Load Balancing Using PCC & RouterOS
About Me

• Steve Discher, from College Station, Texas, USA
• Class of ’87 Texas A&M University
• Using MikroTik since early 2004 when I started my first WISP
• Author of the book “RouterOS by Example”
• MikroTik Certified Trainer and teach RouterOS classes, MyWISPTraining.com
• Operate a wireless distribution company, ISPSupplies.com
1. What is load balancing and why would I want it?
2. Which method should I pick and how does it work?
3. Ok, I want it but how do I set it up?
Typical Scenario Requiring Load Balancing

Problem: No high capacity circuits available, DSL only

Distribution: Fiber, Copper, Wireless, etc.

Hotel, Apartments, etc.
Typical Scenario Requiring Load Balancing

Solution: Multiple low capacity circuits, RouterOS load balancing

Hotel, Apartments, etc.

Distribution: Fiber, Copper, Wireless, etc.
I. What is load balancing and why would I want it?
I. What is load balancing and why would I want it?

- Process to utilize multiple internet connections in such a manner as to proportionately distribute internet traffic across all the connections.
1. What is load balancing and why would I want it?

- Process to utilize multiple internet connections in such a manner as to proportionately distribute internet traffic across all the connections.
- Distribution may be symmetrical or asymmetrical depending on circuit availability.
1. What is load balancing and why would I want it?

- Process to utilize multiple internet connections in such a manner as to proportionately distribute internet traffic across all the connections.
- Distribution may be symmetrical or asymmetrical depending on circuit availability.
- Useful when the downstream bandwidth requirement to a single routing device exceeds the capabilities of a single internet circuit.
Options Available

Load Balancing in General
Load Balancing in General

- First, the type of load balancing we are discussing today should not be confused with any type of bonding protocol or sub-packet based load balancing.
Options Available

Load Balancing in General

• First, the type of load balancing we are discussing today should not be confused with any type of bonding protocol or sub-packet based load balancing.
• Bonding, MLPP, etc. require that the protocol be recognized on both the subscriber and provider ends. Not available with commodity internet connections.
Options Available

Load Balancing in General

• First, the type of load balancing we are discussing today should not be confused with any type of bonding protocol or sub-packet based load balancing.
• Bonding, MLPP, etc. require that the protocol be recognized on both the subscriber and provider ends. Not available with commodity internet connections.
• Can’t simply bridge two DSL or Cable modem connections, doesn’t work.
Load Balancing in General

• First, the type of load balancing we are discussing today should not be confused with any type of bonding protocol or sub-packet based load balancing.
• Bonding, MLPP, etc. require that the protocol be recognized on both the subscriber and provider ends. Not available with commodity internet connections.
• Can’t simply bridge two DSL or Cable modem connections, doesn’t work.
• There are several methods to provide load balancing in RouterOS.
Example

88 hits!
Options Available

Load Balancing Options With RouterOS:
Options Available

Load Balancing Options With RouterOS:

• **ECMP** - Equal Cost Multi-Path Routing
Options Available

Load Balancing Options With RouterOS:

• **ECMP** - Equal Cost Multi-Path Routing
  • Per-address pair load balancing
Options Available

Load Balancing Options With RouterOS:

- **ECMP** - Equal Cost Multi-Path Routing
  - Per-address pair load balancing
  - Doesn’t work well for certain protocols, connections break when routing table flushes every ten minutes to prevent DOS attacks
Options Available

Load Balancing Options With RouterOS:

• **ECMP** - Equal Cost Multi-Path Routing
  • Per-address pair load balancing
  • Doesn’t work well for certain protocols, connections break when routing table flushes every ten minutes to prevent DOS attacks
• **Nth Load Balancing** - Per connection load balancing, with the addition of persistent connections
Options Available

Load Balancing Options With RouterOS:

• **ECMP** - Equal Cost Multi-Path Routing
  • Per-address pair load balancing
  • Doesn’t work well for certain protocols, connections break when routing table flushes every ten minutes to prevent DOS attacks

• **Nth Load Balancing** - Per connection load balancing, with the addition of persistent connections

