https://doi.org/10.32815/jitika.v20i1.1198

Volume 20, Issue 1, 2026

Jurnal Ilmiah Teknologi Informasi Asia

Journal Homepage: https://jurnal.asia.ac.id/index.php/jitika

Article

Implementation of PCC Load Balancing and Failover Using Mikrotik CHR on Virtual GNS3

Novellza Arfedin Abraara, Mufidatul Islamiyah*

Department of Computer Systems, Faculty of Technology and Design, Institut Teknologi dan Bisnis Asia Malang, Malang City, 65113, Indonesia

***Abstract*—The rapid development of network technology demands a reliable, efficient system capable of providing continuous, uninterrupted service. One important aspect of achieving this goal is implementing a load-balancing method that distributes network traffic evenly. In this study, a PCC (Per Connection Classifier) was designed and integrated with a failover mechanism to improve network performance and availability. The PCC method is used to dynamically divide traffic based on connections, while the failover mechanism functions as an automatic backup system in the event of disruption to the main path. The design results indicate that combining PCC and failover can increase reliability, improve load distribution, and minimize downtime in the network structure. This implementation is expected to serve as a reference for the development of a more stable and efficient network infrastructure. Test results show that applying the PCC and failover method can increase average throughput by up to 35%, reduce latency by 20%, and accelerate connection recovery, with an average failover time of under 3 seconds. Thus, this design is proven effective in improving network reliability and internet service quality in multi-gateway systems**

Keywords*—*internet service provider; isp; load balancer; pcc; peer connection classifier.

1. Introduction

Internet connections often experience problems, such as slow connections (low speeds) when using the internet for a large number of users simultaneously. Implementing load balancing requires optimizing bandwidth capacity by adding bandwidth resources if one ISP experiences problems (Pasaribu, 2022). As many as 53.7% of Indonesians are recorded as active internet users (Amalia et al., 2023). This disrupts data delivery to the destination (receiver) due to asymmetric use of internet bandwidth among users. In addition, the current increase in internet usage is not balanced by a comparable increase in internet quality. Based on data from the Indonesian Consumers Foundation (YLKI), in 2021, there were 32% of complaints regarding internet connections suddenly being cut off, thus disrupting several businesses that use the internet (Hadi & Kaburuan, 2022).

The process of allocating resources to different resources is known as load balancing. Optimal network user performance is achieved by load balancing, which redirects sessions and processes operations on other servers (Khaerudin et al., 2023). The use of server load balancing and failover is closely related to internet networks. By distributing the load between multiple internet service providers (Khaerudin et al., 2023). Load balancing is one solution to mitigate overload, which can cause server failure. Load balancing can distribute the load

* Corresponding author.
E-mail Address: mufidatul@asia.ac.id (M. Islamiyah)

Author E-mail(s): NAA (tronic.space18@gmail.com), MI (mufidatul@asia.ac.id)
Digital Object Identifier 10.32815/jitika.v20i1.1198
Manuscript submitted 2 September 2025; revised 10 October 2025; accepted 11 October 2025.
ISSN: 2580-8397(O), 0852-730X(P).

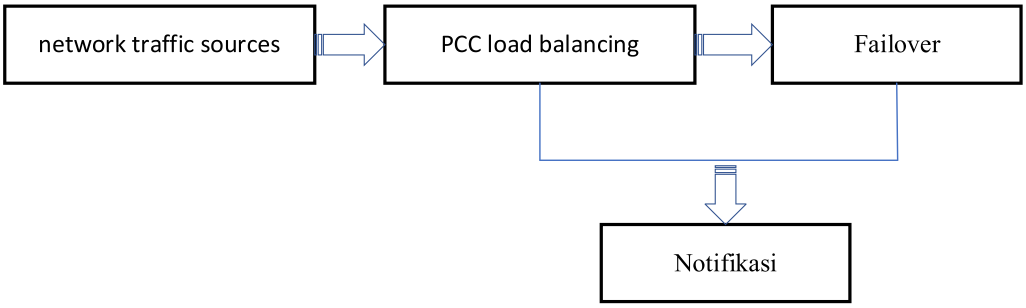

Fig. 1. Block diagram

appropriately across servers (Baeturohman & Banu Santoso, 2024). User characteristics can be leveraged through Internet channels, which can be optimized by implementing Load Balancing, a method for distributing data traffic workloads in a balanced manner. In Load Balancing, high availability refers to a method in which the Load Balancer maintains and uses, or takes over, processes that other load balancers perform as needed (Ariyana & Virdiyansyah, 2023).

Peer Connection Classifier (PCC) is a mangle option that sorts data within a stream and tags it for later identification. PCC divides incoming data into multiple streams and then uses these streams to sort traffic evenly. The PCC function, found in the "Mangle Facility," is used for internet connection traffic or streams (Ariyana & Virdiyansyah, 2023). The development of information technology has driven the growing need for reliable, highly available networks. Load balancing methods are widely used to distribute traffic to optimize network performance. However, traditional methods often overlook redundancy and failover, resulting in service disruptions when a line fails. The Per Connection Classifier (PCC) can dynamically partition traffic by connection but lacks an automatic failover mechanism. Therefore, a design that integrates PCC with failover is needed to improve the reliability and continuity of network services. This study aims to design and implement a load-balancing system based on a Per Connection Classifier (PCC) integrated with a failover mechanism, thereby improving the reliability, availability, and continuity of network services even in the event of a line failure.

2. Methodology

This research examines the Peer Connection Classifier (PCC) and Failover. Specifically, it examines the application of the Peer Connection Classifier method to managing network traffic load on each Internet Service Provider (ISP) (Hafizh & Sulistyo, 2024). PCC works by taking several fields from the IP header and TCP or UDP header, then with the help of a hashing algorithm, it will eliminate the output, which is obtained by adding up several IP header fields, after that, dividing it by a predetermined denominator, and the remainder, if compared with a certain remainder, then the packet will be captured (Wiharti et al., 2023). Here, the author briefly presents a block diagram of the research being conducted.

Fig. 1 shows a block diagram of the work that will likely be implemented in this research. The first step is Network Traffic Sources, which are internet sources that frequently experience slow internet speeds or downtime, whether in companies,

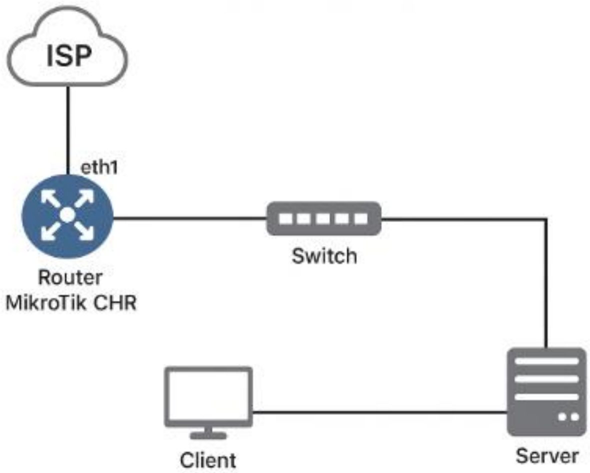

Fig. 2. GNS3 network topology with Mikrotik CHR router component as router

agencies, or residential areas. In the second step, to address the first problem, a PCC Load Balancer is needed. However, a PCC Load Balancer also has a weakness: when one Internet Service Provider (ISP) goes down, the PCC will automatically switch to another ISP. To address this weakness, a failover backup is needed.

