© 2022 Little Lion Scientific

ISSN: 1992-8645

www.jatit.org



ETHERNET LINK NETWORK DESIGN USING AUTO FAILOVER AND LOAD BALANCING TECHNOLOGY IN THROUGHPUT OPTIMIZATION

MUHAMMAD RIFQI NUR HADI¹, EMIL R. KABURUAN²

^{1,2} Informatics Engineering Department, Mercu Buana University, Jakarta 11650, Indonesia E-mail: ¹41518110002@student.mercubuana.ac.id, ²emil.kaburuan@mercubuana.ac.id

ABSTRACT

The era of information technology is currently developing rapidly, so people need a stable internet connection and able to support data and information exchange activities quickly. To support these needs, the network must be supported with backup links to minimize downtime and also so that high availability networks can be maintained. When there are many requests from network users, network devices will be burdened because they have to do a lot of service processes for requests from these users. this causes the connection to be slow and the connection to be lost if the network device cannot serve all the requests. The solution is to divide the traffic load that comes to network devices. The Load Balancing method can be used in dividing the traffic load that enters the network through several available network links so that it is not centered on one ISP (Internet Service Provider). The purpose of this study is to increase the throughput value so that traffic can run optimally. So that it can maintain network stability with the Load Balancing method and reduce the occurrence of downtime due to one ISP (Internet Service Provider) experiencing network problems by applying the Autofailover technology method. The results showed an increase in the throughput value after using the load balancing method, The measurement of the throughput value based on the TIPHON index has an average value of "4 (excellent)". By maximizing the throughput value, it is expected to increase the upload speed and download speed of an ethernet link network. Furthermore, by applying the Autofailover method as a backup link when one connection is problematic or experiencing downtime, the backup link will automatically run to support all network traffic.

Keywords: Network , Load Balancing, Internet Service Provider, Failover, Throughput

1. INTRODUCTION

The rapid development of internet technology is currently influenced by the increasing number of human needs and the expansion of human knowledge with digital information technology. So that technology users will always look for up to date information. In 2021, the number of internet users in Indonesia has increased by 11 percent from the previous year, from 175.4 million to 202.6 million users. However, the current increase in the number of internet network users is not supported by a comparable increase in the quality of the internet network. with a fast internet network can help in various businesses and speed up communication. Based on data from the Indonesian Consumers Foundation (YLKI) in 2021, there were 32 percent of complaints about sudden internet connection drops, which resulted in communication being cut off and disrupted several businesses using the internet network. In addition, one of the problems that usually occurs in the community is the problem of bandwidth obtained, because a lot or less bandwidth will affect access for users, be it for browsing, streaming, downloading and uploading. If client get a little bandwidth, the connection will be slow, so users feel dissatisfied with internet usage.

To overcome this problem, we need a network method that can prevent network disconnection and increase the stability of a network when there are many requests from users. Several previous studies have provided an overview of the load balancing system which is one way that can be used to share the traffic load from the client on several internet connections, it can be used as a backup/failover when one of the internet connections is interrupted. Researchers are interested in implementing and combining these two things into one and making it simpler so that it can be easily applied by network users to overcome the problems mentioned above. One of the shortcomings

<u>15th August 2022. Vol.100. No 15</u> © 2022 Little Lion Scientific

ISSN: 1992-8645

www.jatit.org

E-ISSN: 1817-3195

in previous research [9] is that it only uses one of the two methods that we present, namely the failover method with two Internet service provider (ISP) connections, so that one ISP only works when the main ISP is disconnected and makes it not work. effective. In another study [15], they only applied load balancing technology. When all ports are downtimed, the entire domain is inaccessible because there is no failover system on their containers.

Load balance is a process and technology that distributes traffic between multiple servers using network-based devices [1]. This device (load balancing server) holds or captures traffic destined for an address and then redirects that traffic to many servers. The load balance process is transparent to users who make requests to the load balancer server. The Failover method will back up the main connection and change the connection from the main connection to the backup connection will run automatically so it is very useful if you are experiencing problems with disconnection at the Main ISP (Internet Service Provider) [8].

2. METHOD ANALYSIS AND TOPOLOGY DESIGN

In this paper, the author uses the PPDIOO (Prepare, Plan, Design, Implement, Operate, and Optimize) method. PPDIOO is a network design and development method developed by Cisco. This method consists of several stages of network development including, Prepare (preparation), Plan (Planning), Design, Implementation, Operate (Operation) and Optimize (Optimization).

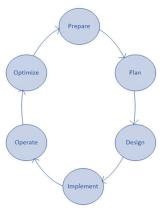


Figure 1: PPDIOO Method

2.1 Preparation

Preparation is stage to determine device requirements, develop network strategies, and

propose network architecture concepts. In this stage, the preparation and data collection of the application (software) or hardware that will be used is carried out. The following is a table of some of the devices used in this study.

Table 1: device requirement

No	Device Name	Туре	Information
1	Laptop	Hardware	Intel(R) Core(TM) i5-3437U, CPU @ 1.90GHz (with SSE4.2), 4GB Ram
2	Mikrotik Router	Hardware	Type RB941-2 nD
3	ZTE F609 router	Hardware	ISP A (CBN)
4	Fiberhome router	Hardware	ISP B (TELKOM)
5	Winbox v6.48.2	Software	Mikrotik RB941- 2nD Router Operating System
6	Wireshark v3.6.2-0	Software	Application for Throughput Testing
7	Opera Mini	Software	Web Browser Application
8	Windows 10	Software	Laptop Operating System

2.2 Planning

Planning is the stage of network design based on the objectives, facilities, and network requirements. This is useful for describing the characteristics of a network, which aims to assess the network. The following is a research planning flowchart.

<u>15th August 2022. Vol.100. No 15</u> © 2022 Little Lion Scientific

ISSN: 1992-8645

www.jatit.org



E-ISSN: 1817-3195

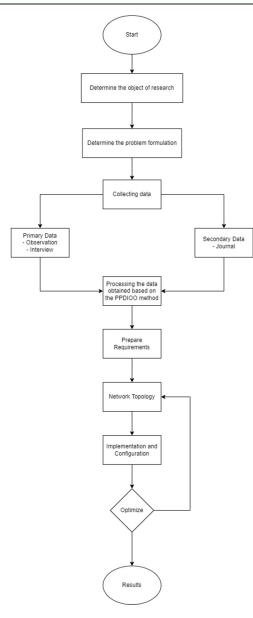


Figure 2: Research Planning Flowchart

2.3 Design

At this design stage is to create a network topology based on the technical requirements and plans that have been made. The design and description of the network architectural topology must be comprehensive and detailed in order to explain the series of network systems that will be implemented. In the picture below is the existing topology used by PT. Fiberstar POP Meruya which is located at Ruko Permata Regency Jl. H. Kelik No.D/32, West Jakarta City, Special Capital Region of Jakarta.

