International Journal of Electrical, Energy and Power System Engineering (IJEEPSE)
e-ISSN: 2654-4644
Vol. 4, No. 1, pp. 127-133, February 2021
Accredited by KEMENRISTEKBRIN, No. 200/M/KPT/2020
http://www.ijeepse.ejournal.unri.ac.id

Peer Connection Classifier Method for Load Balancing Technique

Ery Safrianti
Electrical Engineering Department
Riau University
Pekanbaru, Indonesia
esafriant@eng.unri.ac.id

Linna Oktaviana Sari
Electrical Engineering Department
Riau University
Pekanbaru, Indonesia
linnaosari@lecturer.unri.ac.id

Astri Satiarini
Electrical Engineering Department
Riau University
Pekanbaru, Indonesia
astri.satiarini@student.unri.ac.id

*corresponding author: *Ery Safrianti, esafrianti @eng.unri.ac.id*

***Abstract*— A large number of requests for internet access causes a long response time resulting in an overload problem. This problem occurs in offices that provide public services such as the Soeman HS Regional Library and Archives Office in Riau Province. So that service work is not disrupted due to overload, network optimization is carried out using Load Balancing Techniques. Load Balancing will balance load traffic on two or more connection lines so that traffic can run optimally. The method used is the Peer Connection Classifier (PCC). This method 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 Load Balancing with the PCC method. The router will manage outgoing requests from users through the Internet Service Provider 1 (ISP 1) line or ISP line 2 to be able to enter the internet connection. The test results show equal distribution of outgoing access to ISP 1 and ISP 2 lines so that there is no overload on any ISP lines. This configuration will be applied to the Mikrotik router using the Winbox application.**

***Keywords*—Failover, ISP Lines. Load Balancing, Peer Connection Classifier**

I. Introduction

The Internet has become the largest access to telecommunications services and sources of information in the world. Internet services that exist today include direct communication or discussion (Usenet News, email, mailing lists), (email, chat), remote login, distributed information sources (World Wide Web, Gopher), and file traffic (Telnet, FTP), and various other services.

One agency that uses internet services is the Riau Province Library and Archive Office named Soeman HS. This agency is engaged in libraries, archives, and documentation that are open to the public. The Soeman HS Library also provides internet-connected computers on each floor to make it easier for visitors to find books. Apart from reading books, visitors can also visit a booth called the e-kiosk, one of the facilities provided by the Soeman HS library. The e-kiosk consists of 43 Personal Computers (PCs) on various floors, namely 12 PCs on the ground floor, 10 PCs on the 1st floor, 16 PCs on the 2nd floor, and 5 PCs on the 3rd floor.

In addition to visitors, employees who work at the Soeman HS library also use internet access as a support medium in their work and activities, such as registering new members, collecting data on borrowing books, entering book data, and others. The divisions in charge of providing these services are the Division of Automation, Preservation, Cooperation, and Networking. This division has several tasks, namely implementing provincial library database management, managing library websites and internet networks as well as developing communication formats between libraries in districts/cities throughout Riau Province, carrying out data collection, processing, and statistical reporting of library collection preservation/preservation activities, and carry out cooperation between library networks. This division is in charge of controlling the server and is responsible for the network in the Soeman HS Library. Besides, this division is also in charge of entering employee data, entering data for new member registrants, and entering data for books that will become collections of the Soeman HS Library. All data will be entered into the Inlislite application. The Inlislite application is a library-specific database application provided by the central government which is useful for entering registrant data for employees, new members, book data, and others.

Soeman HS Library has problems with internet access. The number of requests for internet access causes long response times and overloads. The high demand for internet access occurs because of the number of visitors who access the internet and employees who use the internet to support their performance in providing services to visitors. Although the HS Soeman Library uses 2 ISPs, the distribution of the load is not balanced. Access using 2 Mikrotik so that it cannot balance the network load and perform backups if one ISP has a problem. This causes an accumulation of loads on one ISP and creates an overload that is detrimental to users or clients connected to one of these ISPs. When overload occurs, it

Received: January 30, 2021 | Revised: February 17, 2021 | Accepted: February 24, 2021

obstructs the work of employees and has the effect of reducing work efficiency. There is inconvenience towards visitor services and many complaints regarding internet speed. This requires a fast and stable network connection so that the work of employees can run efficiently and provide comfort to visitors. Another problem that occurs is that if one ISP is disconnected, the network connection connected to that ISP will be disconnected. To solve the problem in the Soeman HS library, network optimization will be carried out using Load Balancing techniques and the application of failover techniques.

With the enormous need for the internet, administrators provide an alternative to optimizing the existing network by separating the internet paths based on departments within a company. According to [1] this method is considered less effective because one day there will be imbalances in the user's internet conditions. If Department A has a small bandwidth but is used by many users and department B with a lot of bandwidth but is used for only a few users, then the internet access in department A will be slower than in department B. The solution to overcome this problem is to use load balancing techniques which will be effective to take advantage of internet bandwidth, this technology is also an effective solution to reduce imbalances in internet bandwidth. Load Balancing is a technique or method used in sharing the load on a web server in a network. To maximize traffic and traffic running optimally, this technique will distribute the network equally on two existing connection lines or even more. This technique also distributes the workload evenly on two or more computers, network links, CPUs, hard drives, or other resources, to get optimal resource utilization [2].

Following the existing problems, research on the design and implementation of Load Balancing was carried out. This study aims to optimize the network at the Riau Provincial Library and Archives Service. The implementation of Load Balancing will reduce response time, maximize throughput, share traffic load equally, and implement failover techniques that can move gateways to other available ISP lines if one of them is disconnected. The method to be used will be adjusted to the consideration of the conditions and the ease with which it is applied.

II. LITERATURE REVIEW

A. *Previous Research*

Research conducted by Dina Farouk Altayeb and Fatima Abdelghani Mustafa provides a technical overview of various load balancing algorithms. In this study it is proven that Load Balancing helps distribute the total available VM load to increase resource utilization and response time. This is a situation where some nodes are heavily loaded while others are idle or doing very little work. This research applies a new algorithm and compares the performance with the Load Balancing algorithm using the Cloud Analyst simulator. Performance is compared based on the computational response time with respect to stability, resource utilization, dynamics [3].

Research conducted by Venubabu Kunamneni discusses the DSBP algorithm in this study is able to play an important role focusing on load balancing of different data centers to facilitate information across multiple levels of logistics in real-world computing environments. Therefore, it is concluded that the DBSP algorithm has an effective outcome in logistical operations. There is also DSBP analytics which has better results compared to Round Robin, supports active and load balancing algorithms that are updated at the same time to replace response times, cost transfer data and data in the provided data center. The significance of this research is the demonstration of the DSBP algorithm using a collaborative cloud of advanced technology which will definitely help to provide efficient information and manage operations to obtain information from different locations in a distributed data center. Cloud Computing is a broad concept and load balancing plays a very important role. As we all know, there are several advantages with Load Balancing for IT Environment, especially dynamic implementations. Dynamic load balancing helps with comprehensive failover capabilities in the event of a server failure [4].

Research conducted by Alan Fauzi, Alex Wijaya, Irman Effendy is useful for optimizing network performance by providing optimal bandwidth and dividing traffic load equally. As well as the application of fail over techniques to make one gateway as a single connection if the other gateway is dead. The results show that the traffic load of the two ISPs is balanced and when ISP 2 dies, ISP 1 will remain alive as a single connection [5].

The research conducted by Eudes Raymond Gene is useful for solving problems when one of the ISPs experiences a disconnection, this can be seen from the automatic switching of connections to the gateway from an active ISP, so that network performance continues to run normally. The system built can also divide the connection path equally based on the size of the request packet. In Nth Load Balancing, two gateways are used interchangeably according to the round robin algorithm, while in PCC Load Balancing one connection uses a gateway according to the hashing / modulo method based on the source, destination address and port address. With these two methods, all internet requests from users will go to the router that has been configured with the Nth and PCC methods first so that the router will set the path for the exit request from the user via the ISP 1 line or ISP 2 line to get to the internet connection. The test results show an equal distribution of outgoing access to the ISP 1 line and ISP 2 line, so that there is no overload on one of these ISP lines [6].

Research conducted by Muhammad Iqbal Firdaus compared two load balancing methods, namely the ECMP method and the PCC method. From the results of the research conducted, it was found that the PCC method can produce better throughput than the ECMP method. The PCC method has better durability or reliability than the ECMP method when there is network interference. Meanwhile, the ECMP method produces better RTT than the PCC method. In the comparison of the value of jitter and packet loss that has been tested in the two methods, the difference is not too significant. In addition, the level of degradation in both of them is still tolerable and is in the very good category [7]. 2(Firdaus, 2017).

B. *Load Balancing*

Load Balancing is a technique used to optimize the network by dividing the load on the webserver in the network. For traffic to run optimally, this Load Balancing Technique will distribute the network traffic load on two or more connection lines which will be divided equally. Load Balancing can also distribute workloads evenly on two or more computers, CPUs, hard drives, network links, or other resources, to get optimal resource utilization [2].

In a Load Balancing system, the load sharing process has its techniques to match the characteristics of the servers behind it. Load Balancing on a computer network is useful for dividing bandwidth between the primary backbone and backup bandwidth. Therefore, a backup backbone that is different from primary is needed in terms of routing, last mile, and even service providers [8]. Some of the advantages of applying Load Balancing techniques are as follows:

1. Flexibility: the server becomes part of the many servers that form the cluster and is no longer the core system and main resource.

2. Scalability: when changes occur in system components, the system no longer requires redesigning the entire system architecture to adapt again.

3. Security: security rules can be implemented easily for all traffic passing through the load balancer. Security on Load Balancing is adapted from Mirotic security, namely Firewall. Load Balancing applies a NAT configuration that functions as a firewall for network security.

4. High-availability: Load balancers can know the real server condition in the system automatically, if there is a real server that dies it will be removed from the real server list, and if the real server is back on, it will be included in the real server list. Load balancers can also be redundantly configured with other load balancers [9].

C. *Peer Connection Classifier (PCC).*

PCC is a method that specifies a packet to a specific connection gateway. PCC classifies connection traffic going through or out of the router into several groups. This grouping can be distinguished by src-address, dst-address, src-port, and dst-port. Mirotic will remember the gateway path that was passed at the beginning of the connection traffic so that subsequent data packets that are still related to the previous data packet will be passed on the same gateway path. Because the PCC method passes data packets through the same gateway, this method has a drawback, namely that overloading one of the gateways can occur [6]. Fig. 1 is the algorithm for the PCC method.

The advantages and disadvantages of the PCC method are as follows:

a. Pros: Being able to specify a gateway for each data packet that is still in contact with data that has previously been passed on one of the gateways, the relationship between the client and server is more secure because it uses the same path, does not bother the end-user or end-user, streaming is more stable.

b. Weaknesses: there is a temporary delay when many requests come in [10].

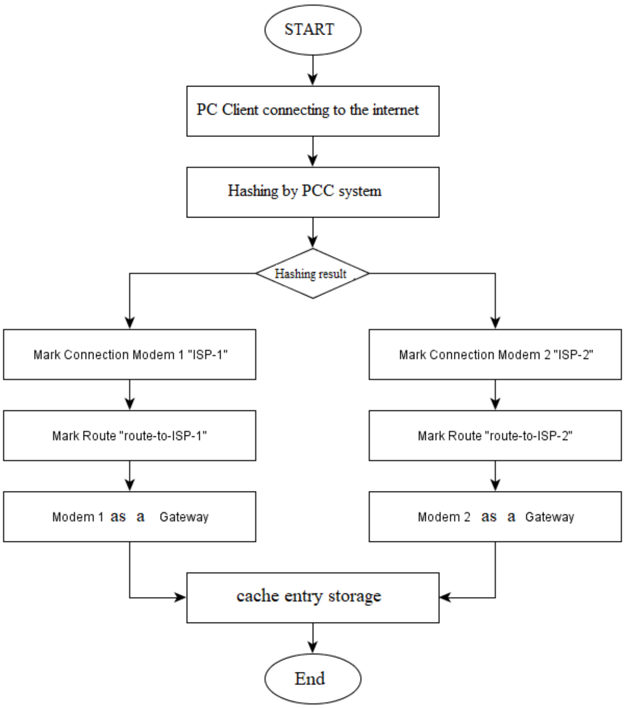

START
PC Client connecting to the internet
Hashing by PCC system
Hashing result
Mark Connection Modem 1 "ISP-1"
Mark Connection Modem 2 "ISP-2"
Mark Route "route-to-ISP-1"
Mark Route "route-to-ISP-2"
Modem 1 as a Gateway
Modem 2 as a Gateway
cache entry storage
End

Fig. 1. PCC Algorithm

D. *Failover*

The definition of failover in terms of internetworking computer is the ability of a system to be able to move manually or automatically if one of the systems fails so that it becomes a backup for the failing system. If gateway 1 is disconnected, the backup gateway will replace gateway 1. If gateway 1 returns to normal, the connection path used again becomes gateway 1. And so does gateway 2 when it is disconnected. The failover algorithm is shown in Fig. 2.

