Implementation of Load Balancing and Failover with Three ISPs using PCC Case Study: CV. Setia Kawan

Alvian, DhannyPermatasariPutri Faculty of Computer Science Universitas Mercu Buana Jakarta, Indonesia

Abstract:- The internet, now a day, has important rules to search for information, learning, searching for news, and entertainment. The problem that often arises is that sometimes there is instability on the network or internet providers who often experience downtime and slow internet connections, which have become human obstacles to their internet network needs. The implementation of load balancing techniques and Failover techniques allows traffic to flow evenly and prevent overload on one connection. This system is made to solve problems on the internet network; the network is designed using three ISP provider with load balancing and failover technique to support network performance when downtime or disconnect so that the line network can switch smoothly directly to another ISP which are still available. As the result, the user or client will not have trouble when downloading or uploading their work.

Keywords:- Load Balancing, Failover, Per Connection Classifier (PCC), Network.

I. INTRODUCTION

The internet, now a day, has important rules to search for information, learning, searching for news, and entertainment. The internet has made people attach to the need for an internet network. However, the problem that often arises is that sometimes there is instability on the network or internet providers who often experience downtime and slow internet connections, which have become human obstacles to their internet network needs. Established implementation requires overcoming this by implementing load-balancing techniques and using 3 ISPs in the network.

The implementation of load balancing techniques will provide benefits to users for using internet facilities. Because load balancing can divide the traffic load into the two connection lines in a balanced way, allowing traffic to flow evenly and preventing overload on one connection. Meanwhile, the failover technique is used to deal with an ISP if it disconnects or goes down so that the other ISP can automatically back up to another ISPs. Failover is the ability of a system to switch to a backup system, either manually or automatically, when the condition of one of the systems fails.And at this time at CV SetiaKawan, overload events are unavoidable because the average active user exceeds the capacity that must settle.The following is

data on the occurrence of downtime on the system within 1	
year (counting from 2021 to 2022).	

Month	Week-1	Week-2	Week-3	Week-4
Jan 2021	2 x	1x	3x	2 x
Feb 2021	2 x	3x	2 x	3x
Mar 2021	1x	lx	2 x	2 x
Apr 2021	3x	2 x	2 x	1x
May 2021	2 x	2 x	1x	3x
Jun 2021	lx	3x	2 x	1x
Jul 2021	3x	2 x	2 x	2 x
Aug 2021	2 x	2 x	3x	1x
Sep 2021	1x	4x	2 x	2 x
Oct 2021	4x	2 x	2 x	3x
Nov 2021	3x	2 x	4x	2 x
Dec 2021	2 x	1x	4x	3x
Jan 2022	4x	3x	3x	4 x
Total		119x down t	ime in 1 a year	

Table 1: Downtime Table

From the data above, the increasing needs of internet users amid the current Covid-19 pandemic, causemany downtime failures. This becomes question of how to avoid overload on an internet network with load balancing and implementing the failover method.

A. Load Balancing

Load balancing is a technique to even out two connection lines that must balance on a network, which allows traffic to travel more efficiently. It also enables throughput optimization to avoid overloading a single connection path. It can make a connection more stable and optimal. The conditions that apply to the common scheduling algorithms on Load Balancers are Round Robin Scheduling Algorithm and Least Connection Algorithm. To distribute connection traffic loads on two or more connection lines in a balanced way so that traffic runs optimally, the load balancing methods that can be used are ECMP (Equal-Cost Multiple Path), PCC (Per-Connection Classifier) and NTH.

Per Connection Classifier (PCC)

The PCC load balancing method is a load balancing method that combines Per Connection Load Balancing with Per Address Pair Load Balancing. With these two techniques, PCC in LAN networks will be more adaptable.

Equal Cost Multi-Path (ECMP)

Equal Cost Multi-Path (ECMP) is to automatically rotate the output selection path on the gateway. There are two or more gateway paths for outgoing packets from this router. With this ECMP application approach, outgoing and incoming packets that pass through the track gateway will have the same load.

> Nth

Nth is the load-balancing mechanism included in the proxy. This method works with the operating method of utilizing a round-robin algorithm that can disconnect distribution solutions that will mangle to routes that have been built for a load-balancing approach.

B. Failover

Failover is a method that uses several kinds of connection lines to get a destination network. But under normal circumstances, the implementation is done using only one link. The other links are used as backups and will be used when the main link is down.

II. LITERATURE REVIEW

Research and implementation were made by Eudes Raymond in 2018 about the Implementation with two ISPs using method Connection N and PCC[6], Systems built using the Nth load balancing approach and the PCC load balancing method can solve the problem if the ISP loses connectivity.

Another in 2020 by Mustafa and Ramayanti about implementation of Load Balancing and Failover to the Device Mikrotik Router Using the NTH Method (Case Study: PT.GO-JEK Indonesia) [2], using the NHT approach, balances the traffic on the two connection lines to prevent overloading one connection line.