• **Hybrid / Custom Setups** - Solutions based on one or more methods above with the addition of scripts or policy routing to make the solution more intelligent.
Options Available

Load Balancing Options With RouterOS:

- **ECMP** - Equal Cost Multi-Path Routing
  - Per-address pair load balancing
  - Doesn’t work well for certain protocols, connections break when routing table flushes every ten minutes to prevent DOS attacks
- **Nth Load Balancing** - Per connection load balancing, with the addition of persistent connections
- **Hybrid / Custom Setups** - Solutions based on one or more methods above with the addition of scripts or policy routing to make the solution more intelligent.
- **Bandwidth based load balancing** - MPLS, Traffic Engineering, etc.
Options Available

Load Balancing Options With RouterOS:

- **ECMP** - Equal Cost Multi-Path Routing
  - Per-address pair load balancing
  - Doesn’t work well for certain protocols, connections break when routing table flushes every ten minutes to prevent DOS attacks
- **Nth Load Balancing** - Per connection load balancing, with the addition of persistent connections
- **Hybrid / Custom Setups** - Solutions based on one or more methods above with the addition of scripts or policy routing to make the solution more intelligent.
- **Bandwidth based load balancing** - MPLS, Traffic Engineering, etc.
- **PCC** - Per Connection Classifier
Options Available

Load Balancing Options With RouterOS:

• **ECMP** - Equal Cost Multi-Path Routing
  • Per-address pair load balancing
  • Doesn’t work well for certain protocols, connections break when routing table flushes every ten minutes to prevent DOS attacks
• **Nth Load Balancing** - Per connection load balancing, with the addition of persistent connections
• **Hybrid / Custom Setups** - Solutions based on one or more methods above with the addition of scripts or policy routing to make the solution more intelligent.
• **Bandwidth based load balancing** - MPLS, Traffic Engineering, etc.
• **PCC** - Per Connection Classifier
  • Simple, effective, scalable, no nasty side effects
Options Available

Load Balancing Options With RouterOS:

• **ECMP** - Equal Cost Multi-Path Routing
  • Per-address pair load balancing
  • Doesn’t work well for certain protocols, connections break when routing table flushes every ten minutes to prevent DOS attacks

• **Nth Load Balancing** - Per connection load balancing, with the addition of persistent connections

• **Hybrid / Custom Setups** - Solutions based on one or more methods above with the addition of scripts or policy routing to make the solution more intelligent.

• **Bandwidth based load balancing** - MPLS, Traffic Engineering, etc.

• **PCC** - Per Connection Classifier
  • Simple, effective, scalable, no nasty side effects
  • Per-address pair load balancing method
2. How does it work?
2. How does it work?

- PCC divides the incoming data into streams and then uses routing rules to sort the traffic evenly (or not) across multiple WAN connections.
2. How does it work?

• PCC divides the incoming data into streams and then uses routing rules to sort the traffic evenly (or not) across multiple WAN connections.
• This is done by:
2. How does it work?

- PCC divides the incoming data into streams and then uses routing rules to sort the traffic evenly (or not) across multiple WAN connections.
- This is done by:
  1. Using a hashing algorithm to first sort the traffic based on source address, source port, destination address, destination port or various combinations thereof.
2. How does it work?

• PCC divides the incoming data into streams and then uses routing rules to sort the traffic evenly (or not) across multiple WAN connections.
• This is done by:
  1. Using a hashing algorithm to first sort the traffic based on source address, source port, destination address, destination port or various combinations thereof.
  2. Using packet marking and routing marks and several routing tables to ensure traffic follows a specified route out the specified WAN interface.
2. How does it work?

- PCC divides the incoming data into streams and then uses routing rules to sort the traffic evenly (or not) across multiple WAN connections.
- This is done by:
  1. Using a hashing algorithm to first sort the traffic based on source address, source port, destination address, destination port or various combinations thereof.
  2. Using packet marking and routing marks and several routing tables to ensure traffic follows a specified route out the specified WAN interface.
Understand the Solution
Understand the Solution

- MikroTik RouterOS is extremely powerful and configurable, so this can be a double edged sword, several possible solutions to the same problem
Understand the Solution

- MikroTik RouterOS is extremely powerful and configurable, so this can be a double edged sword, several possible solutions to the same problem
- Each has multiple moving pieces
Understand the Solution

- MikroTik RouterOS is extremely powerful and configurable, so this can be a double edged sword, several possible solutions to the same problem
- Each has multiple moving pieces
- Greatest success with any solution by understanding the pieces and what they do.
Understanding the PCC Load Balancing Solution

Terms...
Understanding the PCC Load Balancing Solution

Terms...