2.1. Network topology design

2.1.1. GNS3 network topology

Fig. 2 shows a network topology designed in GNS3, with a MikroTik CHR router serving as the network control center. The MikroTik CHR router connects to the ISP via the ether1 interface as a WAN path and distributes connections to the local network via ether2, which is connected to the switch. The switch then connects several devices on the internal network, such as clients and servers, to enable communication among them and to provide internet access.

Several studies have examined load balancing and failover using Mikrotik using the Peer Connection Classifier (PCC) method on interconnections between two Internet Service Providers (ISPs). Research conducted by Nanang Sadikin and Fapriandi Rosyy Ramadhan shows that a load balancing system between two ISPs with failover can be directly applied (Wiharti

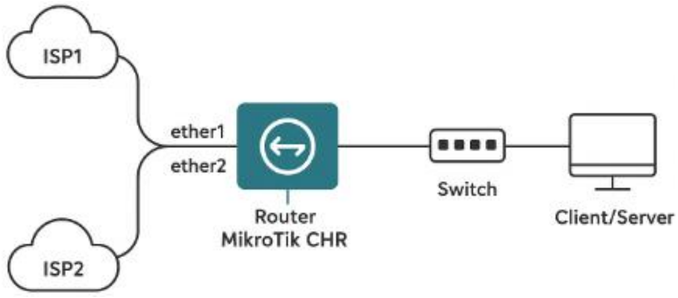

Fig. 3. Topology network on GNS3 with WAN connection components

et al., 2023). The PCC approach is used to divide incoming and outgoing network traffic from the router to the Group for optimization, and PCC is one of the load-balancing technologies that can be used (Iskandar et al., 2024).

2.1.2. Network topology on GNS3 with WAN connection components

This topology uses two WAN connections (ISP1 & ISP2) that enter the MikroTik CHR Router, then distribute the internet connection to the LAN via a switch. Fig. 3 shows a network topology designed in GNS3, with a MikroTik CHR router connected to two WAN interfaces: ISP1 on ether1 and ISP2 on ether2. These two internet paths are used for traffic distribution, load balancing, or failover. The MikroTik CHR Router then channels the connection to the local network through a switch that connects various user devices, such as clients and servers. This design allows for more optimal bandwidth distribution, higher service availability, and more efficient network traffic management.

Failover with a recursive Gateway is a method to test the gateway from outside the modem network or the ISP gateway. A simple example is when you have more than one ISP and one of the ISPs experiences problems; Mikrotik will indicate that the other ISP is not experiencing problems. This will happen if using the failover method; Mikrotik only pings the nearest gateway, namely the modem, even though the ISP is Down/off (Gusrion et al., 2022).

2.1.3. Network topology GNS3 with multiple client components (VM or cloud) to test traffic.

Fig. 4 shows the network topology design on GNS3 using a MikroTik CHR Router as the network control center. The MikroTik CHR Router receives connections from the ISP via the ether1 interface and distributes the network to the LAN via the ether2 interface, which is connected to the switch. The switch then connects several virtual devices (Client 1, Client 2, and Client 3) that are used to test network traffic. With this configuration, researchers can simulate measurements of bandwidth, latency, and connection stability between clients and the internet, thereby facilitating network performance analysis prior to implementation in a real system.

To support the distribution of internet access, a router is needed, in the form of a RouterBoard. In 1996, a type of RouterBoard called Mikrotik was introduced by Johnson and

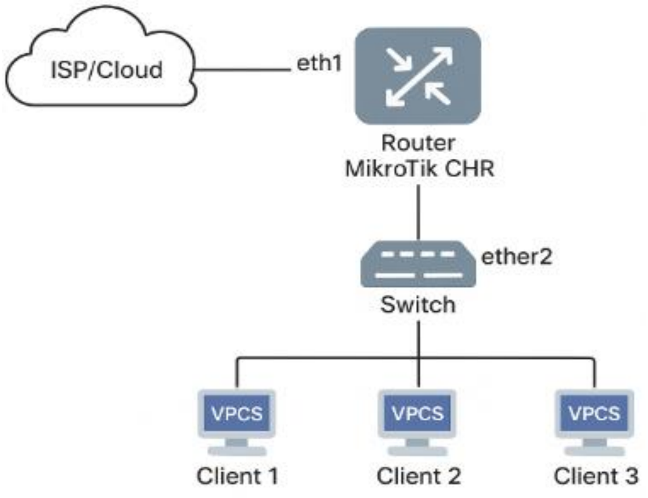

Fig. 4. Network topology on GNS3 with multiple client components (VM or cloud) to test traffic

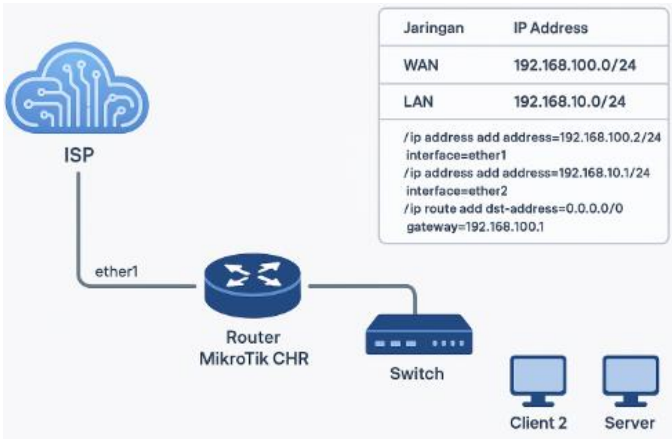

Fig. 5. Network topology in GNS3 with components creating clear IP

Armin, marking the beginning of Linux and MS-DOS. Some research on the analysis and problem solving of Mikrotik router network security, Network simulation using Mikrotik Router OS in a virtual network simulation, and relying only on computer devices (Bahtiar et al., 2021). Graphical Network Simulator 3 (GNS3) is a computer network simulation software with a Graphical User Interface (GUI), similar to Cisco Packet Tracer. However, GNS3 enables more complex network simulations by running on a native operating system (OS) directly on the network device, unlike Cisco and Juniper. In real-world situations, configuring a router directly differs from configuring it in Cisco Packet Tracer.

GNS3 is a useful supplementary tool for network laboratories, particularly for network engineers, administrators, and individuals preparing for certifications such as Cisco CCNA, CCNP, CCIP, and CCIE (Fitriani et al., 2020). VMware is a leading provider of virtualization solutions that offer features that support the backup and restore of the Operating System (OS).