III. METHOD

A. Data collection

Conducting interviews and observations is a technique used by the author to obtain research data. The purpose of collecting qualitative data (interviews and observations) is to collect reliable and objective data because this data is collected directly from the informants in the case study, namely interviewing the head of the Network Engineer section at CV. SetiaKawan. B. Research stage

Below shown the flow of the research stage.

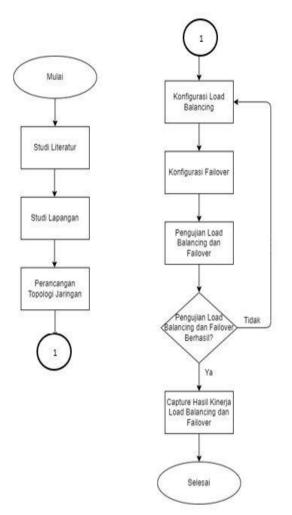


Fig. 1: Research Stage

For the problems in the companies, such as the frequency of internet downtime, this can occur up to 1-2 times per month. The problem happened when the company was still using only 1 ISP. To overcome these problems author implemented the method, by making the network topology modification. The implementation is by using 3 ISPs in one network design. Then the author will carry out the load-balancing configuration process. At this load-balancing configuration stage, the authorsuse a Mikrotik device.

IV. RESULT AND DISCUSSION

A. Prepare Load Balancing

Load balancing is required on small- or large-scale networks that have two or more gateways to ensure stability and network availability which is always available so that communication remains connected even when interruptions occur. The network must be able to minimize connection interruptions on the main network so that the system can continuously exchange data and information.

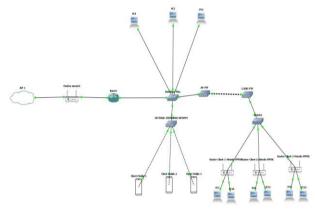


Fig. 2: Topology Before Load Balancing

The implementation is with the previous condition that only uses 1 ISP change to use 3 ISP in a network connection and add load balancing.

The Hardware &Software

- Mikrotik Router
- Router
- Switch
- Fiber Optic
- LAN cable
- Winbox Virtual Machine
- Windows Operating system

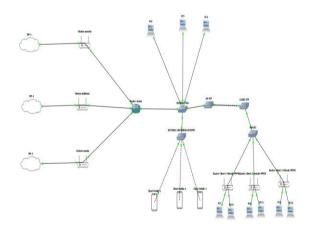


Fig. 3: Topology after Load Balancing

B. Load Balancing Configuration

The first step is to install Internet LAN from ISP Oxygen, ISP Indihome and ISP Remala in one Mikrotik router, then connect it to a client using a LAN cable from the Mikrotik router to the client's computer. The configuration:

/int	erface bridge
add	name=bridge-klient
/int	erface ethernet
set	[find default-name=ether]] name=ether1-isp1-oxygen
set	[find default-name=ether2.] name=ether2-isp2-indihome
set	[find default-name=ether3.] name=ether3-isp3-remala

Assign IP addresses in the following order.

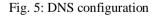
/ip address	
add address=192.10	58.100.100/24 interface=ether1-isp1-
oxygen network=19	2.168.100.0
add address=172.10	6.1.1/24 interface=bridge-klient
network=172.16.1.0	
add address=192.10	58.200.200/24 interface=ether3-isp3-
remala network=19	2.168.200.0
add address=192.10	58.1.150/24 interface=ether2-isp2-
indihome network=	=192.168.1.0

This is what shows the configuration:

🗡 Quick Set		Add	Address List							
Î	CAPsMAN	+								
-	Interfaces		Address /	Network	Interface	Comment				
2	Wireless		172.16.1.1/24	172.16.1.0	bridge-klient					
t			+ 192.168.1.150/24	192.168.1.0	ether2-isp2-indi					
X	Bridge		+ 192.168.100.100/24	192.168.100.0	ether1-isp1-oxy					
à	PPP		+ 192.168.200.200/24	192.168.200.0	ether3-isp3-rem					
 +	Switch									
•	Mesh									
255	IP	1								
0	MPLS	P								
5	Routing	1								
	System	1								
-	Queues									
-	Files									

Fig. 4: Address List

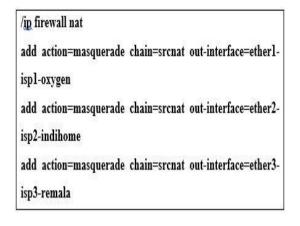
Servers:	208.67.222.222	\$	OK
Dynamic Servers:			Cancel
Use DoH Server:		_	Apply
	Verify DoH Certificate		Static
	✓ Allow Remote Requests		Cache



/ Quick Set	DHCP S	Server									
CAPSMAN	DHCP	Network	s Lea	ases Optio	ns C	Option	Sets Ver	ndor Classes	Alerts		
Interfaces	+		7	DHCP Co	nfig	DHO	P Setup				
🗍 Wireless	Na	me		Interface		1	Relay	Lease Time		Address Pool	Add AR.
🔀 Bridge	dho	:p1		bridge-klie	nt				00:10:00) dhcp_pool0	no
🛓 PPP											
T Switch											
Switch											
Mesh											
Mesh											
Mesh IP MPLS											