1. **Packet** - The container for our data, header and payload.
Understanding the PCC Load Balancing Solution

Terms...

1. **Packet** - The container for our data, header and payload.
2. **Connections** - “Conduit” through which host to host communication occurs, based on Src/Dst addresses and ports
Understanding the PCC Load Balancing Solution

Terms...

1. **Packet** - The container for our data, header and payload.
2. **Connections** - “Conduit” through which host to host communication occurs, based on Src/Dst addresses and ports.
3. **Mangle Facility** - Firewall function within RouterOS that allows you to create a mark which is then associated with packets that can be identified later by other functions like firewall rules or routing tables.
Understanding the PCC Load Balancing Solution
Understanding the PCC Load Balancing Solution

4. **PCC** - Per Connection Classifier, function contained with the “Mangle Facility” to sort traffic into streams
Understanding the PCC Load Balancing Solution

4. **PCC** - Per Connection Classifier, function contained with the “Mangle Facility” to sort traffic into streams

5. **Routing Table** - Route rules, the rules the router uses to determine what to do with a packet. By comparing the destination address in the packet to the list of routes, the router decides which interface to send the packet out. By adding a routing mark with mangle, we can have multiple routing tables!
Understanding the PCC Load Balancing Solution

1. What is a packet?

A packet is like a letter & envelope. The front is the header and the letter inside the envelope is the payload.
Understanding the PCC Load Balancing Solution

IPv4 Header

<table>
<thead>
<tr>
<th>Source Address (sender)</th>
<th>Destination Address (receiver)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Port</td>
</tr>
<tr>
<td>Protocol</td>
<td></td>
</tr>
</tbody>
</table>
2. What are connections?

Connections are always in one of three states - new, established, or related.

- **NEW CONNECTION**: Places the phone call
- **ANSWERS CALL, MAINTAINS THE CONVERSATION**: Establishes the connection
- **ANOTHER PARTY TO A THREE WAY CALL**: Related connection

**COMPUTER** ➔ **PLACES THE PHONE CALL** ➔ **PHONE** ➔ **SERVER**

**COMPUTER** ➔ **PLACES THE PHONE CALL** ➔ **PHONE** ➔ **SERVER**
Understanding the PCC Load Balancing Solution

3. What is the mangle facility?

If - Then: Identify and then perform some action.
Understanding the PCC Load Balancing Solution

4. What is PCC?

Per Connection Classifier is a mangle option that sorts data into streams that can be marked for identification later.
Understanding the PCC Load Balancing Solution

Where is it found?
Understanding the PCC Load Balancing Solution

How does PCC work?

• "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 and the Remainder 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."
Understanding the PCC Load Balancing Solution

PCC uses a hashing algorithm.

• A hashing algorithm is a mathematical function that takes an input and returns an output.
• The output will always be the same for a specified input.
• Example of a simple hash:
  
  Input x 100 = hash value
Understanding the PCC Load Balancing Solution

PCC uses modular arithmetic (clock arithmetic).

- Numerators, Denominators and Remainders are parts of modular arithmetic.
- It is represented by a % sign and it is spoken as “mod”.
- To work modular math, think of it as "how many are left over (Remainder) after you've subtracted the second value (Denominator) from the first (Numerator) as many times as possible without going negative?"

- Here are some examples of modular math:

  Numerator = 3 Denominator = 3

  3 % 3 = 0 because 3 - 3 = 0 left over

  or

  4 % 3 = 1 because 4 - 3 = 1 left over

  5 % 3 = 2 because 5 - 3 = 2 left over

  6 % 3 = 0, because 6 - 3 = 3, subtract 3 again = 0 left over
Understanding the PCC Load Balancing Solution

Modular math helps us understand how to create the PCC rules!