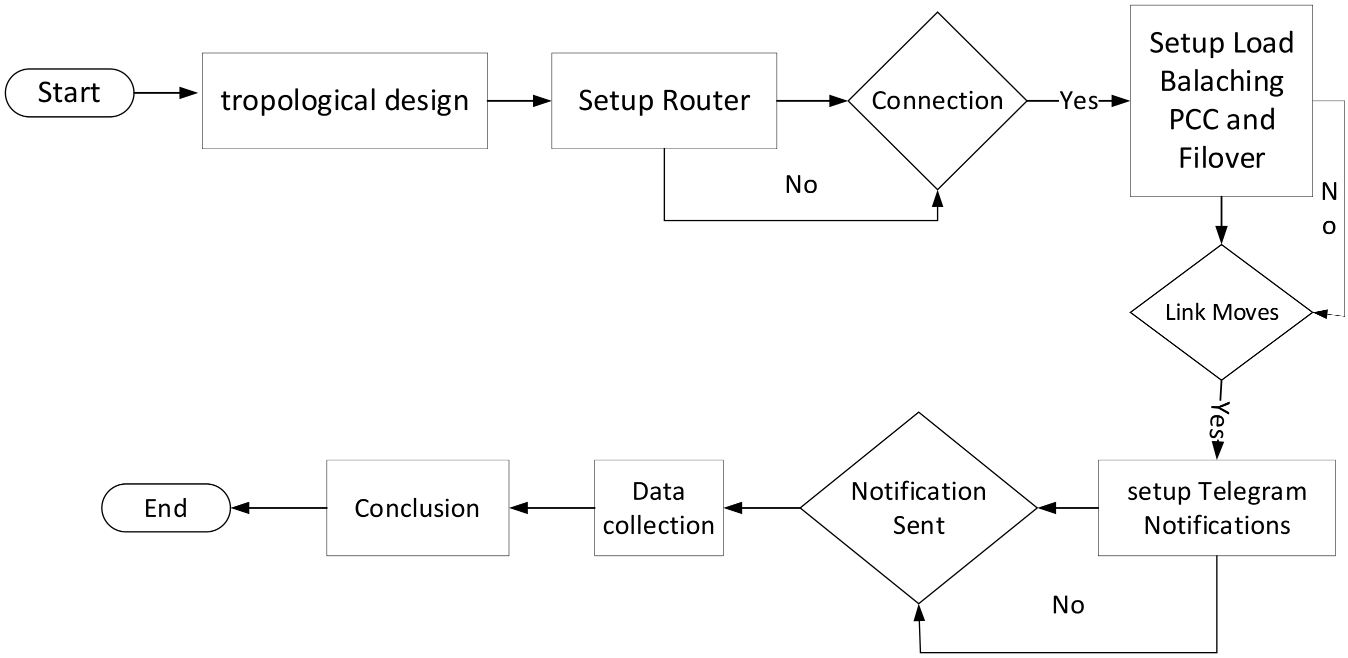

Fig. 6. Testing phase flowchart

One of VMware's flagship features is Snapshot, which allows the OS to be restored to its previous state quickly and efficiently, thus minimizing downtime and data loss (Rahman et al., 2024).

2.1.4. Network topology in GNS3 with components, creating clear IP addresses and routing schemes.

Fig. 5 illustrates a network topology simulated in the GNS3 environment, centered on a MikroTik Cloud Hosted Router (CHR) serving as the gateway. The architecture connects upstream to an ISP cloud via interface ether1 (assigned the WAN IP 192.168.100.2/24), while downstream connectivity is provided to a Switch supporting two end devices ("Client 2" and "Server") on the LAN subnet 192.168.10.0/24. The accompanying configuration inset explicitly lists the RouterOS commands used to configure these interfaces and establish a default static route (dst-address=0.0.0.0/0) pointing to the ISP gateway at 192.168.100.1, which is standard practice for enabling internet access for the local network.

2.2. Flowchart

2.2.1. Testing phase flowchart

The author explains a little in Fig. 6, which is a Flowchart of the research stage, in which the process the author carried out was designing the topology form he intended to use. After designing, setting up the Mikrotik Router OS, testing the Router OS connection, and setting up the PCC Load Balancing and failover.

2.2.2. Load balancing testing flowchart.

At this stage, the author conducted the testing process

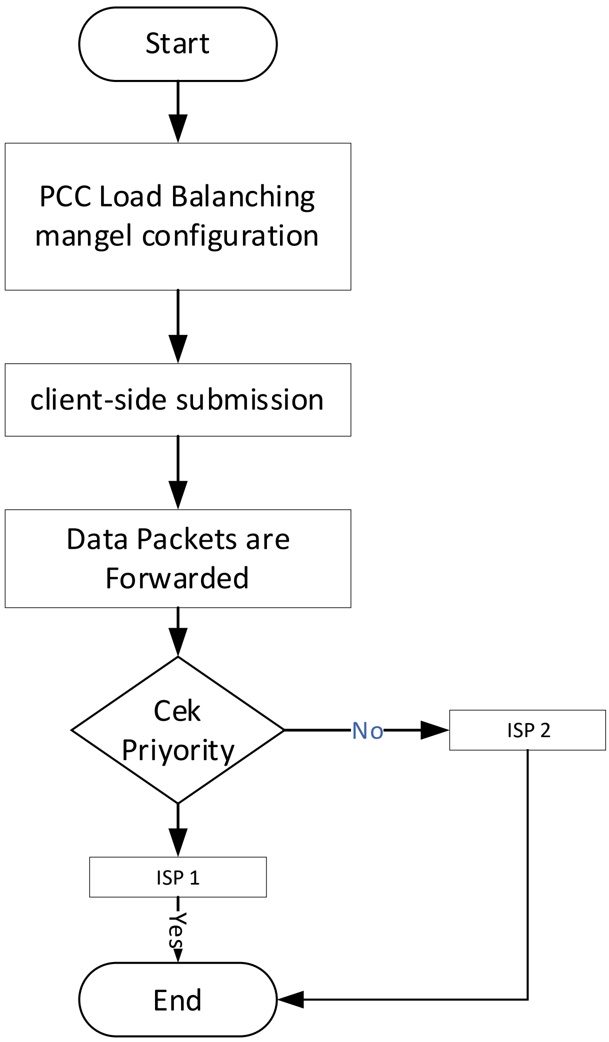

Fig. 7. Load balancing test

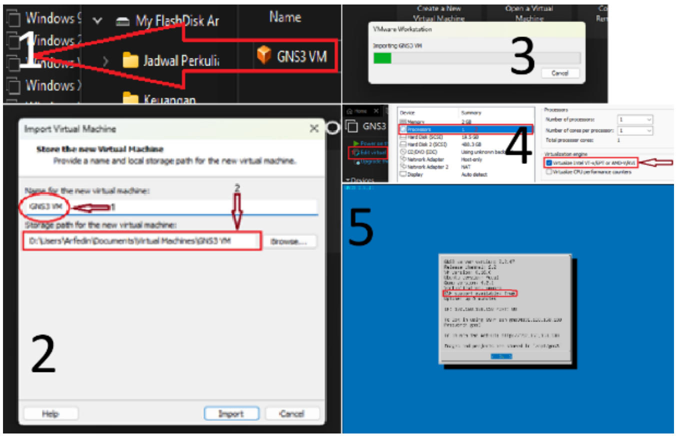

Fig. 8. Install GNS3 VM

Table 1. Interface of Each Router

NO	Tabel Interface Mikrotik		
	Interface	IP Address	Gateway
1	Ether 0 ISP 1	DHCP NAT	
2	Ether 1 ISP-1	192.168.100.1/24	192.168.100.1
3	Ether 0 ISP-2	DHCP NAT	
4	Ether 1 ISP-2	19.16.200.1/24	19.16.200.1
5	Ether 0 PCC	192.168.100.2/24	192.168.100.1
6	Ether 1 - PCC	19.16.200.2/24	19.16.200.1
7	Ether 2 - PCC	192.168.25.1/24	192.168.25.1

according to the flowchart in Fig. 7, which involves configuring load balancing on the MikroTik RouterOS in several steps. The first stage is configuring the manager; the second stage is configuring the PCC and failover. After that, the client is tested. The author also tested a virtual machine-based client. Load Balanching is one of the many features available on Mikrotik, whether in the form of RouterBoard or in the form of Router OS or Cloud Host Router (CHR), is a technique with the aim of distributing traffic loads on two or more Internet sources, in this case an Internet Service Provider (ISP), in a balanced manner and running optimally, by maximizing Delay, Latency, Packet Loss, Throughput and avoiding Overload on the connection path (Suwito & Lukman, 2022).