Fig. 6: Configuration DHCP server

NAT configuration can be done with the following command:



C. Mangle Configuration

Mangle is a kind of 'marker' that marks packets for future processing with special marks. The function mangle is to tag the route packets according to the current routing rules. The authors will use the PCC load-balancing method using mangle rules. In the PCC approach mangle configuration stage, the author uses various mangle sequences, such as:

- Chain Pre-routing
- Chain Input
- Chain Output

The configuration command is as follows:

/ip firewall mangle

add action=mark-connection chain=input in-interface=etherlispl-oxygen \ new-connection-mark=koneksi ispl passthrough=no

add action=mark-connection chain=input in-interface=ether2isp2-indihome \

new-connection-mark=koneksi isp2 passthrough=no

add action=mark-connection chain=input in-interface=ether3isp3-remala \

new-connection-mark=koneksi_isp3 passthrough=no

add action=mark-routing chain=output connection-

mark=koneksi_ispl \

new-routing-mark=ke_ispl passthrough=no

add action=mark-routing chain=output connection-

mark=koneksi_isp2 \

new-routing-mark=ke_isp2 passthrough=no

add action=mark-routing chain=output connection-

mark=koneksi_isp3 \

new-routing-mark=ke_isp3 passthrough=no

```
add action=mark-connection chain=prerouting
comment=pcc dst-address-type=\
  !local in-interface=bridge-klient new-connection-
mark=koneksi_ispl \
  passthrough=yes per-connection-classifier=both-
addresses-and-ports:3/0
add action=mark-connection chain=prerouting dst-
address-type=!local \
  in-interface=bridge-klient new-connection-
mark=koneksi_isp2 passthrough=\
 yes per-connection-classifier=both-addresses-and-
ports:3/1
add action=mark-connection chain=prerouting dst-
address-type=!local \
  in-interface=bridge-klient new-connection-
mark=koneksi_isp3 passthrough=\
 yes per-connection-classifier=both-addresses-and-
ports:3/2
```

D. Routing Configuration and Failover

For the first step, create a static route that functions as a recursive gateway trigger. This rule will use as a recursive gateway trigger. The author uses a public IP on the internet, for ISP1 IP = 9.9.9.9, for ISP2 IP = 1.1.1.1, and for ISP3 IP = 8.8.8.8.

To distinguish between ISP1 and ISP2 triggers, set the scope parameter in the rule. In this case, the scope of ISP1 is 30, the scope of ISP2 is 31, and the scope of ISP3 is 32. Here are the configuration commands:

Static Route Configuration

add comment="ping isp1" distance=1 dst-address=9.9.9.9/32

gateway=192.168.100.1

add comment="ping isp2" distance=1 dst-address=1.1.1.1/32

gateway=192.168.1.1 scope=31

add comment="ping isp3" distance=1 dst-address=8.8.8.8/32

gateway=192.168.200.1 scope=32

Default Route Configuration

/ip route
add check-gateway=ping comment="rec isp1" distance=1
gateway=9.9.9.9 \
routing-mark=ke_ispl target-scope=30
add check-gateway=ping comment="rec isp2" distance=1
gateway=1.1.1.1 \
routing-mark=ke_isp2 target-scope=31
add check-gateway=ping comment="rec isp3" distance=1
gateway=8.8.8.8 \
routing-mark=ke_isp3 target-scope=32

➢ Backup Route Configuration

add chee	ck-gateway=ping comment="backup isp3 ke isp1"
distance	=2 gateway=\
8.8.8.8	3 routing-mark=ke_isp1 target-scope=32
add cheo	ck-gateway=ping comment="backup isp2 ke isp1"
distance	=2 gateway=\
1.1.1.1	l routing-mark=ke_isp1 target-scope=31
add cheo	ck-gateway=ping comment="backup isp1 ke isp2"
distance	=2 gateway=\
9.9.9.9	9 routing-mark=ke_isp2 target-scope=30
add cheo	ck-gateway=ping comment="backup isp3 ke isp2"
distance	=3 gateway=\
8.8.8.8	3 routing-mark=ke_isp2 target-scope=32
add cheo	ck-gateway=ping comment="backup isp2 ke isp3"
distance	=3 gateway=\
1.1.1.1	l routing-mark=ke_isp3 target-scope=32
add cheo	ck-gateway=ping comment="backup isp1 ke isp3"
listanco	=3 gateway=\
listance	