Example: 2 WAN Connections

2 PCC Rules Required

- The first line means "produce the output of the hash function given the packet's source IP address, divide it by 2 and if the remainder is 0, perform the action of marking the connection as WAN1".

- The second line means "produce the output of the hash function given the packet's source IP address, divide it by 2 and if the remainder is 1, perform the action of marking the connection as WAN2".
Understanding the PCC Load Balancing Solution

How to set PCC, Remember:

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

3 WAN connections:
   3 / 0 First WAN
   3 / 1 Second WAN
   3 / 2 Third WAN and so on...
Understanding the PCC Load Balancing Solution

5. What is a routing table?

Routes determine which interface a packet is sent out. They also tell the router which upstream or downstream router will take the packet to its next hop until it reaches its final destination.
Understanding the PCC Load Balancing Solution

Details of a route, key pieces are destination and gateway.
Understanding the PCC Load Balancing Solution

Multiple routing tables with route marks

May have multiple routes to same destination network, different gateways in different routing tables!
Understanding the PCC Load Balancing Solution

**Multiple routing tables with route marks**

May have multiple routes to same destination network, different gateways in different routing tables!
Understanding the PCC Load Balancing Solution

Multiple routing tables with route marks

May have multiple routes to same destination network, different gateways in different routing tables!
Understanding the PCC Load Balancing Solution

Multiple routing tables with route marks

May have multiple routes to same destination network, different gateways in different routing tables!
Understanding the PCC Load Balancing Solution

Review:
Understanding the PCC Load Balancing Solution

Review:

1. **Packet** - Container for IP data
Understanding the PCC Load Balancing Solution

Review:

1. **Packet** - Container for IP data
2. **Connections** - Bi-directional conduit for communication between two hosts
Understanding the PCC Load Balancing Solution

Review:

1. **Packet** - Container for IP data
2. **Connections** - Bi-directional conduit for communication between two hosts
3. **Mangle Facility** - Manipulates packets by adding marks
Understanding the PCC Load Balancing Solution

Review:

1. **Packet** - Container for IP data
2. **Connections** - Bi-directional conduit for communication between two hosts
3. **Mangle Facility** - Manipulates packets by adding marks
4. **PCC** - Divides data into streams (based on marks)
Understanding the PCC Load Balancing Solution

Review:

1. **Packet** - Container for IP data
2. **Connections** - Bi-directional conduit for communication between two hosts
3. **Mangle Facility** - Manipulates packets by adding marks
4. **PCC** - Divides data into streams (based on marks)
5. **Routing Table** - List of route rules to direct packets and we can have multiple tables based on routing marks
3. Ok, I want it but how do I set it up?

Hotel, Apartments, etc.
3. Ok, I want it but how do I set it up?

Scenario: One router, many clients, three DSL connections

Hotel, Apartments, etc.
Step by Step Configuration

Test Setup
Step by Step Configuration

1. Set up the basic portion of the network (MTCNA, Wiki, etc):
   • Private IP address on LAN interface
   • DHCP Server on LAN interface
   • DNS server
   • Static IP for WAN or DHCP client on WAN
   • Firewall if required
Step by Step Configuration

1. Set up the basic portion of the network (MTCNA, Wiki, etc):
   • Private IP address on LAN interface
   • DHCP Server on LAN interface
   • DNS server
   • Static IP for WAN or DHCP client on WAN
   • Firewall if required

2. Create load balancing part of the configuration:
   • Mangle rules
   • Routing tables
Step by Step Configuration

1. Set up the basic portion of the network (MTCNA, Wiki, etc):
   - Private IP address on LAN interface
   - DHCP Server on LAN interface
   - DNS server
   - Static IP for WAN or DHCP client on WAN
   - Firewall if required

2. Create load balancing part of the configuration:
   - Mangle rules
   - Routing tables
Step by Step Configuration

Physical interface connections
Step by Step Configuration

1. Set up the basic portion of the network (MTCNA, Wiki, etc):

   - **IP Addresses**
   - **DHCP Client - WAN**
   - **DNS Client & Caching**
   - **Masquerade Rules**
Step by Step Configuration

2. Create load balancing part of the configuration:

- Create various mangle rules to mark connections
- Create mangle rules to associate routing marks with packets based on their connection mark.
- Create routes to send traffic out the WAN connections in a predetermined manner.
Step by Step Configuration

Step 1: Create some accept rules.