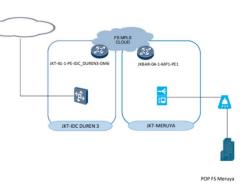


Figure 3: Existing Topology

One of the problems with the existing topology is that it has not been equipped with a failover method. So that when the main network connection is experiencing problems such as Fiber Optic Cut, all activities that use internet access will be disrupted. therefore, we made changes to the topology by adding failover technology and backup connections.

2.4 Implementation

At this stage, the installation and configuration of the network architecture topology that has been described will be carried out.Implementation at this stage is to describe the implementation in the field, set-up and configuration used from the network design that has been made.

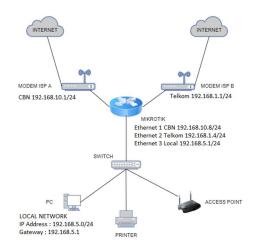


Figure 4: Proposed New Topology

Proposed New Topology at figure 4 can be described as a topology that uses failover technology for backup links if one port or cable is problematic or experiencing downtime and Load Balancing which combines two links into one virtual link so that we will get a greater throughput bandwidth. LinkThe backup that has been configured with failover will replace the disconnected link and when the link is back to normal, the connection path that is

ISSN: 1992-8645

www.jatit.org



E-ISSN: 1817-3195

used again becomes the main link, so that the connection on the network will always be connected.

2.5 Operation

Perform testing experiments for configurations on failover and load balancing that have been carried out. Tests are carried out on router devices by looking at the throughput that can be obtained. As well as failover testing by turning off one network as a simulation if there is a downtime at one ISP, then the backup ISP will automatically replace the down ISP link.

2.6 Optimization

At this stage it is possible to modify the network design and configuration if there are many network problems that arise to improve performance, to get maximum results, and maintain network stability.

3. DATASET

In this paper, we use two types of data, primary data and secondary data which serves as a comparison to the previous literature. Premier data is data obtained directly from research subjects using measurement tools or data retrieval tools directly on the subject as a source of information (Azwar, 2007). In this study, researchers made observations on the speed of internet access (download and upload) through the website *https://speedtest.net*. At the time of observation on March 22, 2022, at 07.57 Indonesian Time (GMT +7), it was found that Telkom's ISP internet speed limit decreased. The speedtest results show a download speed of 0.65 Mbps and an upload speed of 0.25 Mbps.

Table	2: Speedtest	Observations
10000	specencest	00000.00000

Date	Download	Upload	Status
	Speed	Speed	
	(Mbps)	(Mbps)	
March 16,	10.43	3.52	Normal
2022			
March 21, 2022	10.55	3.48	Normal
March 22, 2022	0.65	0.25	Down

SHARE 🖉 🕑 🖲 🤆		27428866	⊘ RES	JLTS	SETTING
® PING n 1	ns © DOWNLI 0.65		© UPLO/ 0.2		
	Connections Multi	HOW D	CUSTOME WITH YOU		
	PT. Telekomunikasi			4	
	ndonesia				

Figure 5: The Speedtest Results

This decrease in internet bandwidth speed occurs due to interference with the fiber optic cable network which causes the received power value at the Optical Network Terminal (ONT) to be -33.01 dBm, lower than the IEEE 802.8 standard that has sbeen set, with a maximum value of -28 dBm. Due to the decrease in bandwidth, so the throughput value obtained by the client becomes small.

						Logou
	Status	Network	Security	Application	Management	
Device Information	Status »	Optical Info » Op	tical Info			
Wireless Status						
Wan Status	ON	his page, you can que	ery state of optical po	wer.		
Lau Status	Optical	Info				
Optical Info	Transn	nited Power	-40.00 dBm			
Optical Info	Receiv	ed Power	-33.01 dBm			
VoIP Status	Operat	ing Temperature	49.55 °C			
	Supply	Voltage	3.23 V			
	Bias C	urrent	Am 00.0			

Figure 6: ONT Attenuation Value

Throughput is the effective data transfer rate, measured in bps. Throughput is a measure in real time of how fast data is sent on the network. Throughput can be calculated by the following equation :

The following are throughput standards according to TIPHON :

Throughput	throughput	Index
Category		
Bad	0 - 338 kbps	0
Poor	338 – 700 kbps	1
Fair	700 – 1200 kbps	2
Good	1200 kbps – 2.1	3
	Mbps	
Excellent	> 2.1 Mbps	4

ISSN: 1992-8645

www.jatit.org

Ir

E-ISSN: 1817-3195

4. SOURCE CODE AND CONFIGURATION

Source code describes the application used for multiple configurations in designing load balancing and failover methods.

4.1 Winbox

Winbox is a software for configuring a GUI-based Mikrotik Router. Winbox can be used on devices running Windows, Linux, and MACOS (OSX) using Wine. In this study, the source code is used to configure Load balancing and failover on the Mikrotik RouterRB941-2nD by using the Winbox Application,The source code or configuration used in this study includes the following commands.

a. Ethernet interfaces configuration on the Mikrotik Router via the winbox application. Configuration consists of Ethernet 1 CBN Provider, Ethernet 2 TELKOM Provider, and Ethernet 3 LOCAL CONNECTION.

General	ether1-CBN>	Protect	Overall Stats	Bx Stats		ОК
		ether1-		Thotats	_	Cancel
					_	
Type: Ethernet						Apply
	MTU:	Disable				
	Actual MTU:	1500		Comment		
	L2 MTU:	1598				Torch
	Max L2 MTU:	2028				Cable Test
	MAC Address:	C4:AD:	34:86:2F:1F			Blink
	ARP:	enable	d		∓	
	ARP Timeout:				-	Reset MAC Address
	, a a milliout.					Reset Counters
nabled			running	slav		link ok

Figure 7: Ethernet 1 Interface Configuration

Interface <	ether2-TLKM>		
General	Ethernet Loop	Protect Overall Stats Rx Stats	ОК
	Name	ether2-TLKM	Cancel
	Туре	Ethernet	Apply
	MTU	Disable	
	Actual MTU	Comment	
	L2 MTU	Torch	
	Max L2 MTU	Cable Test	
	MAC Address	Blink	
	ARP	enabled	Reset MAC Address
	ARP Timeout	▼	Reset Counters

Figure 8: Ethernet 2 Interface Configuration

enaces	ether3-LOCAL>		0			
eneral	Ethernet Loop	Protect	Overall Stats	Rx Stats		ОК
	Name:	ether3-	LOCAL			Cancel
	Туре:	Etherne	et			Apply
	MTU:	1500				Disable
	Actual MTU:	1500		Comment		
	L2 MTU: 1598				Torch	
	Max L2 MTU:	2028				Cable Test
	MAC Address:	C4:AD:	34:86:2F:21			Blink
	ARP:	enable	d		₹	Reset MAC Address
	ARP Timeout:				•	Reset Counters

Figure 9: Ethernet 3 Interface Configuration

b. Add IP Address for the three interfaces and IP Gateway on each interface.

