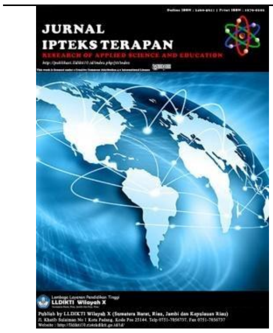


Vol.16 No.4 | Dec, 2022

LOAD BALANCE PCC AND FAILOVER WITH RECURSIVE GATEWAY

Deval Gusrion[1], Rima Liana Gema*[2], Silky Safira[3], Aulia Fitrul Hadi[4], Silfia Andini[5]

[12345] Universitas Putra Indonesia YPTK Padang

* Corresponding Email: rimalianagema@upiyptk.ac.id

Submit :
08/08/2022

Accept:
25/12/2022

Publish:
31/12/2022

Abstract

The continuous flow of information has become a necessity for organizations. The internet moves information quickly to support the activities of its users, PT. Graha Cipta Bangko Jaya. These organizations must keep running their business even when internet service is unavailable. There are several ways to overcome this problem, one of which is to use at least two different internet sources, which will be combined with failover techniques on the internet connection so that if one internet source is disconnected, it will be automatically transferred to another internet source. The failover technique is usually combined with the load balance technique, and there are several methods for the load balance, one of which is PCC (Per Connection Classifier). The PCC load balance and failover method are commonly used in the gateway check feature on the ip route menu. However, when implementing the gateway check feature, it can only check on the gateway device so that if there is a problem at the provider, it will not be able to be monitored by the router side. So that the router can check directly with the provider, it can add a recursive gateway technique to failover. A device that can support the above method is the Mikrotik Router. A Mikrotik router is a device or operating system specifically designed for routing in computer networks. Later the results of this research can ensure the availability of the internet within the organization and increase the operational productivity of the organization.

Keywords: Load Balance, Per Connection Classifier (PCC), Failover, Recursive Gateway, Mikrotik

doi : https://doi.org/10.22216/jit.v16i4 715-724
1979-9292 / 2460-5611 ©2021 © 2022 LLDIKTI Wilayah X

JIT is Sinta 3 Journal (https://sinta3.kemdikbud.go.id/journals/profile/2143) accredited by Ministry of Research & Technology, Republic Indonesia

INTRODUCTION

Business and industry development tends to be more complex from year to year. Many business and industrial organizations have developed because they have adopted and integrated the internet network into their business processes. Two internet sources are available to Indonesian users: wired and wireless. PT. Graha Cipta Bangko Jaya is one organization with the leading internet source from cable-based ISPs[7]. PT. Graha Cipta Bangko Jaya is a Palm Oil Mill (PKS) that utilizes the internet network in daily activities, such as sending reports, zoom meetings and most importantly, weighing palm fruit directly connected to the head office in Jakarta. When there is a very down network problem, it affects the company's performance in carrying out its functions. As a result, queues of cars carrying palm oil can be created because the delivery of the weighing results to the head office is hampered. This happens because only one ISP (Internet Service Provider) is used, and if the ISP line fails or there is a problem with the local network connecting to the internet, no action is taken to restore the network[4][5].

Therefore, to get maximum network stability when the ISP used is experiencing problems, it is necessary to add a new internet source that allows transferring internet access sources from the primary ISP to a new ISP or vice versa so that the internet can still be available and its availability guaranteed. Several methods can overcome this problem, namely the Load Balance and Failover methods[6][8].

Load balance distributes traffic loads on two or more lines to achieve a balanced connection, more optimal traffic, maximum data throughput, minimal delay, and no overload. Load balance can be applied in companies with at least two Internet connections [1]. In load balance, there are several methods, one of which is PCC (Per Connection Classifier), where PCC can be used to classify connection traffic going through or out of the router into several groups and divide the load into both internet connection lines to avoid overload [2]. At the same time, failover is a technique that applies multiple paths to reach the destination network. However, under normal circumstances, only one ISP is used. Other ISPs serve as backups and will only be used when the primary ISP dies [3][9]. The failover method usually carried out by PCC load balance is the gateway check feature on the ip route menu. However, when implementing the gateway check feature, it can only check on the gateway device so that if there is a problem at the provider, it will not be able to be monitored by the router side. So that the router can check directly with the provider, it can add even a recursive gateway technique[10].

RESEARCH METHODS

To complete this report, the research methods used are:

a. Observation (Observation)
The author makes field observations by looking directly at and studying the problems in computer networks at PT. Graha Cipta Bangko Jaya.

b. Interview (Interview)
In this case, the author asks questions directly to one of the staff who knows about computer networks at PT. Graha Cipta Bangko Jaya.

c. Library Research (Library Research)
The research was conducted to study and collect information related to this research. These various sources are obtained from scientific journals, theses, research reports, books, the internet, and other literature so that the data obtained can be used as a basis for the following research stage.

d. Laboratory Research
This research was conducted by the direct practice of the analysis results aimed at testing the correctness of the designed system.

RESULTS

In this section, we will discuss the stages of implementing PCC load balance and failover with the recursive gateway method in the form of a configuration in the form of screenshots of the router configuration and the results of system testing.