So that the router can still access the internet, add a default gateway configuration without the mark-routing parameter. The result in the routing table will be the following:

			ista	and	eck-gateway=ping comment= e=1 gateway=\ 168.1.1,192.168.200.1,192.168		t untu	k mikro	tik"
		_							
Route Lie Routes		ktho	ps R	ules	VRF				
	Nex		os R		VRF				
	Nex V	x		7	VRF Gateway	Check Gateway	Distance	Routing Mark	Pref. Source
Routes	Nex Dst	X Ad	dress	7		Check Gateway	Distance	Routing Mark	Pref. Source 172.16.1.1
Routes	Nex Dist	X Ad	dress 16.1.0	7	Gateway	Check Gateway	Distance	Routing Mark 0 0	
Routes + -	Neo Dst	X Ad 172	dress 16.1.0 168.1	V24 .0/24	Gateway bridge-klient reachable	Check Gateway	Distance	Routing Mark 0 0 0	172.16.1.1
Routes + -	Nex Dist	X Ad 172 192	dress 16.1.0 168.1 168.1	2/24 .0/24 .00.0/.	Gateway bridge-klient reachable ether2-sp2-indhome reachable	Check Gateway	Distance	Routing Mark 0 0 0 0	172.16.1.1 192.168.1.150
Route L Routes + - DAC DAC DAC DAC DAC	Ner Dst	X Ad 172 192 192	dress 16.1.0 168.1 168.2	0/24 .0/24 .0/24 .00.0/.	Gataway bridge-kilent reachable ether2-isp2-iordhome reachable .ether1-isp1-oxygen reachable	Check Gateway	Distance	Routing Mark 0 0 0 0	172.16.1.1 192.168.1.15 192.168.100.

Fig. 7: Default Route Mikrotik

Of all the stages described earlier, the final result of this recursive is as follows:

/ Quick Set	Roube U	2						8 ×
CAPSMAN	Routes	Nexthops Rules	vis:					
interfaces	+	1 1 7				Fins	[at	1
Weekasa		Dut Address	Galaxier/	Check Galaxies	Distance	Routing Mark	Prel Sout	-
Bridge	DAC.	▶ 172.16.1.024	bridge-klent reachable			0	172.16.1.1	£.,
ppp	DAC					0	192 168 1	
	DAC		. ether1-isp1-oxygen reachable			0	192,168,1	
T Switch	DAC		ether3-sp3-remails reachable			0	192, 168.2	/20.
Mesh		okup isp1 ke isp2						
ΨP	5	P00004	9.833 wousive via 192.168.100.1 ether5-lop1-orggen	ping		2 km mm2		
2 MPLS	= 03	okup isp1 Ke isp3						
	3	\$ 00000 ¢	9.8.9.3 recursive via 192, 168 100.1 wher 1-op1-copper	hed		Ske mil		
J. Routing	::00	ckup isp2 ke isp1	1.1.1.1 monsive via 152.168.1.1 wher2-sp2-indhome			2ke isst		
System	3	ckup so2 ke so3	1.1.1.1 recursive via 102.105.1.1 ether2-op2-indhome	ping		244_021		
Convec	2.00	B 0 0 0 0 0	1.1.1.1 mounter via 192.198.1.1 adm/J ing/-indicate			3ke mel		
Files	1	okup sp3 ke sp1	1.1.1.1 mountain via 102. Ibi. 1.1 mountaine	bad		314 403		
E Los	2		8.8.8.3 recursive via 192 198 200.1 ether3-inc3-emaile	ping		2 km mpt		
	:: 54	ckup iss3 ke iss2		1-1				
RADIUS	5	00000	8.8.8.9 securities via 152 155 200.1 atten3-sp3-semala	ping		She mm2		
/ Tools	- 145	enst unt A mikrotik						
IN New Terrinal	45	B 00000	192 193 1 1 reachable attw2-ac2-indihome. 192 168 200 1 machable attw3-isp3-remain. 192 168 100 1 reachable attwr1-isp1-orygen	ping		1		
· DertX	: 97	ig ap1						
	AS	\$ 9399	192, 198, 100, 1 reachable effer 1-sp1-oxygen			1		
	:: pir	g isp2						
🔮 Partition	45	▶ 1.1.1.1	192.163.1.1 reachable ether2-ap2-inditionve			1		
Wake Support of		ig isp3						
New Winflox	AS	8.8.8.8	192, 198, 200, 1 machable ether3-isp3-mmale			1		
	0.70							
En En	AS	▶ 0.5.0.00	9.833 recursive via 192.188.100.1 ether1-isp1-cuppen	prg		the_ispt		
	01					101000		
Windows	AS	▶ 00.000 €	1.1.1.1 recursive via 192.198.1.1 efter2-inp2-indhame	246		1 ke_ing2		
	:: /01							
	AS	▶ 0.0.0.00 €	8.8.8 recursive via 192.198.200.1 ether3-isp3-remaila	ping		t ke_ep3		

Fig. 8: Recursive Failover Configuration Results

E. Load Balancing Test

In the first test, the authorsimplement load balancing using the PCC method. This PCC system always maintains the path that was passed at the beginning of the connection traffic flow.

The following is the result of the connection that runs when the client downloads in the conditions before load balancing is applied and after load balancing is applied:

CAP\$MAN	Elter Bules	NAT Mande Raw	Service Ports Cor	nections	Address Lists La	aver7 Protocols			
Interfaces									
	- 7	Tracking							
NireGuard		Src. Address /	Dst. Address		Connection Mark			Orig./Repl. Rate	Orig./Repl. Bytes
H Bridge	SC	192.168.177.1	172.19.9.18	1 (ic		00:00:00		0 bps/0 bps	56 B/56 B
	C	192.168.177.1	172.19.9.206	1 (ic		00:00:02		0 bps/0 bps	168 B/0 B
🛓 PPP	C	192.168.177.1	172.19.9.61	1 (ic		00:00:02		0 bps/0 bps	168 B/0 B
Mesh	SC	192.168.177.1	172.19.9.201	1 (c		00:00:00		0 bps/0 bps	56 B/56 B
	SC	192.168.177.1	172.19.9.20	1 (ic		00:00:00		0 bps/0 bps	56 B/56 B
+ · ·	36	192.168.177.1	172.19.9.30	1 (c		00:00:01		0 bps/0 bps	56 B/56 B
MPLS	SC	192.168.177.1	172.19.9.1	1 (ic		00:00:03		0 bps/0 bps	56 B/56 B
🐏 IPv6	SC	192.168.177.1	172.19.9.4	1 (c		00:00:03		0 bps/0 bps	56 B/56 B
-	SC	192.168.177.1	172.19.9.203	1 (ic		00:00:05		0 bps/0 bps	56 B/56 B
🔀 Routing	SC	192.168.177.1	172.19.9.22	1 (ic		00:00:05		0 bps/0 bps	56 B/56 B
🖉 System	SC	192.168.177.1	172.19.9.12	1 (ic		00:00:05		0 bps/0 bps	56 B/56 B
Queues	C	192.168.177.1	172.19.9.26	1 (ic		00:00:09		0 bps/0 bps	56 B/0 B
•	SAC	192.168.177.1.33034	172,19.9.18:8291	6 (tcp)		23:59:54	established	0 bos/0 bos	16.1 MB/24.8 MB
📔 Files	SAC	192.168.177.1:33898	172.19.9.207.8291	6 (top)		00:00:05	time wait	0 bps/0 bps	216 B/112 B
E Log	SAC	192.168.177.1:37792	172.19.9.252.8291	6 (tcp)		23:59:52	established	0 bps/0 bps	2639.6 KB/3922
19 RADIUS	SAC	192,168,177,1:38132	172.19.9.27:8291	6 (top)		00:00:08	ime wait	0 bos/0 bos	216 B/112 B
	SAC	192.168.177.1:39628	172.19.9.250:8291	6 (tcp)		00:00:06	time wait	0 bps/0 bps	216 B/112 B
🕺 Tools	SAC	192,168,177,1:39752	172.19.9.66:8291	6 tcp		23:59:51	established	0 bos/0 bos	16.0 MB/24.7 MB
80 New Terminal	SAC	192.168.177.1:39950	172.19.9.30:8291	6 (tcp)		23:59:59	established	1632 bos/1088 bos	16.0 MB/24.5 MB
Dot1X	C	192.168.177.1:40150	172.19.9.204.8291	6 tcp		00:00:00	sin sent	0 bos/0 bos	180 B/0 B
	SAC	192,168,177,1:40818	172.19.9.15:8291	6 (tcp)		23:59:58	established	832 bos/2.1 kbos	7.2 MB/11.0 MB
🕓 Dude	SAC	192.168.177.1:40836	172.19.9.21:8291	6 tcp		23:59:53	established	0 bos/0 bos	5.2 MB/7.9 MB
Make Supout of	C	192.168.177.1:41514	172.19.9.48:8291	6 (top)		00:00:03	syn sent	480 bos/0 bos	120 B/0 B
New WinBox	SAC	192.168.177.1.42192	172.19.9.203.8291	6 (tcp)		23:59:54	established	0 bos/0 bos	16.0 MB/25.7 MB
-	SAC	192.168.177.1:42954	172.19.9.28:8291	6 tcp		00:00:08		0 bos/0 bos	216 B/112 B
🛃 Ext	SAC	192.168.177.1:43190	172 19 9 208 8291	6 (tcp)				1632 bps/1088 bps	16.0 MB/24.6 MB
	SAC	192 168 177 1-44384	172 19 9 1 8291	6 tcp				1632 bos/1088 bos	16.9 MB/75.0 MB

