East Asian Journal of Multidisciplinary Research (EAJMR)
Vol. 2, No. 1, 2023 : 249-262

A Hotspot Server and Two Line ISP Load Balance and Failover Using the Mikrotik RB951UI 2HND with PCC Method

Muhammad Khaerudin[1], Andy Achmad Hendharsetiawan[2]*, Asep Rhamdani Mahbub[3], Tukino[4], Siti Setiawati[5]
[1,2,3,5]Fakultas Ilmu Komputer, Universitas Bhayangkara
[4]Fakultas Teknologi dan Ilmu Komputer dan Sistem Informasi, UBP Karawang
Corresponding Author: Andy Achmad Hendharsetiawan
andy.achmad@dsn.ubharajaya.ac.id

A R T I C L E I N F O

Keywords: Load Balancing, Failover, Hostpot, Per Connection Classifier

Received : 05 November
Revised : 05 December
Accepted: 05 January

A B S T R A C T

When one connection fails, failover makes sure the connection is always available, and the hotspot server can make it simpler for customers to access the internet with a username and password. The loss of an internet connection, a slow connection, and output that is insufficient for your bandwidth are some common issues with the internet network. Managing hotspot servers is less of a worry for many schools and colleges, as they often just use one ISP (internet service provider) connection. The drawback of employing a single line ISP is that blended learning-based lectures will currently cease to exist if the ISP goes down. Therefore, the Mikrotik RB951Ui can do load balancing, failover, and hotspot server management. When using the Per Connection Classifier (PCC) method, which in this study was successful in overcoming the aforementioned issues, the internet connection became stable because the load was split between the two ISPs, and when the internet at one of the ISPs went down, there were still other connections that backed up. Additionally, there is a wifi hotspot management system that uses a username, password, and bandwidth restrictions for each user.

DOI: https://10.55927/eajmr.v2i1.2591
ISSN-E: 2828-1519
https://journal.formosapublisher.org/index.php/eajmr/index

INTRODUCTION

The process of allocating tasks to different resources is known as load balancing. The optimum performance for network users is delivered by this load balancing, which switches session sessions and processes operations on other servers to help the network avoid prolonged downtime. Failover, or changing the connection to an alternative path, happens when a system, piece of hardware, or network fails. In public spaces like libraries, campus parks, and other locations, Wireless LAN technology is used through the creation of hotspots. Because these techniques can make it simple and comfortable to access the internet network, the usage of load balancing, failover, and hotspot servers is intimately tied to the internet network. By distributing the load among numerous Internet service providers, load balancing makes guarantee that no internet service is overextended on a single provider. When a connection drops, the hotspot server can make it simpler for users to access the internet with a username and password. The connection is always available thanks to failover.(Pradana, Purboyo, and Latuconsina 2019)

Due to the fact that today's primary instrument for facilitating learning and teaching is the internet, internet network issues regularly arise. These include poor connections, dropped internet connections, and output that isn't enough to fill your capacity. Some formal educational organizations, like schools and even colleges, only use one ISP (internet service provider) line to manage hotspot servers. The drawback of employing a single ISP is that if the ISP goes out of business or passes away, all online administrative and educational activities will cease to function. Students and students must have internet connectivity while on campus because contemporary school activities and lectures have begun merging offline learning with online learning, commonly known as blended learning method learning activities. Of course, if the network administrator just uses one ISP connection line and there is no hotspot server control, there could be a significant issue.(Ardianto, Alfaresi, and Darmadi 2018)

Education providers, such as schools and campuses, can use the Hostpot Server and the two-line internet connection method from two ISPs by using the PCC method and the load balancing technique with the Mikrotik RB951Ui router in order to get around the problems that frequently occur on the internet network. Its goal is to split up incoming data to network devices so that it can be split over several ISPs, used to increase throughput, and prevented from congested on a single connection line. A failover approach will also be used in this study, enabling the backup ISP to assume control of and maintain all network traffic in the event that the primary ISP fails. For enterprise-wide TCP/IP services like the Web, Terminal Services, proxies, virtual private networks (VPNs), and streaming media, network load balancing offers scalability and high availability. Businesses using TCP/IP services, such as e-commerce systems that link clients to transactional applications and back-end databases, benefit particularly from network load balancing.(Mishra 2015)

THEORETICAL REVIEW

Load Balancing

The concept of load balancing is used to balance the load or load on an organization using the IT infrastructure. to combine various resources so that everyone can utilize it to the fullest extent possible for Internet service providers. As computer networks scale up and experience a dramatic increase in data flow, networking becomes increasingly important. Load balancing, or balancing the load on the network, will be essential whenever something similar happens. By allowing access to network resources that are dispersed across multiple other networks rather than being centralized, service load balancing improves the overall reliability and consistency of computer network performance.(Rahman et al. n.d.)