MikroTik Interface Initialization

Interface initialization helps facilitate the MikroTik configuration by giving a name to each interface according to the function and desire.

1. DHCP Client Configuration

A DHCP Client is a network device or computer that requests an IP address request from a DHCP server with the aim of being able to connect to the internet with the IP assigned by the DHCP Server. At this stage, the aim is to obtain an IP address from the ISP. The Mikrotik Router will act as a DHCP client. For DHCP-client configuration, you can use the following command:

```
"/ ip dhcp-client
add interface=ISP1 disabled=no
add-default-route=no"
```

2. Giving IP Address

At this stage, an IP address will be assigned to each interface used for the implementation of load balancing and failover. Since in my research I used a DHCP client on ISP1 and ISP2, the IP addresses on the ISP1 and ISP2 interfaces were automatically filled in by themselves. To assign an IP address to MikroTik, you can use the following command:

```
"/ ip address
```

ISSN : 1979-9292
E-ISSN : 2460-5611

```
add address=192.168.157.1/24
network=192.168.157.0
interface=Lokal
broadcast=192.168.157.255”
```

3. Konfigurasi IP DNS Server

DNS, or Domain Name System, is a technology for translating domain IP addresses, because actual addressing on the network uses IP addresses. A DNS server is useful for mapping a computer's host name to an IP address. At this stage, the DNS address used is the IP address of each ISP. The configuration is as follows:

```
“/ ip dns
set servers=8.8.8.8,1.1.1.1
allow-remote-requests=yes “
```

4. NAT Configuration

After configuring IP and DNS, you must add NAT (Network Address Translation) configuration. NAT is useful for clients connected to the internet. NAT will change the packet's source address, specifically the client address with a private IP address, so that the internet can recognize it by translating it into a public IP address. This NAT setting uses the Masquerading NAT method. Since the provider used only provides one public IP address, all client IP addresses will be mapped to one public IP address.

For NAT configuration, because this research uses two ISPs, then add two src-nat rules pointing to their respective ISPs with the command:

```
“/ ip firewall nat
add action=masquerade out-
interface=ISP1 chain=srcnat
add action=masquerade out-“
```

5. Mangle Configuration

Mangle helps mark a package, where the marking is done with the desired terms and conditions. The report results will then be used for specific purposes depending on the selected action. In the PCC method, packet marking is based on checking all packets, especially on src-IP, DST-IP, src-port and DST-port. From these parameters, connection marks and routing marks can be performed, which are then used to process specific packets.

The first step in managing an externally initiated connection is to ensure that when a connection request arrives, the connection response goes through the same interface (from the same public IP). Mark all incoming connections to remember the interface used with the command:

```
“/ ip firewall mangle
add in-interface=ether2
action=accept DST-
address=192.168.137.0/24
chain=prerouting
add in-interface=ether2
action=accept DST-
```

```
address=192.168.244.0/24
chain=prerouting
add new-connection-mark=ISP1
action=mark-connection
connection-mark=no-mark in-
interface=ISP1
chain=prerouting
add new-connection-mark=ISP2
action=mark-connection
connection-mark=no-mark in-
interface=ISP2
chain=prerouting”
```

Use of Action mark-routing can only be used to mangle chain output and prerouting, while mangle chain prerouting captures all traffic destined for routers. To avoid this, DST-address-type= !Local. Then add a PCC rule to split traffic into groups based on source and destination addresses (both addresses). Since the two ISPs have different speeds (4Mbps and 2Mbps), the traffic load is divided into three. The first two sections go through the ISP1 gateway, and the last one goes through the ISP2 gateway.

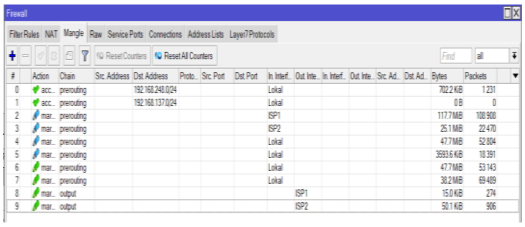
```
“/ ip firewall mangle
add DST-address-type=!Local
connection-mark=no-mark in-
interface=ether2
chain=prerouting
  new-connection-mark=ISP1
action=mark-connection per-
connection-classifier=both-
addresses:3/0
add DST-address-type=!Local
connection-mark=no-mark in-
interface=ether2
chain=prerouting
  new-connection-mark=ISP1
action=mark-connection per-
connection-classifier=both-
addresses:3/1
add DST-address-type=!Local
connection-mark=no-mark in-
interface=ether2
chain=prerouting
  new-connection-mark=ISP2
action=mark-connection per-
connection-classifier=both-
addresses:3/2”
```

After creating the PCC rule, add a mark-routing action based on the connection marker created. Remember to specify the parameters in the interface because policy routing is only needed for traffic destined for the internet.

```
/ ip firewall mangle
add action=mark-routing in-
interface=ether2 connection-
mark=ISP1 chain=prerouting
   new-routing-mark= to_ISP1
add action=mark-routing in-
interface=ether2 connection-
mark=ISP2 chain=prerouting
   new-routing-mark= to_ISP2
add new-routing-mark=to_ISP1
action=mark-routing
connection-mark=ISP1
chain=output
add new-routing-mark=to_ISP2
action=mark-routing
connection-mark=ISP2
chain=output”
```