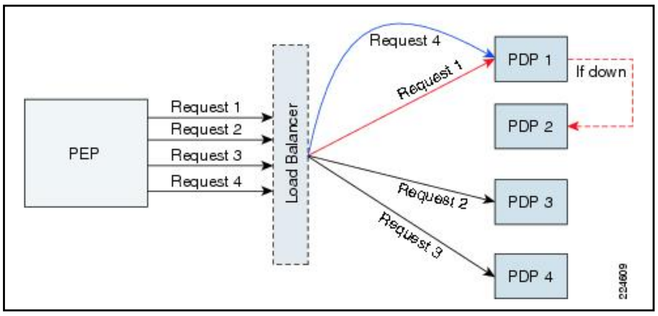


Fig. 2. Failover Algorithm

Thus, it can be concluded that the purpose of failover in this multihomed study is to replace or a disconnected ISP connection backup system with other ISP connections [11].

Received: January 30, 2021 | Revised: February 17, 2021 | Accepted: February 24, 2021

III. METHODOLOGY

A. *Load Balancing Configuration Design*

To configure Load Balancing, it takes steps in configuration. Load Balancing configuration scheme can be seen in Fig. 3.

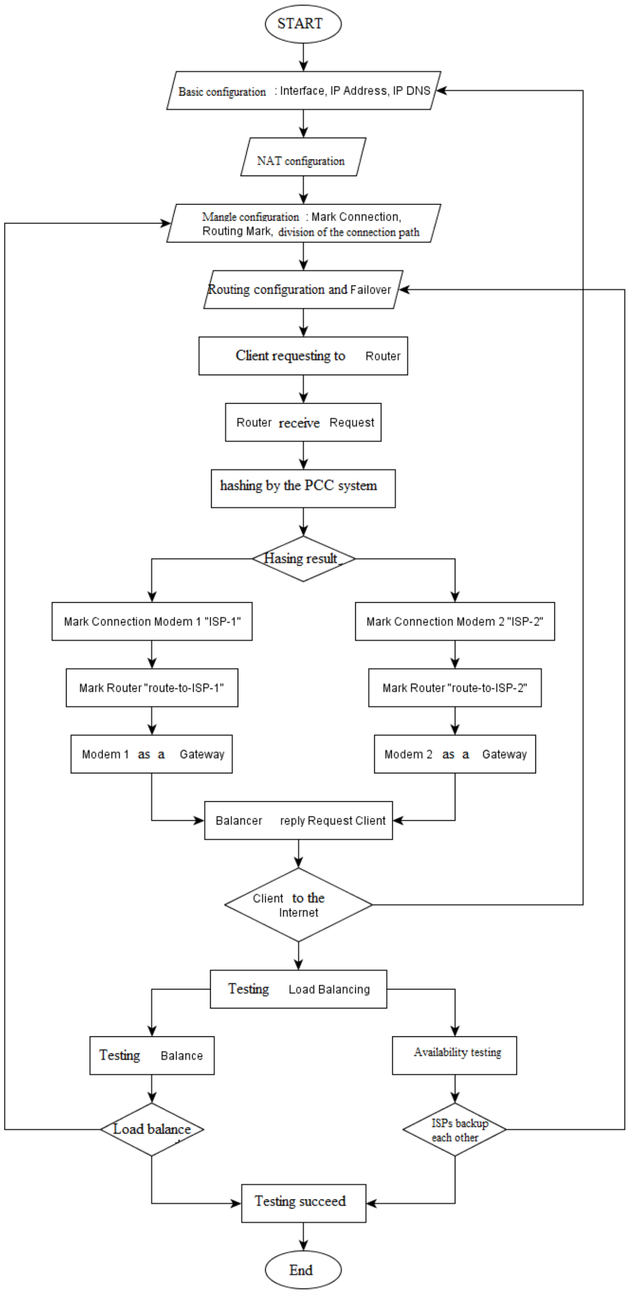

START
Basic configuration : Interface, IP Address, IP DNS
NAT configuration
Mangle configuration : Mark Connection, Routing Mark, division of the connection path
Routing configuration and Failover
Client requesting to Router
Router receive Request
hashing by the PCC system
Hasing result
Mark Connection Modem 1 "ISP-1"
Mark Connection Modem 2 "ISP-2"
Mark Router "route-to-ISP-1"
Mark Router "route-to-ISP-2"
Modem 1 as a Gateway
Modem 2 as a Gateway
Balancer reply Request Client
Client to the Internet
Testing Load Balancing
Testing Balance
Availability testing
Load balance
ISPs backup each other
Testing succeed
End

Fig. 3. Load Balancing Configuration Schematic

To configure Load Balancing, several steps are needed, namely as follows.

1. Basic Configuration.

Load Balancing configuration requires several steps, the first is to perform basic configuration. At this stage, the first thing to do is to configure the interface that is used as a route in and out of the internet via the Mirotic Router. And after going through the initial check, then establish a connection with the ISP and make an IP address request (IP-DHCP). Next, configure the IP address for each ethernet and DNS that will be used.

2. NAT Configuration.

After configuring IP and DNS, then you have to add NAT configuration. NAT is useful so that the client can connect to the internet. NAT will change the source address of the packet, which is the client address that has a private IP address so that it can be recognized by the internet by translating it into a public IP address. This NAT setting uses the Masquerading NAT method. Because the provider used only provides one public IP, so all IP addresses from the client will be mapped to one public IP.

3. Mangle Configuration.

Mangle is useful for marking a package, where the marking is done according to the conditions and conditions we want. After that, the results of the marking will be used for specific needs based on the selected action. In the mangle configuration using the PCC method, packet marking is based on the original stateful packet inspection, namely src-IP, dst-IP, src-port, and dst-port. From these parameters, connection marks and routing marks can be performed, which can then be used for specific packet processing.

4. Routing configuration.

Next, we will map the route or connection path based on the routing mark that has been made in the mangle configuration. The first routing mark will use the gateway from ISP 1 and the second routing mark will use the gateway ISP 2.

5. Failover configuration.

Failover is useful for dealing with the disconnection of one of the lines/ISP. It is expected that this system will move the gateway automatically to an available or active path. The feature used takes advantage of the gateway checking process by sending an ICMP echo request to an address that can be used to detect a path failure. In this way, path failures caused by failed hops in the data transaction process can also be detected.