Failover

The failover strategy is used to prevent issues caused by a rise in traffic brought on by the strain of managing numerous requests from Internet Service Provider users. In the event that one of the devices or the network from the internet service provider malfunctions, there is still one supplier of internet service devices that may be used as a backup or substitute.(Suwito 2022)

Hotspot

A wireless standard is hotspot. Only the proper components can connect to a network that runs without wirles. DNS, DHCP, Proxy, and Firewalls are just a few of the technological features that a hotspot server incorporates. However, you don't need to worry about the complexity of the functions when setting up a Hotspot server because Mikrotik will provide assistance in the form of a Setup Wizard.

Network Monitoring

In a computer network, various computers are connected to one another. Each computer has unique resources that it pooled with the power of other computers. Occasionally, the administrator must identify the root reason of a severe network slowdown. An administrator needs to keep an eye on the network in order to monitor data flow on it effectively.(Setyawan 2014)

METHODOLOGY

According to research by S. Dhakal, M. and colleagues, the analytical model for one-shot load balancing based on regeneration theory has been validated by comparing the outcomes of real-time load balancing experiments conducted via a two-node wireless LAN network with a Monte Carlo simulation. Our findings demonstrate that, regardless of the initial workload distribution and processing speed(Pradana, Purboyo, and Latuconsina 2019). The first step in performing this research is gathering data by conducting interviews regarding network topology, network architecture, and management, as well as by looking at the current network infrastructure to

identify any issues. After that, a problem analysis is conducted, and various potential remedies are suggested, including (Hidayat et al. 2021)

Proposed Network Scheme

The addition of one Internet service provider (ISP) service from an existing ISP provider is an alternate network design. With the inclusion of the ISP, it will act as a backup internet line such that, in the event that the first ISP experiences a connection drop, the backup ISP will take over the first ISP's position without further action from the user. Applying a feature method in the Mikrotik Router called the failover technique, a feature method in the Mikrotik Router called Load Balancing PCC, as well as network administration utilizing a mikrotik hotspot, are required to produce a solution that can function properly. As a result, the process of teaching and learning won't be disrupted if there are issues.(Riskiono and Pasha 2020)

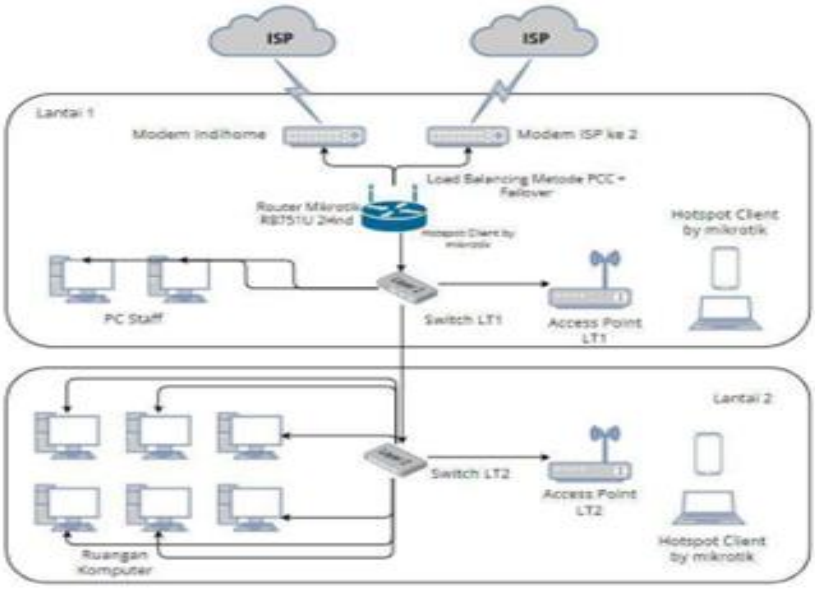

Figure 1. Proposed Computer Network Schematic

Figure 1 can utilize two ISP lines with load balancing, depending on the technique utilized. All user requests will be handled by a router that has been set up for load balancing by splitting the traffic load between two gateways simultaneously, and they will be routed to either the ISP-1 line or the ISP-2 line in accordance with the regulations on the mangle.(Suwito 2022)

Per Connection Classifier (PCC)

Data packets can be assigned to a specific connection gateway using the Per Connection Classifier (PCC) technique. PCC classifies the groupings of connection traffic going through or leaving routers. By using the src-address, dst-address, src-port, and/or dst-port, one can identify this grouping. For the next relevant data packet to be sent on the same gateway path as the previous data packet, Mikrotik will remember the gateway path that connection traffic first traveled through.(Octavriana, Joni, and Ibadillah 2021)

Flowchart Design

A flowchart is a chart that describe the sequence of processes in detail and the relationship between a process and the process others in a program, where on the flowchart there are also symbols that has its own function (Imaniawan 2019)

Figure 2. The flowchart was created by Mikrotik

Figure 2 This study's proposed Mikrotik Configuration Flowchart serves as the flowchart design. Description: Open the Winbox program in the Neighbors column as the first step. Choose the Mikrotik Mac Address that belongs to Microtik. Using Winbox, log in with your Mikrotik username and password. When you log in successfully, the screen will look like the one below

Implementation

The winbox program must first be opened in the Neighbors column. Choose the Mikrotik Mac Address that belongs to Microtik.