The following is the result of setting the PCC load balance on the firewall mangle:

ISSN : 1979-9292
E-ISSN : 2460-5611



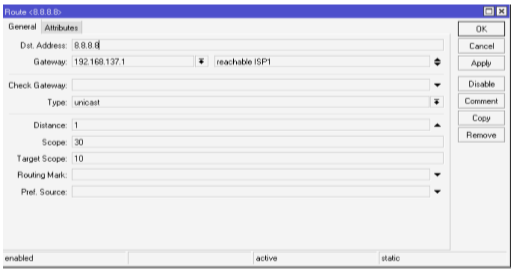
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Interf...	Out. Inte...	In. Interf...	Out. Inte...	Src. Ad...	Dst. Ad...	Bytes	Packets
0	acc...	prerouting		192.168.248.0/24				Lokal						702.2 KiB	1 231
1	acc...	prerouting		192.168.137.0/24				Lokal						0 B	0
2	mar...	prerouting						ISP1						117.7 MiB	108 908
3	mar...	prerouting						ISP2						25.1 MiB	22 470
4	mar...	prerouting						Lokal						47.7 MiB	52 804
5	mar...	prerouting						Lokal						3593.6 KiB	18 391
6	mar...	prerouting						Lokal						47.7 MiB	53 143
7	mar...	prerouting						Lokal						38.2 MiB	69 489
8	mar...	output							ISP1					15.0 KiB	274
9	mar...	output							ISP2					50.1 KiB	906

Figure 1. Results of PCC Marking Load Balance on Firewall Mangle

Making Failover with Recursive Gateway method

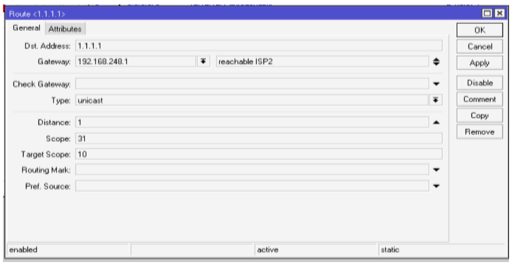
Failover with a Recursive Gateway is one way to check the gateway outside the modem network or the ISP gateway (NAP), an easy example is when we have more than one ISP, and one ISP is having problems, Mikrotik will still respond that the status of that ISP no problem or refined, this happens if you only use the failover method, because Mikrotik only pings the nearest gateway, namely the modem, when in fact the ISP is down / to. Therefore, adding a recursive gateway method is necessary to check the gateway outside the modem network or the ISP gateway.

The first step is to create a static route that will be used as a trigger for the recursive gateway. This rule is used as the recursive gateway default route. In this design, the author uses IP on the internet, namely IP = 8.8.8.8 for ISP1 and IP = 1.1.1.1 for ISP2.



Route <8.8.8.8>
General | Attributes
Dst. Address: 8.8.8.8
Gateway: 192.168.137.1 reachable ISP1
Check Gateway:
Type: unicast
Distance: 1
Scope: 30
Target Scope: 10
Routing Mark:
Pref. Source:
enabled active static

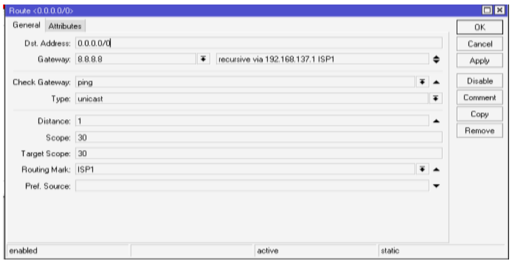
Figure 2. Configuring Recursive Gateway Default Route on ISP1



Route <1.1.1.1>
General | Attributes
Dst. Address: 1.1.1.1
Gateway: 192.168.248.1 reachable ISP2
Check Gateway:
Type: unicast
Distance: 1
Scope: 31
Target Scope: 10
Routing Mark:
Pref. Source:
enabled active static

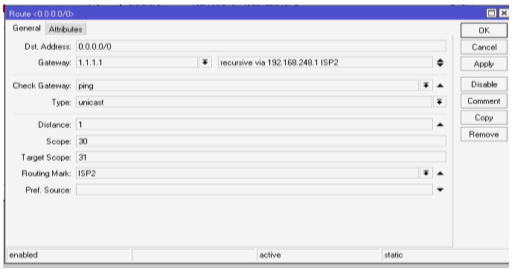
Figure 3. Configuring the Recursive Gateway Default Route on ISP2

Next, to distinguish between ISP1 and ISP2 triggers, change the Scope parameter in the rule. In this study, the scope of ISP1 is 30, and the scope of ISP2 is 31. Furthermore, the Distance for manipulating the main gateway still uses the value one because its function is not as a failover but as a check-gateway. Moreover, do not forget to enable ping on the check-gateway feature.



