ISSN No:-2456-2165

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	2x	1x	3x	2x
Feb 2021	2x	3x	2x	3x
Mar 2021	1x	1x	2x	2x
Apr 2021	3x	2x	2x	1x
May 2021	2x	2x	1x	3x
Jun 2021	1x	3x	2x	1x
Jul 2021	3x	2x	2x	2x
Aug 2021	2x	2x	3x	1x
Sep 2021	1x	4x	2x	2x
Oct 2021	4x	2x	2x	3x
Nov 2021	3x	2x	4x	2x
Dec 2021	2x	1x	4x	3x
Jan 2022	4x	3x	3x	4x
Total	119x down time 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 becomesa 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.

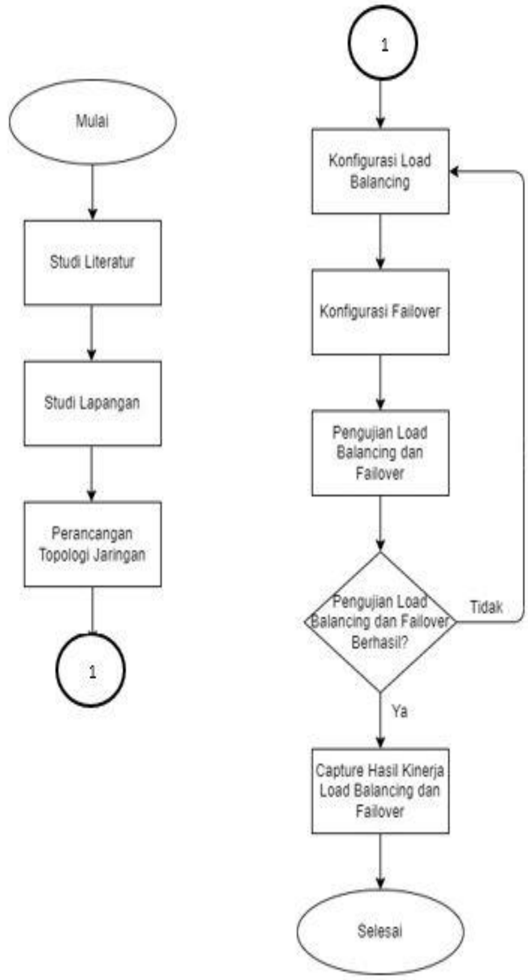

Fig. 1: Research Stage

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.

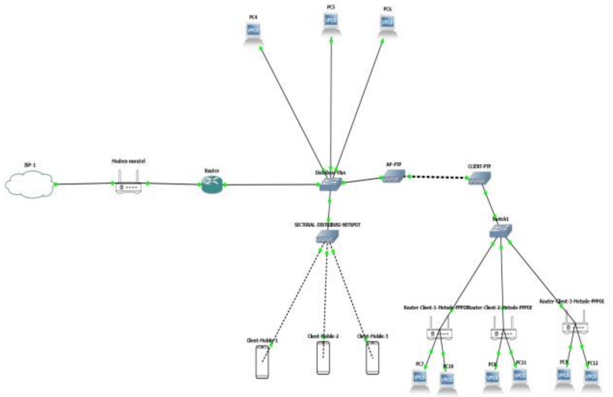

Fig. 2: Topology Before Load Balancing

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

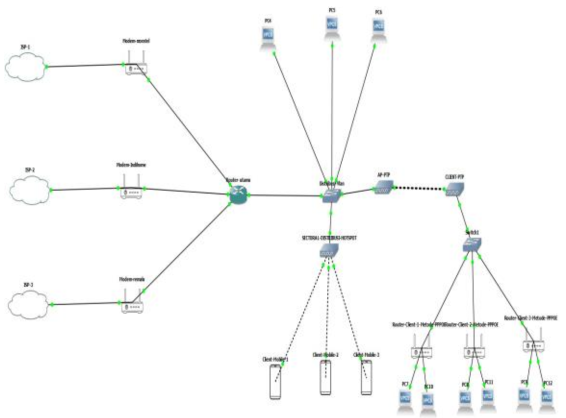

Fig. 3: Topology after Load Balancing

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:

```
/interface bridge
add name=bridge-klient
/interface ethernet
set [ find default-name=ether1 ] 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=192.168.100.100/24 interface=ether1-isp1-
oxygen network=192.168.100.0
add address=172.16.1.1/24 interface=bridge-klient
network=172.16.1.0
add address=192.168.200.200/24 interface=ether3-isp3-
remala network=192.168.200.0
add address=192.168.1.150/24 interface=ether2-isp2-
indihome network=192.168.1.0
```