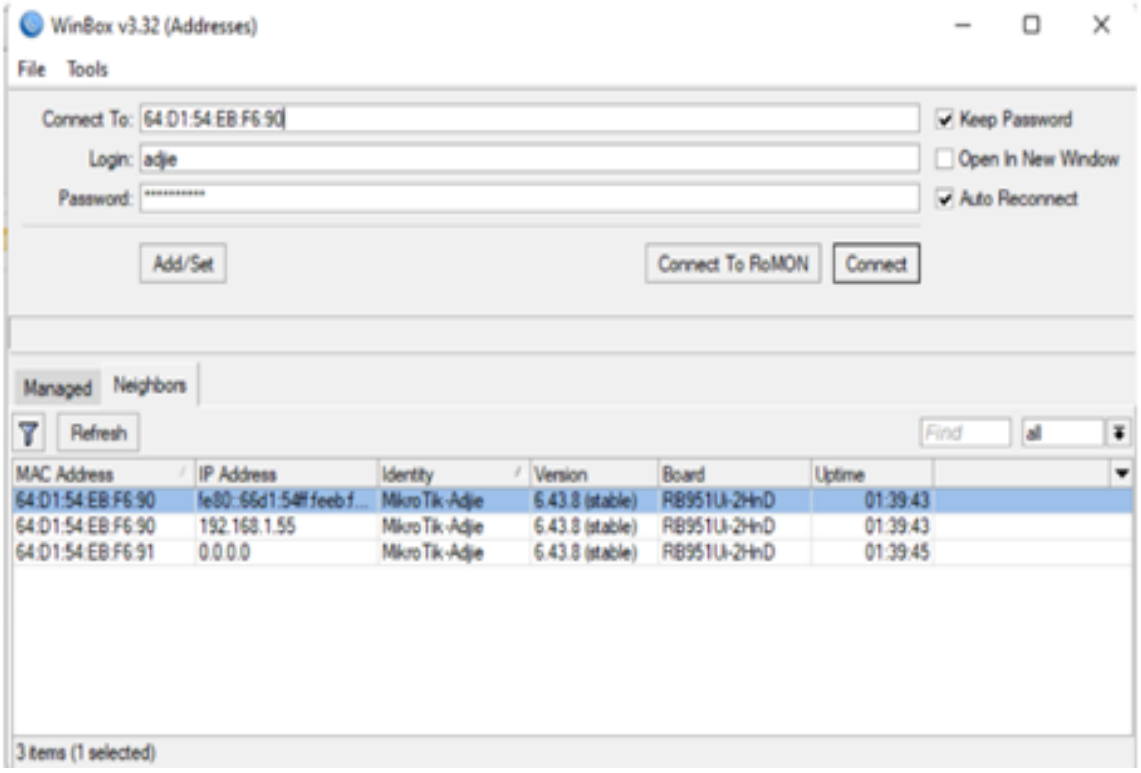

Figure 3. Winbox login for Mikrotik

Figure 3 using a username and password to log in. Windows-based software called Winbox is frequently used for configuring proxies. Why can you still use Winbox with converter programs like Wine and others if your operating system is Linux or macOS even though it is Windows-based? Winbox is inherently incompatible with Linux OS and Mac OS without converter software, such as wine and others. When you log in for the first time, a menu titled RouterOS Default Configuration will show up. Since each routerboard is unique depending on the type of device it is, when using Winbox for the first time, the routerboard already has a factory default configuration, also known as RouterOS Default Configuration.