B. *Load Balancing Testing*

At this stage, several load balancing performance tests will be carried out in each method, including the following:

1. Balance: performance will be tested on the Load Balancing method in terms of equalizing the connection load on each connection line, both at ISP 1 and ISP 2. The test is carried out in two ways, namely:

a. Two clients access the same website/site so that you can see the distribution of the connection path. If each client can access the site through a different gateway path from each server, then Load Balancing is running well.

b. One client accesses the same site through two different browsers. If the connection path that is passed by the router as a load balancer is different between the two browsers, then Load Balancing is running properly.

2. Availability: if there is a dead server (ISP), the load balancer will stop requests to the server (ISP) and divert them to another server (ISP). Testing is done by disconnecting from one server (ISP) in turn. This stage is the result of testing for the failover technique implementation.

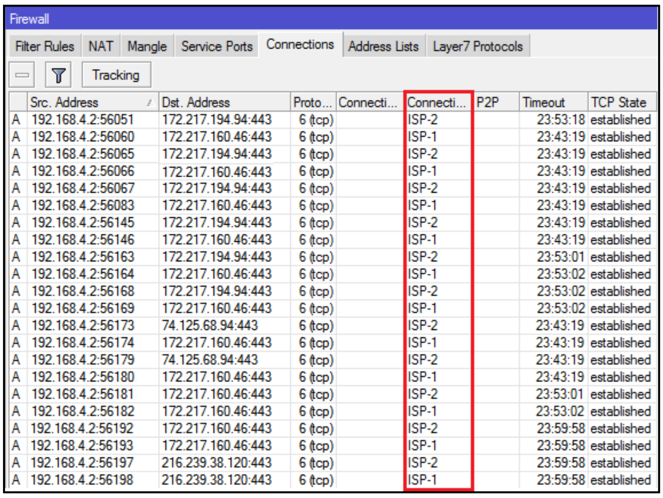
IV. RESULT AND DISCUSSION

A. *Load Balancing Testing*

In the balance test, what will be tested is the balance of traffic loads on both ISPs and.

1. One client accesses the same site on two different browsers.

In this test, the client will access youtube.com via the Google Chrome and Mozilla Firefox browsers. The results of monitoring the connection in this test are as follows:



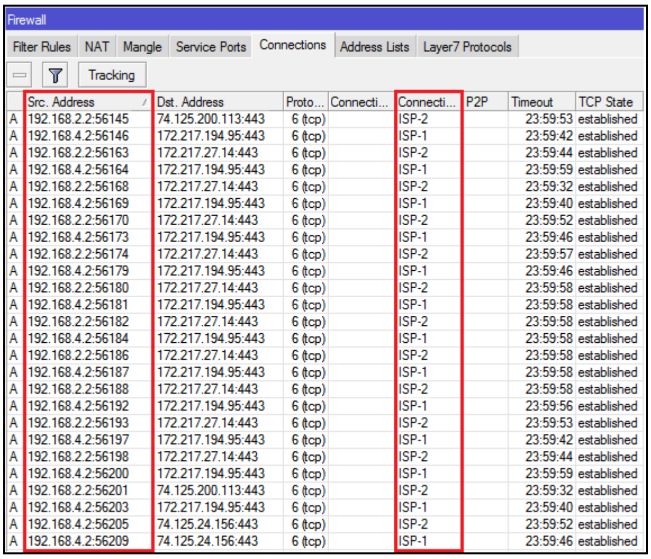
	Src. Address	Dst. Address	Proto...	Connecti...	Connecti...	P2P	Timeout	TCP State
A	192.168.4.2:56051	172.217.194.94:443	6 (tcp)		ISP-2		23:53:18	established
A	192.168.4.2:56060	172.217.160.46:443	6 (tcp)		ISP-1		23:43:19	established
A	192.168.4.2:56065	172.217.194.94:443	6 (tcp)		ISP-2		23:43:19	established
A	192.168.4.2:56066	172.217.160.46:443	6 (tcp)		ISP-1		23:43:19	established
A	192.168.4.2:56067	172.217.194.94:443	6 (tcp)		ISP-2		23:43:19	established
A	192.168.4.2:56083	172.217.160.46:443	6 (tcp)		ISP-1		23:43:19	established
A	192.168.4.2:56145	172.217.194.94:443	6 (tcp)		ISP-2		23:43:19	established
A	192.168.4.2:56146	172.217.160.46:443	6 (tcp)		ISP-1		23:43:19	established
A	192.168.4.2:56163	172.217.194.94:443	6 (tcp)		ISP-2		23:53:01	established
A	192.168.4.2:56164	172.217.160.46:443	6 (tcp)		ISP-1		23:53:02	established
A	192.168.4.2:56168	172.217.194.94:443	6 (tcp)		ISP-2		23:53:02	established
A	192.168.4.2:56169	172.217.160.46:443	6 (tcp)		ISP-1		23:53:02	established
A	192.168.4.2:56173	74.125.68.94:443	6 (tcp)		ISP-2		23:43:19	established
A	192.168.4.2:56174	172.217.160.46:443	6 (tcp)		ISP-1		23:43:19	established
A	192.168.4.2:56179	74.125.68.94:443	6 (tcp)		ISP-2		23:43:19	established
A	192.168.4.2:56180	172.217.160.46:443	6 (tcp)		ISP-1		23:43:19	established
A	192.168.4.2:56181	172.217.160.46:443	6 (tcp)		ISP-2		23:53:01	established
A	192.168.4.2:56182	172.217.160.46:443	6 (tcp)		ISP-1		23:53:02	established
A	192.168.4.2:56192	172.217.160.46:443	6 (tcp)		ISP-2		23:59:58	established
A	192.168.4.2:56193	172.217.160.46:443	6 (tcp)		ISP-1		23:59:58	established
A	192.168.4.2:56197	216.239.38.120:443	6 (tcp)		ISP-2		23:59:58	established
A	192.168.4.2:56198	216.239.38.120:443	6 (tcp)		ISP-1		23:59:58	established

Fig. 4. Testing Balance on One Client

As seen in Fig. 4, the router divides the connection evenly and alternately. This can be seen from the connection path that is passed by IP 192.168.4.2 alternately to ISP-1 and ISP-2.

2. Two clients access the same site.

In this test two clients will access the same site, namely youtube.com through their respective devices. The results of monitoring the connection in this test are shown in Fig. 5.