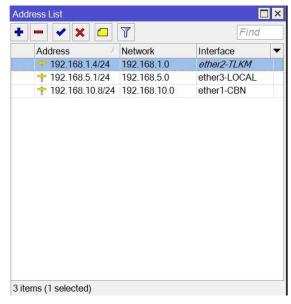


Figure 10: IP Address List

4.2 Load Balancing Configuration

After configuring the IP address on the Mikrotik, the next step is to implement load balancing on the Mikrotik Router. The use of the Load Balancing method aims to make the link more optimal by dividing the traffic load on the two connection lines in a balanced way so that it can avoid overload on one link.

a. Configuring Network Address Translation (NAT) Firewall

In configuring Load balancing, it is necessary to change the local IP address or private IP address to Public IP, this is because the local IP address or private IP address is not allowed to enter the WAN network or the internet. For that, the "srcnat" configuration is carried out with the "masquerade" action of both ISPs to hide the local IP address or private IP address and replace it with the public IP address installed on the router.

Journal of Theoretical and Applied Information Technology <u>15th August 2022. Vol.100. No 15</u> © 2022 Little Lion Scientific



E-ISSN: 1817-3195

AT Rule	<>						NA
General	Advanced	Extra	Action	Statist	ics	ОК	G
	Chain:	rcnat			₹	Cancel	
Src.	Address:				-	Apply	
Dst.	Address:				•	Disable	
	Protocol:				-	Comment	
	Src. Port:				-	Сору	
	Dst. Port:				*	Remove	
1	Any. Port:				-	Reset Counters	
In.	Interface:				-	Reset All Counters	
Out.	Interface:	ethe	r1-CBN	:	F 🔺		
In. Inter	face List:				-		
O <mark>ut. Inte</mark> r	face List:				-		С
Pac	ket Mark:				-		
Connect	ion Mark:				-		(
Rout	ing <mark>Mark</mark> :				•		
Routi	ng Table:				•		
Connect	tion Type:				-		

Figure 11: Ethernet 1 Network Address Translation Configuration

NAT Rule <>	
General Advanced Extra Action Statistics	OK
Action: masquerade	Cancel
Log	Apply
Log Prefix:	Disable
To Ports:	Comment
	Сору
	Remove
	Reset Counters
	Reset All Counters

Figure 12: Ethernet 1 Network Address Translation Masquerade Action

General	Advanced	Extra	Action	Statistics	5	ОК
	Chain: s	rcnat			₹	Cancel
Src.	Address:				•	Apply
Dst.	Address:				•	Disable
	Protocol:				•	Comment
	Src. Port:				w	Сору
	Dst. Port:				*	Remove
	Any. Port:				*	Reset Counters
In.	Interface:				•	Reset All Counters
Out.	Interface:	ether	2-TLKM	Ŧ	•	
					•	
In. Inte	rface List:					
	rface List:				•	
Out. Inte					• •	
Out. Inte Pac	rface List:				• • •	
Out. Inte Pac Connec	rface List:				• • •	
Out. Inte Pac Connec Rou	rface List:				• • • •	

Figure 13: Ethernet 2 Network Address Translation Configuration

NAT Rule	<>					
General	Advanced	Extra	Action	Statistics	5	ОК
A	ction: masq	uerade	8		₹	Cancel
	Lo	3				Apply
Log F	Prefix:				•	Disable
	Ports:				-	Comment
101					•	Сору
						Remove
						Reset Counters
						Reset All Counters

Figure 14: Ethernet 2 Network Address Translation Masquerade Action

<u>15th August 2022. Vol.100. No 15</u> © 2022 Little Lion Scientific

ISSN: 1992-8645

www.jatit.org



E-ISSN: 1817-3195

er R	Rules NAT Mangle Raw Service	ce Ports Connections	Address Lists Layer7 Protocol	5						
	- 🖉 🕾 🖆 🍸 🕫 Reset	Counters Counters	All Counters						Find	
	Section: Passthrough: Rate:	mark connection yes 220 bps	Chain: New Connection Mark: Packet Rate:	input ISPCBN_CONN 0	In Interface: Bytes:	ether1-CBN 184.0 KiB	Log: Packets:	no 3 230		
		mark connection yes 220 bps	Chain: New Connection Mark: Packet Rate:	input ISPTLKM_CONN 0	In. Interface: Bytes:	ether2-TLKM 142.4 KiB	Log. Packets:	no 2.576		
	Action: Passthrough: Rate:	mark routing no 0 bps	Chain: New Routing Mark: Packet Rate:	output to-CBN 0	Connection Mark: Bytes:	ISPCBN_CONN 4236 B	Log: Packets:	no 65		
	Action: Passthrough: Rate:	mark routing no 0 bps	Chain: New Routing Mark: Packet Rate:	output to-TLKM 0	Connection Mark: Bytes:	ISPTLKM_CONN 3652 B	Log: Packets:	no 71		
		accept 130.4 KiB 192.168.10.0/24	Chain: Packets:	prerouting 1 697	In. Interface: Rate:	ether3-LOCAL 0 bps	Log: Packet Rate:	no 0		
		accept 2386 B 192.168.1.0/24	Chain: Packets:	prerouting 33	In. Interface: Rate:	ether3-LOCAL 0 bps	Log: Packet Rate:	no O		
	Action: Dst. Address Type/Address Ty New Connection Mark: Packet Rate:	mark connection local ISPCBN_CONN 0	Chain: Dst Address Type/Invert Bytes:	prerouting yes 5.4 MiB	In: Interface: Log: Packets:	ether3-LOCAL no 41 490	Per Connection Classifier: Passthrough: Rate:	both addresses and p yes 0 bps		
	Action: Dst. Address Type/Address Ty New Connection Mark: Packet Rate:	mark connection local ISPTLKM_CONN 0	Chain: Dst.Address Type/Invert Bytes:	prerouting yes 5.5 MiB	In. Interface: Log: Packets:	ether3-LOCAL no 21 302	Per Connection Classifier: Passthrough: Rate:	both addresses and p yes 0 bps		
	Action: Log: Packets:	mark routing no 41 464	Chain: Passthrough: Rate:	prerouting yes 0 bps	In. Interface: New Routing Mark: Packet Rate:	ether3-LOCAL to-CBN 0	Connection Mark: Bytes:	ISPCBN_CONN 5.4 MIB		
	Action: Log: Packets:	mark routing no 21.275	Chain: Passthrough: Rate:	prerouting yes 0 bps	In. Interface: New Routing Mark: Packet Rate:	ether3-LOCAL to-TLKM 0	Connection Mark: Bytes:	ISPTLKM_CONN 5.5 MIB		

Figure 15: Mangle Settings

b. Mangle Settings

Mangle is a tool that serves to perform the marking function of data packets to be performed bandwidth management or routing. (Mikrotik, 2005). Mangle on Mikrotik Firewall can be used to mark data packets. The marking can be used for other features such as Filter, Routing, NAT, or Queue. In its implementation, the mangle can be used to perform load balance, the router that performs the load balance is usually the main router which is also used to perform bandwidth management.