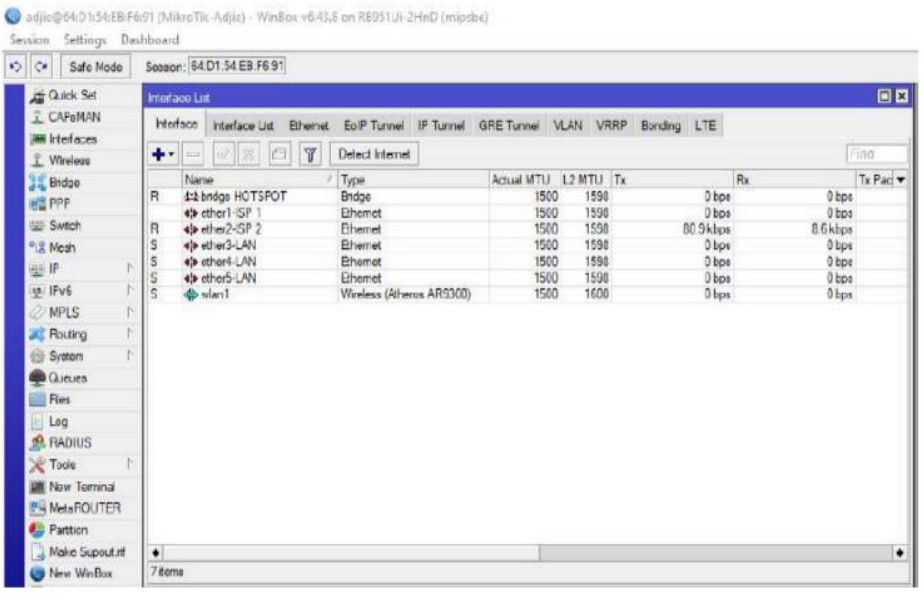

Figure 4. Configure Interface Name

Figure 4 Once you have successfully logged in, you will see the screen below. Configure the ether3, ether4, ether5, and wlan1 interfaces as members of the bridge for Bridge-Hotspot.

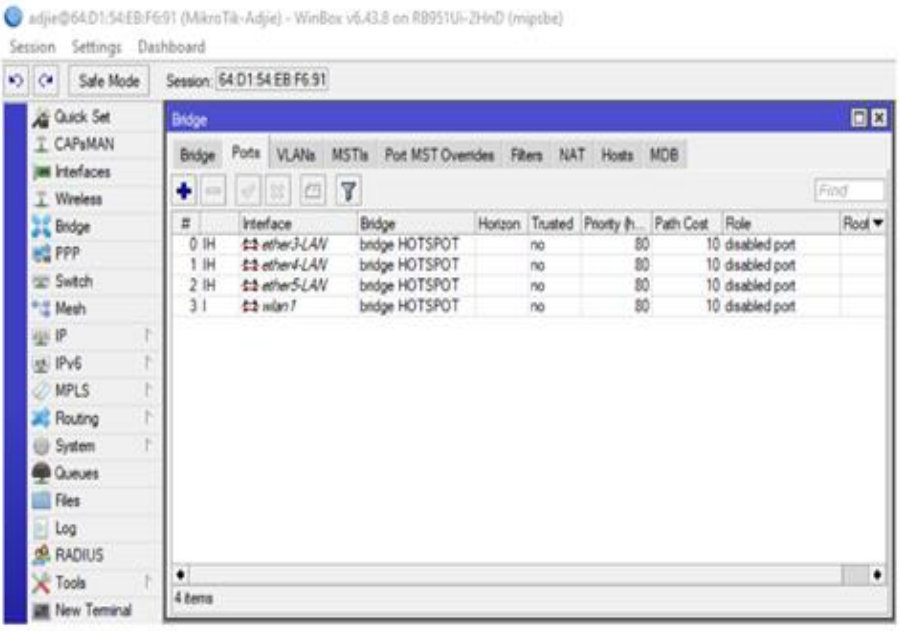

Figure 5. Interface Bridge Configuration

Figure 5 Then, set up the bridge interfaces for the Bridge-Hotspot. The Wlan1 interface can then be configured by clicking on it and choosing the Wireless submenu. The parameters are then as follows.

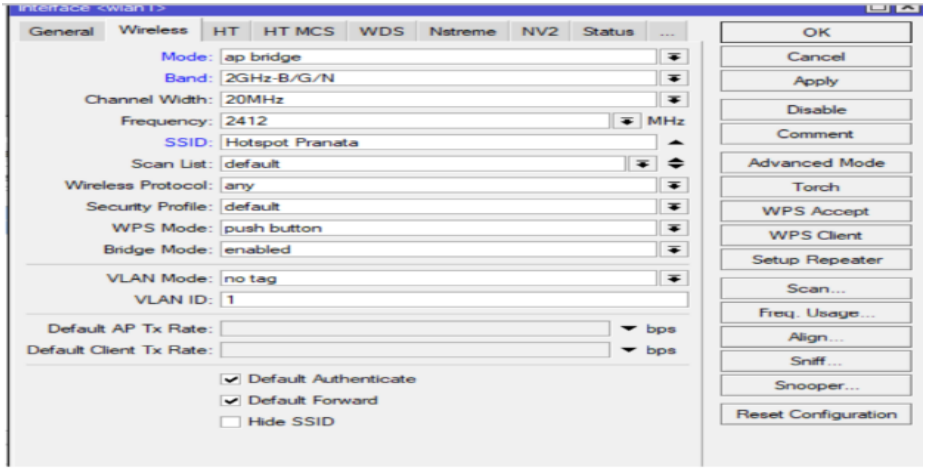

Figure 6. Configure Wlan1 Interfaces

Figure 6 By selecting the Wireless submenu from the Wireless menu and clicking on the Wlan1 interface, you may configure the interface. To generate a WiFi password in MikroTik, click here. Due to the fact that we will use it by connecting the MikroTik wireless to SSID HOME with Password 12345678. When the wifi functionality is activated, we use the Scan function. Scan is used to establish a connection between the proxy wifi and one of the desired SSIDs.