We have to manually force local traffic to connected networks to stay in the main routing table.

• Background - Any subnet for which the router has an IP address configured is called a connected network, meaning packets to that network are sent out an interface and can reach their destination without using another router to get there.
Step by Step Configuration

Step 1 continued...

The problem using mangles here is it will force traffic to follow alternate routing tables (not main) Traffic to these connected networks would go out the WAN interfaces and not reach their intended destinations.

Connected network example

```
10.0.0.1/24
10.0.1.1/24
10.0.2.1/24
```
Step by Step Configuration

Step I continued...

Solution:

• The “accept” action causes the packet to leave the mangle chain, thereby not marking it and allowing that traffic to use the main routing table.
Step by Step Configuration

Step 1 continued...

- One rule for each connected network, in this example these are our WAN networks
Step by Step Configuration

Step 1 Completed

Create one rule for each connected network (WAN’s)

Completed accept mangle rules

/ip firewall mangle
add action=accept chain=prerouting disabled=no dst-address=172.17.0.0/24
add action=accept chain=prerouting disabled=no dst-address=172.18.0.0/24
add action=accept chain=prerouting disabled=no dst-address=172.19.0.0/24
Step by Step Configuration

Step 2: Create Mangle rules that will sort the traffic into streams.

Create the PCC mangles:

• We will use optimal mangle method of marking connections first and then packets because it is the most efficient way to mark traffic, uses least resources.
  • First identify traffic and mark the connection.
  • Second, look for that connection mark and mark the routes.
Step 2 Continued...

Firewall Configuration:

<table>
<thead>
<tr>
<th>#</th>
<th>Action</th>
<th>Chain</th>
<th>Src. Address</th>
<th>Dst. Address</th>
<th>Proto...</th>
<th>Src. Port</th>
<th>Dist. Port</th>
<th>In. Int...</th>
<th>Out. Int...</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>mar...</td>
<td>prerouting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ether5</td>
</tr>
<tr>
<td>1</td>
<td>mar...</td>
<td>prerouting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ether5</td>
</tr>
<tr>
<td>2</td>
<td>mar...</td>
<td>prerouting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ether5</td>
</tr>
</tbody>
</table>
Step by Step Configuration

Step 2 Continued...

![Mangle Rule Configuration](image)
Step by Step Configuration

Step 2 Continued...

[Diagram of firewall configuration interface with various options and settings displayed, including Mangle Rule configurations for different parameters such as source address list, destination address list, layer 7 protocol, content, connection bytes, connection rate, per connection classifier, source MAC address, and connection mark.]
Several choices here, both addresses is the safest option, best balance of performance and reliability.
Step by Step Configuration

Step 2 Continued...

Several choices here, both addresses is the safest option, best balance of performance and reliability.
Step by Step Configuration

Step 2 Continued...

Several choices here, both addresses is the safest option, best balance of performance and reliability.

The mangle chain prerouting will be capturing all traffic, even traffic that is going to the router itself. To avoid this we will use dst-address-type=!local.
Step by Step Configuration

Step 2 Continued...

Several choices here, both addresses is the safest option, best balance of performance and reliability.

The mangle chain prerouting will be capturing all traffic, even traffic that is going to the router itself. To avoid this we will use `dst-address-type=!local`. 
Step by Step Configuration

Step 2 Continued...