Route <0.0.0.0/0>
General | Attributes
Dst. Address: 0.0.0.0/0
Gateway: 8.8.8.8 recursive via 192.168.137.1 ISP1
Check Gateway: ping
Type: unicast
Distance: 1
Scope: 30
Target Scope: 30
Routing Mark: ISP1
Pref. Source:
enabled active static

Figure 3. Configuring Check Gateway and Routing Mark on ISP1


Route <0.0.0.0/0>

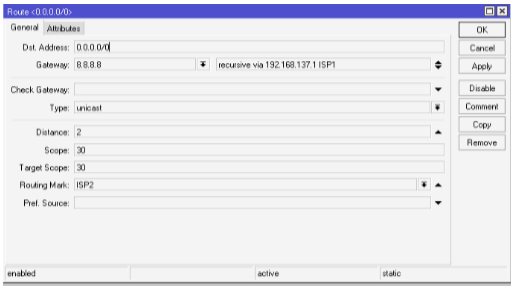
Dst. Address: 0.0.0.0/0
Gateway: 1.1.1.1 recursive via 192.168.248.1 ISP2
Check Gateway: ping
Type: unicast
Distance: 1
Scope: 30
Target Scope: 31
Routing Mark: ISP2
Pref. Source:

enabled | active | static

Figure 4. Configuring Check Gateway and Routing Mark on ISP2

Then add a default route based on the previously created PCC mark-routing. The gateway can use a predetermined IP, 8.8.8.8 for ISP1 and 1.1.1.1 for ISP2. For failover to work, as usual, we still specify the order of the Distance gateway main (primary) or a backup gateway (backup). Distance with a smaller value will take precedence, and a more considerable Distance will work as a backup. After that, so that the recursive can run normally, point to the Target-Scope based on the trigger rule created earlier.

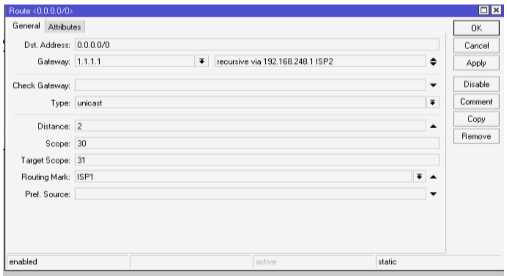
“ISP's default route 1 uses target scope=30
ISP 2 default route using target scope=31”


Route <0.0.0.0/0>

Dst. Address: 0.0.0.0/0
Gateway: 8.8.8.8 recursive via 192.168.137.1 ISP1
Check Gateway:
Type: unicast
Distance: 2
Scope: 30
Target Scope: 30
Routing Mark: ISP2
Pref. Source:

enabled | active | static

Figure 5. Configuring Routing Mark as Backup Gateway from ISP1

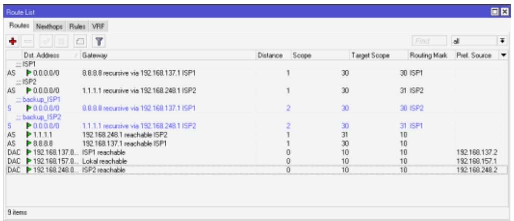

Route <0.0.0.0/0>

Dst. Address: 0.0.0.0/0
Gateway: 1.1.1.1 recursive via 192.168.248.1 ISP2
Check Gateway:
Type: unicast
Distance: 2
Scope: 30
Target Scope: 31
Routing Mark: ISP1
Pref. Source:

enabled | active | static

Figure 6. Configuring Routing Mark as Backup Gateway from ISP2

After all the steps are done, the complete routing rule can be seen in the image below:


Route List

	Dst. Address	Gateway	Distance	Scope	Target Scope	Routing Mark	Pref. Source
	;;; ISP1						
AS	0.0.0.0/0	8.8.8.8 recursive via 192.168.137.1 ISP1	1	30	30	ISP1	
	;;; ISP2						
AS	0.0.0.0/0	1.1.1.1 recursive via 192.168.248.1 ISP2	1	30	31	ISP2	
	;;; backup_ISP1						
S	0.0.0.0/0	8.8.8.8 recursive via 192.168.137.1 ISP1	2	30	30	ISP2	
	;;; backup_ISP2						
S	0.0.0.0/0	1.1.1.1 recursive via 192.168.248.1 ISP2	2	30	31	ISP1	
AS	1.1.1.1	192.168.248.1 reachable ISP2	1	31	10		
AS	8.8.8.8	192.168.137.1 reachable ISP1	1	30	10		
DAC	192.168.137.0...	ISP1 reachable	0	10	10		192.168.137.2
DAC	192.168.157.0...	Lokal reachable	0	10	10		192.168.157.1
DAC	192.168.248.0...	ISP2 reachable	0	10	10		192.168.248.2