Load balance is a technique to distribute the traffic load on two or more connection lines in a balanced way so that traffic can run optimally and there is no overload on any of the connection lines. One of the Load balance techniques is PCC (Per Connection Classifier). By using the PCC feature, we can group connection traffic that passes through or enters the router into several groups. The router will remember the gateway path that was passed at the beginning of the connection traffic so that the next packet that is still connected will be passed on the same path as before.

In some previous literature, the PCC load balance is shown to be distributed only on 1 LAN network. In this paper, we will distribute 2 Wan connections into 2 WANs (as shown in Figure 4). Of the several rules below, the first thing to do is to provide an accept action on local traffic so that local traffic is not marked as a connection to the internet network. Then give a signal to traffic from ISP 1 (CBN) then the traffic will be returned back through ISP1 as well as if there is traffic from ISP2 (TELKOM). Next is the PCC load balance method. And the next Mangle is to mark the traffic so that routing can be done.

Figure 15 shows the mangle configuration is used to mark data packets so that they are easy to manage so that the IP Address configuration and connection paths or links are not confused.

4.3 Failover Configuration

By having multiple gateways for a destination, we can perform a backup path mechanism commonly known as Failover. Failover is one of the techniques that can be used on Mikrotik, this technique works if one of the links experiences downtime, the backup link will replace it automatically (Towidjojo, 2016). By using the winbox application, failover can be done by setting the value on distance.

a. Distance Settings

Distance serves to determine the routing path that will be a priority or be a backup link. By default the distance value on MikroTik is 0 (Zero) -8 (Eight). So, the smaller the value on the distance, the more prioritized the link will be. To configure failover, we must first determine which link will be the priority and become the backup link.

Routes	Nexthops Rules	VRF				
• -						
	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source	Comment
AS	0.0.0.0/0	192.168.10.1 reachable ether 1-CBN		1		
S	0.0.0.00	192,168.1.1 reachable ether2-TLKM		2		

Figure 16: Distance Settings

From the picture above, it can be seen that the CBN ISP has a distance value of "1" because the CBN ISP is the main link used, while the Telkom ISP has a distance value of "2" as a backup link.

ISSN: 1992-8645

<u>www.jatit.org</u>



b. Check Gateway Parameters

The Check Gateway parameter works is by sending an ARP Request or Test Ping for 10 seconds to the Gateway ISP. This aims to ensure that the ISP is still connected to the internet network , if for 10 seconds the Gateway ISP does not respond it will be considered a "Gateway Time-Out" and if there are 3 gateway time-outs in succession, then the ISP is called "Unreachable".

In Figure 17, the main ethernet 1 connection is being disabled, causing the CBN ISP connected to ethernet 1 to be unreachable. When an Unreachable occurs on this main link, failover will automatically move the connection path to the backup link.

5. EXPERIMENT STAGE OF FAILOVER AND LOAD BALANCING METHOD FOR OPTIMIZING THROUGHPUT VALUE

This stage is a testing process on Load balancing and failover configurations that are carried out using Winbox and Wireshark applications. In this paper, the authors carried out several experimental stages as follows.

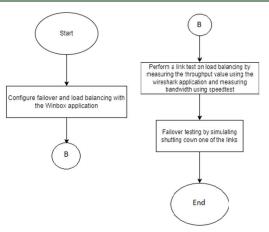


Figure 18: Flowchart of Experimental Stages

Before configuring the Mikrotik with load balancing and failover methods, the Ethernet 1 interface from the Mikrotik was combined to Ethernet ONT ISP CBN, Ethernet 2 to Ethernet ONT ISP Telkom, and Ethernet 3 to the Local Network.

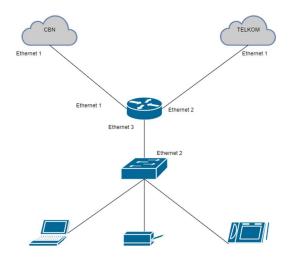


Figure 19: Ethernet Links Configuration

Interface	List														8
Interfac	e Interface List E	Ethernet EoIP Tunnel	IP Tunnel GRE	Tunnel	VLAN VRRP Bonding	LTE									
+ -		T Detect Internet													Find
	Name	Туре	Actual MTU	L2 MTU	Тх	Rx	1	Fx Packet (p/s)	F	Rx Packet (p/s)	FP Tx		FP Rx		FP Tx Packet (
Х	ether1-CBN	Ethernet	1500	1598	0 bp	5	0 bps		0	C		0 bps	6	0 bps	
R	ether2-TLKM	Ethernet	1500	1598	512 bp	5	512 bps		1	1		480 bps	6	480 bps	
R	ether3-LOCAL	Ethernet	1500	1598	81.3 kbp	5	7.5 kbps		11	11		80.9 kbps	5	7.2 kbps	
Route Li	st														
Routes	Nexthops Rules	VRF													
+ -		7												Find	all 🛛
	Dst. Address	Gateway			Distance	Routing Mark	Pref. S	ource Comme	ent						
AS	0.0.0/0	192.168.1.1 reachab	le ether2-TLKM			2									
AS	▶ 0.0.0.0/0	192.168.1.1 reachab	le ether2-TLKM			1 to-ISP-TLKM									
S	▶ 0.0.0.0/0	192.168.10.1 unread	hable			1									
S	0.0.0/0	192.168.10.1 unread	hable			1 to-ISP-CBN									

Figure 17: Interface List and Route List

<u>15th August 2022. Vol.100. No 15</u> © 2022 Little Lion Scientific

ISSN: 1992-8645

www.jatit.org

JATIT

E-ISSN: 1817-3195

Load balancing configuration by adding IP addresses, DNS settings, NAT firewall settings with actions masquerade ,and Mangle configuration. In making these settings, carefulness is needed so as not to make the wrong configuration. Next, Failover configuration is performed using the distance and check gateway parameters. The distance parameter is used to select the main link connection path and the backup link connection path. While the check gateway parameter is used to ensure the main link connection is in good condition or not. If the link is down then the link will be unreachable.

a. Load Balancing Test

After configuring load balancing and failover, the next step is to test the link load balancing using the Wireshark application to monitor the throughput value of the link. Testing is carried out with the following conditions:

- 1. The first attempt is to download a file of 124 mb.
- 2. The second experiment was conducted by testing the bandwidth speed through the speedtest.net page.
- 3. The third attempt is to stream 4K resolution video.

b. Failover Test

In the Failover test, it is carried out using a scenario of shutting down one of the ISPs. To ensure that this method is successful, use the traceroute command to see which connection path is being used when one of the ISPs is experiencing downtime.