Fig. 9: Testing Downloads on the Client Before Load Balancing

D	iia	nc	m	g

Tracking						
	Src. Address	Dst. Address	Protocol Connection Mark	Timeout TCP State		
¢	0.0.0.0:68	255.255.255.255.67	17 (udp) koneksi_isp2	00:00:09		
SACs	172.16.1.253:49716	20.198.162.78.443	6 (tcp) koneksi_isp1	23:57:46 established		
SACs	172.16.1.253:49741	40.99.10.82:443	6 (tcp) koneksi_isp1	21:08:18 established		
SACs	172.16.1.253:49788	72.25.64.2:443	6 (tcp) koneksi_isp2	23:59:35 established		
SACs	172.16.1.253.49817	20.197.71.89:443	6 (tcp) koneksi_isp1	23:59:34 established		
SACs	172.16.1.253:49835	34.201.182.184:443	6 (tcp) koneksi_isp2	23:59:27 established		
SACs	172.16.1.253:49865	13.76.153.29:443	6 (tcp) koneksi_isp1	23:59:26 established		
SACs	172.16.1.253.49871	50.16.23.154.443	6 (tcp) koneksi_isp3	23:59:48 established		
SACs	172.16.1.253:50115	104.91.72.56:80	6 (tcp) koneksi_isp1	06:07:34 established		
SACs	172.16.1.253:50116	118.98.77.115:80	6 (tcp) koneksi_isp3	06:07:34 established		
SACs	172.16.1.253:50168	52.98.90.2:443	6 (tcp) koneksi_isp3	14:46:15 established		
SACs	172.16.1.253:50171	40.99.8.194:443	6 (tcp) koneksi_isp1	14:43:51 established		
SACs	172.16.1.253:52754	162.159.130.232:443	6 (tcp) koneksi_isp2	23:59:44 established		
SACs	172.16.1.253:52755	52.111.240.14:443	6 (tcp) koneksi_isp2	23:59:38 established		
SACs	172.16.1.253:52762	54.192.116.104:443	6 (tcp) koneksi_isp1	23:59:17 established		
SACs	172.16.1.253:52763	52.200.37.22:443	6 (tcp) koneksi_isp2	23:59:18 established		
SACs	172.16.1.253.52764	54.204.87.86:443	6 (tcp) koneksi_isp2	23:59:33 established		
SACs	172.16.1.253:53136	162.159.134.233:443	17 (udp) koneksi_isp2	00.02.26		
SACs	172.16.1.253:53794	162.159.128.233:443	17 (udp) koneksi_isp1	00:02:06		
С	172.16.1.253.54915	172.16.1.255:54915	17 (udp) koneksi_isp2	00:00:09		
SACs	172.16.1.253.57339	35.186.224.47:443	6 (tcp) koneksi_isp3	23:59:31 established		
SACs	172.16.1.253.57427	162.159.133.234:443	6 (top) koneksi_isp1	23:59:59 established		
SACs	172.16.1.253:58451	52.111.240.14:443	6 (top) koneksi_isp2	23:59:45 established		
SACs	172.16.1.253:58453	52.111.240.14:443	6 (top) koneksi_isp3	23:59:45 established		

Fig. 10: Testing Downloads on the Client After Load Balancing

From the results above, the condition before the implementation of load balancing, there was only 1 IP line which Moratel(as provider),-caused the overload.

Meanwhile, after implementing load balancing, of course, the traffic will run evenly and automatically, and there will be no more overload things that will occur because the paths are divided into more balanced and even distributions.

F. Connection Balance Test (Balance)

The authors will then verify the connection balance, utilizing the Winbox program to monitor the network before and after load balancing. The result:

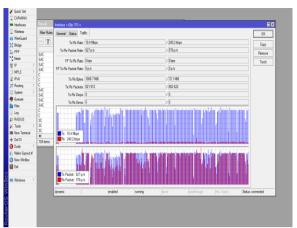


Fig. 11: Connection Graph Before Load Balancing

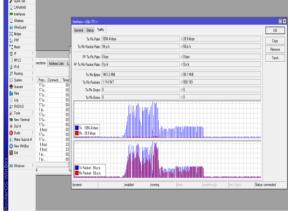


Fig. 12: Graph Down Time on Connection



Fig. 13: Connection Graph of Each ISP After Load Balancing

The result is that PCC load balancing effectively distributed packets and bytes over both interfaces. Based on the results, it is possible to conclude that this PCC loadbalancing approach can share deployment packets by balancing them across all gateways.

G. Failover Testing

The authors examine the information obtained to evaluate the performance of the load-balancing system that was created. It compensates for connection failures caused by one of the ISPs. Even if one of each internet service provider's connections is lost, the system will still have two ISPs or one other ISP that can be accessed as a backup internet connection with failover.

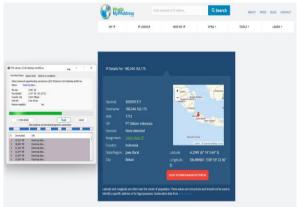
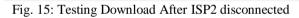


Fig. 14: Download Testing Using 3 ISPs

		from Reports or P Address	Introduced to Position. Q Search		ABOUT PRESS BLOG CONTACT	
	arri#	и соокци насели и	VPNS -	10013 *	LEASTN +	
	IP Details For: 103.166	1031				
🕼 Thi alumi 22.04 daling ondelas 🧠 — — — X						
Handhar beragter Hannharden (1994) Hannharden (19	Services Notes	2010) C1221 Fredita Sta Joya Heinard Sta Sta Sta Sta Sta Lattude D Sta				



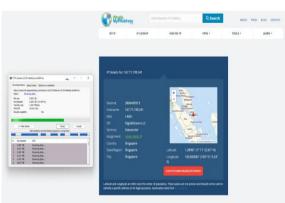


Fig. 16: Testing Download After ISP2 and ISP1 disconnected

From the results, the downloads continued to run smoothly without any connection problems being interrupted. Because it will automatically switch if ISP2 disconnected then ISP1 and ISP3 will become the default gateways that support the operation of the entire network. It can be monitored from the IP address checked through the IP checker website, namely https://whatismyipaddress.com.