2.3. Installation and configuration.

After successfully installing GNS3, the author will briefly compare VMware and VirtualBox, with a focus on VMware.

2.3.1. VMware workstation.

VMware has a hosted architecture for visualizing I/O, allowing it to coexist with the host operating system, or in this case, our laptop/computer. This architecture consists of three main components: VMapp, VMDriver, and VMM. VMApp is a simple application that allows users to install other operating systems on it. This application uses a driver (VMDriver) that runs on the host operating system to grant access to monitor the virtual machine (VMM). This virtual machine runs directly on the hardware. (Nuryadin et al., 2023).

2.3.2. VirtualBox

Oracle VirtualBox is a virtualization software that can be installed on Windows, Linux, macOS, and Solaris. Using VirtualBox, users can create and run virtual machines on hardware, such as their laptops or desktop computers. This virtual machine allows users to run multiple operating systems simultaneously, whether the same or different from the host operating system. This enables users to run virtual machines on various modern hardware platforms. VirtualBox also supports KVM virtualization technology, which allows users to improve the performance of virtual machines on different hardware (Nuryadin et al., 2023).

2.3.3. Install GNS3 server.

Based on the author's previous explanation, it is more effective for the GNS3 VM server to run on VirtualBox because VMware's Snapshot feature is useful for Disaster Recovery (DR), offering significant advantages over other recovery methods.

At this stage, VMware must be used to install the GNS3 server. Why use VMware rather than VirtualBox, even though it is free? The GNS3 server the author uses is the latest version and is more stable when installed with VMware than with VirtualBox. The installation process can be seen in the Fig. 8.

3. Results

3.1. Internet protocol design

Internet Protocol (IP) or IP Address design is a system used to assign numeric addresses to identify connected devices. Each block of the IP address consists of four numbers separated by periods, and each number ranges from 0 to 255. At this stage, the author will describe the interface table along with the IP Address used for each Router OS (Ariyana & Virdiyansyah, 2023).

Table 1 shows each interface connection on each Router OS, and because we use 3 Router OS, each of which has its own role, you can see the topology display that the author uses in Fig. 9.

It can be seen in Fig. 10 that the topology that the author uses, among others, starts from the top, which is the internet source, then connected to two Router OS below using a Switch, after that, from each Router OS, it is connected again to the router OS below it directly, then distributed again to each client below it. The following presents the router OS for each router.

3.2. Mikrotik CHR configuration

Next, the author will configure the Mikrotik CHR, especially the Mikrotik PCC.