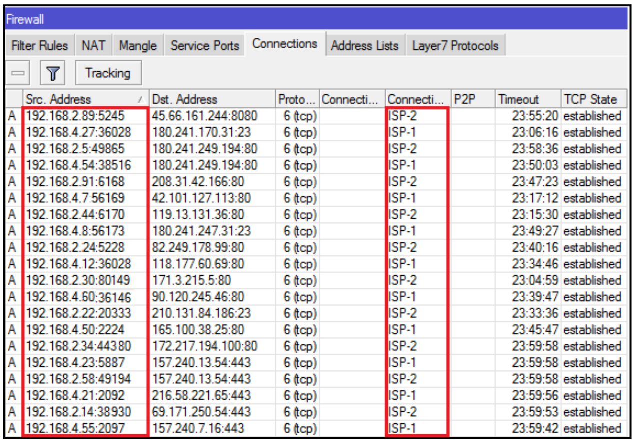


	Src. Address	Dst. Address	Proto...	Connecti...	Connecti...	P2P	Timeout	TCP State
A	192.168.2.2:56145	74.125.200.113:443	6 (tcp)		ISP-2		23:59:53	established
A	192.168.4.2:56146	172.217.194.95:443	6 (tcp)		ISP-1		23:59:42	established
A	192.168.2.2:56163	172.217.27.14:443	6 (tcp)		ISP-2		23:59:44	established
A	192.168.4.2:56164	172.217.194.95:443	6 (tcp)		ISP-1		23:59:59	established
A	192.168.2.2:56168	172.217.27.14:443	6 (tcp)		ISP-2		23:59:32	established
A	192.168.4.2:56169	172.217.194.95:443	6 (tcp)		ISP-1		23:59:40	established
A	192.168.2.2:56170	172.217.27.14:443	6 (tcp)		ISP-2		23:59:52	established
A	192.168.4.2:56173	172.217.194.95:443	6 (tcp)		ISP-1		23:59:46	established
A	192.168.2.2:56174	172.217.27.14:443	6 (tcp)		ISP-2		23:59:57	established
A	192.168.4.2:56179	172.217.194.95:443	6 (tcp)		ISP-1		23:59:46	established
A	192.168.2.2:56180	172.217.27.14:443	6 (tcp)		ISP-2		23:59:58	established
A	192.168.4.2:56181	172.217.194.95:443	6 (tcp)		ISP-1		23:59:58	established
A	192.168.2.2:56182	172.217.27.14:443	6 (tcp)		ISP-2		23:59:58	established
A	192.168.4.2:56184	172.217.194.95:443	6 (tcp)		ISP-1		23:59:58	established
A	192.168.2.2:56186	172.217.27.14:443	6 (tcp)		ISP-2		23:59:58	established
A	192.168.4.2:56187	172.217.194.95:443	6 (tcp)		ISP-1		23:59:58	established
A	192.168.2.2:56188	172.217.27.14:443	6 (tcp)		ISP-2		23:59:58	established
A	192.168.4.2:56192	172.217.194.95:443	6 (tcp)		ISP-1		23:59:56	established
A	192.168.2.2:56193	172.217.27.14:443	6 (tcp)		ISP-2		23:59:53	established
A	192.168.4.2:56197	172.217.194.95:443	6 (tcp)		ISP-1		23:59:42	established
A	192.168.2.2:56198	172.217.27.14:443	6 (tcp)		ISP-2		23:59:44	established
A	192.168.4.2:56200	172.217.194.95:443	6 (tcp)		ISP-1		23:59:59	established
A	192.168.2.2:56201	74.125.200.113:443	6 (tcp)		ISP-2		23:59:32	established
A	192.168.4.2:56203	172.217.194.95:443	6 (tcp)		ISP-1		23:59:40	established
A	192.168.4.2:56205	74.125.24.156:443	6 (tcp)		ISP-2		23:59:52	established
A	192.168.4.2:56209	74.125.24.156:443	6 (tcp)		ISP-1		23:59:46	established

Fig. 5. Testing Balance on Two Clients

As seen in Fig. 5, 2 clients are connected, namely on IP 192.168.2.2 and 192.168.4.2 through different connection lines. IP 192.168.2.2 passes through the ISP-2 connection line. Meanwhile, IP 192.168.4.2 passes through the ISP-1 connection line.

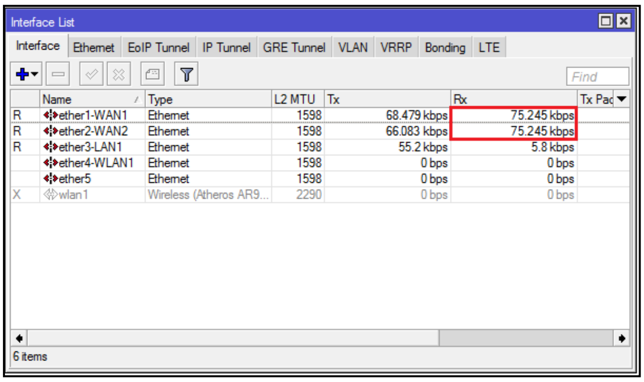
In addition to the above tests, it is necessary to prove network traffic with many clients and a balanced bandwidth load on ISP 1 and ISP 2. In Fig. 6 the network traffic will be displayed.



	Src. Address	Dst. Address	Proto...	Connecti...	Connecti...	P2P	Timeout	TCP State
A	192.168.2.89:5245	45.66.161.244:8080	6 (tcp)		ISP-2		23:55:20	established
A	192.168.4.27:36028	180.241.170.31:23	6 (tcp)		ISP-1		23:06:16	established
A	192.168.2.5:49865	180.241.249.194:80	6 (tcp)		ISP-2		23:58:36	established
A	192.168.4.54:38516	180.241.249.194:80	6 (tcp)		ISP-1		23:50:03	established
A	192.168.2.91:6168	208.31.42.166:80	6 (tcp)		ISP-2		23:47:23	established
A	192.168.4.7 56169	42.101.127.113:80	6 (tcp)		ISP-1		23:17:12	established
A	192.168.2.44:6170	119.13.131.36:80	6 (tcp)		ISP-2		23:15:30	established
A	192.168.4.8:56173	180.241.247.31:23	6 (tcp)		ISP-1		23:49:27	established
A	192.168.2.24:5228	82.249.178.99:80	6 (tcp)		ISP-2		23:40:16	established
A	192.168.4.12:36028	118.177.60.69:80	6 (tcp)		ISP-1		23:34:46	established
A	192.168.2.30:80149	171.3.215.5:80	6 (tcp)		ISP-2		23:04:59	established
A	192.168.4.60:36146	90.120.245.46:80	6 (tcp)		ISP-1		23:39:47	established
A	192.168.2.22:20333	210.131.84.186:23	6 (tcp)		ISP-2		23:33:36	established
A	192.168.4.50:2224	165.100.38.25:80	6 (tcp)		ISP-1		23:45:47	established
A	192.168.2.34:44380	172.217.194.100:80	6 (tcp)		ISP-2		23:59:58	established
A	192.168.4.23:5887	157.240.13.54:443	6 (tcp)		ISP-1		23:59:58	established
A	192.168.2.58:49194	157.240.13.54:443	6 (tcp)		ISP-2		23:59:58	established
A	192.168.4.21:2092	216.58.221.65:443	6 (tcp)		ISP-1		23:59:56	established
A	192.168.2.14:38930	69.171.250.54:443	6 (tcp)		ISP-2		23:59:53	established
A	192.168.4.55:2097	157.240.7.16:443	6 (tcp)		ISP-1		23:59:42	established

Fig. 6. Network Traffic

It can be seen in Fig. 6 that there is network traffic when many clients access the internet. It can be seen in the connection column that the ISP is accessed alternately and in a balanced way. Next is the load testing at each ISP, which can be seen on the following list interface menu.