6. RESULT OF ALL EXPERIMENTS

6.1 Load Balancing Test Results

The results obtained from each test of the load balancing method are as follows :

a. First Test Result

In the first test, the activity of downloading a file of 124 mb was carried out using the CBN ISP and Telkom ISP which had not done load balancing. Figure 20 shows CBN ISP has a throughput value of 9.95 Mbps while Telkom's ISP has a throughput value of 9.58 Mbps (Figure 21).

Wireshark - Capture	File Properties - Ethe	ernet		-	
Details					
File					
Name: Length: Hash (SHA256):	150 MB		np\wireshark_Ethernet7E Scc85e2cbea43ea2c47e		
Hash (RIPEMD 160):	8abd67447348b45d				
Hash (SHA 1):	f402b11f6ff36ce9cd		11ff02c		
Format:	Wireshark/ pcap	ng			
Encapsulation:	Ethernet				
Time					
First packet:	2022-03-16 14:58:2	2			
Last packet:	2022-03-16 15:00:1	в			
Elapsed:	00:01:56				
Capture					
Hardware:	Intel(R) Core(TM) i5-	-3437U CPU @ 1.9	0GHz (with SSE4.2)		
OS:	64-bit Windows 10 (21H1), build 19043	3		
Application:	Dumpcap (Wireshark) 3.6.2 (v3.6.2-0-	g626020d9b3c3)		
Interfaces					
Interface	Dropped packets	Capture filter	Link type	Packet si (snaplen)	
Ethernet	0 (0.0%)	none	Ethernet	2621448	oytes
Statistics					
<u>Measurement</u> Packets	Captured 187230		Displayed 187230 (100.0%)	Marked	
Time span, s	116.122		116.122	-	
Average pps	1612.4		1612.4	-	
Average packet size, B	772		772		
Bytes	144495841		144495841 (100.0%)	0	
Average bytes/s	1244 k		1244 k	-	
Average bits/s	9954 k	5	954 k	-	

Figure 20: First Test Results CBN Throughput

Wireshark · Capture	File Properties - Eth	ernet							
etails									
File									
Name:		AppData\Local\Temp	wireshark_EthernetNCS	52I1.pcapng					
Length:	144 MB								
Hash (SHA256):			25171cbc8dd0aceccc40b	8c9c445cd0					
Hash (RIPEMD 160):	9bc32578aad37783								
Hash (SHA1):		9862dc33368c55d47c2588a775ab63d7511d06f							
Format:	Wireshark/ pcap	ng							
Encapsulation:	Ethernet								
Time									
First packet:	2022-03-16 15:55:3	9							
Last packet:	2022-03-16 15:57:3	6							
Elapsed:	00:01:57								
Capture									
Hardware:	Intel(R) Core(TM) i5	-3437U CPU @ 1.900	GHz (with SSE4.2)						
OS:	64-bit Windows 10 (21H1), build 19043							
Application:	Dumpcap (Wireshark	() 3.6.2 (v3.6.2-0-g6	26020d9b3c3)						
Interfaces									
Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)					
Ethernet	0 (0.0%)	none	Ethernet	262144 bytes					
Statistics									
Measurement	Captured		played	Marked					
Packets	139510		9510 (100.0%)	-					
Time span, s	117.218		7.218	-					
Average pps	1190.2		90.2	-					
Average packet size, B	1006	10		-					
Bytes	140402211		0402211 (100.0%)	0					
Average bytes/s	1197 k		97 k	-					
Average bits/s	9582 k	95	32 k	_					

Figure 21: First Test Results TELKOM Throughput

Then, after merging the links from the two ISPs using the load balancing method, in figure 22 we got an increase in the total throughput value to 10 Mbps.

<u>15th August 2022. Vol.100. No 15</u> © 2022 Little Lion Scientific

ISSN: 1992-8645

www.jatit.org

Wireshark · Capture	File Properties - Eth	ernet		- 0	>
etails					
File					
Name:		AppData\Local\Te	mp\wireshark_Ethernet	tAQ29I1.pcapng	
Length:	150 MB				
Hash (SHA256):			ba93865bd621aa8c7ac	08d69eba087766e	
Hash (RIPEMD 160):	2d41233ab234820d				
Hash (SHA1):	a0648131d798b4b5		92f98a5298		
Format:	Wireshark/ pcap	ng			
Encapsulation:	Ethernet				
Time					
First packet:	2022-03-16 16:12:1	1			
Last packet:	2022-03-16 16:14:0	6			
Elapsed:	00:01:54				
Capture					
Hardware:	Intel(R) Core(TM) i5	-3437U CPU @ 1	90GHz (with SSE4.2)		
OS:	64-bit Windows 10 (21H1), build 190-	43		
Application:	Dumpcap (Wireshark	() 3.6.2 (v3.6.2-	0-g626020d9b3c3)		
Interfaces					
Interface	Dropped packets	Capture filte	Link type	Packet size limit (snaplen)	
Ethernet	0 (0.0%)	none	Ethernet	262144 bytes	
Statistics					
Measurement	Captured	1	Displayed	Marked	
Packets	166363		166363 (100.0%)	_	
Time span, s	114.124		114.124	-	
Average pps	1457.7		1457.7	_	
Average packet size, B	873		873	-	
Bytes	145280552		145280552 (100.0%)	0	
Average bytes/s	1273 k		1273 k	_	
Average bits/s	10 M		10 M	-	

Figure 22: First Test Results Load Balancing Throughput

b. Second Test Result

The second test was carried out by testing the bandwidth speed through the Ookla Speedtest https://www.speedtest.net page. The test results can be seen in Table 4.

Based on data from Table 4, the bandwidth speed that uses the load balancing method is higher than the speed of the ISP that does not use the load balancing method.

c. Third Test Result

The third test is to stream 4K resolution video for 4 minutes. The CBN ISP has a throughput value of 1.1 Mbps (Figure 23) while the Telkom ISP has a throughput value of only 723 Kbps (Figure 24). However, when the two ISPs are combined with the load balancing method, the throughput value increases significantly by 5.42 Mbps (Figure 25).

From the load balancing test results that have been carried out, the load balancing method is proven to increase the throughput value and bandwidth access speed. All the test results of the load balancing method can be seen in Table 5.