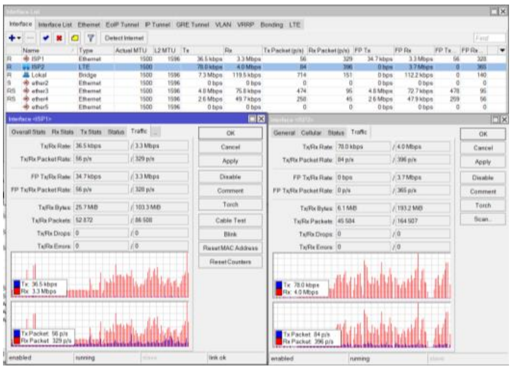
9 items

Figure 7. Results of Making Routing Rules

TEST

The test is run to analyze the PCC Load Balance method by watching videos from two different sources, namely through the website www.youtube.com and another through www.drive.google.com, and to prove whether the PCC method can mark which gateway or path can be used. Testing the PCC method can be carried out in the hope of being efficient and approaching the break-even point. If there is a use of the number of connections, the amount of traffic passing through ISP1 and ISP2 can be monitored by the Winbox application itself as follows:

ISSN : 1979-9292
E-ISSN : 2460-5611



Interface List

	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx...	FP Rx...
R	ISP1	Ethernet	1500	1596	36.5 kbps	3.3 Mbps	56	329	34.7 kbps	3.3 Mbps	56	328
R	ISP2	LTE	1500		78.0 kbps	4.0 Mbps	84	396	0 bps	3.7 Mbps	0	365
R	Lokal	Bridge	1500	1596	7.3 Mbps	119.5 kbps	714	151	0 bps	112.2 kbps	0	140
S	ether2	Ethernet	1500	1596	0 bps	0 bps	0	0	0 bps	0 bps	0	0
RS	ether3	Ethernet	1500	1596	4.0 Mbps	75.6 kbps	474	95	4.0 Mbps	72.7 kbps	478	95
RS	ether4	Ethernet	1500	1596	2.6 Mbps	49.7 kbps	250	45	2.6 Mbps	47.9 kbps	259	56
	ether5	Ethernet	1500	1596	0 bps	0 bps	0	0	0 bps	0 bps	0	0

Interface <ISP1>

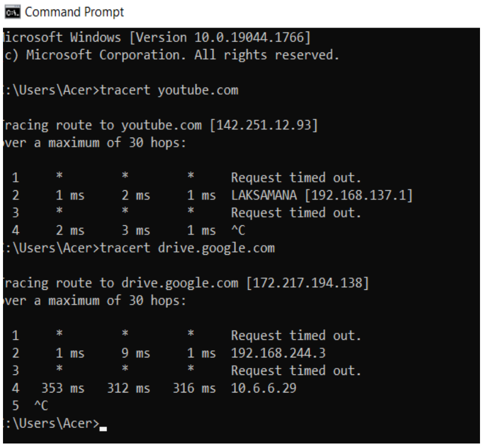
Tx/Rx Rate: 36.5 kbps / 3.3 Mbps
Tx/Rx Packet Rate: 56 p/s / 329 p/s
FP Tx/Rx Rate: 34.7 kbps / 3.3 Mbps
FP Tx/Rx Packet Rate: 56 p/s / 328 p/s
Tx/Rx Bytes: 25.7 MiB / 103.3 MiB
Tx/Rx Packets: 52 872 / 86 508
Tx/Rx Drops: 0 / 0
Tx/Rx Errors: 0 / 0

Interface <ISP2>

Tx/Rx Rate: 78.0 kbps / 4.0 Mbps
Tx/Rx Packet Rate: 84 p/s / 396 p/s
FP Tx/Rx Rate: 0 bps / 3.7 Mbps
FP Tx/Rx Packet Rate: 0 p/s / 365 p/s
Tx/Rx Bytes: 6.1 MiB / 193.2 MiB
Tx/Rx Packets: 45 504 / 164 507
Tx/Rx Drops: 0 / 0
Tx/Rx Errors: 0 / 0

Figure 8. Testing the Application of the PCC Load Balance Method

The test results show that the two ISP lines are active simultaneously when accessing videos on different websites. It can be seen in the upstream interface (ISP) and Rx traffic. Rates 3.3 Mbps and 4.0 Mbps according to the connection speed at each ISP. Next, we can see which ISP path is used when accessing a website by doing a traceroute. Traceroute can be done by opening a command prompt and typing tracert followed by the website you want to monitor, as shown below:



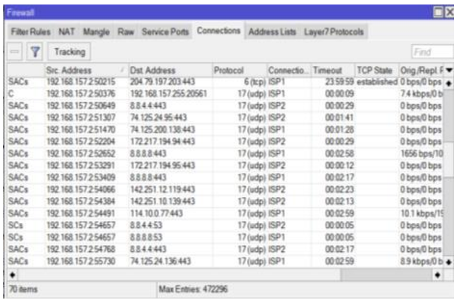
Command Prompt

```
icrosoft Windows [Version 10.0.19044.1766]
c) Microsoft Corporation. All rights reserved.

:\Users\Acer>tracert youtube.com

racing route to youtube.com [142.251.12.93]
ver a maximum of 30 hops:

1     *        *        *     Request timed out.
2     1 ms     2 ms     1 ms  LAKSAMANA [192.168.137.1]
3     *        *        *     Request timed out.
4     2 ms     3 ms     1 ms  ^C
:\Users\Acer>tracert drive.google.com

racing route to drive.google.com [172.217.194.138]
ver a maximum of 30 hops:

1     *        *        *     Request timed out.
2     1 ms     9 ms     1 ms  192.168.244.3
3     *        *        *     Request timed out.
4   353 ms   312 ms   316 ms  10.6.6.29
5   ^C
:\Users\Acer>_
```