	Name	Type	L2 MTU	Tx	Rx	Tx Pac
R	ether1-WAN1	Ethernet	1598	68.479 kbps	75.245 kbps	
R	ether2-WAN2	Ethernet	1598	66.083 kbps	75.245 kbps	
R	ether3-LAN1	Ethernet	1598	55.2 kbps	5.8 kbps	
	ether4-WLAN1	Ethernet	1598	0 bps	0 bps	
	ether5	Ethernet	1598	0 bps	0 bps	
X	wlan1	Wireless (Atheros AR9...	2290	0 bps	0 bps	

6 items

Fig. 7. Balanced Bandwidth Load

As seen in Fig. 7, the bandwidth load on ISP 1 and ISP 2 is balanced after the implementation of Load Balancing. Then the optimization is done by configuring Load Balancing which is done successfully with an even distribution of each ISP.

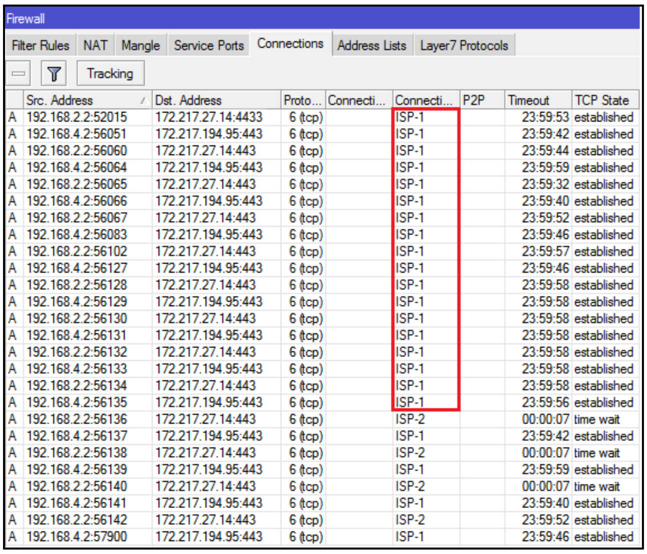
B. *Availability*

In the availability test, what will be tested is the failover technique. How to test it by disconnecting an ISP and the connection paths will be seen.

1. ISP 1.

In this test, the ISP connection line will be terminated and it will automatically switch to ISP 1 as shown in Fig. 8.

Received: January 30, 2021 | Revised: February 17, 2021 | Accepted: February 24, 2021



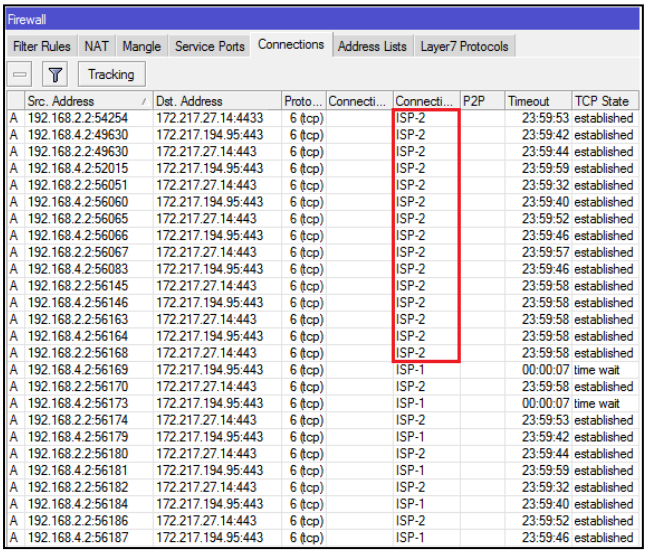
	Src. Address	Dst. Address	Proto...	Connecti...	Connecti...	P2P	Timeout	TCP State
A	192.168.2.2:52015	172.217.27.14:4433	6 (tcp)		ISP-1		23:59:53	established
A	192.168.4.2:56051	172.217.194.95:443	6 (tcp)		ISP-1		23:59:42	established
A	192.168.2.2:56060	172.217.27.14:443	6 (tcp)		ISP-1		23:59:44	established
A	192.168.4.2:56064	172.217.194.95:443	6 (tcp)		ISP-1		23:59:59	established
A	192.168.2.2:56065	172.217.27.14:443	6 (tcp)		ISP-1		23:59:32	established
A	192.168.4.2:56066	172.217.194.95:443	6 (tcp)		ISP-1		23:59:40	established
A	192.168.2.2:56067	172.217.27.14:443	6 (tcp)		ISP-1		23:59:52	established
A	192.168.4.2:56083	172.217.194.95:443	6 (tcp)		ISP-1		23:59:46	established
A	192.168.2.2:56102	172.217.27.14:443	6 (tcp)		ISP-1		23:59:57	established
A	192.168.4.2:56127	172.217.194.95:443	6 (tcp)		ISP-1		23:59:46	established
A	192.168.2.2:56128	172.217.27.14:443	6 (tcp)		ISP-1		23:59:58	established
A	192.168.4.2:56129	172.217.194.95:443	6 (tcp)		ISP-1		23:59:58	established
A	192.168.2.2:56130	172.217.27.14:443	6 (tcp)		ISP-1		23:59:58	established
A	192.168.4.2:56131	172.217.194.95:443	6 (tcp)		ISP-1		23:59:58	established
A	192.168.2.2:56132	172.217.27.14:443	6 (tcp)		ISP-1		23:59:58	established
A	192.168.4.2:56133	172.217.194.95:443	6 (tcp)		ISP-1		23:59:58	established
A	192.168.2.2:56134	172.217.27.14:443	6 (tcp)		ISP-1		23:59:58	established
A	192.168.4.2:56135	172.217.194.95:443	6 (tcp)		ISP-1		23:59:56	established
A	192.168.2.2:56136	172.217.27.14:443	6 (tcp)		ISP-2		00:00:07	time wait
A	192.168.4.2:56137	172.217.194.95:443	6 (tcp)		ISP-1		23:59:42	established
A	192.168.2.2:56138	172.217.27.14:443	6 (tcp)		ISP-2		00:00:07	time wait
A	192.168.4.2:56139	172.217.194.95:443	6 (tcp)		ISP-1		23:59:59	established
A	192.168.2.2:56140	172.217.27.14:443	6 (tcp)		ISP-2		00:00:07	time wait
A	192.168.4.2:56141	172.217.194.95:443	6 (tcp)		ISP-1		23:59:40	established
A	192.168.2.2:56142	172.217.27.14:443	6 (tcp)		ISP-2		23:59:52	established
A	192.168.4.2:57900	172.217.194.95:443	6 (tcp)		ISP-1		23:59:46	established