At the beginning of the download process, it still uses ISP2, - Indihome with IP 180.244.162.175. And after the ISP2 is disconnected, the download process continues, but the resulting speed decreases by 10Mbps and the total speed becomes 20Mbps. Also, the IP that passed is using ISP1 and ISP2 connections, namely Moratel and Remala, and the connected IP is 103.160.12.81.

If ISP2 and ISP1 disconnected, the download process will also continue, but the speed will decrease to 20mbps and the total speed is only 10mbps and the IP that is skipped is only a connection from ISP3, namely Remala with IP 167.71.199.241.

V. CONCLUSION

Based on the theory and discussion in the previous chapters that have been done, it can be concluded that.

- The design of load balancing on a system can help to build a good performance. Load balancing can divide the load more evenly and can divide one traffic lane into several connecting lines symmetrically.
- The system design implemented by using the failover technique succeeded in solving the problem, -in the form that if one of the ISPs is down, failover will automatically back up the other internet networks that are still running.
- In the aspect of choosing an ISP, the authors suggest choosing an ISP that can download and upload speeds that are not much different. So, that when browsing or doing other things you don't experience slow connection speeds due to the different response times for each ISP.
- It is recommended to use two load balancer proxy devices, so that load balancing performance is more stable and can share the workload with other proxy devices and not burden only one proxy.

REFERENCES

- [1.] Frayogi, W. Yahya, and R. A. Setiawan, "Perbandingan Kinerja RouterOS Mikrotik dan Zeroshell pada Mekanisme Load Balancing Serta Failover," J. Pengemb. Teknol. Inf. dan Ilmu Komput., vol. 2, no. 7, pp. 2689–2697, 2018.
- [2.] Mustofa and D. Ramayanti, "Implementasi Load Balancing dan Failover to Device Mikrotik Router Menggunakan Metode NTH (Studi Kasus: PT.GO-JEK Indonesia)," J. Teknol. Inf. dan Ilmu Komput., vol. 7, no. 1, pp. 139–144, 2020, doi: 10.25126/jtiik.2020701638.
- [3.] Suryanto, T. Prasetyo, and N. Hikmah, "Implementasi Load Balancing Menggunakan Metode Per Connection Classifier (PCC) Dengan Failover Berbasis Mikrotik Router," Semin. Nas. Inov. dan Tren, vol. 1, no. 1, pp. A230–A238, 2018.
- [4.] Abdullah, "Implementasi teknik Load Balancing Dan Failover Dengan Metode ECMP Dalam Peningkatan Kualitas Layanan Jaringan, IJ Jurnal Sains Komputer dan Teknologi Informasi," J. Sains Komput. dan Teknol. Inf., vol. 3, no. 1, pp. 111– 115, 2020.