This is what shows the configuration:

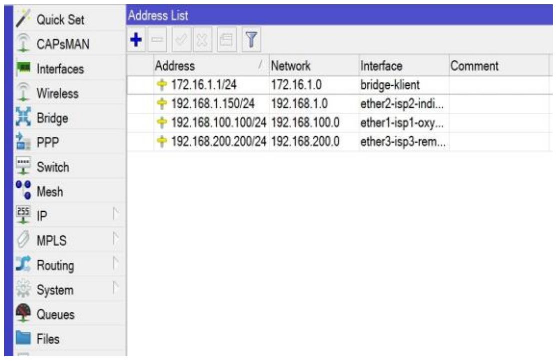

Fig. 4: Address List

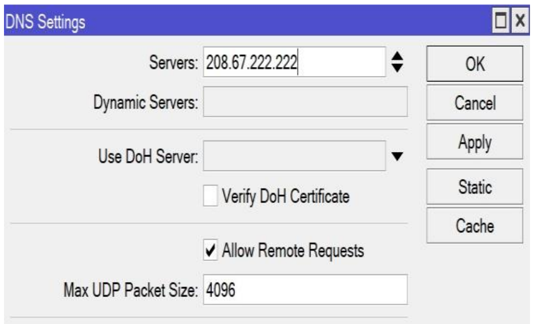

Fig. 5: DNS configuration

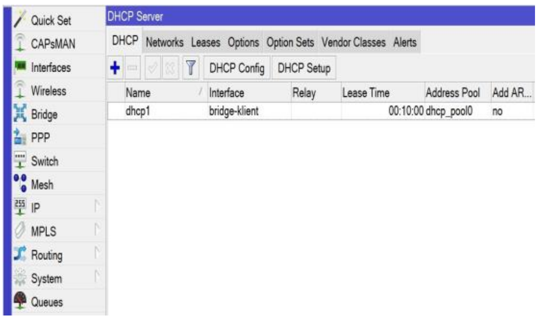

Fig. 6: Configuration DHCP server

NAT configuration can be done with the following command:

```
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1-
isp1-oxygen
add action=masquerade chain=srcnat out-interface=ether2-
isp2-indihome
add action=masquerade chain=srcnat out-interface=ether3-
isp3-remala
```

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=ether1-
isp1-oxygen \
  new-connection-mark=koneksi_isp1 passthrough=no
add action=mark-connection chain=input in-interface=ether2-
isp2-indihome \
  new-connection-mark=koneksi_isp2 passthrough=no
add action=mark-connection chain=input in-interface=ether3-
isp3-remala \
  new-connection-mark=koneksi_isp3 passthrough=no
```

```
add action=mark-routing chain=output connection-
mark=koneksi_isp1 \
  new-routing-mark=ke_isp1 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_isp1 \
  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_isp1 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 check-gateway=ping comment="backup isp3 ke isp1"
distance=2 gateway=\
  8.8.8.8 routing-mark=ke_isp1 target-scope=32

add check-gateway=ping comment="backup isp2 ke isp1"
distance=2 gateway=\
  1.1.1.1 routing-mark=ke_isp1 target-scope=31

add check-gateway=ping comment="backup isp1 ke isp2"
distance=2 gateway=\
  9.9.9.9 routing-mark=ke_isp2 target-scope=30

add check-gateway=ping comment="backup isp3 ke isp2"
distance=3 gateway=\
  8.8.8.8 routing-mark=ke_isp2 target-scope=32

add check-gateway=ping comment="backup isp2 ke isp3"
distance=3 gateway=\
  1.1.1.1 routing-mark=ke_isp3 target-scope=32
add check-gateway=ping comment="backup isp1 ke isp3"
distance=3 gateway=\
  9.9.9.9 routing-mark=ke_isp3 target-scope=30
```

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:

```
add check-gateway=ping comment="internet untuk mikrotik"
distance=1 gateway=\
  192.168.1.1,192.168.200.1,192.168.100.1
```

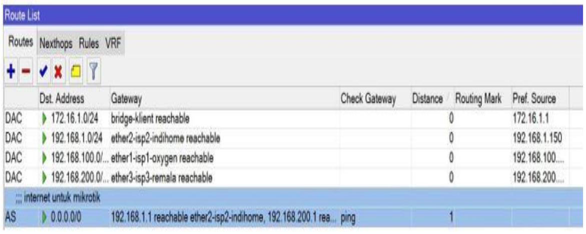

Fig. 7: Default Route Mikrotik

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

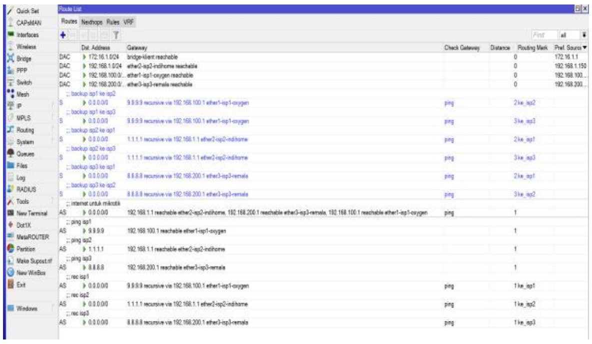

Fig. 8: Recursive Failover Configuration Results

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:

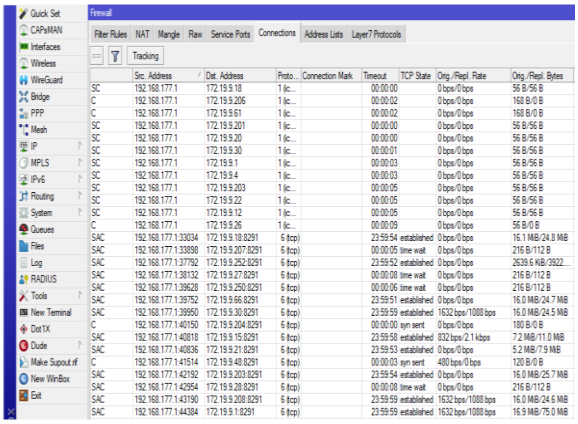

Fig. 9: Testing Downloads on the Client Before Load Balancing

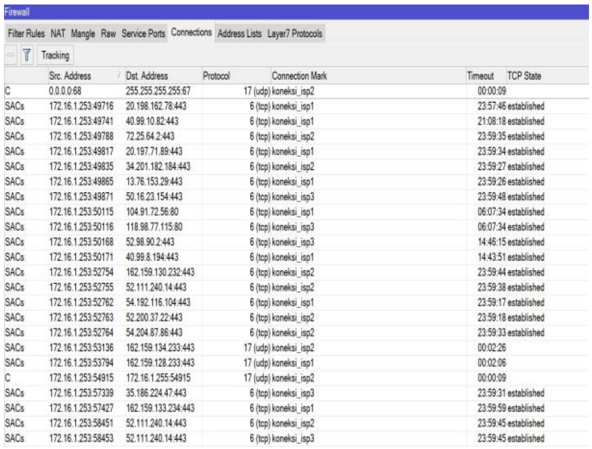

Fig. 10: Testing Downloads on the Client After Load Balancing

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:

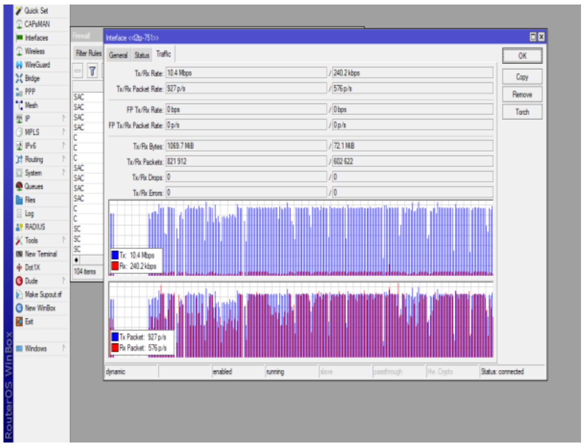