Testing

The results of the guest user's speedtest and hotspot login are displayed in Figure. The result achieved by the Speedtest User is

Figure 7. User Speedtest Results

Figure 7 The results of the guest user's speedtest and hotspot login are displayed in Figure. The result achieved by the Speedtest User is.

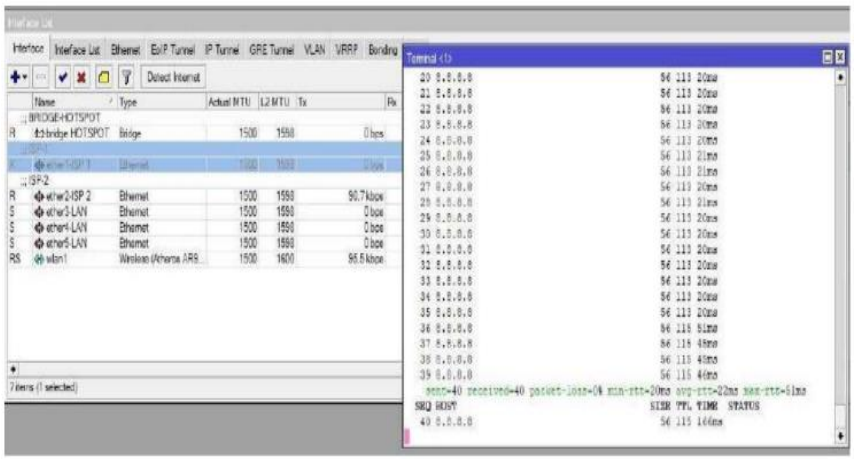

Figure 8. Test turn off ISP interface 1

Figure 8 The results of the built-in failover configuration confirm what was predicted. As seen in the accompanying figure Test turning off the ISP1 interface, the internet will quickly switch to ISP2 after the ISP1 interface is turned off.

RESULTS

PCC Internet Load Balancing Test Results

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

00 Reset Counters | 00 Reset All Counters

#	Action	Chain	Src. Address	Proto...	Sr...	Dst....	In. Interface	Out. Int...	Bytes	Packets	Dst. Address
0	mark connection	prerouting					bridge HOTSPOT		416.7 KiB	3 869	
1	mark connection	prerouting					bridge HOTSPOT		409.1 KiB	3 884	
2	mark routing	prerouting					bridge HOTSPOT		19.1 MiB	66 712	
3	mark routing	prerouting					bridge HOTSPOT		9.1 MiB	66 167	
4	mark connection	prerouting					ether1-ISP 1		519.3 KiB	2 813	
5	mark connection	prerouting					ether2-ISP 2		144.6 KiB	1 145	
6	mark routing	output							683.0 KiB	4 501	
7	mark routing	output							695.3 KiB	4 552	

Figure 9. PCC Work Load Balancing Results

Figure 9 Here is the result of PCC load balancing, showing Bytes and Packets Filled indicates Traffic has been skipped on both ISP 1 and ISP 2 interfaces

Examine The Graph Results For Each Interface

The following findings were obtained from the monitoring statistics graph produced by ISP1, ISP2, and Bridge1 Hotspot.