“In Interface” is where the clients are, the LAN interface. Several choices here, both addresses is the safest option, best balance of performance and reliability. The mangle chain prerouting will be capturing all traffic, even traffic that is going to the router itself. To avoid this we will use dst-address-type=!local.
Step by Step Configuration

Step 2 Completed

Create one PCC mangle rule for each WAN connection

Completed PCC Mangle Rules

```
ip firewall mangle
add action=mark-connection chain=prerouting connection-mark=no-mark disabled=no dst-address-type=!local
 in-interface=ether5 new-connection-mark=WAN1 passthrough=yes per-connection-classifier=both-addresses:3/0
add action=mark-connection chain=prerouting connection-mark=no-mark disabled=no dst-address-type=!local
 in-interface=ether5 new-connection-mark=WAN2 passthrough=yes per-connection-classifier=both-addresses:3/1
add action=mark-connection chain=prerouting connection-mark=no-mark disabled=no dst-address-type=!local
 in-interface=ether5 new-connection-mark=WAN3 passthrough=yes per-connection-classifier=both-addresses:3/2
```
Step by Step Configuration

Step 3: Create the mangles to add the routing marks to the packets based on the connection mark in the PREROUTING CHAIN:
Step 3: Create the mangles to add the routing marks to the packets based on the connection mark in the PREROUTING CHAIN:
Step by Step Configuration

Step 3: Create the mangles to add the routing marks to the packets based on the connection mark in the PREROUTING CHAIN:
Step by Step Configuration

Step 3: Create the mangles to add the routing marks to the packets based on the connection mark in the PREROUTING CHAIN:

<table>
<thead>
<tr>
<th>Mangle Rule &lt;&gt;</th>
<th>General</th>
<th>Advanced</th>
<th>Extra</th>
<th>Action</th>
<th>Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chain:</td>
<td>prerouting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Src. Address:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dst. Address:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Src. Port:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dst. Port:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any. Port:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P2P:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In. Interface:</td>
<td>ether5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Out. Interface:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packet Mark:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection Mark:</td>
<td>WAN1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This is where we mark routing for the bulk of our traffic.
Step by Step Configuration

Step 3 Continued for OUTPUT CHAIN...
### Step by Step Configuration

**Step 3 Continued for OUTPUT CHAIN...**

![Mangle Rule Configuration Table](image-url)
Step by Step Configuration

Step 3 Continued for OUTPUT CHAIN...

<table>
<thead>
<tr>
<th>General</th>
<th>Advanced</th>
<th>Extra</th>
<th>Action</th>
<th>Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chain:</td>
<td>output</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Src. Address: |       |
| Dst. Address: |       |

| Protocol: |       |
| Src. Port: |       |
| Dst. Port: |       |
| Any. Port: |       |
| P2P: |       |

| In. Interface: |       |
| Out. Interface: |       |

| Packet Mark: |       |
| Connection Mark: | WAN1 |
| Routing Mark: |       |
| Routing Table: |       |

**Action:** mark routing

**New Routing Mark:** ether1-mark

**Passthrough**
Step by Step Configuration

Step 3 Continued for OUTPUT CHAIN...

This rule ensures traffic from the router itself returns through the proper interface.
Step by Step Configuration

Step 3 Completed

Create one rule for each WAN connection, in prerouting chain and same in output chain

Completed route marking rules

/ip firewall mangle

```
add action=mark-routing chain=prerouting connection-mark=WAN1 disabled=no in-interface=ether5 \ new-routing-mark=ether1-mark passthrough=yes
add action=mark-routing chain=prerouting connection-mark=WAN2 disabled=no in-interface=ether5 \ new-routing-mark=ether2-mark passthrough=yes
add action=mark-routing chain=prerouting connection-mark=WAN3 disabled=no in-interface=ether5 \ new-routing-mark=ether3-mark passthrough=yes
add action=mark-routing chain=output connection-mark=WAN1 disabled=no new-routing-mark=ether1-mark passthrough=yes
add action=mark-routing chain=output connection-mark=WAN3 disabled=no new-routing-mark=ether3-mark passthrough=yes
add action=mark-routing chain=output connection-mark=WAN2 disabled=no new-routing-mark=ether2-mark passthrough=yes
```
Step 4: Identify which WAN interface the traffic came in and mark the connections appropriately.
Step 4: Identify which WAN interface the traffic came in and mark the connections appropriately.
Step 4: Identify which WAN interface the traffic came in and mark the connections appropriately.
Step by Step Configuration