Wireshark · Capture	File Properties - Ethe	ernet			-		\times
etails							
File							
Name:	C:\Users\TOSHIBA\4	ppData\Local\Tem	p\wireshark_EthernetPYC	UI1.pcapng			
Length:	41 MB						
Hash (SHA256):			dbd068a1c2ea8a053e395	b4f153fdfd3			
Hash (RIPEMD 160):	8afbe258990b8984a						
Hash (SHA 1):	fa32f653aee79e8c8		a2ddbf13				
Format:	Wireshark/ pcape	ng					
Encapsulation:	Ethernet						
Time							
First packet:	2022-03-21 13:36:0	3					
Last packet:	2022-03-21 13:40:4	D					
Elapsed:	00:04:37						
Capture							
Hardware:	Intel(R) Core(TM) i5-	3437U CPU @ 1.9	0GHz (with SSE4.2)				
OS:	64-bit Windows 10 (2	21H1), build 19043					
Application:	Dumpcap (Wireshark) 3.6.2 (v3.6.2-0-	g626020d9b3c3)				
Interfaces							
Interface	Dropped packets	Capture filter	Link type		cket size	e limit	
Ethernet	0 (0.0%)	none	Ethernet		2144 by	tes	
Statistics							
Measurement	Captured	D	isplayed	Marked			
Packets	48442	4	8442 (100.0%)	-			
Time span, s	277.623	2	77.623	_			
Average pps	174.5	1	74.5	_			
Average packet size, B	815		15	-			
Bytes	39496260	3	9496260 (100.0%)	0			
Average bytes/s	142 k		42 k	-			
Average bits/s	1138 k	1	138 k	-			

Figure 23: Third Test Results CBN Throughput

Wireshark · Capture	File Properties - Eth	ernet		- 0	>
etails					
File					1
Name:		AppData\Local\Temp\w	ireshark_EthernetB3	Z2I1.pcapng	
Length:	24 MB				
Hash (SHA256):		e464d95e2fdf78f6494		190ef27dbfe	
Hash (RIPEMD 160):		1629f80e3bddfae90fr			
Hash (SHA1):		92cbd4d73e6023c7b3	16db6		
Format:	Wireshark/ pcap	ng			
Encapsulation:	Ethernet				
Time					
First packet:	2022-03-21 13:43:5	0			
Last packet:	2022-03-21 13:48:0	6			
Elapsed:	00:04:15				
Capture					
Hardware:		-3437U CPU @ 1.90GH	z (with SSE4.2)		
OS:	64-bit Windows 10 (21H1), build 19043			
Application:	Dumpcap (Wireshark) 3.6.2 (v3.6.2-0-g62	5020d9b3c3)		
Interfaces					
Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)	
Ethernet	0 (0.0%)	none	Ethernet	262144 bytes	
Statistics					
Measurement	Captured	Displa		Marked	
Packets	25947		(100.0%)		
Time span, s	255.993	255.9		-	
Average pps	101.4	101.4		-	
Average packet size, B	893	893		-	
Bytes	23162208		208 (100.0%)	0	
Average bytes/s	90 k	90 k		-	
Average bits/s	723 k	723 k		-	

Figure 24: Third Test Results TELKOM Throughput

Measurement	Captured	Displayed	Marked
Packets	240839	240839 (100.0%)	-
Time span, s	338.967	338.967	-
Average pps	710.5	710.5	-
Average packet size, B	955	955	-
Bytes	230019568	230019568 (100.0%)	0
Average bytes/s	678 k	678 k	-
Average bits/s	5428 k	5428 k	-

Figure 25: Third Test Results Load Balancing Throughput



E-ISSN: 1817-3195



ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 4: Second Result Test

ISP/Method	Ping (ms)	Download Speed (Mbps)	Upload Speed (Mbps)	Throughput (Mbps)
CBN ISP	3	9.85	9.55	7.63
TELKOM ISP	1	10.57	3.12	5.51
LOAD BALANCING	17	19.92	12.33	13

Table 5: All of Load Balancing Test Result

No	Test Type	ISP/Method	SP/Method Throughput (Mbps)		Index throughput
		CBN	9.95	Excellent	4
1	Download	TELKOM	9.58	Excellent	4
		Load Balancing	10	Excellent	4
		CBN	7.63	Excellent	4
2	Speedtest	TELKOM	5.51	Excellent	4
		Load Balancing	13	Excellent	4
		CBN	1.1	Fair	2
3	Streaming	TELKOM	0.72	Fair	2
		Load Balancing	5.42	Excellent	4

<u>15th August 2022. Vol.100. No 15</u> © 2022 Little Lion Scientific

ISSN: 1992-8645

www.jatit.org



E-ISSN: 1817-3195

From all load balancing experiments that have been carried out, (data can be seen from Table 5) The load balancing method has increased the value of throughput. This is in accordance with the statement that the use of load balancing can take advantage of the existing bandwidth and increase throughput, compared to not using the load balancing method [1]. With Load Balancing technology, benefits can be obtained such as guaranteeing service reliability, availability and scalability of a network [4] so that benefits can be obtained such as ensuring a stable internet. This experiment also proves that an ethernet network that applies the load balancing method will balance the traffic load on the two connection lines, so that traffic can run optimally [10]. This happens because load balancing will divide the load based on the source, destination address and port address. All internet requests from users will go to the Router that has been configured with the PCC method, so that the Router will manage outgoing requests from users via ISP line 1 or ISP line 2 to be able to enter the internet connection.

6.2 Failover Test Results

In the failover test, it is done by trying a scenario to disable the main link on ethernet 1 as shown in the figure 26.

Log							
7	Freeze						
#	Time	Buffer	Topics	Message			
0	Mar/21/2022 13:53:36	memory	system, error, critical	router was rebooted without proper shutdown			
1	Mar/21/2022 13:53:47	memory	interface, info	ether1-CBN link up (speed 100M, full duplex)			
2	Mar/21/2022 13:53:47	memory	interface, info	ether2-TLKM link up (speed 100M, full duplex)			
3	Mar/23/2022 16:49:40	memory	interface, info	ether3-LOCAL link up (speed 100M, full duplex)			
4	Mar/23/2022 16:49:58	memory	dhcp, info	dhcp1 assigned 192.168.5.252 to B8:6B:23:CF:3B:1F			
5	Mar/23/2022 16:54:14	memory	interface, info	ether1-CBN link down			
6	Mar/23/2022 16:54:14	memory	interface, info	ether2-TLKM link down			
7	Mar/23/2022 16:54:14	memory	interface, info	ether3-LOCAL link down			
8	Mar/23/2022 16:54:15	memory	interface, info	ether1-CBN link up (speed 100M, full duplex)			
9	Mar/23/2022 16:54:15	memory	interface, info	ether2-TLKM link up (speed 100M, full duplex)			
10	Mar/23/2022 16:54:15	memory	interface, info	ether3-LOCAL link up (speed 100M, full duplex)			
11	Mar/23/2022 16:54:31	memory	interface, info	ether2-TLKM link down			
12	Mar/23/2022 16:56:37	memory	interface, info	ether2-TLKM link up (speed 100M, full duplex)			
13	Mar/23/2022 16:56:39	memory	interface, info	ether1-CBN link down			
14	Mar/23/2022 17:05:23	memory	interface, info	ether1-CBN link up (speed 100M, full duplex)			
15	Mar/23/2022 17:05:43	memory	interface, info	ether3-LOCAL link down			
16	Mar/23/2022 17:06:07	memory	interface, info	ether3-LOCAL link up (speed 10M, full duplex)			
17	Mar/23/2022 17:06:08	memory	interface, info	ether3-LOCAL link down			
18	Mar/23/2022 17:06:10	memory	interface, info	ether3-LOCAL link up (speed 100M, full duplex)			
19	Mar/23/2022 17:22:07	memory	system, info, account	user admin logged in from 192.168.5.253 via winbox			
20	Mar/23/2022 17:22:20	memory	system, info	device changed by admin			
21	Mar/23/2022 17:22:20	memory	interface, info	ether1-CBN link down			
22	Mar/23/2022 17:23:36	memory	system, info	device changed by admin			
23	Mar/23/2022 17:23:39	memory	interface, info	ether1-CBN link up (speed 100M, full duplex)			
24	Mar/23/2022 17:23:59	memory	interface, info	ether1-CBN link down			