Figure 8. ISP 1 Availability Testing

It can be seen in the picture above that when the ISP 2 connection is lost, the entire connection is diverted or backed up to ISP 1.

2. ISP 2.

In this test, the ISP connection line will be terminated and it will automatically switch to ISP 2 as shown in Fig. 9.



	Src. Address	Dst. Address	Proto...	Connecti...	Connecti...	P2P	Timeout	TCP State
A	192.168.2.2:54254	172.217.27.14:4433	6 (tcp)		ISP-2		23:59:53	established
A	192.168.4.2:49630	172.217.194.95:443	6 (tcp)		ISP-2		23:59:42	established
A	192.168.2.2:49630	172.217.27.14:443	6 (tcp)		ISP-2		23:59:44	established
A	192.168.4.2:52015	172.217.194.95:443	6 (tcp)		ISP-2		23:59:59	established
A	192.168.2.2:56051	172.217.27.14:443	6 (tcp)		ISP-2		23:59:32	established
A	192.168.4.2:56060	172.217.194.95:443	6 (tcp)		ISP-2		23:59:40	established
A	192.168.2.2:56065	172.217.27.14:443	6 (tcp)		ISP-2		23:59:52	established
A	192.168.4.2:56066	172.217.194.95:443	6 (tcp)		ISP-2		23:59:46	established
A	192.168.2.2:56067	172.217.27.14:443	6 (tcp)		ISP-2		23:59:57	established
A	192.168.4.2:56083	172.217.194.95:443	6 (tcp)		ISP-2		23:59:46	established
A	192.168.2.2:56145	172.217.27.14:443	6 (tcp)		ISP-2		23:59:58	established
A	192.168.4.2:56146	172.217.194.95:443	6 (tcp)		ISP-2		23:59:58	established
A	192.168.2.2:56163	172.217.27.14:443	6 (tcp)		ISP-2		23:59:58	established
A	192.168.4.2:56164	172.217.194.95:443	6 (tcp)		ISP-2		23:59:58	established
A	192.168.2.2:56168	172.217.27.14:443	6 (tcp)		ISP-2		23:59:58	established
A	192.168.4.2:56169	172.217.194.95:443	6 (tcp)		ISP-1		00:00:07	time wait
A	192.168.2.2:56170	172.217.27.14:443	6 (tcp)		ISP-2		23:59:58	established
A	192.168.4.2:56173	172.217.194.95:443	6 (tcp)		ISP-1		00:00:07	time wait
A	192.168.2.2:56174	172.217.27.14:443	6 (tcp)		ISP-2		23:59:53	established
A	192.168.4.2:56179	172.217.194.95:443	6 (tcp)		ISP-1		23:59:42	established
A	192.168.2.2:56180	172.217.27.14:443	6 (tcp)		ISP-2		23:59:44	established
A	192.168.4.2:56181	172.217.194.95:443	6 (tcp)		ISP-1		23:59:59	established
A	192.168.2.2:56182	172.217.27.14:443	6 (tcp)		ISP-2		23:59:32	established
A	192.168.4.2:56184	172.217.194.95:443	6 (tcp)		ISP-1		23:59:40	established
A	192.168.2.2:56186	172.217.27.14:443	6 (tcp)		ISP-2		23:59:52	established
A	192.168.4.2:56187	172.217.194.95:443	6 (tcp)		ISP-1		23:59:46	established

Figure 9. ISP 2 Availability Testing

It can be seen in the picture above that when the ISP 1 connection is lost, all connections are diverted or backed up to ISP 2.

C. Network Connection Testing Comparison

In this network connection comparison stage, throughput, delay, and packet loss comparisons will be made between before Load Balancing is applied and afterload Balancing is applied.

TABLE 1. COMPARISON OF AVERAGE THROUGHPUT

Time	Throughput (Kbps)	
	Before	After
09.00	456	1381.3
13.00	232.3	1052
16.00	384.3	1277.3

In Table 1. there is a comparison of the average throughput value. At 09.00, the average throughput value before Load Balancing is 456 Kbps which according to the TIPHON standard means sufficient, while after the implementation of Load Balancing the average throughput value is 1381.3 Kbps which according to the TIPHON standard is very good. At 1:00 p.m., the average throughput value before Load Balancing is 232.3 Kbps which according to the TIPHON standard means bad, while after the implementation of Load Balancing the average throughput value is 1052 Kbps which according to the TIPHON standard is good. At 16.00, the average value of throughput before Load Balancing is 384.3 Kbps which according to the TIPHON standard is sufficient, while after the implementation of Load Balancing the average throughput value is 1277.3 Kbps which according to the TIPHON standard is very good. To see the difference in value in more detail, here is Fig. 10. a comparison chart for the Throughput value.