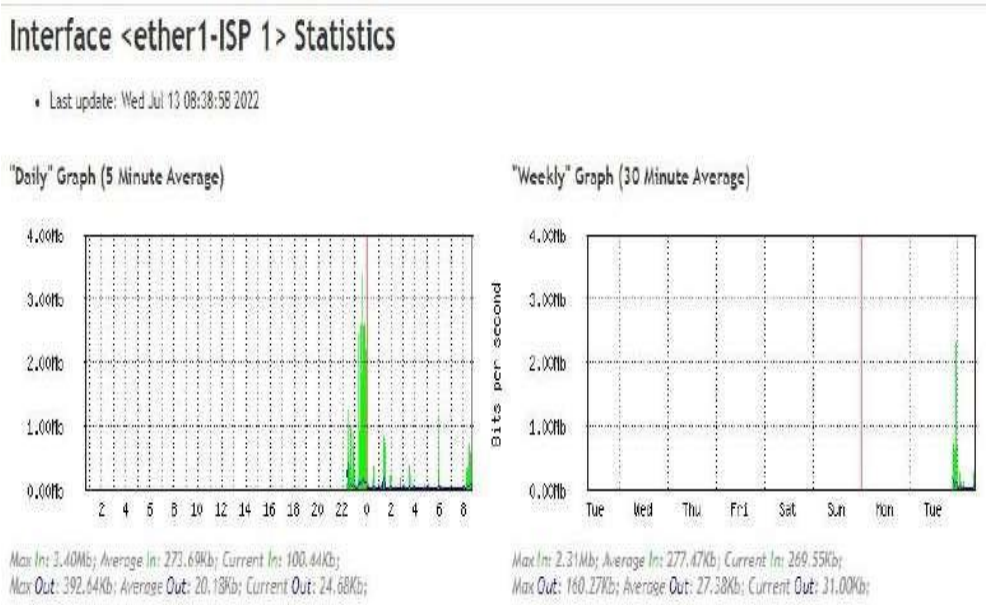

Figure 10. Monitoring data graph for ether1-ISP1.

Figure 10 Whether the bandwidth obtained is consistent with the bandwidth service information from the ISP or just records bandwidth usage statistics by the client, the network administrator must record bandwidth usage for reporting purposes. The network administrator can utilize the "Graphing" feature on MikroTik to capture data in graph format.

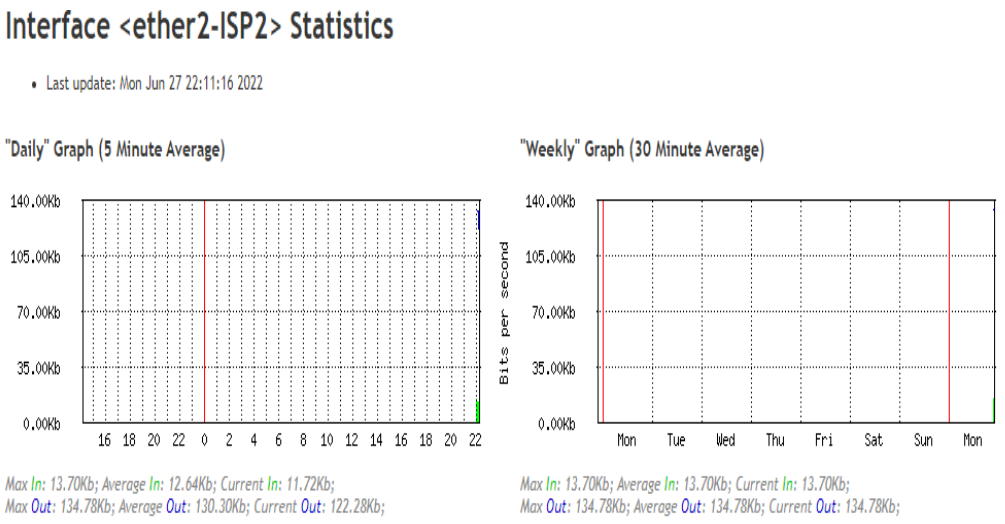

Figure 11. Monitoring data graph for ether2-ISP2

Figure 11 The author performs testing by downloading files and keeping track of both ISPs. It is evident from the two traffic coming from each interface, ISP 1 and ISP 2, that there is strong connectivity at each gateway, as evidenced by interface traffic ether 2.

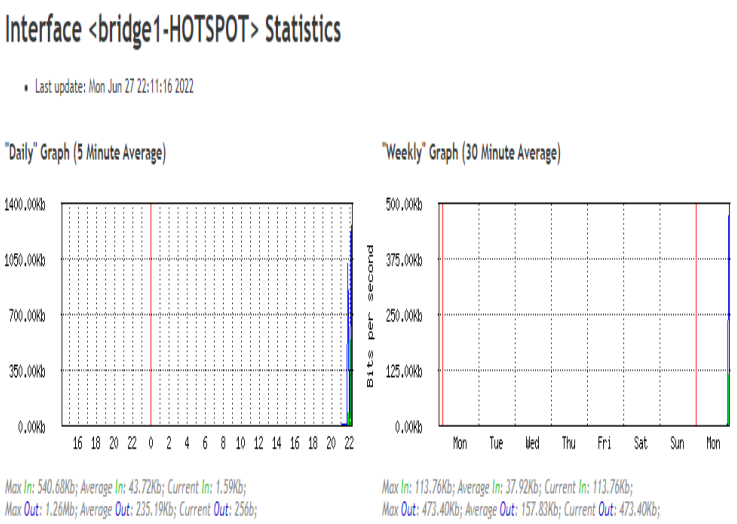

Figure 12. Graph of Bridge1-HOTSPOT monitoring statistics

Figure 12 A list of host connectivity statuses is displayed. Every minute, the system will check the host's connectivity. Users can only view the host's active specifications.

