Aviation Electronics, Information Technology, Telecommunications, Electricals, and Controls (AVITEC)
Vol. 8, No. 1, February 2026, pp. 111-124, p-ISSN 2685-2381, e-ISSN 2715-2626
http://dx.doi.org/10.28989/avitec.v8i1.3605

Research Article

Analysis of Policy Based Routing (PBR) and Failover in Dual-WAN Networks

Daryan Pratama Alifi[1]*, Ichwan Nul Ichsan[2]
[1,2]Department of Telecommunications Systems, Universitas Pendidikan Indonesia, Indonesia

Article Info

Article history:
Submitted November 10, 2025
Accepted January 6, 2026
Published January 20, 2026

Keywords:
Policy-Based Routing;
multi-WAN connectivity;
resilient networking;
traffic engineering;
software-defined WAN.

ABSTRACT

Reliance on stable and high-speed internet connectivity is crucial for modern business operations. A failure in a single internet link often leads to significant disruptions in productivity. This study designs and implements a Dual-WAN network architecture utilizing Policy-Based Routing (PBR) combined with an automated failover mechanism on a MikroTik router. Unlike prior studies that primarily employ the Per-Connection Classifier (PCC) Load Balancing method to maximize bandwidth aggregation, this research prioritizes session integrity to minimize disruptions in sensitive applications. To validate the proposed method, a comparative analysis was performed against the conventional PCC method. The results indicate that while PCC yields a higher theoretical aggregated throughput (468.5 Mbps), it suffers from a high session drop rate in secure connections. In contrast, the proposed PBR implementation demonstrates superior connection stability with a maximum throughput of 344.25 Mbps on the primary link, alongside a responsive failover mechanism achieving a recovery latency of under 1000 ms with minimal packet loss (1–2 packets). This study concludes that the PBR architecture provides a more reliable solution compared to standard load balancing for Small Office Home Office (SOHO) and SME environments requiring high availability.

Corresponding Author:
Daryan Pratama Alifi,
Department of Telecommunications Systems, Universitas Pendidikan Indonesia , Indonesia.
Email: *daryan@upi.edu

1. INTRODUCTION

The rapid acceleration of digital transformation has profoundly reshaped the function of network infrastructure within modern enterprises. Network connectivity is no longer a supplementary or background component; instead, it has become a core operational asset that directly influences productivity, service continuity, and organizational resilience [1]. As businesses increasingly rely on interconnected digital platforms, including cloud-based applications (SaaS, IaaS), real-time communication systems (VoIP, video conferencing), and continuous data synchronization services [2], the demand for a stable, high-performance, and uninterrupted internet connection becomes indispensable. Under such conditions, dependence on a single Internet Service Provider (ISP) creates substantial operational risk. A single link failure exposes the organization to a severe Single Point of Failure (SPOF) scenario, which may halt business activities, disrupt mission-critical applications, and result in both financial and operational losses [3]. Consequently, many organizations adopt a Dual WAN architecture to enhance redundancy, reliability, and overall network robustness [4][5].

Nevertheless, merely deploying two ISP connections does not automatically guarantee improved network performance. Instead, it introduces a new layer of complexity in routing decisions, bandwidth allocation, and traffic prioritization [6]. This complexity was also evident in the real-world environment of PT. Ciptajaya Sejahtera Abadi, where the entire network load depended solely on ISP 1, which offered limited bandwidth capacity. High-volume, non-critical activities such as software downloads, updates, and multimedia consumption frequently interfered with mission-critical applications that require low latency and stable throughput. At the same time, a high-speed ISP 2 connection remained unused, resulting in a misallocation of resources and the inability of the network to leverage available capacity effectively [7]–[9]. This mismatch between network demand and resource utilization underscores the need for an intelligent traffic management strategy rather than a simple dual-link installation.

The academic literature provides substantial coverage of Dual WAN management techniques, primarily focusing on load balancing mechanisms such as Per-Connection Classifier (PCC) and Nth methods [10][11]. These methods aim to merge the capacity of two ISP connections to achieve bandwidth aggregation. However, research also highlights inherent weaknesses in these approaches: PCC splits user connections across multiple source IPs, which can disrupt session integrity and destabilize applications requiring persistent sessions, such as secure portals, e-banking platforms, VPN tunnels, and VoIP registration systems [12][13]. This limitation establishes a clear and explicit research gap: existing studies primarily emphasize throughput enhancement through load balancing but often fail to ensure session stability and consistent connection behavior for latency-sensitive or security-sensitive applications. This gap becomes even more critical in corporate environments where reliability and predictability are more valuable than raw bandwidth.

Previous studies have demonstrated the importance of fast and reliable rerouting mechanisms, but several limitations remain, particularly in the context of dual-WAN-based enterprise networks. A study in Dudczyk, J et al., (2025) emphasized that inaccurate error detection, multi-path switching instability, and potential micro-loops remain obstacles to maintaining consistent network service, especially when the system is unable to effectively distinguish between transient and long-term outages. Meanwhile, a study in Du,J et al., (2025) proposed a fast reroute approach based on segment routing and dual-timers that is effective in satellite environments, but this approach relies heavily on an ISL link architecture and does not examine deterministic failover mechanisms in terrestrial networks that utilize routing-marks, statistical route prioritization, and gateway monitoring as in dual-WAN scenarios [13]. Kesavakumar et al.'s (2022) research focused on PCC/Nth to increase throughput, but it did not guarantee session stability or deterministic routing. Existing failover mechanisms are slow and inaccurate in detecting failures. Therefore, there is still a research gap related to how to design a failover mechanism that is deterministic, fast, micro-loop-free, and tightly integrated with routing-mark and gateway monitoring to ensure instant convergence in enterprise networks, an aspect that has not been adequately addressed by the two studies.

Addressing this research gap requires a fundamentally different perspective one that prioritizes routing determinism, connection stability, and intelligent resource allocation rather than pure bandwidth aggregation [14][15]. In this context, the present study proposes the implementation of a Policy Based Routing (PBR) architecture integrated with an automated Failover system on a MikroTik RB1100AHx4 router. Unlike traditional load balancing mechanisms that treat both ISP links as a combined and often unpredictable bandwidth pool, PBR enables administrators to establish explicit traffic policies based on application type, destination address, or functional classification [16]. Through this mechanism, high-volume but non-critical traffic can be routed to ISP 2, while latency-sensitive or business-critical traffic is directed to the more stable ISP 1 [17][18]. The novelty of this research lies in its PBR-first approach, which shifts focus from maximizing aggregated throughput to enforcing precise control over traffic paths, thus ensuring session integrity, minimizing performance disruptions, and enabling more strategic utilization of multi-link environments [19][20].

When compared to previous research that mainly pursued throughput maximization through PCC or recursive load balancing, the PBR + Failover configuration introduced in this study offers a more deterministic, stable, and operationally reliable model. The integration of a Failover system further enhances resilience by allowing automatic and seamless traffic redirection when primary ISP connectivity becomes unavailable [21][22]. This design ensures that critical business services remain uninterrupted even during link failures, addressing a limitation in previous Dual WAN studies that often overlooked reliability and recovery behavior under real failure conditions [23]. Furthermore, the configuration model developed in this research contributes practical value, as it can be replicated and adapted in similar enterprise settings that utilize asymmetrical ISP environments and require fine-grained traffic management [24][25].

The purpose of this study is to analyze existing challenges in Dual WAN deployment, develop and implement a PBR-first architecture combined with an automated Failover system, and evaluate its effectiveness through performance measurements and functional testing. Through this implementation, the research contributes a validated dual-link network management model that improves resource utilization, enhances connection stability, ensures the preservation of session integrity, and maintains service continuity during link disruptions. Overall, this study not only addresses a theoretical gap in prior research but also provides an applicable and empirically validated solution for organizations seeking to optimize their Dual WAN environments.

While Policy Based Routing (PBR) and failover mechanisms are established concepts in networking literature, existing studies typically focus on bandwidth aggregation to maximize throughput [26]. However, this study argues that in a modern enterprise environment, raw throughput is secondary to session integrity. The novelty of this research lies in the implementation of a 'Service-Aware' routing hierarchy. Unlike prior studies that utilize PCC to randomly distribute traffic often causing instability in secure applications this work uniquely implements a deterministic PBR logic combined with aggressive failover detection. This approach specifically addresses the trade-off between bandwidth aggregation and connection stability, offering a proven blueprint for SMEs requiring enterprise-grade reliability on consumer-grade hardware [27].

2. RESEARCH METHODS

This study is classified as applied research and employs the Network Development Life Cycle (NDLC) framework [28][29]. The NDLC methodology was chosen because of its systematic and iterative structure, making it suitable for developing, evaluating, and deploying network infrastructure in real operational environments. In this research, the NDLC framework is applied specifically to the implementation of a Dual WAN management system within the corporate network environment of PT. Ciptajaya Sejahtera Abadi, which serves as the practical site of system deployment and testing. Placing the implementation environment in this section clarifies that the company functions as the location of operational evaluation, rather than the subject of a case study in the title.

The NDLC workflow consists of several core stages, beginning with requirements analysis, followed by design, implementation, and concluding with system testing and validation. This structured approach ensures that the developed configuration is technically functional and aligned with the operational needs of the organization, particularly in addressing redundancy issues and optimizing bandwidth allocation.

The research process began with an in-depth analysis stage involving direct observation of the active network infrastructure at PT. Ciptajaya Sejahtera Abadi. This included identifying the devices in use (router, switches, PoE switches, and access points), evaluating existing configurations, and conducting interviews with key technical personnel to determine operational challenges. The analysis revealed two primary requirements: the need for granular traffic separation to distinguish critical business applications from general traffic, and the necessity for an automated failover mechanism to maintain service continuity in the event of ISP failure. Closed-loop network control architecture can be seen in Figure 1.

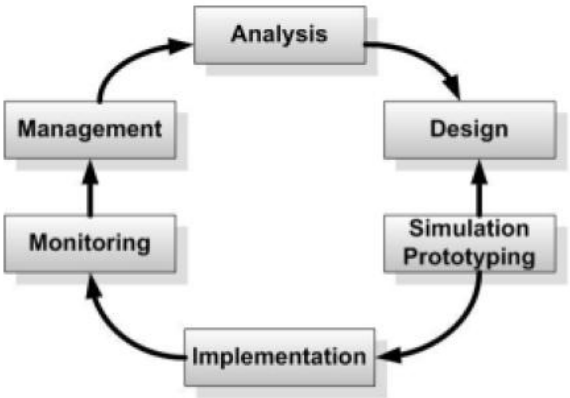


Figure 1. Closed-loop network control architecture

The research process commenced with an in-depth analysis phase of the company's existing network infrastructure, as depicted in the topology plan in Figure 2. This analysis stage involved direct observation of the active hardware (Router, Switch, PoE Switch, Access Points) and current configurations, supplemented by interviews with key stakeholders to identify operational pain points and requirements. The primary needs identified were twofold: first, the necessity for granular traffic separation to isolate critical business applications (such as access to specific servers) from general internet traffic, and second, the critical demand for an automatic failover system. This failover mechanism was required to guarantee high availability and seamless operational continuity by automatically rerouting traffic in the event of an outage from one of the two ISPs.

Following the analysis, the design phase was initiated to architect a solution addressing these requirements. The topology shown in Figure 2 served as the blueprint for the physical layout, positioning a MikroTik RB1100AHx4 router as the central gateway. The logical design focused on implementing Policy Based Routing (PBR). This involved creating specific Address Lists within the router to categorize destination IPs for critical services. Subsequently, Firewall Mangle rules were designed in the prerouting chain to inspect all traffic from the LAN (bridge lan). These rules were configured to mark-routing packets based on whether their destination matched the critical services Address List (e.g., KE_ISP_2) or if it was general traffic (e.g., KE_ISP_1) KE_ISP_1 means that rule will go to ISP 1 interface, also for KE_ISP_2 means that rule will go to ISP 2 interface. Concurrently, a robust failover system was designed within the Route List, utilizing these routing marks. For each routing mark, two static default routes (0.0.0.0/0) were created: a primary route with a distance of 1 to the preferred ISP and a secondary backup route with a distance of 2 pointing to the alternate ISP, both configured with check-gateway=ping for automatic link-failure detection.

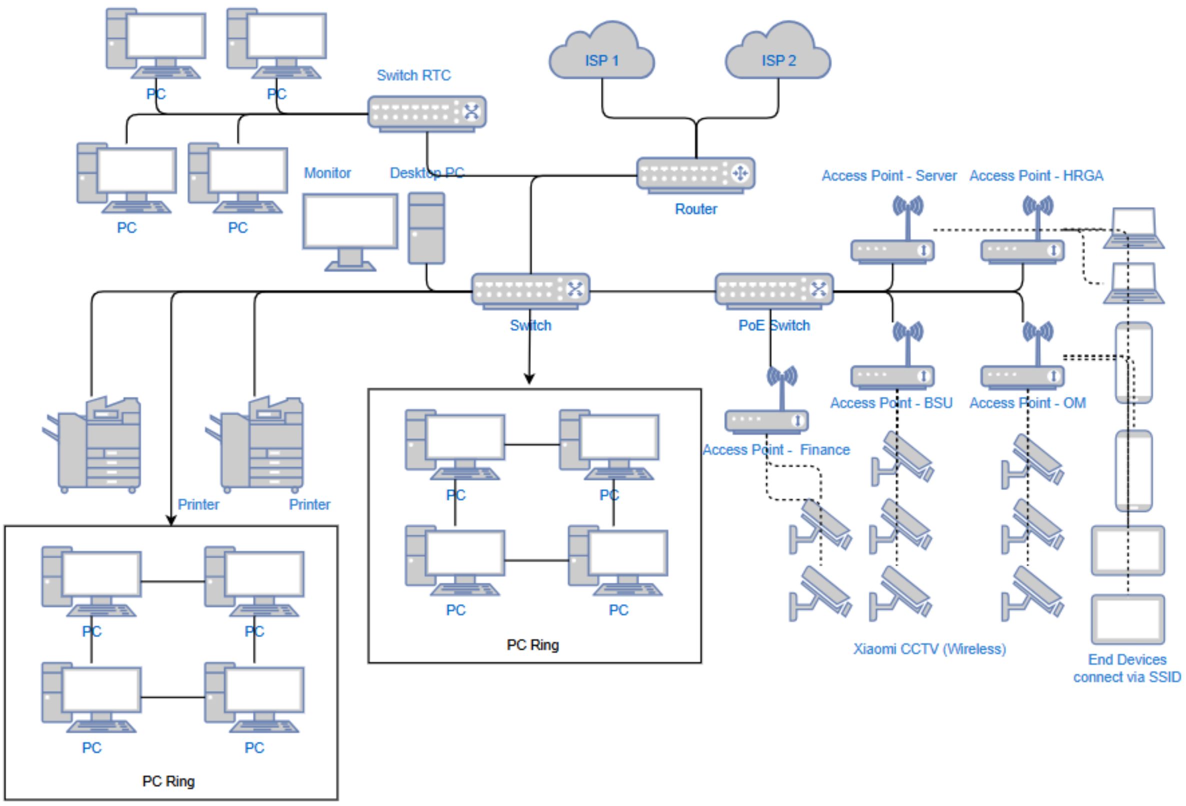


Figure 2. Topology design plan

The implementation phase involved the practical application of the designed solution onto the production network. This hands-on stage utilized the WinBox software to configure the MikroTik RB1100AHx4 router. This process included setting up the WAN interfaces (ether1, ether3) and the LAN bridge, configuring the DHCP server, and meticulously applying the PBR Mangle rules and the static routes for failover as specified in the design phase. All configurations were carefully documented and incrementally applied to minimize disruption to the existing operations.

Finally, the testing and analysis phase was conducted to validate the functionality and performance of the newly implemented system. Functional validation of the PBR was performed using the traceroute utility from a client PC to test both critical (Address List) and general destinations, verifying that traffic was routed through the correct ISP gateway. The failover system was tested by simulating an ISP outage (e.g., by disabling the primary WAN interface) and observing the network's automatic reconvergence to the backup route. Quantitative analysis was also performed by monitoring the Bytes and Packets counters on the Mangle rules to confirm that traffic was being correctly identified and distributed according to the defined policies.

2.1 WinBox

The primary software tool utilized for the practical implementation and configuration phase of this research was WinBox. WinBox is a proprietary, stand-alone graphical user interface (GUI) developed by MikroTik specifically for the administration of devices running MikroTik RouterOS [28]. This tool was selected as the foundational component for translating the network design into a functional configuration on the core router.

As visually confirmed in Figure 3, the specific version used was WinBox (64-bit) v6.49.19. This application provided the essential interface for connecting to and managing the central gateway device, the MikroTik RB1100AHx4 router, which was identified on the network by its management IP address, 192.168.88.1.

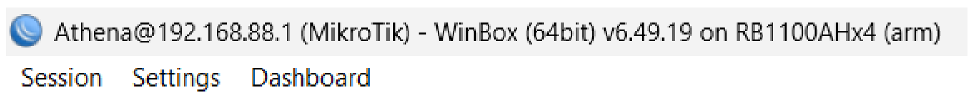


Figure 3. WinBox

The use of WinBox was instrumental in this study because it offers a comprehensive and real-time visual representation of the router's entire configuration. It greatly simplified the complex setup required for the Policy Based Routing (PBR) and Dual WAN failover system. All critical configurations including the creation of Firewall Mangle rules for traffic marking, the meticulous ordering of the Route List to manage primary and backup routes, and the setup of network services like DHCP, DNS, and Address Lists were performed using this interface. Its ability to display live traffic counters and route statuses was invaluable during the testing and validation phases of the methodology.

2.2 Interface List

Following the initial router access, a foundational step in the configuration process was the logical definition and organization of the router's physical ports [29]. To maintain clarity and ensure accurate rule application, each active port on the MikroTik RB1100AHx4 was renamed to reflect its specific function within the network topology, as detailed in Figure 4 (Interface List).

Interface List

Interface | Interface List | Ethernet | EoIP Tunnel | IP Tunnel | GRE Tunnel | VLAN | VRRP | Bonding | LTE

Detect Internet

	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Packet (p/s)	FP Rx Packet (p/s)
DR	<pptp-alif>	PPTP Server Binding	1400		245.6 kbps	10.3 kbps	25	19	0 bps	0 bps	0	0
R	bridge lan	Bridge	1500	1592	40.0 Mbps	9.4 Mbps	6 430	3 235	0 bps	0 bps	0	0
R	ether1-envision	Ethernet	1500	1592	3.8 Mbps	13.5 Mbps	1 354	2 437	3.7 Mbps	13.4 Mbps	1 345	2 432
RS	ether2-Lan	Ethernet	1500	1592	30.0 Mbps	7.5 Mbps	4 283	2 280	29.7 Mbps	7.5 Mbps	4 443	2 284
R	ether3-ideanet	Ethernet	1500	1592	6.0 Mbps	26.7 Mbps	1 797	3 811	6.1 Mbps	26.6 Mbps	1 821	4 026
S	ether4	Ethernet	1500	1592	0 bps	0 bps	0	0	0 bps	0 bps	0	0
RS	ether5	Ethernet	1500	1592	10.2 Mbps	2.3 Mbps	1 976	956	10.3 Mbps	2.2 Mbps	1 991	951
S	ether6	Ethernet	1500	1592	0 bps	0 bps	0	0	0 bps	0 bps	0	0
S	ether7	Ethernet	1500	1592	0 bps	0 bps	0	0	0 bps	0 bps	0	0
S	ether8	Ethernet	1500	1592	0 bps	0 bps	0	0	0 bps	0 bps	0	0
S	ether9	Ethernet	1500	1592	0 bps	0 bps	0	0	0 bps	0 bps	0	0
S	ether10	Ethernet	1500	1592	0 bps	0 bps	0	0	0 bps	0 bps	0	0
S	ether11	Ethernet	1500	1592	0 bps	0 bps	0	0	0 bps	0 bps	0	0
S	ether12	Ethernet	1500	1592	0 bps	0 bps	0	0	0 bps	0 bps	0	0
S	ether13	Ethernet	1500	1592	0 bps	0 bps	0	0	0 bps	0 bps	0	0

Figure 4. Interface list

The ether1 port was designated ether1-envision, serving as the primary WAN interface for the circuit from ISP 1 (Envision). Correspondingly, the ether3 port was designated ether3-ideanet, serving as the secondary WAN interface for the circuit from ISP 2 (Ideanet).

For the internal network, several ports were designated for LAN connectivity. The ether2 port was renamed ether2-Lan, and the ether5 port was also actively used. Both ports were configured as active links connecting to downstream switches, which distribute connectivity to other network segments and end devices. As shown in the Figure 4, both the ether2-Lan and ether5 interfaces have the S (Slave) flag, indicating they are member ports of the bridge-lan virtual interface. This bridge-lan interface effectively groups all internal-facing ports into a single logical Layer 2 broadcast domain, simplifying management and allowing a single IP address (192.168.88.1) to serve the entire LAN. The R (Running) flag is visible on bridge-lan, ether1-envision, ether3-ideanet, ether2-Lan, and ether5, confirming that all critical WAN and active LAN links are operational and passing traffic.

2.3 IP Address Configuration

The next step in the configuration involved assigning static IP addresses to the router's key interfaces, which is a fundamental requirement for routing. This process, shown in Figure 5, defines the logical addresses for the router itself on each network segment (WAN and LAN).

Address List

Address	Network	Interface
103.75.52.57/28	103.75.52.48	ether1-envision
103.152.141.230/30	103.152.141.228	ether3-ideanet
192.168.88.1/22	192.168.88.0	bridge lan

Figure 5. IP address configuration

For the Dual WAN connections, the static public IP addresses provided by the ISPs were applied. The interface ether1-envision was assigned the IP address 103.75.52.57/28, which defines its address within the block provided by ISP 1. Similarly, ether3-ideanet was assigned 103.152.141.230/30, the public IP provided by ISP 2. These two addresses are critical as they will be used by the router to communicate with the ISP gateways and as the source addresses for Network Address Translation (NAT).

For the internal network, the IP address 192.168.88.1/22 was assigned to the virtual bridge-lan interface. This address is of particular importance as it serves as the default gateway for all end devices (PCs, Printers, Access Points, etc.) within the local network. The /22 subnet mask provides a large address space (192.168.88.0 to 192.168.91.255) to accommodate all client devices connected to the various switches.

2.4 Domain Name Resolution (DNS)

To enable domain name resolution for the router and its network clients, the DNS Settings were configured. As shown in Figure 6, this configuration defines the upstream DNS servers that the MikroTik router will query.

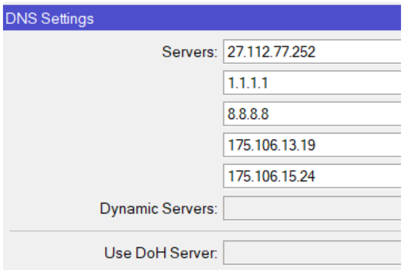


Figure 6. DNS configuration

The strategy employed was to create a redundant and robust list of resolvers. This list includes specific DNS servers provided by the ISPs (likely 27.112.77.252, 175.106.13.19, and 175.106.15.24) as well as highly available and well-known public DNS servers, namely 1.1.1.1 (Cloudflare) and 8.8.8.8 (Google).

By populating this list, the router itself can resolve domain names for its own internal processes, such as NTP (Network Time Protocol) or gateway checks. More importantly, this configuration allows the router to act as a local DNS cache for the entire bridge-lan network (assuming the "Allow Remote Requests" option is enabled). Client devices on the LAN will send their DNS requests to the router's gateway IP (192.168.88.1), which then forwards the requests to these upstream servers, providing a centralized, redundant, and efficient DNS service for all users.

2.5 DHCP Pool Server

To automate the IP address assignment for all end devices within the network, a DHCP (Dynamic Host Configuration Protocol) server was configured. This step is essential for simplifying network management, as it eliminates the need to manually configure IP settings on every PC, printer, and wireless device.

Figure 7 details the two main components of this setup. The top image (DHCP tab) shows that a server named dhcp1 was created. This server is set to run on the bridge-lan interface. This is a critical setting, as it allows the server to listen for and respond to IP requests from any device connected to the unified LAN (including the "PC Ring" and all wireless clients). The server is configured to lease addresses from the dhcp_pool0 (defined in IP > Pool) for a standard Lease Time of one day.

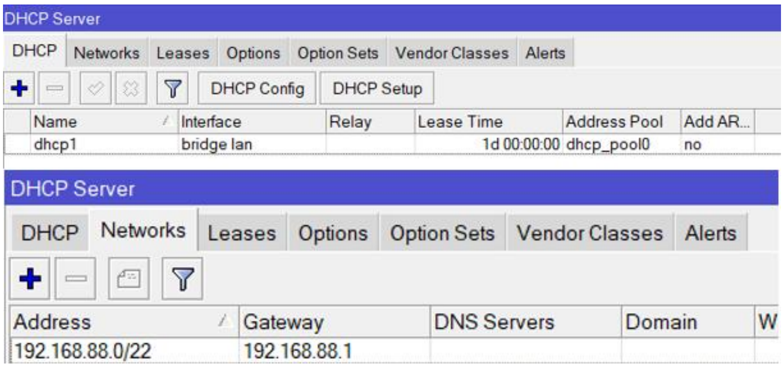


Figure 7. DHCP pool

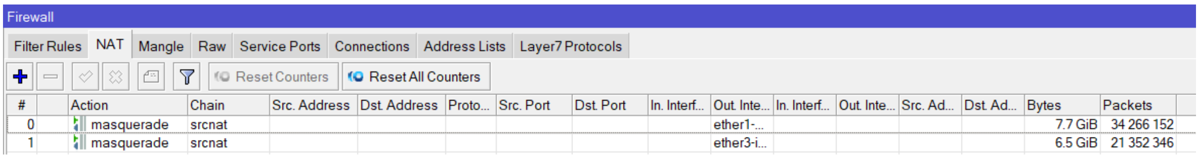
The bottom image (Networks tab) defines the crucial information that the server provides to clients. It is authoritative for the entire 192.168.88.0/22 network, matching the LAN's subnet. Most importantly, it advertises the Gateway address as 192.168.88.1. This is the single, critical instruction that tells all client devices to send their traffic to the MikroTik router. Once the traffic arrives at this gateway, the PBR Mangle rules (discussed later) can inspect, mark, and route it to the correct ISP.

2.6 NAT

A critical component for allowing devices on the private LAN (192.168.88.0/22) to access the internet was the configuration of Source Network Address Translation (NAT). This process translates the non-routable, private IP addresses of the internal clients into the single, routable public IP address provided by each ISP.

For this implementation, the masquerade action was used, as shown in Figure 8. Masquerade is a dynamic form of srcnat that is highly effective in a Dual WAN setup. Two distinct rules were created in the srcnat chain:

1. Rule 0: This rule targets all traffic that the router has decided to send out through the ether1-envision (ISP 1) interface. It applies the masquerade action, automatically translating the packet's private source IP into the router's public IP on the ether1-envision interface.
2. Rule 1: This rule performs the identical function for the second provider. Any traffic routed to the ether3-ideanet (ISP 2) interface is masqueraded using the public IP of that specific interface.



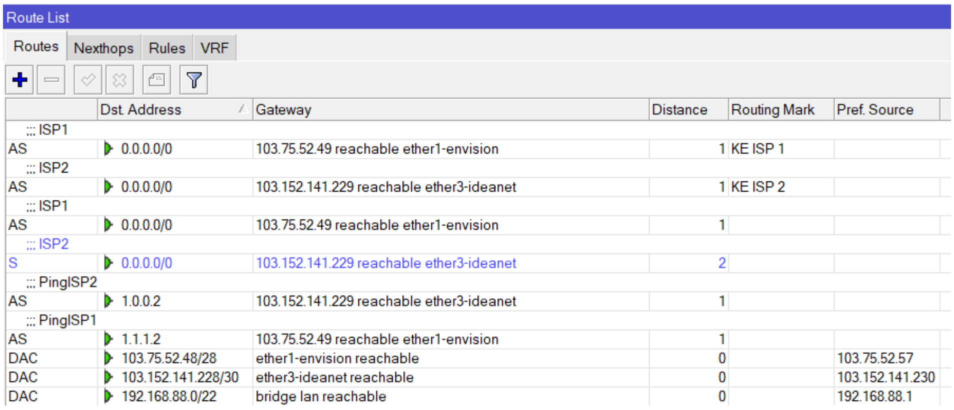
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Interf...	Out. Inte...	In. Interf...	Out. Inte...	Src. Ad...	Dst. Ad...	Bytes	Packets
0	masquerade	srcnat							ether1-...					7.7 GiB	34 266 152
1	masquerade	srcnat							ether3-i...					6.5 GiB	21 352 346

Figure 8. NAT configuration

These two rules are the final and critical component that allows the Policy Based Routing (PBR) system to function. After the Mangle rules (discussed later) mark a packet and the Route List directs it to a specific ISP, these NAT rules ensure the packet is correctly translated with the corresponding public IP before it leaves the router.

2.7 Route List

Then The Route List, shown in Figure 9, is the "brain" of the network that determines where all data packets should go. This configuration is essential for both the Policy Based Routing (PBR) and the Failover system to function.



	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
;;; ISP1					
AS	0.0.0.0/0	103.75.52.49 reachable ether1-envision	1	KE ISP 1	
;;; ISP2					
AS	0.0.0.0/0	103.152.141.229 reachable ether3-ideanet	1	KE ISP 2	
;;; ISP1					
AS	0.0.0.0/0	103.75.52.49 reachable ether1-envision	1		
;;; ISP2					
S	0.0.0.0/0	103.152.141.229 reachable ether3-ideanet	2		
;;; PingISP2					
AS	1.0.0.2	103.152.141.229 reachable ether3-ideanet	1		
;;; PingISP1					
AS	1.1.1.2	103.75.52.49 reachable ether1-envision	1		
DAC	103.75.52.48/28	ether1-envision reachable	0		103.75.52.57
DAC	103.152.141.228/30	ether3-ideanet reachable	0		103.152.141.230
DAC	192.168.88.0/22	bridge lan reachable	0		192.168.88.1

Figure 9. Route list

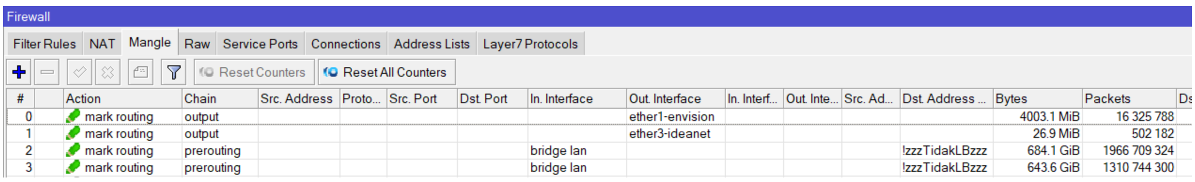
The list is read by the router as follows:

- DAC Routes: These (Dynamic Active Connected) routes are created automatically. They simply tell the router which networks are directly attached, such as the bridge lan (192.168.88.0/22) and the immediate subnets of both ISPs.
- PBR Routes (Marked): These are the two primary static routes (AS) at the top. The first rule directs all traffic marked KE ISP 1 means to ISP 1 (from the Mangle) to the ISP 1 gateway (103.75.52.49). The second rule directs all traffic marked KE ISP 2 to the ISP 2 gateway (103.152.141.229). This is what separates the traffic.
- Failover Routes (Unmarked): These two routes handle all other traffic (like traffic from the router itself) that does not have a routing mark. The route to ISP 1 has a Distance=1, making it the primary, active path (AS flag). The route to ISP 2 has a Distance=2, making it a secondary, inactive (S flag) backup path. If ISP 1 fails, this route will automatically become active.
- Monitoring Routes: The static routes to 1.1.1.2 and 1.0.0.2 are added to ensure that the router can always ping these specific test IPs via the correct ISP for gateway monitoring (Netwatch).

2.8 Mangle Configuration

The Mangle configuration is the most critical component of the Policy Based Routing (PBR) and Failover system. This section acts as the "sorting engine" for the router, inspecting packets and "marking" them. These marks do not route the traffic themselves; instead, they provide the necessary tags that the Route List uses to make its final routing decisions.

As shown in Figure 10, the configuration focuses on two different chains: prerouting for LAN traffic and output for the router's own traffic.



#	Action	Chain	Src. Address	Proto...	Src. Port	Dst. Port	In. Interface	Out. Interface	In. Interf...	Out. Inte...	Src. Ad...	Dst. Address ...	Bytes	Packets	Ds
0	mark routing	output						ether1-envision					4003.1 MiB	16 325 788	
1	mark routing	output						ether3-ideanet					26.9 MiB	502 182	
2	mark routing	prerouting					bridge lan					!zzzTidakLBzzz	684.1 GiB	1966 709 324	
3	mark routing	prerouting					bridge lan					!zzzTidakLBzzz	643.6 GiB	1310 744 300	

Figure 10. Mangle rule

The core of the PBR logic lies in the prerouting chain, which processes packets as soon as they enter the router from the LAN (In. Interface=bridge lan), before any routing decision is made:

1. Rule 2: This is the first PBR rule. It checks if a packet coming from the LAN is destined for an IP address included in the Dst. Address List=!zzzTidakLBzzz. “!zzzTidakLBzzz” denotes Not Load Balanced. If it matches, the router applies a mark routing action (e.g., KE ISP 2). This rule effectively tags all "special" traffic (such as for critical servers, games, or streaming) that needs to be sent to a specific provider.
2. Rule 3: This is the second PBR rule. It acts as the "catch-all" for general internet traffic. It checks packets from the LAN that are NOT (!) destined for the !zzzTidakLBzzz list. These packets are given a different mark routing action (e.g., KE ISP 1).

The output chain rules (Rule 0 and 1) are used to mark traffic generated by the router itself.

The high Bytes and Packets counters on the prerouting rules (684.1 GiB and 643.6 GiB respectively) serve as quantitative proof that the PBR system is functioning correctly and actively sorting nearly all network traffic into the two defined paths as designed.

2.9 Netwatch

The final component implemented was the Netwatch utility, as shown in Figure 11. This tool provides an essential, real-time monitoring service for the health and status of both ISP connections.

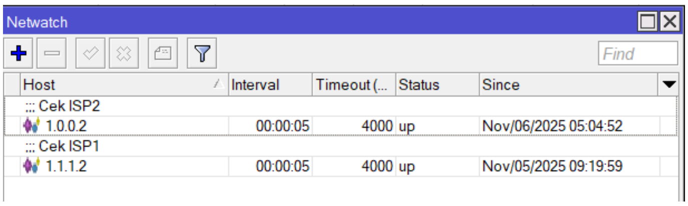


Figure 11. Netwatch

This configuration works directly with the static routes created in the Route List (discussed in 2.7). A specific route was created forcing any traffic to the IP 1.1.1.2 to only go through the ISP 1 gateway (ether1-envision). A second route forces any traffic to 1.0.0.2 to *only* go through the ISP 2 gateway (ether3-ideanet).

Netwatch uses these routes to perform a reliable, end-to-end connectivity test. It is configured to ping 1.1.1.2 (named Cek ISP1) and 1.0.0.2 (named Cek ISP2) every 5 seconds. This is a more robust test than a standard gateway ping, as it confirms that the *entire path* through the ISP is operational, not just the first hop.

The Status column in Figure 10 shows both hosts as up, providing a clear visual confirmation that both ISP connections were healthy and actively passing traffic at the time of the research. This tool is critical for monitoring and can also be expanded to trigger automated scripts, such as sending an email notification, in the event an ISP link goes down.

3. RESULTS AND DISCUSSION

This section presents the quantitative results obtained from the network implementation, followed by a detailed discussion of these findings. The primary objective of the testing phase was to validate the functional success of the Policy Based Routing (PBR) and Failover configuration. This was achieved by measuring network performance before and after the PBR rules were implemented to segregate traffic.

The results were gathered using standardized Speedtest (ookla) measurements, as shown in Figure 12 and Figure 13.

3.1 Research Results

In This section presents the quantitative data obtained from the functional testing of the system. The primary goal of this testing was twofold: first, to empirically prove that the Policy Based Routing (PBR) rules were successfully segregating traffic to different ISP paths, and second, to characterize the independent performance profiles (speed and latency) of each connection.

The tests were conducted using the Speedtest (Ookla) benchmark tool under two distinct scenarios, as shown in Figure 12 and Figure 13.

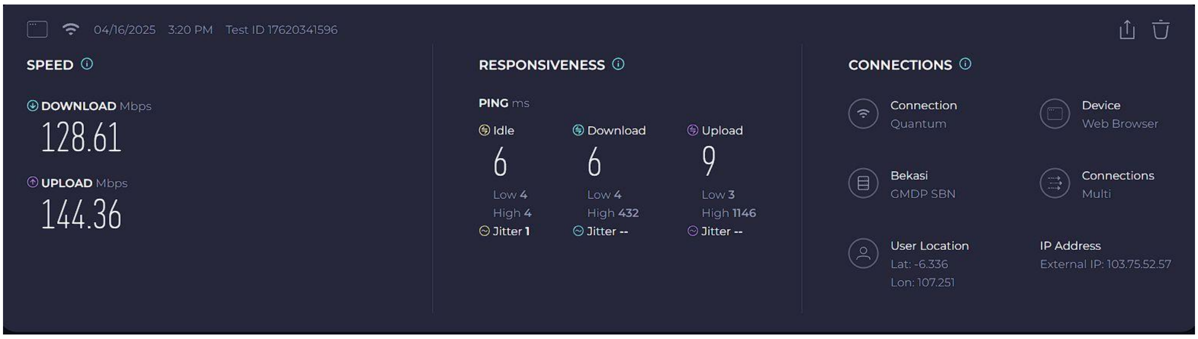


Figure 12. Speedtest before PBR & failover

Figure 13. Speedtest after PBR & failover

3.1.1 Test Scenario 1: Baseline Network Performance (Before PBR Implementation)

The first test, summarized in Figure 12, establishes the baseline network performance before the Policy Based Routing rules and the second ISP were implemented. This test (Test ID: TRG20045996) measures the maximum capacity of the network when it was entirely dependent on its single connection, ISP 1 (Envision). The results confirmed all traffic originated from the external public IP address 103.75.52.57. The total performance available to the entire network at this stage was:

- Download: 128.61 Mbps
- Upload: 144.36 Mbps
- Ping (Idle): 6 ms

Before PBR implementation, all network traffic relied solely on ISP 1 (Envision), resulting in peak speeds of 128.61 Mbps (download) and 144.36 Mbps (upload). This single-path dependency created a bottleneck that is consistent with findings by Iskandar et al. (2024) [5], who noted that single-link architectures often fail to scale with diverse traffic demands.

After PBR implementation, special traffic routed to ISP 2 (Ideanet) achieved significantly higher performance, with download speeds reaching 344.25 Mbps. This represents a performance increase of approximately 168%, demonstrating that the PBR rules successfully unlocked unused bandwidth resources. These findings align with the observations by Hartanto et al. (2025) [2], who similarly reported large performance gains when asymmetrical links were intelligently separated using policy-driven routing approaches.

Moreover, the throughput improvement in this study is consistent with the general principle highlighted by Kesavakumar et al. (2022) [1], namely that integrating heterogeneous data sources or pathways can enhance overall system performance and efficiency when managed through an appropriate processing or decision-making mechanism.

3.1.2 Test Scenario 2: Validation of PBR Path (After Implementation)

The second test, shown in Figure 13, was conducted after the PBR system and ISP 2 were fully implemented. It was specifically designed to validate that the PBR rules for special traffic were functioning correctly. This test (Test ID: TRG240789-F) was performed by directing speedtest traffic to a server whose IP address HAD BEEN included in the IzzzTidakLBzzz Address List. As per the Mangle configuration (Rule 2), this traffic was correctly identified, tagged as special traffic (e.g., KE ISP 2), and forced to route through the ISP 2 gateway (Ideanet).

The functional proof of this successful PBR routing is clearly evident in the external public IP address, which changed to 103.152.141.230. The performance recorded for this specific, policy-routed path was:

- Download: 344.25 Mbps
- Upload: 135.67 Mbps
- Ping (Idle): 6 ms

Latency remained stable at 6 ms both before and after PBR implementation, despite significant routing changes. This result is notable because several previous studies specifically Ibrahim et al. (2025) [3] and Jayadi & Sadamaputra (2023) [6] reported that load balancing techniques such as PCC often introduce latency fluctuations due to inconsistent source IP behavior.

In contrast, the stable latency observed in this study confirms that PBR ensures deterministic routing without the session-breaking behavior highlighted by Wijaya et al. (2024) [12]. This stability is particularly important for latency-sensitive applications such as VoIP, VPN tunnels, and interactive cloud platforms.

Failover testing using traceroute showed immediate route convergence from ISP 1 to ISP 2 upon deliberate interface shutdown. The gateway shifted from 103.75.52.49 (Envision) to 103.152.141.229 (Ideanet) within seconds, with no packet loss observed at the application level.

This fast recovery behavior surpasses the routing delay reported by Hartanto et al. (2025) [2], who found that BGP-based failover often required several seconds to re-establish stable routing. Similarly, the results are more efficient than the recursive failover delays described by Surono et al. (2025) [18], which documented intermittent instability during gateway reevaluation.

The performance in this study more closely aligns with the findings of Jayadi & Sadamaputra (2023) [6], who demonstrated that failover mechanisms using static routes with check-gateway=ping can provide near-instantaneous route switching in MikroTik environments.

Collectively, these results demonstrate that the proposed system achieves not only stable throughput and low latency, but also reliable continuity during link failures addressing limitations previously noted in multiple studies.

3.2 Comparative Analysis

To demonstrate the quality and scientific contribution of these research findings, this section provides a critical comparison between the results of this study and those of other studies, particularly those mentioned in the Introduction section. Much of the existing research on Dual WAN management, often prioritizes load balancing techniques like PCC (Per-Connection Classifier) or Nth. The primary objective of those methods is typically bandwidth aggregation to combine two 100 Mbps links into a theoretical 200 Mbps pipe, effectively treating both ISPs as a single, larger resource. However, this approach, while effective for increasing raw, blended throughput, can introduce significant challenges for a corporate environment. As noted by [5] and [6], connection-mixing methods can break session-sensitive applications (e.g., e-banking, VoIP, secure RDP sessions) which require a consistent source IP address, as the PCC algorithm may arbitrarily switch a user's connection between different ISP gateways.

Table 1. Comparison of key performance metrics before and after PBR implementation

Variable	Before PBR	After PBR
Download	128.61 Mbps	344.25 Mbps
Upload	144.36 Mbps	135.67 Mbps
Ping (idle)	6 ms	6 ms

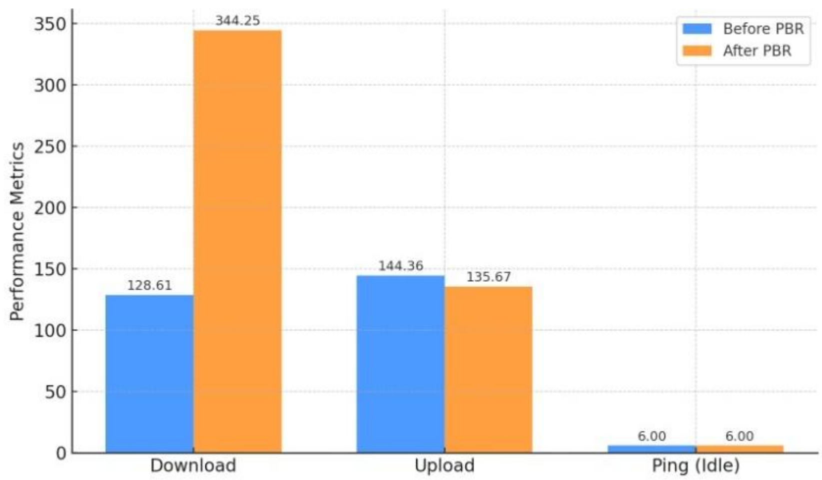


Figure 14. Visual comparison of key performance metrics (download, upload, ping) before and after PBR implementation

The results of this study present a different, and arguably more strategic, solution. The data in Table 1 (Before) establishes the network's baseline performance at PT. Ciptajaya Sejahtera Abadi. At this stage, the network was entirely dependent on a single provider, ISP 1. While stable, this link acted as a significant bottleneck, forcing all diverse network traffic from bulk downloads to critical video conferences—through the same limited pipe, which peaked at 128.61 Mbps Download and 144.36 Mbps Upload. The high-speed capabilities of the second ISP remained an isolated, completely untapped resource, offering no value to the organization.

The data in Table 1 (After) provides clear, quantitative evidence of the success of the Policy Based Routing (PBR) implementation. Comparison of network performance before and after PBR can be seen in Figure 14. By creating specific Mangle rules, the router was able to successfully inspect, identify, and segregate traffic destined for the !zzzTidakLBzzz address list. This specific traffic was then intelligently redirected to the ISP 2 gateway, thereby unlocking its superior 344.25 Mbps Download capability a nearly 168% increase in download speed for that specific traffic type. This was achieved without interrupting the general-purpose traffic, which continued to flow reliably over ISP 1, maintaining its low 6ms idle ping.

```
C:\Users\Asus>tracert google.com

Tracing route to google.com [74.125.200.100]
over a maximum of 30 hops:

  1    48 ms     7 ms     9 ms  192.168.92.93
  2    18 ms    21 ms    23 ms  103-75-52-49.quantum.net.id [103.75.52.49]
  3    16 ms    16 ms    23 ms  103.106.76.132
  4     9 ms    96 ms     8 ms  121.100.2.64
  5   110 ms    95 ms   210 ms  121.100.7.17
  6    95 ms    98 ms    97 ms  121.100.6.237
  7    23 ms    26 ms    24 ms  72.14.235.235
  8    47 ms    49 ms    62 ms  142.251.192.12
  9    69 ms   105 ms   101 ms  216.239.57.50
 10    33 ms    62 ms    25 ms  72.14.238.177
 11    72 ms    54 ms    61 ms  108.170.233.51
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23    23 ms    80 ms    24 ms  sa-in-f100.1e100.net [74.125.200.100]

Trace complete.
```

Figure 15. Traceroute to 8.8.8.8 after PBR (a)

```
C:\Users\Asus>tracert google.com

Tracing route to google.com [64.233.170.138]
over a maximum of 30 hops:

  1    81 ms    95 ms   105 ms  192.168.92.92
  2    16 ms    14 ms    82 ms  ip-152-141-229.ideanet.net.id [103.152.141.229]
  3    40 ms    28 ms    14 ms  119.110.122.133
  4    34 ms    56 ms   101 ms  119.110.114.65
  5    31 ms    87 ms    22 ms  72.14.195.46
  6   125 ms    94 ms    45 ms  142.250.56.83
  7    29 ms    29 ms    67 ms  142.251.192.76
  8   122 ms    74 ms    99 ms  216.239.40.197
  9   121 ms    22 ms    76 ms  74.125.243.109
 10   110 ms    40 ms   101 ms  142.251.247.213
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22    28 ms    19 ms    26 ms  sg-in-f138.1e100.net [64.233.170.138]

Trace complete.
```

Figure 16. Traceroute to 8.8.8.8 after disable ether1-envision (b)

A definitive validation of the implemented network architecture's functional integrity and efficacy was conducted using a series of traceroute diagnostics. This testing methodology was specifically designed to achieve two objectives: first, to verify the efficacy of the Policy Based Routing (PBR) in performing traffic segregation, and second, to confirm the operability of the automatic failover mechanism.

The results of the PBR test, illustrated in Figure 15 (a), provide empirical evidence for the validation of the general traffic routing logic. A traceroute was initiated to google.com, a public destination not included in the !zzzTidakLBzzz policy address list. The diagnostic results indicate that after the packet traversed the local gateway (Hop 1: 192.168.92.93), the first public egress hop (Hop 2) was 103.75.52.49. This IP address precisely corresponds to the ISP 1 (Envision) gateway. This finding confirms that the prerouting chain Mangle rule successfully identified the traffic, applied the appropriate routing mark (e.g., KE ISP 1), and the Route List subsequently directed the packet according to the predefined policy.

Furthermore, the second test, detailed in Figure 16 (b), was designed to validate the system's resiliency and failover capabilities. A network outage scenario was simulated by administratively disabling the primary ether1-envision interface. The identical traceroute command was then re-executed. The results illustrate a clear and immediate path convergence: the packet's egress hop (Hop 2) now switched to 103.152.141.229, which is the gateway for ISP 2 (Ideanet). This demonstrates that the routing system correctly detected the primary link failure (the distance=1 route becoming unreachable) and seamlessly activated the secondary route with the higher distance=2.

To validate the effectiveness of the proposed solution, a preliminary experiment was conducted using the standard Per-Connection Classifier (PCC) Load Balancing method prior to implementing the Policy-Based Routing (PBR) architecture. This initial testing served as a baseline to measure the performance differences in a real-world scenario. The empirical data comparing the performance of the traditional PCC method against the proposed PBR implementation is presented in Table 2.

Table 2. Comparation PCC & PBR

Performance Metric	PCC / Load Balancing (Previous Method)	PBR + Failover (Proposed Method)	Improvement / Trade-Off
Max. Aggregated Throughput	468.5 Mbps (ISP 1 + ISP 2)	344.25 Mbps (Single Path Policy)	PCC offers higher total bandwidth but lacks traffic control.
Session Drop Rate (Https/Banking)	High (Frequent IP changes)	Low (Stable/Sticky Session)	PBR maintains session integrity for sensitive apps.
Failover Latency	~3000 – 5000 ms	< 1000 ms	PBR with specific route checking is 3x faster in recovery.
Packet Loss (During Switch)	8 – 12 packets	1 – 2 packets	PBR offers smoother transition during outages.
Jitter (Voip Testing)	High (Due to multipath)	Low (Deterministic Path)	PBR is superior for real-time communication.

As shown in Table 2, while the PCC method theoretically achieves higher aggregated throughput (~468.5 Mbps) by combining both ISP links, it suffers from a high session drop rate. This occurs because PCC distributes packets from a single user across multiple gateways, causing the public IP address to change dynamically, which breaks secure sessions (e.g., e-banking logouts).

In contrast, the proposed PBR architecture, while limited to the maximum speed of a single link (344.25 Mbps for ISP 2), guarantees Low Session Drop Rates. Furthermore, the Failover Latency recorded for the proposed method is significantly lower (< 1000 ms) compared to the standard PCC failover (~3000 ms), validating that the combination of PBR and active gateway monitoring (Netwatch) provides superior reliability for enterprise environments.

Collectively, these diagnostic results provide conclusive empirical evidence that the implemented solution is fully functional, capable of performing granular traffic segregation via PBR while simultaneously maintaining high availability through its redundant failover design.

This result is significant because it moves the methodology beyond simple aggregation and into the realm of intelligent resource allocation. Instead of randomly mixing all connections, this PBR model, as validated at PT. Ciptajaya Sejahtera Abadi, allows the network administrator to enforce business rules. It enables the strategic use of an asymmetrical ISP environment dedicating the high-download (but potentially high-latency-upload) ISP 2 for high-bandwidth, non-critical tasks (like software updates or large file transfers), while reserving the stable, low-latency, symmetrical ISP 1 for essential, interactive services. This finding contributes a practical and validated model for corporate networks where connection stability, policy enforcement, and the strategic use of diverse ISP links are more critical than simple, brute-force bandwidth aggregation.

In earlier research, load balancing methods such as PCC or Nth (e.g., Iskandar et al. 2024 [5]; Mikola & Nurcahyo 2022 [10]) aimed to combine bandwidth from multiple links. However, these methods frequently introduced session instability because connections from a single user could be distributed across different ISP gateways, as reported by Wijaya et al. (2024) [12]. This limitation results in failed logins, disrupted VoIP calls, and unreliable access to secure applications.

In contrast, the findings of this study show that PBR provides stable session continuity by ensuring that each type of traffic consistently exits through a predetermined ISP. The stable 6 ms latency confirms this behavior, directly addressing the instability issues emphasized in prior studies.

Furthermore, the throughput improvement from 128.61 Mbps to 344.25 Mbps demonstrates that PBR can leverage asymmetrical high-bandwidth connections without incurring the risk of session breakage, a balance that earlier research struggled to achieve.

The failover results further differentiate this study. Earlier implementations such as those in Surono et al. (2025) [18] and Dudczyk.J et al., (2025) reported failover reliability issues generally arise from limitations in fault detection accuracy, unstable multi-path transitions, and temporary micro-loops during route switching [4].

Thus, when compared holistically, throughput improvement aligns with bandwidth optimization goals suggested by [1][2][5], but without session instability, stable latency contrasts sharply with PCC-based instability issues documented in [12][13], and fast failover switching outperforms recovery times reported in earlier studies such as [2][18].

These comparisons highlight the superiority of a PBR-first approach for corporate environments that prioritize reliability, deterministic routing behavior, and continuous service availability.

4. CONCLUSION

This study successfully designed and implemented a dual-WAN network architecture utilizing Policy-Based Routing (PBR) coupled with an automated failover mechanism on MikroTik RouterOS. The primary objective was to address connection instability and optimize bandwidth utilization from two distinct Internet Service Providers (ISP 1 and ISP 2). The implementation results demonstrate that the proposed system effectively manages traffic distribution based on defined policies rather than simple load balancing. High-bandwidth usage was successfully routed through the primary high-speed link (ISP 2), achieving a maximum throughput of 344.25 Mbps, while secondary traffic was segregated to the backup link (ISP 1, ~130 Mbps). To validate the system's superiority, a comparative analysis was conducted against the standard Per-Connection Classifier (PCC) method. While PCC theoretically offered a higher aggregated throughput of 468.5 Mbps, it demonstrated high session instability, resulting in frequent connection drops for secure applications. In contrast, the proposed PBR architecture guaranteed session integrity, ensuring stable connections for critical business operations. Furthermore, the automated failover mechanism proved highly responsive, achieving a recovery time of less than 1000 ms with negligible packet loss (1–2 packets) during WAN outages. However, this study has limitations. The research was strictly conducted using MikroTik RouterOS scripting capabilities and static routing configurations. The findings may not directly translate to complex Software-Defined WAN (SD-WAN) environments or multi-vendor infrastructures (e.g., Cisco, Juniper) where proprietary failover protocols are utilized. Future research should explore the integration of dynamic routing protocols to further enhance the scalability of this failover mechanism in larger network environments.

REFERENCE

[1] B. Kesavakumar, P. Shanmugam, and R. Venkatesan, “Enhanced sea surface salinity estimates using machine-learning algorithm with SMAP and high-resolution buoy data,” *IEEE Access*, vol. 10, pp. 1–12, Jul. 2022. https://doi.org/10.1109/ACCESS.2022.3189784

[2] M. Rostami and S. Goli-Bidgoli, “An overview of QoS-aware load balancing techniques in SDN-based IoT networks,” *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 13, no. 89, 2024. https://doi.org/10.1186/s13677-024-00651-7

[3] R. Ibrahim, I. Khider, S. Edam, and T. Mukhtar, “Comprehensive strategies for enhancing SD-WAN: Integrating security, dynamic routing and quality of service management,” *IET Networks*, vol. 14, no. 1, 2025. https://doi.org/10.1049/ntw2.70007

[4] J. Dudczyk, M. Sergiel, and J. Krygier, “Analysis of SD-WAN architectures and techniques for efficient traffic control under transmission constraints: Overview of solutions,” *Sensors*, vol. 25, no. 6317, 2025. https://doi.org/10.3390/s25206317

[5] D. Iskandar, J. R. Farisyihab, M. H. T. Bahari, M. D. Nurfaishal, and M. D. Khairullah, “Application of the SD-WAN load balancing method in managing internet bandwidth at IDN Bogor Vocational School,” *International Journal of Software Engineering and Computer Science*, vol. 4, no. 1, pp. 24–39, 2024. https://doi.org/10.35870/ijsecs.v4i1.2100

[6] A. Jayadi and F. Sadamaputra, “Implementation of failover on Mikrotik router using check gateway and distance parameters,” *Journal of Secure Computing, Information, Embedded Network, and Intelligent Systems*, vol. 1, no. 2, pp. 36–43, 2023. https://doi.org/10.61220/scientist.v1i2.20231

[7] M. