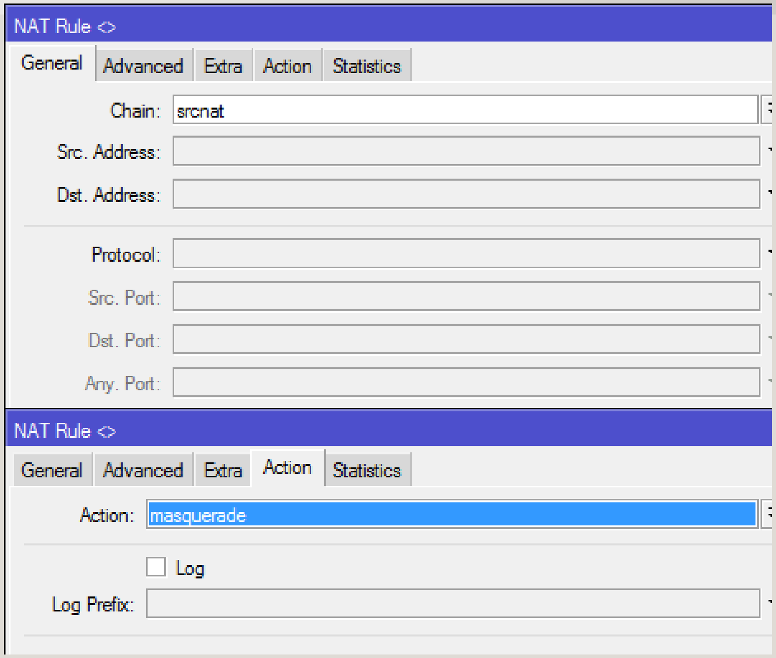


	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	192.168.0.1 reachable WAN1	1	to_WAN1	
AS	0.0.0.0/0	192.168.1.1 reachable WAN2	1	to_WAN2	
S	0.0.0.0/0	192.168.0.1 reachable WAN1	1		
S	0.0.0.0/0	192.168.1.1 reachable WAN2	2		
DS	0.0.0.0/0	192.168.0.1 reachable WAN1	1		
DAS	0.0.0.0/0	192.168.1.1 reachable WAN2	0		
DAC	192.168.0.0/24	WAN1 reachable	0		192.168.0.2
DAC	192.168.1.0/24	WAN2 reachable	0		192.168.1.109
DAC	192.168.3.0/24	LAN reachable	0		192.168.3.1
DC	192.168.88.0/...	ether2-master-local unreachable	255		192.168.88.1

TYPICAL SCENARIO (DUAL WAN)

Add NAT Rules

- Go to IP>Firewall >NAT
  Click on red + sign
  Chain=srcnat
  Out interface=WAN1
  Action=masquerade
- Add another rule for WAN2.



NAT Rule <>

Chain: srcnat
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:

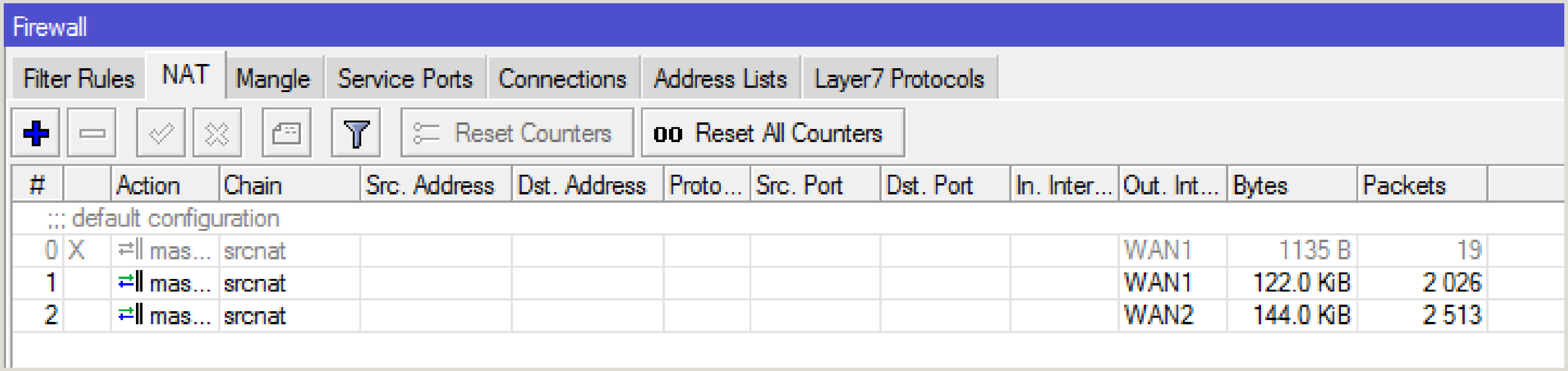
NAT Rule <>

Action: masquerade
□ Log
Log Prefix:

TYPICAL SCENARIO (DUAL WAN)

NAT Table

- Your NAT rules will look like this.

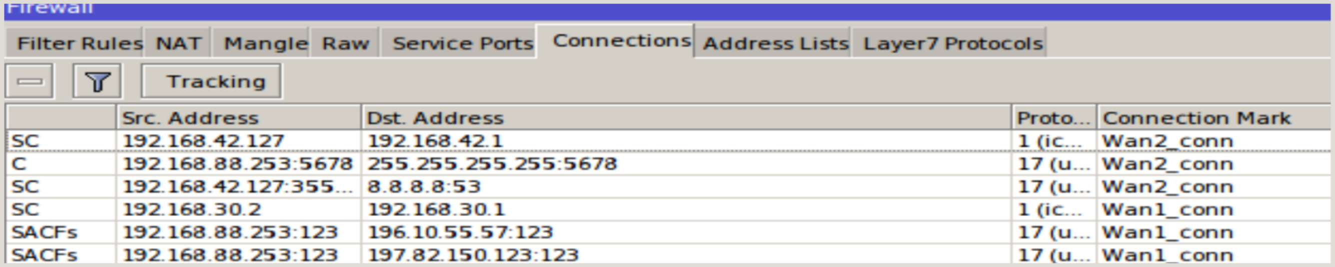


#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; default configuration												
0	X	⇄ mas...	srcnat							WAN1	1135 B	19
1		⇄ mas...	srcnat							WAN1	122.0 KiB	2 026
2		⇄ mas...	srcnat							WAN2	144.0 KiB	2 513

TYPICAL SCENARIO (DUAL WAN)

Validation

- Always check the connection table to ensure mangles are working for connections



	Src. Address	Dst. Address	Proto...	Connection Mark
SC	192.168.42.127	192.168.42.1	1 (ic...	Wan2_conn
C	192.168.88.253:5678	255.255.255.255:5678	17 (u...	Wan2_conn
SC	192.168.42.127:355...	8.8.8.8:53	17 (u...	Wan2_conn
SC	192.168.30.2	192.168.30.1	1 (ic...	Wan1_conn
SACFs	192.168.88.253:123	196.10.55.57:123	17 (u...	Wan1_conn
SACFs	192.168.88.253:123	197.82.150.123:123	17 (u...	Wan1_conn

- Always check the Traffic Tab of each WAN interface
- It is highly recommended to use Open DNS like Google, because may some users are accessing ISP1's DNS server through ISP2's connection, and ISP1 is blocking DNS requests outside their IPs

RECAP

- New connections inbound on each WAN get marked
- Outbound connections with that mark get a routing mark
- LAN traffic heading outbound gets load balanced with the same routing marks
- Routing marks match default gateway routes and head out that specified interface
- Verification of the Load balancing setup

SUMMARY

Using a load balanced multi-WAN setup helps us meet a few design goals:

- Failover in case of ISP failure
- Increase total available bandwidth for users
- Distribute bandwidth utilization across providers
- Avoiding the overload of any single internet connection
- Improving the reliability and availability through redundancy
- Optimizing the connectivity

Thank you for listening

Enjoy your MUM

Reference:

https://wiki.mikrotik.com/wiki/Manual:PCC

https://wiki.mikrotik.com/wiki/How_PCC_works_(beginner)

https://wiki.mikrotik.com/wiki/Manual:Hotspot_with_PCC