- [5.] Wartono, B. Soedijono, and E. Pramono, "Analisa Optimasi Penggunaan Bandwidth Dengan Failover Dan Load Balance Pada Mikrotik," J. Inf. Politek. Indonusa Surakarta, vol. 5, no. 3, pp. 33–39, 2019.
- [6.] 2018 Gene, Eudes Raymond, "Implementasi Load Balancing Dengan Dua Isp Menggunakan Metode (Koneksi Ke-N) Dan Per Connection Classifier (Pcc) Pada Mikrotik," Skripsi. Univ. Sanata Dharma, p. 63, 2018, [Online]. Available: Gene, Eudes Raymond.
- [7.] H. J. Marpaung, "Management Hotspot Dengan Load Balance 3 ISP Menggunakan Mikrotik RB1100AHX4 Untuk Menstabilkan Koneksi Internet," JURTEKSI - J. Teknol. dan Sist. Inf., vol. VII, no. 3, pp. 311–316, 2021.
- [8.] Satiarini, E. Safrianti, and L. O. Sari, "Optimalisasi Jaringan Menggunakan Teknik Load Balancing Metode Peer Connection Classifier (Studi Kasus: Dinas Perpustakaan Dan Kearsipan Provinsi Riau)," J. Online Mhs. Univ. Riau, vol. 7, no. 1, pp. 1–8, 2020.
- [9.] D. K. Hakim, A. Yahyo, T. Informatika, U. Muhammadiyah, and P. Nth, "IMPLEMENTASI LOAD BALANCING MENGGUNAKAN JARINGAN INDIHOME DAN TELKOMSEL PADA MIKROTIK ROUTER DENGAN METODE NTH," vol. 13, no. 1, pp. 13–23, 2019.
- [10.] M. K. Anwar and I. Nurhaida, "Implementasi Load Balancing Menggunakan Metode Equal Cost Multi Path (ECMP) Pada Interkoneksi Jaringan," J. Telekomun. dan Komput., vol. 9, no. 1, p. 39, 2019, doi: 10.22441/incomtech.v9i1.5003.
- [11.] S. Hidayat, A. E. Widodo, A. Kencono, and Y. Nuryamin, "Implementasi Load Balancing Dengan Metode PCC Pada Balai Besar Pelatihan Kesehatan (BBPK) Jakarta," vol. 9, no. 1, 2021.
- [12.] P. Yandi, G. Made, A. Sasmita, and K. Suar, "Analisis Dan Optimalisasi Jaringan Menggunakan Metode Per Connection Classifier (Studi Kasus: Cas Tech)," JITTER - J. Ilm. Teknol. dan Komput., vol. 1, no. 1, 2020.
- [13.] S. D. Riskiono and D. Pasha, "ANALISIS METODE LOAD BALANCING DALAM MENINGKATKAN KINERJA WEBSITE E-LEARNING," J. Teknoinfo, vol. 14, no. 1, pp. 22– 26, 2020.
- [14.] Dartono, S. Usanto, and D. Irawan, "Penerapan metode per connection classifier (pcc) pada perancangan load balancing dengan router mikrotik," J. Elektro Inform., vol. 1, no. 1, pp. 14– 20, 2021.
- [15.] Djumhadi and R. S. Roring, "PERANCANGAN DAN IMPLEMENTASI JARINGAN FAILOVER MENGGUNAKAN PROTOKOL SPANNING TREE PADA PT. PLN UP3B KALIMANTAN TIMUR," J. Ilm. Matrik, vol. 22, no. 3, pp. 249– 256, 2020.
- [16.] H. I. Pohan, "Analisis dan Implementasi Internet Gateway Menggunakan Mikrotik Routerboard di Virtualbox," Universitas Pembangunan Panca Budi, 2019.

- [17.] P. N. Permana, "DISTRIBUSI JARINGAN MENGGUNAKAN ROUTING OSPF DENGAN METODE REDISTRIBUTION," J. Simetris, vol. 9, no. 1, pp. 519–532, 2018.
- [18.] R. Rahadjeng and Ritapuspitasari, "ANALISIS JARINGAN LOCAL AREA NETWORK (LAN) PADA PT. MUSTIKA RATU Tbk JAKARTA TIMUR," J. Prosisko, vol. 5, no. 1, pp. 53–60, 2018.
- [19.] F. A. Purwaningrum, A. Purwanto, and E. A. Darmadi, "Optimalisasi jaringan menggunakan firewall," J. IKRA-ITH Inform., vol. 2, no. 3, pp. 17–23, 2018.
- [20.] M. Fakhmi and L. M. Gultom, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Syn Flood dengan Menggunakan Firewall Raw (Studi kasus: Sekolah Menengah Kejuruan Negeri 3 Bengkalis)," in Seminar Nasional Industri dan Teknologi (SNIT), 2021, pp. 260–277.
- [21.] Natali, Fajrillah, and T. M. Diansyah, "IMPLEMENTASI STATIC NAT TERHADAP JARINGAN VLAN MENGGUNAKAN IP DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)," J. Ilm. Inform., vol. 1, no. 1, pp. 51–58, 2016.
- [22.] H. Wintolo, S. Aryanto, and M. Hafish, "Analisis Pengaruh Konfigurasi NAT Statik Berbasis Web Menggunakan Wire Shark," J. Inform., vol. 8, no. 1, pp. 93–98, 2021.
- [23.] F. Ardianto, B. Alfaresi, and A. Darmadi, "RANCANG BANGUN LOAD BALANCING DUA INTERNET SERVICE PROVIDER (ISP) BERBASIS MIKROTIK," J. Surya Energy, vol. 3, no. 1, pp. 198–202, 2018.
- [24.] Afrizal and Fitriani, "Penerapan IPV4 dan IPV6 pada Jaringan yang Terhubung," J. JTIK (Jurnal Teknol. Inf. dan Komunikasi), vol. 3, no. 1, pp. 2–6, 2019.
- [25.] D. Y. Pratama, G. Sukadarmika, and N. P. Sastra, "Analisis Availability Metrics Webserver Penyedia Website Program Studi Teknik Elektro Fakultas Teknik Universitas Udayana," J. Spektrum, vol. 6, no. 3, pp. 35–44, 2019.
- [26.] M. Zakkiyah and M. Rahman, "Internet Service Provider (ISP) RT-RW NET Di Desa Kasiyan Timur Kec. Puger Kab. Jember," J. Pengabdi. Masy. Ipteks, vol. 7, no. 1, pp. 30–36, 2021.
- [27.] D. F. Waidah, D. D. Putra, and Syarifuddin, "PERENCANAAN SISTEM JARINGAN DAN KOMUNIKASI DATA PT. WIRA PENTA KENCANA," J. Tikar, vol. 2, no. 2, pp. 140–152, 2021.