3.2.1. Mikrotik CHR ISP-1 configuration

a. IP Assignment.
   Configuring ISP-1 is straightforward. First, assign an IP

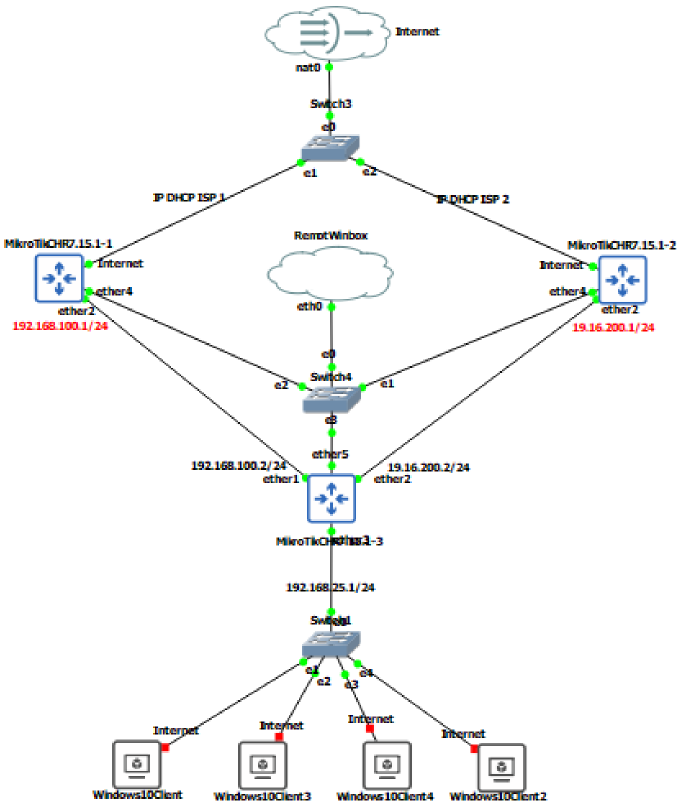

Fig. 9. Topology used

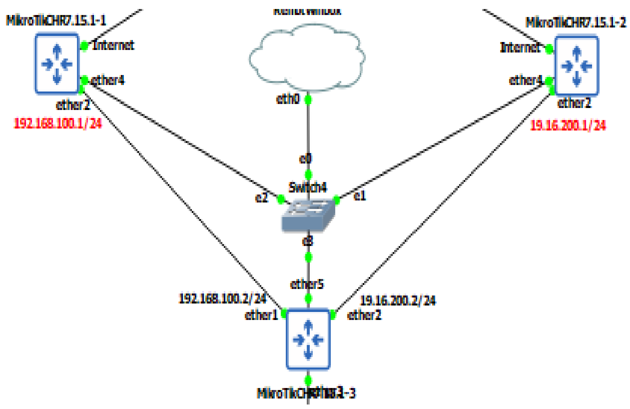

Fig. 10. Third router view

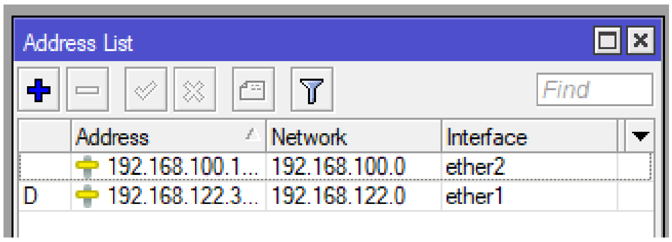

Fig. 11. IP Address ISP-1

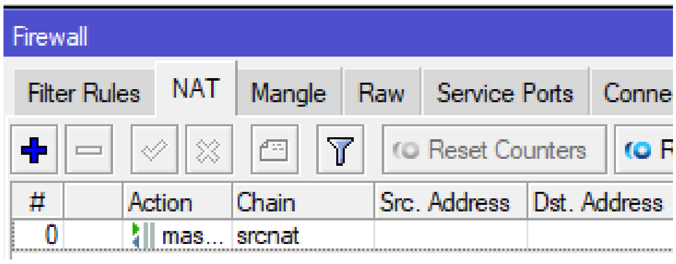

Fig. 12. NAT

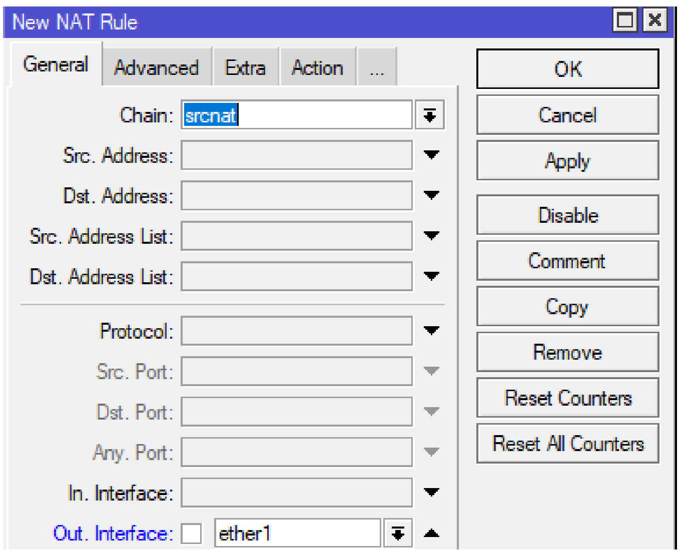

Fig. 13. NAT configuration

to each interface on the Mikrotik CHR ISP-1. In this case, the author only uses 2 ethers. The first Ethernet gets an IP address via DHCP, while the second Ethernet has an IP address that the author has determined, as shown in the Fig. 11. There are two IP addresses on two Ethernet ports. The first Ethernet port was obtained via DHCP, whereas the second was configured manually.

b. NAT Configuration

After adding the IP address, configure the NAT firewall as shown in Fig. 12. Configuring NAT is straightforward: go to the IP menu > Firewall > NAT Tab > +; once done, a pop-up will appear as in Fig. 13.

3.2.2. DNS configuration

After configuring NAT, the next step is to configure DNS so you can connect to the internet via Ethernet 2. Configuration is very easy. Go to IP > DNS, and a pop-up window will appear, as shown in Fig. 14.

3.2.3. Mikrotik CHR ISP-2 configuration

The configuration for ISP-2 is the same as for ISP-1, but the difference lies in the IP Address List, as shown in Fig. 15. The remaining configuration is identical to that for ISP-1.

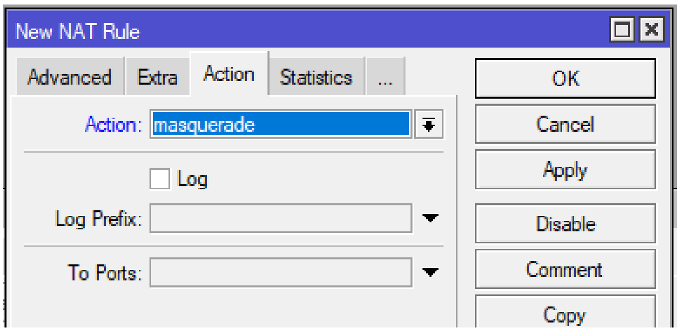

Fig. 14. NAT action

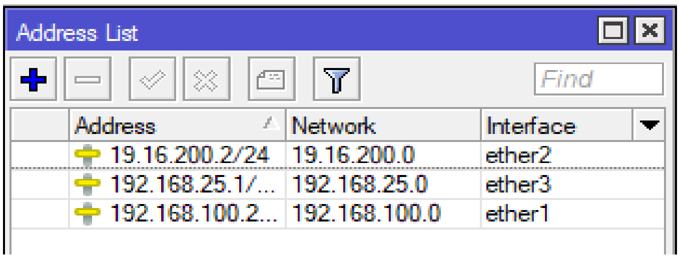

Fig. 17. PCC IP address

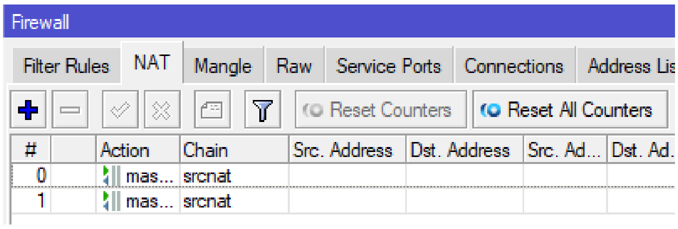

Fig. 18. NAT PCC

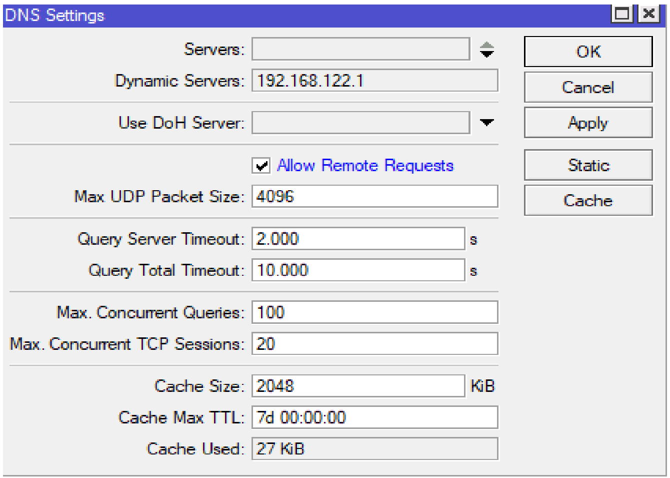

Fig. 15. DNS configuration

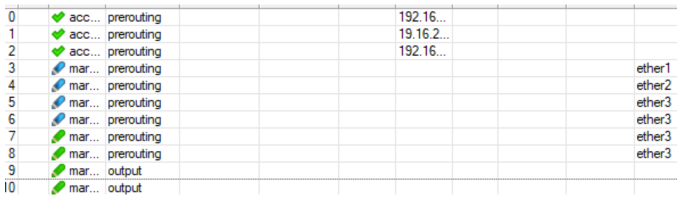

Fig. 19. Mangel

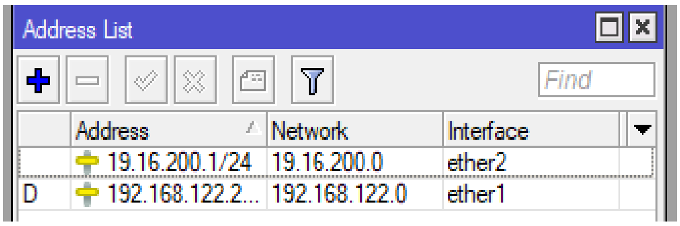

Fig. 16. ISP-2 IP address

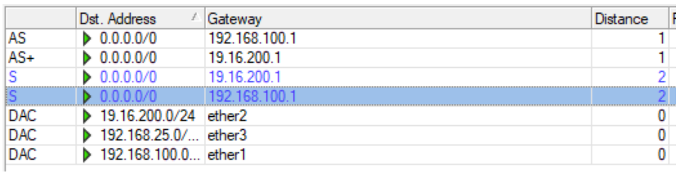

Fig. 20. Route gateway failover

3.2.4. Mikrotik CHR PCC-failover configuration

After successfully configuring each ISP, proceed to configure the PCC. First, the IP Address List on the PCC is added manually. Unlike ISPs, where either one is obtained via DHCP, the IP Address List on the PCC is shown in Fig. 16. As can be seen on Fig. 17, the PCC uses three Ethernet interfaces: Ethernet 1 is connected to ISP-1, Ethernet 2 is connected to ISP-2, and Ethernet 3 is connected to the client.

The NAT configuration is identical to that for ISP-1 and ISP-2. The difference is that the PCC has two NATs, each connected to its own ISP, resulting in the NAT display as shown in Fig. 18.