Figure 9. Traceroute Test

From the results of the two traceroute tests above for different IP addresses, it can be seen that they both go through different ISP gateways. The destination of the website www.youtube.com goes through the ISP1 gateway (192.168.137.1) while the destination website www.drive.google.com goes through the ISP2 gateway (192.168.248.3). After carrying out the above implementation, it was found that the nature of PCC remembers the path traversed by connection traffic, and can then analyze the connections that occur and determine the size of packets that pass through each interface, so that it is known if the PCC method has been successful or not.

The following are the results of monitoring that occurs when the client laptop downloads a file:



Firewall

	Src. Address	Dst. Address	Protocol	Connectio...	Timeout	TCP State	Orig./Repl. F
SACs	192.168.157.2:50215	204.79.197.203:443	6 (tcp)	ISP1	23:59:59	established	0 bps/0 bps
C	192.168.157.2:50376	192.168.157.255:20561	17 (udp)	ISP1	00:00:09		7.4 kbps/0 b
SACs	192.168.157.2:50649	8.8.4.4:443	17 (udp)	ISP2	00:00:29		0 bps/0 bps
SACs	192.168.157.2:51307	74.125.24.95:443	17 (udp)	ISP2	00:01:41		0 bps/0 bps
SACs	192.168.157.2:51470	74.125.200.138:443	17 (udp)	ISP1	00:01:28		0 bps/0 bps
SACs	192.168.157.2:52204	172.217.194.94:443	17 (udp)	ISP2	00:00:29		0 bps/0 bps
SACs	192.168.157.2:52652	8.8.8.8:443	17 (udp)	ISP1	00:02:58		1656 bps/10
SACs	192.168.157.2:53291	172.217.194.95:443	17 (udp)	ISP2	00:00:12		0 bps/0 bps
SACs	192.168.157.2:53409	8.8.8.8:443	17 (udp)	ISP1	00:02:17		0 bps/0 bps
SACs	192.168.157.2:54066	142.251.12.119:443	17 (udp)	ISP2	00:02:23		0 bps/0 bps
SACs	192.168.157.2:54384	142.251.10.139:443	17 (udp)	ISP2	00:02:13		0 bps/0 bps
SACs	192.168.157.2:54491	114.10.0.77:443	17 (udp)	ISP1	00:02:59		10.1 kbps/1:
SCs	192.168.157.2:54657	8.8.4.4:53	17 (udp)	ISP2	00:00:05		0 bps/0 bps
SCs	192.168.157.2:54657	8.8.8.8:53	17 (udp)	ISP1	00:00:05		0 bps/0 bps
SACs	192.168.157.2:54768	8.8.4.4:443	17 (udp)	ISP2	00:02:17		0 bps/0 bps
SACs	192.168.157.2:55730	74.125.24.136:443	17 (udp)	ISP1	00:02:59		8.9 kbps/0 b

70 items	Max Entries: 472296

Figure 10. PCC Testing Works in Classifier

From the observations made, the results of ISP1 and ISP2 connections that have been marked are almost balanced, namely 7 and 8 times. That is, the PCC has marked the connection as balanced and sent it to the routing process. Then the

ISSN : 1979-9292
E-ISSN : 2460-5611

connection marked as ISP1 will be traversed to the Routing-mark Line-1, namely the ISP1 gateway, and the connection marked as ISP2 will be passed to the Routing-mark Route-2, namely the ISP2 gateway. Furthermore, the movement of failover with the recursive gateway method can be seen on the Mikrotik IP-Route menu. After that, for the initial stage of failover testing with this recursive gateway method, ISP1 and ISP2 will be turned on as shown below:

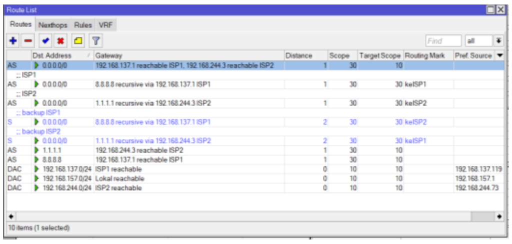

```
Route List
Routes  Nexthops  Rules  VRF
                                                                                         Find   all
      Dst. Address      Gateway                                                Distance  Scope  Target Scope  Routing Mark  Pref. Source
AS    0.0.0.0/0         192.168.137.1 reachable ISP1, 192.168.244.3 reachable ISP2    1     30            10
  ::: ISP1
AS    0.0.0.0/0         8.8.8.8 recursive via 192.168.137.1 ISP1                      1     30            30  kelSP1
  ::: ISP2
AS    0.0.0.0/0         1.1.1.1 recursive via 192.168.244.3 ISP2                      1     30            30  kelSP2
  ::: backup ISP1
S     0.0.0.0/0         8.8.8.8 recursive via 192.168.137.1 ISP1                      2     30            30  kelSP2
  ::: backup ISP2
S     0.0.0.0/0         1.1.1.1 recursive via 192.168.244.3 ISP2                      2     30            30  kelSP1
AS    1.1.1.1           192.168.244.3 reachable ISP2                                  1     30            10
AS    8.8.8.8           192.168.137.1 reachable ISP1                                  1     30            10
DAC   192.168.137.0/24  ISP1 reachable                                                0     10            10                192.168.137.119
DAC   192.168.157.0/24  Lokal reachable                                               0     10            10                192.168.157.1
DAC   192.168.244.0/24  ISP2 reachable                                                0     10            10                192.168.244.73
10 items (1 selected)
```