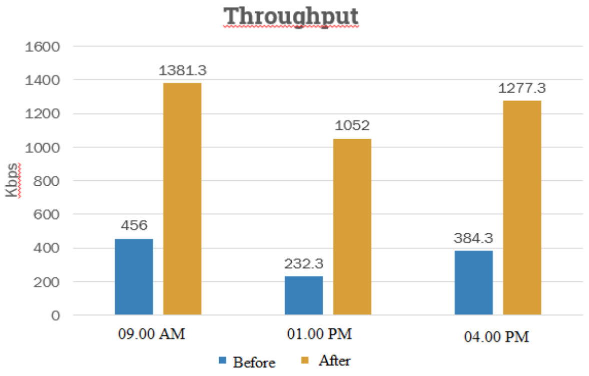


Fig 10. Throughput Value Comparison Graph

TABLE 2. COMPARISON OF AVERAGE DELAY

Time	Delay (ms)	
	Before	After
09.00	438	52.7
13.00	692.3	97
16.00	399.3	111

In Table 2, there is a comparison of the average delay values. At 09.00, the average delay value before Load Balancing is 438 ms which according to the TIPHON standard means moderate, while after the implementation of Load Balancing the average delay value is 52.7 ms which according to the TIPHON standard is very good. At 13.00, the average delay value before Load Balancing is 692.3 ms which according to the TIPHON standard means bad, while after the implementation of Load Balancing the average delay value is 97 ms which according to the TIPHON standard is very good. At 16.00, the average value of delay before Load Balancing is 399.3 ms which according to the TIPHON standard means moderate, while after the implementation of Load Balancing the average delay value becomes 111 ms which according to the TIPHON standard is very good. To see more details about the difference in value, here is Fig. 11. Comparison chart for Delay values.

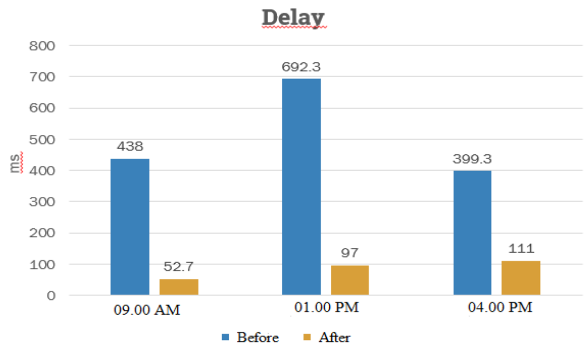


Fig.11. Comparison of Delay Value Graph

TABLE 3. COMPARISON OF AVERAGE PACKET LOSS

Time	Packet Loss (%)	
	Before	After
09.00	4	0
13.00	19	1.3
16.00	2.3	0

In Table 3 there is a comparison of the average packet loss values. At 09.00, the average value of packet loss before Load Balancing is 4% which according to the TIPHON standard means moderate, while after the implementation of Load Balancing the average value of packet loss is 0% which according to the TIPHON standard is very good. At 1:00 p.m., the average value of packet loss before Load Balancing is 19% which according to the TIPHON standard means bad, while after the implementation of Load Balancing the average value of packet loss is 1.3% which according to the TIPHON standard means good. At 16.00, the average value of packet loss before Load Balancing is 2.3% which according to the TIPHON standard means good, while after the implementation of Load Balancing the average packet loss value becomes 0% which according to the TIPHON standard is very good.

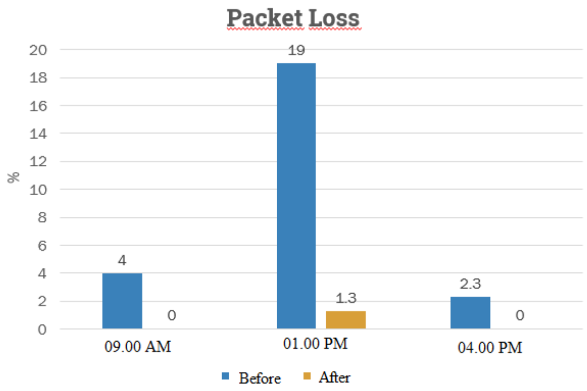


Fig. 12 Comparison Chart of Packet Loss Value

V. Conclusion

The Load Balancing system can share the connection path equally at ISP-1 and ISP-2 at the Riau Province Library and Archives Service based on the request packet so that it does not only burden one ISP. The implementation of the Load Balancing system can solve the problem when one of the ISPs experiences a disconnection. It can be seen from the automatic connection switching to an active ISP gateway, so that network performance continues to run normally. The throughput test in the morning, afternoon, and evening shows a very good change in value after load balancing is applied. The delay and Packet Loss tests also showed a change in value from bad to very good after the implementation of the Load Balancing system.

References

[1] Setiawan, Moh. Agus, “Implementation of load balancing on multihoaming ISPs using the Nth method", Informatics Management Study Program, State University of Surabaya, pp: 16, 32, 33, 2013.

[2] Julianto, Riski, Widhi Yahya, and Sabriansyah Rizqika Akbar, "Implementation of load balancing on the WEB server using CPU resource-based methods in software defined networking" Vol.1, No.9, Journal of Information Technology Development and Computer Science, 2017.

[3] Altayeb, Dina Farouk, dan Fatima Abdelghani Mustafa, “Analysis on load balancing algorithms implementation on cloud computing environment”, Vol.6, No.2. International Journal of Innovative Research in Advanced Engineering, pp: 1-5, 2019.

[4] Kunamneni, Venubabu, Dynamic Load Balancing for the Cloud. Vol. 1, No.1, International Journal of Computer Science and Electrical Engineering, pp: 1-5, 2019.

[5] Fauzi, Alan, Alex Wijaya, and Irman Effendy, Implementation of Load Balancing Peer Connection Classifier (PCC) on the Internet Network at the Prabumulih Regional General Hospital, Binadarma Journal, pp: 1-10, 2017.

[6] Gene, Eudes Raymond, Implementation of Load Balancing with Two ISPs Using the Nth (Nth Connection) Method and the Peer Connection Classifier (PCC) on Mikrotik. Essay, Informatics Engineering Study Program, Sanata Dharma University, pp: 1-77, 2018.

[7] Firdaus, Muhammad Iqbal, "Comparative analysis of load balancing performance with ECMP (Equal Cost Multi-Path) method with PCC (Peer Connection Classifier) method on mikrotik router OS", Vol. 8, No.3, Technologia. pp: 1-6, 2017.

[8] Haryanto, Muhammad Dedy, and Imam Riadi, "Network analysis and optimization using load balancing techniques". Vol.2, No.2, Journal of the Bachelor of Informatics Engineering, pp: 1-9, 2014.

[9] Wednesday, Jefry Alvonsius, Joko Purwadi, and Willy S. Rahajo, "Implementation of web server load balancing using the LVS-NAT method", Vol. 8, No.2, Yogyakarta, 2012.

[10] Ryanto, Leo, "Analysis and design of computer networks using bandwidth management load balancing and website blocking at PT.Onitsuka management consulting", Informatics Management Study Program, Bina Nusantara University, 2017.

[11] Zamzami, Nurul Fadilah. "Implementation of load balancing and failover using mikrotik router OS based on multihomed gateways at internet cafe" Diga ", pp: 1-12, 2010.

Received: January 30, 2021 | Revised: February 17, 2021 | Accepted: February 24, 2021