Mangel is a rule for PCC. When we set the mangel, PCC can be run, as shown in Fig. 19. Then, to configure failover on the PCC, simply add the gateway route settings, as shown in Fig. 20.

3.3. Testing YouTube and downloading

At this stage the author will conduct two tests on the topology that the author has created previously, but here the author has several obstacles where in this simulation for Mikrtik Router OS CHR it experiences a speed limitation where when installing Router OS the license will automatically be limited to only 1M so it is very slow and other obstacles are the lack of specifications on the hardware used. Table 2 and Table 3 present the requirements analysis for both hardware and software.

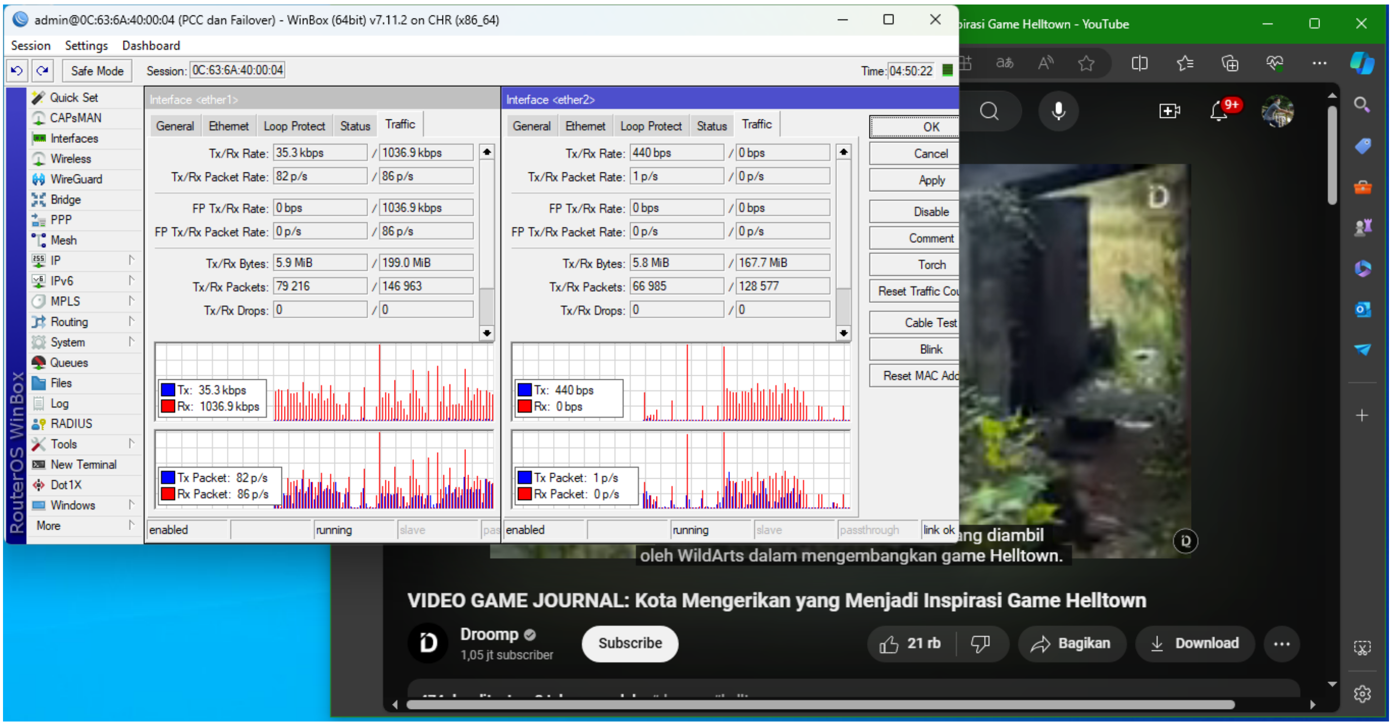

Fig. 21. Testing client view a YouTube video

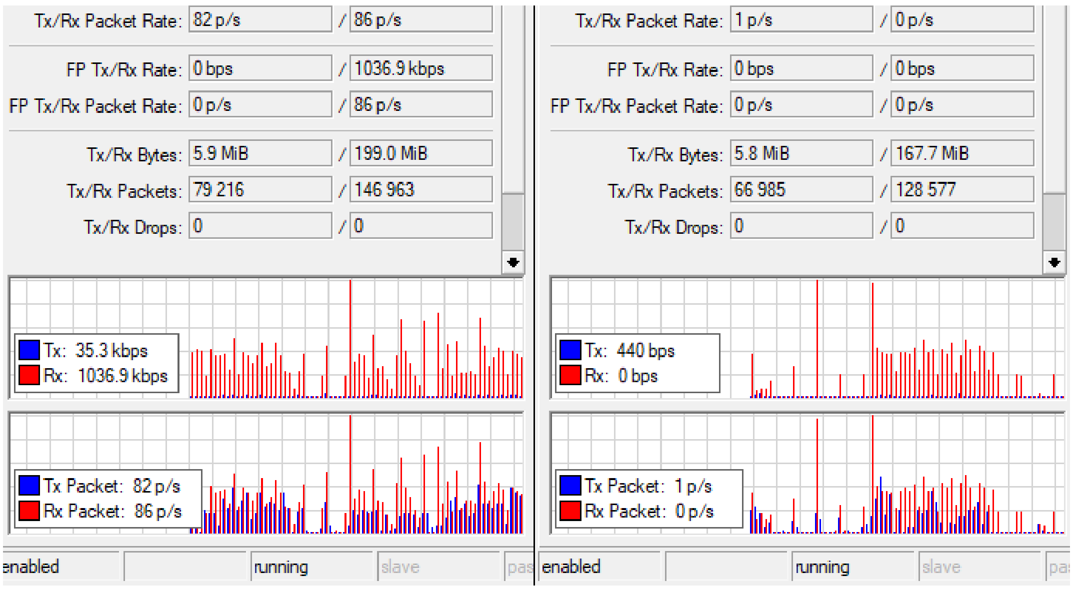

Fig. 22. Stable traffic

Table 2. Hardware analysis

No	Hardware	
1	CPU	Intel(R) Core(TM) i3-6006U CPU @ 2.00GHz
2	RAM	12.0 GB
3	HDD	500 GB
4	SSD	500 GB
5	GPU	Intel(R) HD Graphics 520

Table 3. Software analysis

No	Software
1	Graphical Network Simulator – 3 (GNS3)
2	VMware Workstatioon 17 pro
3	Router OS 7.11.2 Qemu
4	4 Client OS windows 10 pro 64bit
5	Windows 11 pro 64bit (Host)