Figure 11. ISP1 And ISP2 Are On

In Figure above, it can be seen that the ISP1 backup and ISP2 backup are blue, which indicates that the gateway settings are not running because the main gateway settings are still in good condition, so there is no need to use ISP backups. Furthermore, the test is continued by turning off the internet source on ISP.

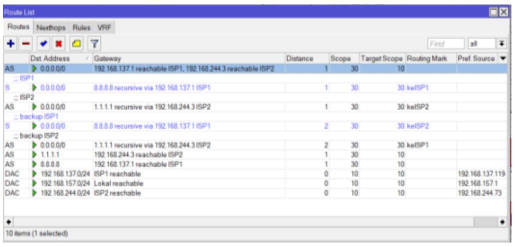

```
Route List
Routes  Nexthops  Rules  VRF
                                                                                         Find   all
      Dst. Address      Gateway                                                Distance  Scope  Target Scope  Routing Mark  Pref. Source
AS    0.0.0.0/0         192.168.137.1 reachable ISP1, 192.168.244.3 reachable ISP2    1     30            10
  ::: ISP1
S     0.0.0.0/0         8.8.8.8 recursive via 192.168.137.1 ISP1                      1     30            30  kelSP1
  ::: ISP2
AS    0.0.0.0/0         1.1.1.1 recursive via 192.168.244.3 ISP2                      1     30            30  kelSP2
  ::: backup ISP1
S     0.0.0.0/0         8.8.8.8 recursive via 192.168.137.1 ISP1                      2     30            30  kelSP2
  ::: backup ISP2
AS    0.0.0.0/0         1.1.1.1 recursive via 192.168.244.3 ISP2                      2     30            30  kelSP1
AS    1.1.1.1           192.168.244.3 reachable ISP2                                  1     30            10
AS    8.8.8.8           192.168.137.1 reachable ISP1                                  1     30            10
DAC   192.168.137.0/24  ISP1 reachable                                                0     10            10                192.168.137.119
DAC   192.168.157.0/24  Lokal reachable                                               0     10            10                192.168.157.1
DAC   192.168.244.0/24  ISP2 reachable                                                0     10            10                192.168.244.73
10 items (1 selected)
```

Figure 12. ISP1 Is Off And ISP2 Is On

Figure above shows a change where when ISP1 is turned off, the ISP1 gateway settings and ISP1 backups are immediately blue or not running and are transferred to ISP2, and ISP2 backup internet sources are used. Then turn on the ISP1 internet source again, then turn off the ISP2 internet source. It will be like the following picture:

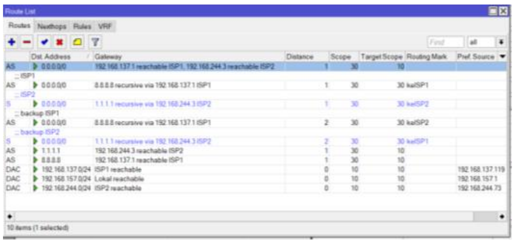

```
Route List
Routes  Nexthops  Rules  VRF
                                                                                         Find   all
      Dst. Address      Gateway                                                Distance  Scope  Target Scope  Routing Mark  Pref. Source
AS    0.0.0.0/0         192.168.137.1 reachable ISP1, 192.168.244.3 reachable ISP2    1     30            10
  ::: ISP1
AS    0.0.0.0/0         8.8.8.8 recursive via 192.168.137.1 ISP1                      1     30            30  kelSP1
  ::: ISP2
S     0.0.0.0/0         1.1.1.1 recursive via 192.168.244.3 ISP2                      1     30            30  kelSP2
  ::: backup ISP1
AS    0.0.0.0/0         8.8.8.8 recursive via 192.168.137.1 ISP1                      2     30            30  kelSP2
  ::: backup ISP2
S     0.0.0.0/0         1.1.1.1 recursive via 192.168.244.3 ISP2                      2     30            30  kelSP1
AS    1.1.1.1           192.168.244.3 reachable ISP2                                  1     30            10
AS    8.8.8.8           192.168.137.1 reachable ISP1                                  1     30            10
DAC   192.168.137.0/24  ISP1 reachable                                                0     10            10                192.168.137.119
DAC   192.168.157.0/24  Lokal reachable                                               0     10            10                192.168.157.1
DAC   192.168.244.0/24  ISP2 reachable                                                0     10            10                192.168.244.73
10 items (1 selected)
```

Figure 13. ISP1 is On, and ISP2 is Off

Figure above shows a change where when ISP1 is turned on and ISP2 is turned off, the gateway settings for ISP1 and backup ISP1 change to black, while for ISP2 and backup ISP2, it turns blue or does not work.