Step 4 Completed

Create one rule for each WAN connection

Completed WAN connection marking rules

```
/ip firewall mangle

add action=mark-connection chain=prerouting connection-mark=no-mark disabled=no \ in-interface=ether1 new-connection-mark=WAN1 passthrough=yes

add action=mark-connection chain=prerouting connection-mark=no-mark disabled=no \ in-interface=ether3 new-connection-mark=WAN3 passthrough=yes

add action=mark-connection chain=prerouting connection-mark=no-mark disabled=no \ in-interface=ether2 new-connection-mark=WAN2 passthrough=yes
```
Step by Step Configuration

Final result: Connections should be marked, route marks added to packets based on connection mark.

Always check the connection table to ensure mangles are working for connections.
Step by Step Configuration

Mangles are done, we now create the routes:
Step by Step Configuration

Mangles are done, we now create the routes:

• We will need one default route for each routing mark, corresponding to each of the WAN connections.
Step by Step Configuration

Mangles are done, we now create the routes:

• We will need one default route for each routing mark, corresponding to each of the WAN connections.
• We will also need one unmarked default route corresponding to each of the WAN connections.
Step by Step Configuration

Step 5: Create the unmarked default routes.
Step by Step Configuration

Step 5: Create the unmarked default routes.
Step by Step Configuration

Step 5: Create the unmarked default routes.
Step by Step Configuration

Step 5: Create the unmarked default routes.

![Route Configuration Screen]

- **Dst Address:** 0.0.0.0
- **Gateway:** 172.19.0.1
- **Type:** unicast
- **Distance:** 1
- **Scope:** 30
- **Target Scope:** 10
- **Routing Mark:**
- **Pref. Source:**

*ISPSupplies*

*LEARN ROUTER OS WITH Learn MikroTik.com*
Step by Step Configuration

Step 5: Create the unmarked default routes.

Provides failover - ensures traffic always has a default route because if there is no active marked route to match a packet, it follows the main routing table!
Step by Step Configuration

Step 5: Create the unmarked default routes.

Provides failover - ensures traffic always has a default route because if there is no active marked route to match a packet, it follows the main routing table!

Considering using distance to prefer one default over another.
Step 6: Create the marked default routes.
Step by Step Configuration

Step 6: Create the marked default routes.

<table>
<thead>
<tr>
<th>General</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dst. Address:</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Gateway:</td>
<td>172.17.0.1 reachable ether1</td>
</tr>
<tr>
<td>Check Gateway:</td>
<td>ping</td>
</tr>
<tr>
<td>Type:</td>
<td>unicast</td>
</tr>
<tr>
<td>Distance:</td>
<td>1</td>
</tr>
<tr>
<td>Scope:</td>
<td>30</td>
</tr>
<tr>
<td>Target Scope:</td>
<td>10</td>
</tr>
<tr>
<td>Routing Mark:</td>
<td>ether1-mark</td>
</tr>
<tr>
<td>Pref. Source:</td>
<td></td>
</tr>
</tbody>
</table>

enabled  active  static
Step by Step Configuration

Step 6: Create the marked default routes.
Step by Step Configuration

Step 6: Create the marked default routes.
Step by Step Configuration

Step 6: Create the marked default routes.

Use “check-gateway” to ensure gateway is alive.

Only need to use “check-gateway” on marked routes because any routes with that gateway become inactive if it fails thereby affecting marked routes too.
Step by Step Configuration

Final result - Routing table

One marked default for each WAN connection, and one unmarked default route for each WAN connection

Completed routing table
Step by Step Configuration

Final result!

Actual screen shots from a load balance configuration in production with 2 WAN connections.
Common Problems

I use DHCP for my WAN addressing, how can I get the marked routes created properly?