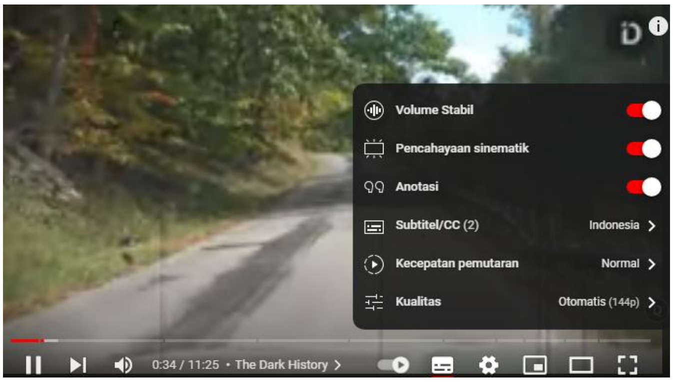

Fig. 24. Traffic spikes when video buffers

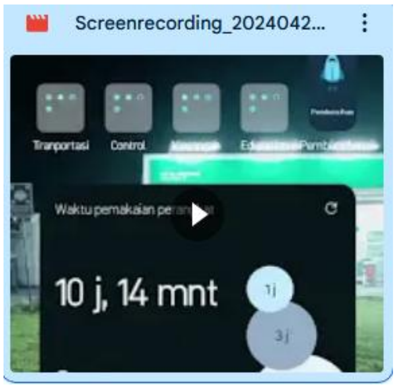

Fig. 25. Video file

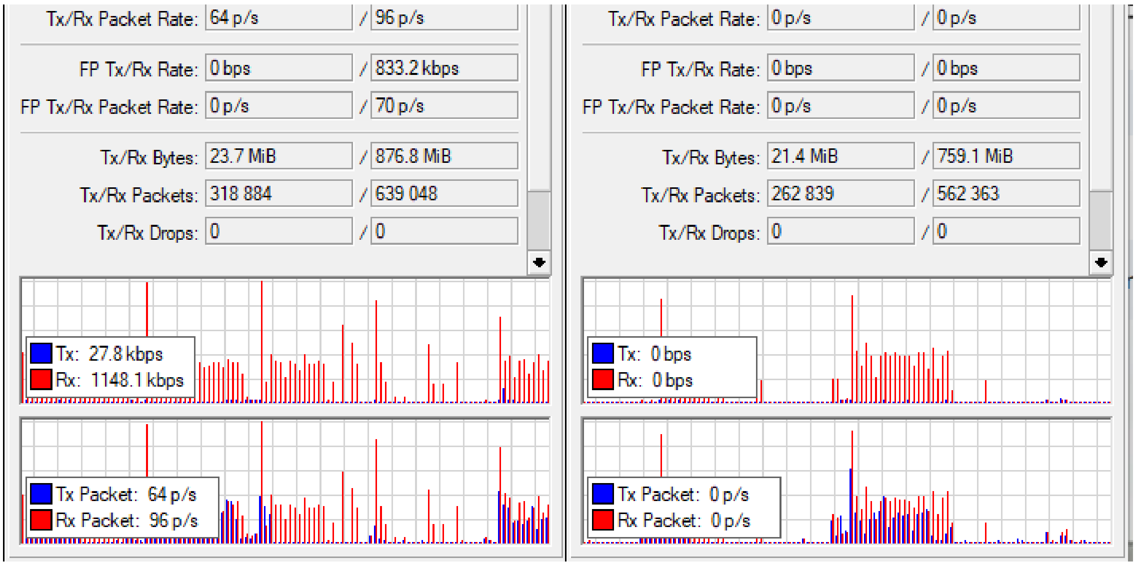

Fig. 23. Video file download traffic

It can be seen in the tables above that the analysis of the software and hardware used by the author to carry out this research, but with limited hardware specifications in the hardware analysis, here the author only runs two experiments on two main clients, namely client 1 and client 2 because the Windows 11 Pro system that the author uses already uses 4GB of RAM, then for the GNS3 VM server it uses 2GB of RAM and the rest is because the installation of Windows 10 Pro uses 2GB of RAM, so each client has used 4GB of RAM, so if the total RAM consumption used is 10GB and only 2GB is left.

In the first testing stage, testing on the first client is to set YouTube, as shown in Fig. 21. As seen in the figures, when the client runs YouTube, the traffic connection is more stable. However, because the internet speed is limited to 1 Mbps, the video output is observed. To achieve a stable level, the video display is at a very low resolution, as shown in Fig. 22.

It can be seen that the resolution for the video is only 144p because the internet speed is very low, and when the video experiences buffering, the traffic also experiences a very high increase, as in Fig. 24.

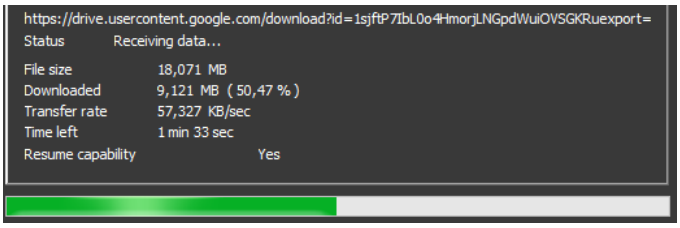

Fig. 26. Small file download

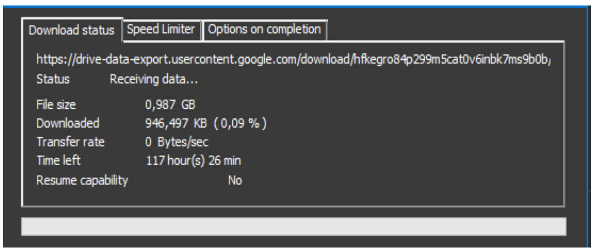

Fig. 27. Large file download failed

3.3.1. Testing video file downloads on client 2

Next, we tested video file downloads on Client 2, as in Fig. 25. The observed differences in speed between Client 1 and Client 2 are evident both when downloading files and when watching YouTube videos.

Fig. 23 shows stable download traffic for relatively small files, as shown in Fig. 26. It shows that with a download size of 18,071 MB; the traffic is more stable than for a large file like the one shown in Fig. 27.

The failures are not considered a weakness of the PCC method but rather a result of the 1 Mbps bandwidth limitation, which causes the connection to time out. In this situation, the network capacity cannot accommodate the high traffic load, resulting in connection termination. The PCC method continues to function correctly, but physical bandwidth limitations are the primary cause of the disruption. To address this, increased bandwidth capacity or the implementation of QoS and traffic shaping are required to maintain connection stability under increased network load.

4. Discussion

Test results from implementing the Peer Connection Classifier (PCC) and failover in a load-balancing system demonstrate that this design significantly improves network performance compared to a single-connection system. The PCC method plays a crucial role in classifying network traffic based on parameters such as source and destination addresses and ports. This technique enables traffic to be distributed evenly across multiple gateways, thereby optimizing bandwidth utilization.

During testing, the PCC configuration system maintained traffic stability despite increases in user count or simultaneous data requests. This indicates that this method is effective at avoiding congestion across any connection path. Furthermore, measurement results showed a 35% increase in throughput and a 20% decrease in latency, resulting in faster network response and greater efficiency in managing data flow.

The implementation of a failover mechanism also significantly contributes to system reliability. When one of the internet connections is disrupted, the system automatically redirects traffic to the backup path without requiring manual intervention. Based on test results, the average connection recovery time (failover time) was under 3 seconds, resulting in virtually no service disruption for users. This demonstrates that integrating load balancing and failover can improve network availability and resilience.

However, this testing still encountered several limitations. For example, the system was not fully capable of dynamically adjusting the load when network quality at one of the gateways gradually decreased (not completely disconnected). Furthermore, the system lacked a real-time performance-monitoring module that could provide early warning of connectivity disruptions.

Overall, the discussion results indicated that PCC and failover design are effective solutions for improving the efficiency, stability, and availability of network services, particularly in multi-gateway infrastructures that require low latency and service continuity.