QoS Test

QoS testing should be carried out to measure the quality of Internet services used for load balancing. Because the quality of internet services is not only measured by the amount of bandwidth provided, the quality of good internet services also has other characteristics such as short delay time, reduced packet loss, and others.

Throughput Test

Gateway Status	Throughput (kbps)			average	Note:
	PC1	PC2	PC3	(kbps)	
ISP1	415	464	298	392	1
ISP2	434	326	283	348	1

Table1. Throughput Testing Before Implementing

Gateway Status		Throughput (kbps)			average	Note:
ISP1	ISP2	PC1	PC2	PC3	(ms)	
ON	ON	1159	886	780	942	2
OFF	ON	554	383	445	461	1
ON	OFF	473	672	115	420	1

Table 2. Throughput Testing After Implementation

CONCLUSION

Based on the results of this study, the following conclusions were obtained:

1 By implementing a load balance using the PCC method, you can distribute the amount of load connected evenly to all the ISP gateways used. However, the size of the packets forwarded to each ISP is unbalanced because the PCC method is broken down only by Connection, not the size of packets passing through the ISP.

2 Per Connection Classifier works by grouping incoming or outgoing connection traffic into groups and then distinguishing based on the source IP address, destination IP address, source port, and destination port.

3 PCC testing is done by dividing the load or traffic volume that passes through ISP1 and ISP2, which is then monitored by the Winbox application.

4 Applying the Failover technique with the Recursive Gateway is already functioning properly. When one of the internet gateway connections is lost, or the Connection is down, all internet connection loads will be transferred automatically to the gateway that is still active.

5 Quality of Service (QoS) testing is carried out using the parameters of packet loss, throughput, delay and jitter on the Wireshark application. It is found that using the PCC load balance of two ISPs, the QoS results are better.

BIBLIOGRAPHY

[1] Leman, D. (2019). Load Balancing 2 Jalur Internet Menggunakan Mikrotik Round Robin. *Riau Journal of Computer Science*, *05*(02), 137–143. https://doi.org/10.30606/rjocs.v5i2.1767

[2] Tantoni, A., Mutawalli, L., & Zaen, M. T. A. (2022). Komparasi QoS Load Balancing Pada 4 Line Internet DENGAN Metode PCC , ECMP Dan NTH. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *6*, 110–119. https://doi.org/10.30865/mib.v6i1.3436

[3] Novianto, D., & Helmud, E. (2019). Implementasi Failover dengan Metode Recursive

ISSN : 1979-9292
E-ISSN : 2460-5611

Gateway Berbasis Router Mikrotik Pada STMIK Atma Luhur Pangkalpinang Program studi Teknik Informatika STMIK Atma Luhur 2) Program studi Sistem Informasi STMIK. *JURNAL ILMIAH INFORMATIKA GLOBAL*. https://doi.org/10.36982/jiig.v10i1.732

[4] KN, N. (2021). ANALISA JARINGAN LOKAL AREA NETWORK (LAN) DI SALAH SATU HOTEL WILAYAH JAKARTA TIMUR. *Jurnal Ilmiah Matrik*. https://doi.org/10.33557/jurnalmatrik.v23i3.1567

[5] Leman, D. (2019). Load Balancing 2 Jalur Internet Menggunakan Mikrotik Round Robin. *Riau Journal of Computer Science*, *05*(02), 137–143. https://doi.org/10.30606/rjocs.v5i2.1767

[6] Rismawati, N., & Mulya, M. F. (2020). Analisis dan Perancangan Simulasi Jaringan MAN (Metropolitan Area Network) dengan Dynamic Routing EIGRP (Enhanced Interior Gateway Routing Protocol) dan Algoritma DUAL (Diffusing Update Algorithm) Menggunakan Cisco Packet Tracer. *Jurnal SISKOM-KB (Sistem Komputer Dan Kecerdasan Buatan)*. https://doi.org/10.47970/siskom-kb.v3i2.147

[7] Santoso, J. D. (2020). Analisis Perbandingan Metode Queue Pada Mikrotik. *Pseudocode*. https://doi.org/10.33369/pseudocode.7.1.1-7

[8] Tantoni, A., Ashari, M., & Zaen, M. T. A. (2020). Analisis Dan Implementasi Jaringan Komputer Brembuk.Net Sebagai Rt/Rw.Net Untuk Mendukung E-Commerce Pada Desa Masbagik Utara. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*. https://doi.org/10.30812/matrik.v19i2.591

[9] Wahyudi, A., Hadi, A. F., & Sovia, R. (2020). Performance Analysis With Wireless Lan Networks Using The Quality Of Service Method. *JITCE (Journal of Information Technology and Computer Engineering)*. https://doi.org/10.25077/jitce.4.01.45-48.2020

[10] Wijaya, A., & Purwanto, T. D. (2019). Implementasi Metode Rekayasa Sistem Jaringan Komputer untuk Pengembangan Jaringan Komputer. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*. https://doi.org/10.26418/jp.v5i3.29925