Fig. 11: Connection Graph Before Load Balancing

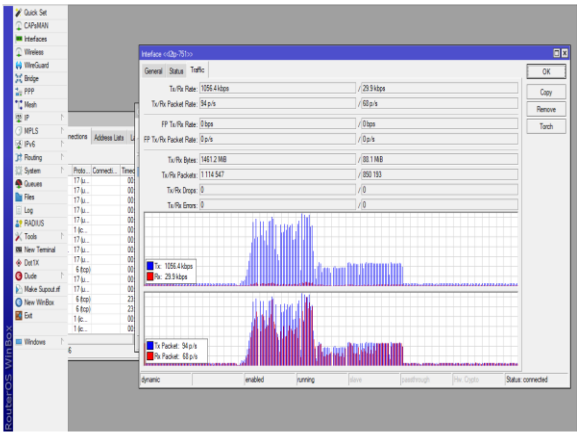

Fig. 12: Graph Down Time on Connection

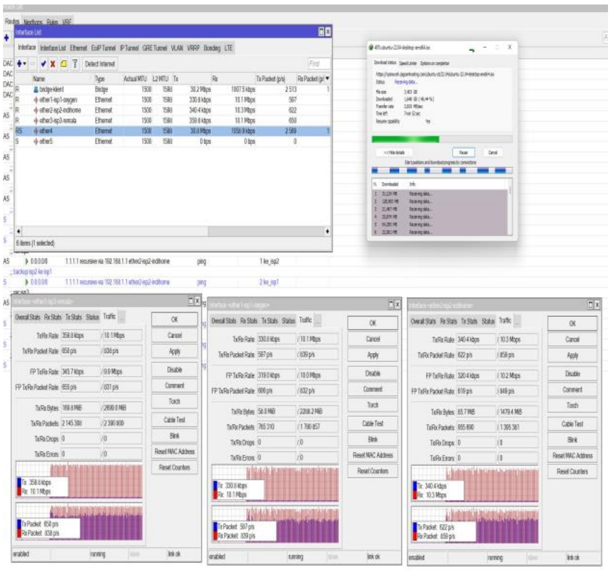

Fig. 13: Connection Graph of Each ISP After Load Balancing

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 load-balancing 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.

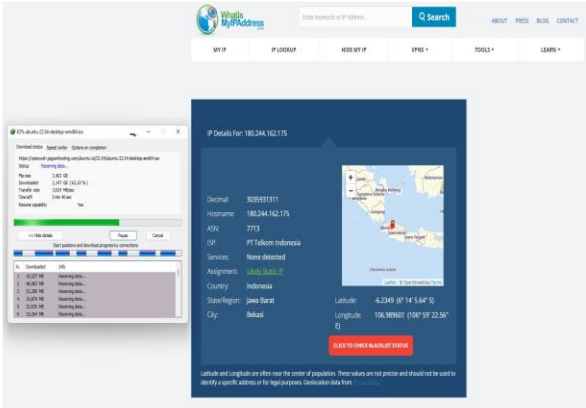

Fig. 14: Download Testing Using 3 ISPs

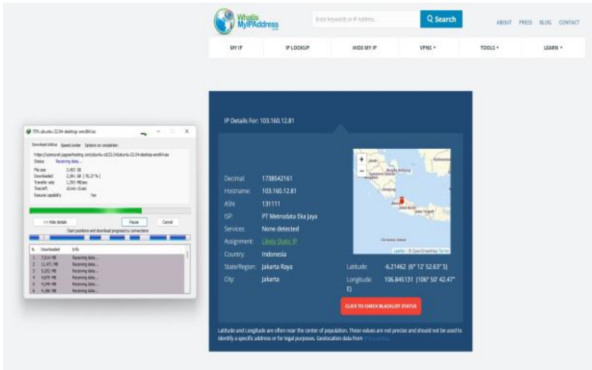

Fig. 15: Testing Download After ISP2 disconnected

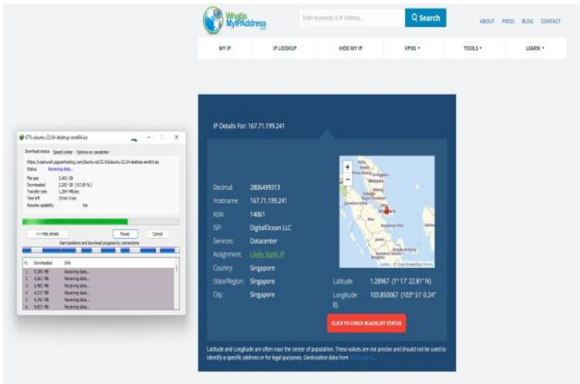

Fig. 16: Testing Download After ISP2 and ISP1 disconnected

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.