/system script
add name=ConfigureDHCPRoutes policy=
    ftp, reboot, read, write, policy, test, winbox, password, sniff, sensitive, api source=":local cli\`
    entcounter\`
    \n:n:local routecounter\`
    \n:n:local duplicatecounter\`
    \n:n:local routeupdated "no"\`
    \n:foreach clientcounter in=[/ip dhcp-client find] do={\`
    \n:n:local routingmarkname ([/ip dhcp-client get \$clientcounter interface] . "-mark")\`
    \n:n:local newroutinggateway [ip dhcp-client get \$clientcounter gateway]\`
    \n:n:foreach routecounter in=[/ip route find where routing-mark=\$routingmarkname] do={\`
    \n:n :local routinggateway [/ip route get [find routing-mark=\$routingmarkname] gateway]\`
    \r
    \n:t:if ([:len \$newroutinggateway] > 0) do={\r
    \n:t :if ("\$""routinggateway"" != \$""newroutinggateway"" ) do={ \r
    \n:t  /ip route set \$routecounter gateway=\$newroutinggateway \r
    \n:t:t:set routeupdated "yes"\r
    \n:t }\r
    \n:t}\r
    \n } \r
    \n :if ([:len \$newroutinggateway] > 0) do={\r
    \n :if (\$routeupdated = "no") do={\r
    \n /ip route add routing-mark=\$routingmarkname gateway=\$newroutinggateway dst-add ress=0.0.0.0/0\r
    \n }\r
    \n}\r
    \n"

Script by Andrew Cox
Common Problems

Before Running Script

<table>
<thead>
<tr>
<th>Route List</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routes</td>
</tr>
<tr>
<td>+</td>
</tr>
<tr>
<td>Dst. Address</td>
</tr>
<tr>
<td>AS</td>
</tr>
<tr>
<td>S</td>
</tr>
<tr>
<td>S</td>
</tr>
</tbody>
</table>

After Running Script

<table>
<thead>
<tr>
<th>Route List</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routes</td>
</tr>
<tr>
<td>+</td>
</tr>
<tr>
<td>Dst. Address</td>
</tr>
<tr>
<td>AS</td>
</tr>
<tr>
<td>AS</td>
</tr>
<tr>
<td>S</td>
</tr>
<tr>
<td>AS</td>
</tr>
</tbody>
</table>
Common Problems

PCC doesn’t seem to work properly with HotSpot or IP Webproxy

• It is possible to make it work but the rules get very detailed and complicated.

Solution: Use two routers, one for load balancing, one for HotSpot or IP Webproxy.

Solution: Use metarouter with host router doing main routing functions, virtual router doing the load balancing.
Common Problems

DNS resolves from some clients, not others

• If you are using two different ISP’s and their respective name servers, possibly some clients are accessing ISP1’s DNS server through ISP2’s connection and ISP1 is blocking DNS requests from outside their IP space.

Solution: Consider OpenDNS, destination NAT with redirect to DNS cache, etc.
Common Problems

Strange http issues, some images load, other don’t, problems with some secure sites

Solution: Try using “both addresses” or “source address“ for PCC classifier. While “both addresses and ports” gives the greatest chance for randomization and better possibility for even distribution, it can create these types of issues.
Common Problems

I can only get asymmetrical connections, one DSL and one cable modem.

Solution: You can “weight” one interface higher and force more traffic through it by repeating the connection marking PCC rule more than once for that connection.

Example for added weight to WAN3.

```
/ip firewall mangle
add action=mark-connection chain=prerouting connection-mark=no-mark disabled=
   no dst-address-type=!local in-interface=ether5 new-connection-mark=WAN1 \ passthrough=yes per-connection-classifier=both-addresses:3/0
add action=mark-connection chain=prerouting connection-mark=no-mark disabled=
   no dst-address-type=!local in-interface=ether5 new-connection-mark=WAN2 \ passthrough=yes per-connection-classifier=both-addresses:3/1
add action=mark-connection chain=prerouting connection-mark=no-mark disabled=
   no dst-address-type=!local in-interface=ether5 new-connection-mark=WAN3 \ passthrough=yes per-connection-classifier=both-addresses:3/2
add action=mark-connection chain=prerouting connection-mark=no-mark disabled=
   no dst-address-type=!local in-interface=ether5 new-connection-mark=WAN3 \ passthrough=yes per-connection-classifier=both-addresses:3/3
```
Thank You!

- MyWISPTraining.com
- LearnMikroTik.com
- ISPSupplies.com
- “RouterOS by Example” available for many distributors or Amazon.com, iTunes