Figure 26: Ethernet 1 CBN Down

Since the CBN ether-1 link (IP Gateway: 192.168.10.1) is experiencing downtime, the status on the route list will change to "unreachable" as shown in the figure 27.

Routes	Nexthops Rules	VRF				
+ -	088	7		Find	all	Ŧ
	Dst. Address /	Gateway	Distance	Routing Mark	Pref. Source	
S	0.0.0.0/0	192.168.10.1 unreachable	1			
AS	0.0.0.0/0	192.168.1.1 reachable ether2-TLKM	2			
S	0.0.0.0/0	192.168.10.1 unreachable	1	to-ISP-CBN		
AS	0.0.0.0/0	192.168.1.1 reachable ether2-TLKM	1	to-ISP-TLKM		
DAC	192.168.1.0/24	ether2-TLKM reachable	C		192.168.1.2	
DAC	192.168.5.0/24	ether3-LOCAL reachable	0		192.168.5.1	

Figure 27: Route List Status

That is, the system check gateway parameters work well. Then do a traceroute to make sure the uplink comes from the backup link. From the traceroute results, the failover method worked well. This is because the route that the packet takes to reach the destination of Google DNS 8.8.8.8 is from a backup link, namely ISP Telkom with IP Address 192.168.1.1.

Basic					Advanced							Start	
Traceroute To:	56					Count					•	Stop	-
Packet Size:					Max	Max Hops:					•	Close	-
Timeout				ms	Src. Address:								_
Protocol	Protocol icmp		Ŧ							•	New Windo	JW	
	33434				Int	erface:					•		
Port						DSCP:							
	Use DNS												
					Routing	Table:					•		
Hop / Host		Loss	Sent Last		Avg	Best	Worst	Std. Dev.	History	Status			
1 192.16	8.1.1	0.0%	43 0.4ms		0.4								
2 10.96.1		0.0%			2.3								
3 180.25		0.0%			12								
4 8.8.8.8		0.0%			1.0								
5 192.16		0.0%			1.3								
6 180.24	0.190.69	27.9%			19.0				and south shine				
7 180.24	0.190.69	23.3%			20.5	15	8 60	1 10.7					
8		100.0%											
9 72.14.2		0.0%			16.0								
	0.240.225	0.0%			17.8								
	1 52 49	0.0%			16.8								
10 108.17 11 142.25 12 8.8.8.8			42 14.6m		14.5	14	3 14						

Figure 28: Traceroute Result

The results of the auto failover test show that the prevention system if the network is disconnected has been successful. Failover as a form of method where this function is very useful if you are experiencing problems with disconnected connections at the Main Internet Service Provider [8]. This method is very effective because this method will automatically change the main network connection to the backup network if the main network is disconnected or is in trouble. When the Primary ISP returns to normal, the Primary ISP immediately replaces its role. Figure 28 shows the final network test. Testing if the Primary ISP is experiencing interference, it can be seen that the backup ISP with IP 192.168.1.1 immediately provides its role as a backup ISP. And from the connection test, it looks like it only takes a moment to change the ISP.

ISSN: 1992-8645

www.jatit.org

4653

Based on this research, the combination of both load balancing and autofailover methods has succeeded in optimizing so that there is an increase in the throughput value, meaning that it has succeeded in achieving its goal of providing significant changes in network speed and stability. So users don't have to worry about data transfer speed and downtime issues.

REFERENCES:

- D. Darmawan and T. Imanto, "Analisa Link Balancing dan Failover 2 Provider Menggunakan Border Gateway Protocol (BGP) Pada Router Cisco 7606s," Jurnal Nasional Teknologi dan Sistem Informasi, vol. 3, no. 3, pp. 326–333, Dec. 2017, doi: 10.25077/teknosi.v3i3.2017.326-333.
- [2] K. NUGROHO and M. S. FALLAH, "Implementasi Load Balancing menggunakan Teknologi EtherChannel pada Jaringan LAN," *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika,* vol. 6, no. 3, p. 420, Oct. 2018, doi: 10.26760/elkomika.v6i3.420.
- [3] A. Husni, E. Budiman, M. Taruk, and H. J. Setyadi, "Teknik Load Balancing Menggunakan Metode Equal Cost Multi Path (Ecmp) Untuk Mengukur Beban Traffic Di Diskominfo Tenggarong," *Prosiding Seminar Ilmu Komputer dan Teknologi Informasi*, vol. 3, no. 1, 2018.
- [4] A. Mustofa and D. Ramayanti, "IMPLEMENTASI LOAD BALANCING DAN FAILOVER TO DEVICE MIKROTIK ROUTER MENGGUNAKAN METODE NTH (STUDI KASUS: PT. GO-JEK INDONESIA)," vol. 7, no. 1, pp. 139–144, 2020, doi: 10.25126/jtiik.202071638.
- [5] S. Alam Haris and H. Suhartono, "Menjaga Kestabilan Jaringan Load Balancing Nth Dengan Teknik Failover Pada PT. Jakarta Samudera Sentosa Jakarta," vol. 6, no. 1, pp. 49–60, 2018.
- [6] F. Fauzi and R. Darmawan, "Analisis dan Perancangan Load Balancing dan Failover menggunakan link kartu GSM," JURNAL JIIFOR, vol. 5, no. 2, p. 39, 2021.
- B. Hartanto, "Perancangan Sistem Jaringan Komputer Menggunakan Teknik Failover Pada Routing Static Yang Bersifat Recursive Connection," *Jurnal Ilmiah SINUS*, vol. 17, no. 2, p. 61, Jul. 2019, doi: 10.30646/sinus.v17i2.422.