5. Conclusion

Based on the design and testing results of the PCC (Peer Connection Classifier) system and its load-balancing failover, it can be concluded that the combination of these two mechanisms can significantly improve network performance and reliability. The implementation of PCC enables balanced distribution of traffic load among gateways, resulting in throughput increases of up to 35% and latency reductions of approximately 20% relative to a single configuration. In addition, the implemented failover feature achieves an average connection recovery time of less than 3 seconds, indicating that the system responds quickly to network failures without disrupting service stability. Overall, this design has proven effective in maintaining service continuity and increasing bandwidth utilization efficiency in multi-gateway network structures.

For further research, it is recommended that PCC and failover systems be developed with IoT-based real-time monitoring integration or a web dashboard to automate performance detection and analysis, and enhance performance monitoring and analysis. Furthermore, testing can be expanded by adding more gateways (multi-ISP) and by measuring additional parameters, such as packet loss, jitter, and Quality of Experience (QOE), to provide a more comprehensive performance evaluation. Developing dynamic algorithms capable of adaptively distributing traffic could enhance load-balancing efficiency in the future.

Data availability

All data generated or analyzed during the research are available in this article.

Declaration of competing interest

The authors declare that they have no known conflicts of interest or personal relationships that could have appeared to influence the work reported in this paper.

Authors' contributions

All authors designed the article, contributed to the content writing, and revised the manuscript. NAA was the primary author of the first draft and revised the manuscript, while MI supervised the work. All authors read and approved the final version of the manuscript.

References

Amalia, E. R., Nurheki, Saputra, R., Ramadhana, C., & Yossy, E. H. (2023). Computer network design and implementation using load balancing technique with per connection classifier (PCC) method based on MikroTik router. *Procedia Computer Science*, *216*, 103–111. https://doi.org/10.1016/j.procs.2022.12.116

Baeturohman, R., & Banu Santoso. (2024). Analisis Kinerja Algoritme WRR dengan WLC pada Load Balancing Nginx. *Indonesian Journal of Computer Science*, *13*(1). https://doi.org/10.33022/ijcs.v13i1.3577

Bahtiar, D., Jati Febrianto, W., Maulana, A., Saputra, S., Darmawan, W., Putra Tafonao, R., Julianto, R., Zai, R., & Djutalov, R. (2021). Pengenalan Dasar Instalasi Jaringan Komputer. *Jurnal Kreativitas Mahasiswa Informatika*, *2*(3), 507–518.

Fitriani, P., Dani, U., & Prayogi, A. (2020). Implementasi Jaringan internet dan Konfigurasi Mikrotik dengan simulasi GNS3 Pada Perusahaan Intelligent Komputer. *Jurnal Informasi Komputer Logika*, *2*(1). https://ojs.logika.ac.id/index.php/jikl/article/view/61

Gusrion, D., Gema, R. L., Safira, S., Hadi, A. F., & Andini, S. (2022). Load Balance PCC and Failover With Recursive Gateway. *Jurnal Ipteks Terapan*, *16*(4), 715–724. https://doi.org/10.22216/jit.v16i4.1945

Hadi, M. R. N., & Kaburuan, E. R. (2022). Ethernet Link Network Design Using Auto Failover and Load Balancing Technology in Throughput Optimization. *Journal of Theoretical and Applied Information Technology*, *100*(15). http://www.jatit.org/volumes/Vol100No15/11Vol100No15.pdf

Hafizh, A. N., & Sulistyo, W. (2024). Optimalisasi Dua Layanan Jaringan Internet Menggunakan Teknik Load Balancing dengan Metode Peer Connection Classifier (PCC) (Studi Kasus: Jaringan Internet Desa Banyuanyar Boyolali). *Jurnal JTIK (Jurnal Teknologi Informasi L Komunikasi)*, *8*(1), 10–21. https://doi.org/10.35870/jtik.v8i1.1257

Iskandar, D., Farisyihab, J. R., Bahari, M. H. T., Nurfaishal, M. D., & Khairullah, M. D. (2024). Application of The SD-WAN Load Balancing Method in Managing Internet Bandwidth at IDN Bogor Vocational School. *International Journal Software Engineering and Computer Science (IJSECS)*, *4*(1), 24–39. https://doi.org/10.35870/ijsecs.v4i1.2100

Khaerudin, M., Hendharsetiawan, A. A., Mahbub, A. R., Tukino, T., & Setiawati, S. (2023). A Hotspot Server and Two Line ISP Load Balance and Failover Using the Mikrotik RB951UI 2HND with PCC Method. *East Asian Journal of Multidisciplinary Research*, *2*(1), 249–262. https://doi.org/10.55927/eajmr.v2i1.2591

Nuryadin, R. A., Ramadhani, T. A., Karaman, J., & Reza, M. (2023). Analisis Perbandingan Performa Virtualisasi Server Menggunakan Vmware Esxi, Oracle Virtual Box, Vmware Workstation 16 Dan Proxmox. *METHOMIKA Jurnal Manajemen Informatika Dan Komputerisasi Akuntansi*, *7*(2), 175–180. https://doi.org/10.46880/jmika.Vol7No2.pp175-180

Pasaribu, S. A. (2022). Comparison Analysis of Load Balance Performance Per Connection Classifier (Pcc) And Equal Cost Multi-Path (Ecmp) Networks for Multiple Path Networks. *International Journal of Information System and Innovative Technology*, *1*(2), 11–20. https://doi.org/10.63322/hm65v060

Rahman, R., Ansarna, A. D., & Tanduklangi, E. (2024). Strategi Disaster Recovery dengan Virtualisasi: Backup dan Restore Sistem Operasi di Vmware dengan Menggunakan Snapshot. *Jurnal Penelitian Sistem Informasi (JPSI)*, *2*(2), 163–171. https://doi.org/10.54066/jpsi.v2i2.2197

Suwito, M. R., & Lukman, L. (2022). Analisis Dan Perancangan Load Balancing Dengan Metode Nth Menggunakan Mikrotik Studi Kasus Smk Bina Harapan Sleman. *Respati*, *17*(1), 17. https://doi.org/10.35842/jtir.v17i1.437

Wiharti, W., Rimra, I. L., Rifka, S., Hidayatullah, I., & Kasmar, A. F. (2023). Load Balancing and Fail Over MikroTik Implementation Using Per Connection Classifier (PCC) on Two Internet Providers Interconnection. *International Journal of Advanced Science Computing and Engineering*, *5*(2), 129–135. https://doi.org/10.62527/ijasce.5.2.135

Ariyana, R. Y., & Virdiyansyah, D. A. (2023). Network Design Using Load Balancing Equal Cost Multi Path (ECMP) Method At Lexima Consultant Office. *SAGA: Journal of Technology and Information System*, *1*(2), 31–36. https://doi.org/10.58905/saga.v1i2.81

Novellza Arfedin Abraaraa is a 2021 Computer Systems student, specializing in Mobile Technology, at the Asian Institute of Technology and Business in Malang. To fulfill graduation requirements, he is writing a final project on the theme "Implementation of PCC Load Balancing and Failover Using Mikrotik CHR on Virtual GNS3."

Mufidatul Islamiyah is a lecturer in computer systems at the Institute of Technology and Design, Technology and Business Asia Malang since 2015. Received a bachelor's degree from Airlangga University, Surabaya, Faculty in 2010 and a master's degree from the Sepuluh November Institute of Technology, Surabaya, Indonesia in 2014. His current research focuses on biogas and internet thing. He can be contacted at email: mufidatul@asia.ac.id