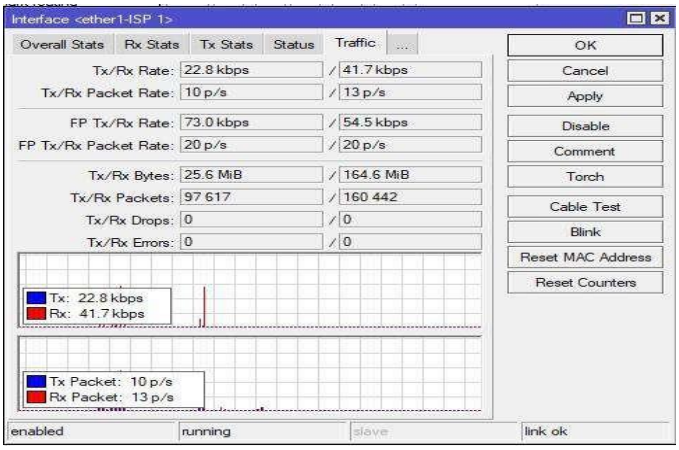

Figure 13. Graph interface data for ISP1 (ether1)

Figure 13 check using the basic Mikrotik PC program for bandwidth tools. Description To calculate the transfer speed during the bandwidth test, use the interface. In bps (bits per second). The previous client and the Bandwidth test server must be able to communicate using an IP Address as the primary requirement. The router will create traffic with the highest speed possible in accordance with the local and remote tx speed values if the local and remote tx speed values are supplied. In the meanwhile, the router will attempt to create traffic up to the device's capabilities limit or the maximum traffic that may be passed over the connection path if the values for both are not set

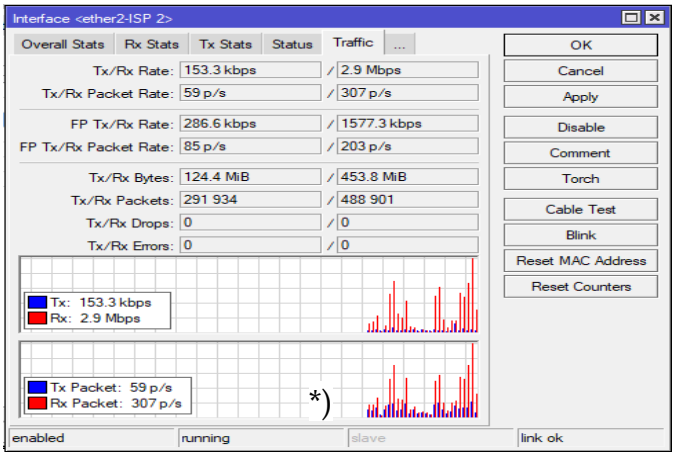

Figure 14. Graph interface ether2-ISP2 statistics

Figure 14 explains why traffic on bandwidth used to visit news websites is routed past ISP2 with the IP address 192.168.1.1. This happens because one of the gateways at one of the ISPs, specifically ISP1, has been turned off so that when tracert is run, ISP2 may still conduct backups. Shows static monitoring being done to view internet traffic on Mikrotik devices (ISP-2) when necessary. For our purposes, it is crucial to determine how much traffic is entering or leaving the network device's port.

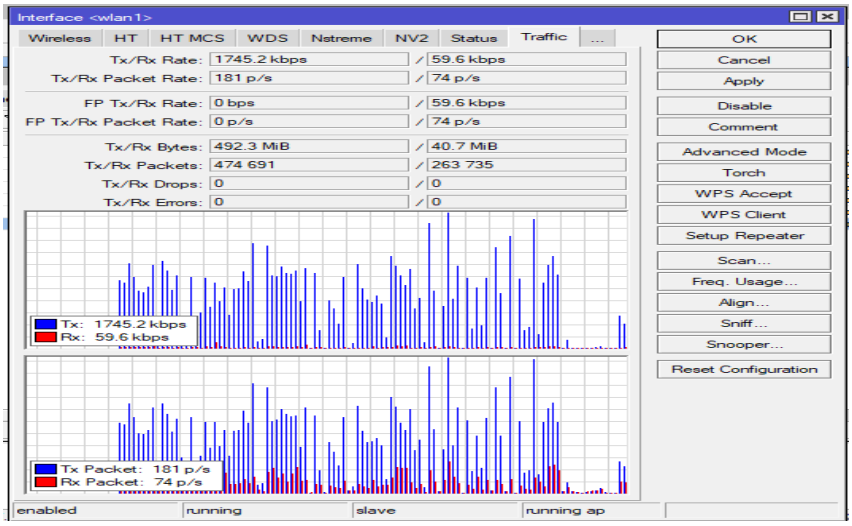

Figure 15. Graph interface statistics WLAN1

Figure 15 shows the results of a test using the Mikrotik Bandwidth Test program to determine the bandwidth graphs present in Wireless LAN1 (WLAN1). The client computer should then download data to computer 1 after that. download to computer 2 next. If the download was previously done alternately, then perform the download simultaneously to check how the bandwidth is distributed. An overview of the network is given by the WLAN Traffic Statistics Tool. The amount of network traffic as a percentage of observed packets is shown in the top frame. Finding out who is the most active in the neighborhood can be made easier with the help of this information.