7. CONCLUSION

This study focuses on the implementation of load balancing in optimizing the results of existing throughput values in an ethernet link network and the use of failover as a network backup method when a disturbance occurs. Content that has a tendency to design topological structures by combining load balancing and failover methods in an ethernet link network design. The design is used as a form of completeness to make the network high availability. High availability is a network concept that can minimize failure or downtime and aims to ensure the level of operational performance of the network so that it can serve users well.

Based on the research results, it can be concluded that the network topology that uses failover and load balancing methods is a network that can guarantee High Availability. This is because the use of the failover method can help the network to prevent network failures caused by long downtime. as well as load balancing methods that can make the network architecture faster to distribute traffic on the network. So as to make network traffic can run optimally and can avoid overload on one connection line. When the two methods are combined, the possibility of network failure will be very small.

The load balancing method is also very good in increasing the throughput value. This is based on all the tests that have been carried out, the throughput value has increased. The throughput value affects the data transfer speed, the higher the throughput value, the faster the data will be sent or received. This method is also proven to increase bandwidth by combining two different connections. Basically, the bandwidth of each ISP does not increase, but with load balancing that uses a multiconnection system, the network gets higher bandwidth than before. The load balancing method is very effective in video streaming activities, based on testing this method increases the throughput value to 5.42 Mbps from previously only 1.1 Mbps (CBN ISP) and 0.72 Mbps (TELKOM ISP).

The use of failover in the network topology is also very important to overcome and prevent offline occurrence on a network. With the increasing number of internet users, the quality of service must also be improved. one way is to reduce downtime on a network. failover can serve as a backup if one of the links is interrupted, so that there is no internet access failure.



ISSN: 1992-8645

www.jatit.org



E-ISSN: 1817-3195

- [8] M. Badrul, "IMPLEMENTASI AUTOMATIC FAILOVER MENGGUNAKAN ROUTER MIKROTIK UNTUK OPTIMALISASI JARINGAN," PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer, vol. 6, no. 2, 2019.
- [9] D. Novianto et al., "Implementasi Failover dengan Metode Recursive 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, vol. 10, no. 1, 2019, doi: 10.36982/jiig.v10i1.732.
- [10] E. Safrianti, L. Oktaviana Sari, and A. Satiarini, "Peer Connection Classifier Method for Load Balancing Technique," *International Journal of Electrical, Energy and Power System Engineering*, vol. 4, no. 1, pp. 127–133, 2021.
- [11] C. Lee, S. Kim, and H. Ryu, "FDVRRP: Router implementation for fast detection and high availability in network failure cases," *ETRI Journal*, vol. 41, no. 4, pp. 473–482, 2019, doi: 10.4218/etrij.2018-0309.
- [12] T. Ashraf, S. S. W. Lee, M. Iqbal, and J. Y. Pan, "Routing path assignment for joint load balancing and fast failure recovery in ip network," *Applied Sciences (Switzerland)*, vol. 11, no. 21, Nov. 2021, doi: 10.3390/app112110504.
- [13] M. Zulfi Rahmanzi, I. Fitri, and dan Andri Aningsih, "Load Balancing Performance in Etherchannel Technology Using the VLAN Trunking Protocol (VTP) Method," Jurnal Mantik, vol. 3, no. 36, pp. 540–547, 2020, [Online]. Available: https://iocscience.org/ejournal/index.php/mant ik/index
- [14] F. Firmansyah, M. Wahyudi, and R. A. Purnama, "Virtual Link Aggregation Network Performance Using MikroTik Bonding," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 2, no. 2, pp. 131–139, Dec. 2020, doi: 10.34306/itsdi.v2i2.394.
- [15] O. Dini, F. Sari, D. Kurniawati, and F. Muriyanto, "OPTIMASI SERVER MENGGUNAKAN LOAD BALANCING MICROSERVICE DOCKER PADA BOT TELEGRAM," Journal of Innovation Research and Knowledge, vol. 1, no. 7, 2021.
- [16] Z. Yin, D. Wang, Y. Zhao, Y. Guo, and S. Han, "Fast Failover for Link Failures in Software Defined Networks," in *Lecture Notes in Computer Science (including subseries)*

Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019, vol. 11635 LNCS, pp. 353–361. doi: 10.1007/978-3-030-24268-8_33.

- [17] X. Zhou, J. Tan, and N. Shroff, "Heavy-traffic Delay Optimality in Pull-based Load Balancing Systems," *Proceedings of the ACM* on Measurement and Analysis of Computing Systems, vol. 2, no. 3, pp. 1–33, Dec. 2018, doi: 10.1145/3287323.
- [18] S. M. M. Gilani, T. Hong, G. Zhao, C. Xu, and M. A. Abbas, "An Empirical Throughput Analysis of Multimedia Applications with OpenFlow-based Dynamic Load Balancing Approach in WLAN," *Journal of Internet Technology*, vol. 20, no. 1, pp. 237–246, 2019, doi: 10.3966/160792642019012001022.
- [19] T. R. Fakhrurrasi, A. Adriansyah, S. Budiyanto, J. Andika, S. C. Haryanti, and U. A. Rachmawati, "LOAD BALANCE OPTIMIZATION IN PEER CLASSIFIER ROBIN METHOD AS HYBRID FROM PEER CONNECTION CLASSIFIER AND ROUND ROBIN METHODS," Journal of Engineering Science and Technology, vol. 16, no. 3, pp. 2528–2543, 2021.
- [20] S. Budiyanto and A. Nugroho, "A new model of genetic zone routing protocol (GZRP): The process of load balancing and offloading on the UMTS - IEEE 802.11g hybrid networks," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 15, no. 2, pp. 598–605, Jun. 2017, doi: 10.12928/TELKOMNIKA.v15i2.5633.
- [21] M. K. Anwar and I. Nurhaida, "Implementasi Load Balancing Menggunakan Metode Equal Cost Multi Path (ECMP) Pada Interkoneksi Jaringan," Jurnal Telekomunikasi dan Komputer, vol. 9, no. 1, p. 39, Apr. 2019, doi: 10.22441/incomtech.v9i1.5003
- [22] A. Darojat and I. Nurhaida, "ANALISA QOS ADMINISTRATIVE DISTANCE STATIC ROUTE PADA FAILOVER VPN IPSEC," Jurnal Ilmu Teknik dan Komputer, vol. 3, no. 1, 2019.
- [23] H. K. Ramadhan and S. Wardhana, "Computer Networks Optimization using Load Balancing Algorithms on the Citrix ADC Virtual Server," *Jurnal Online Informatika*, vol. 6, no. 1, p. 103, Jun. 2021, doi: 10.15575/join.v6i1.672.