DISCUSSIONS

The results of the Failover Configuration's implementation are as anticipated. Deactivate the ISP1 interface. When ISP1's interface is turned off, the internet will immediately switch to ISP2 and vice versa. The internet connection also saw no downtime. After turning off the ISP1 interface and the ISP2 interface, Ping results were also received. Bytes and Packets are full, indicating that Traffic has been passed on both ISP1 and ISP2 interfaces, indicating that the PCC Load Balancing setup has completed load balancing on both ISPs. Positive results are shown in the monitoring graph for each proxy interface; each interface has a statistical log, which shows that traffic is flowing normally.

CONCLUSIONS AND RECOMMENDATIONS

The results of the Failover Configuration's implementation are as anticipated. which the test image demonstrates When the ISP1 interface is turned off, the internet will automatically switch to the ISP2 interface, and vice versa. The Ping Results graphic shows that there is virtually no downtime on the internet connection after turning off the ISP1 interface and images. Ping results after shutting off the ISP2 interface. As seen in the image, it can be noticed that Bytes and Packets are full, indicating that Traffic has been passed on both ISP1 and ISP2 interfaces, demonstrating that the PCC Load Balancing configuration had successful results for load balancing on both ISPs. PCC Workload Balancing When the monitoring graphs for each proxy interface are examined, it is clear that traffic is flowing normally because each interface has a statistical log. can be observed in the ether1-ISP1 interface statistics graphic, the ether2-ISP2 interface statistics graph, the bridge1-HOTSPOT monitoring statistics graphic, the WLAN1 statistics interface graphic, and the ether1-ISP1 interface statistics graph

FURTHER STUDY

Select an ISP (Internet Service Provider) with a strong network reputation and support as both the Primary ISP and the Backup ISP. In this experiment, two line ISP + Failover + Hotspot server load balancing techniques were used. Perhaps in later research, a separate load-balancing system can be added to a three-line ISP or utilized in conjunction with a hotspot server.

ACKNOWLEDGMENT

The author would like to thank all parties, especially the academic community at Bhayangkara University, Jakarta, who helped morally in completing this paper.

REFERENCES

Ardianto, Feby, Bengawan Alfaresi, and Agus Darmadi. 2018. "RANCANG BANGUN LOAD BALANCING DUA INTERNET SERVICE PROVIDER (ISP) BERBASIS MIKROTIK." *Surya Energy* 3: 198–202.

Hidayat, Aziz Setyawan, Andrian Eko Widodo, Aryo Kencono, and Yamin Nuryamin. 2021. "Implementasi Load Balancing Dengan Metode PCC Pada Balai Besar Pelatihan Kesehatan (BBPK) Jakarta." 9(1).

Imaniawan, Fabriyan Fandi Dwi. 2019. "Rancang Bangun Aplikasi Penjualan Material Bangunan." *Indonesian Journal on Software Engineering (IJSE)* 5(2): 101–12.

Mishra, Ms Arti. 2015. "Network Load Balancing and Its Performance Measures." 3(1): 77–81.

Octavriana, Tania, Koko Joni, and Achmad Fiqhi Ibadillah. 2021. "OPTIMALISASI JARINGAN INTERNET DENGAN LOAD BALANCING PADA HIGH TRAFFIC NETWORK." *Jurnal Teknik Informatika* 14: 28–39.

Pradana, Andika Malraherawan, Tito Waluyo Purboyo, and Roswan Latuconsina. 2019. "ANALISIS LOAD BALANCING PADA JARINGAN SOFTWARE DEFINED NETWORK (SDN) MENGGUNAKAN ALGORITMA JARINGAN SYARAF TIRUAN (JST) LOAD BALANCING ANALYSIS ON SOFTWARE DEFINED NETWORK (SDN) USING ARTIFICIAL NEURAL NETWORK (ANN) ALGORITHM." 6(1): 1393–1400.

Rahman, Taufik, Eko Sulistianto, Aji Sudibyo, and Bambang Wijonarko. "Per Connection Classifier Load Balancing Dan Failover MikroTik Pada Dua Line Internet." : 195–209.

Riskiono, Sampurna Dadi, and Donaya Pasha. 2020. "ANALISIS METODE LOAD BALANCING DALAM MENINGKATKAN KINERJA WEBSITE E-LEARNING." 14(1): 22–26.

Setyawan, Raden Arief. 2014. "Analisis Implementasi Load Balancing Dengan Metode Source Hash Scheduling Pada Protocol." 8(2): 204–8.

Suwito, Muhammad Raka. 2022. "Analisis Dan Perancangan Load Balancing Dengan Metode Nth Menggunakan Mikrotik Studi Kasus Smk Bina Harapan Sleman." XVII: 17–25.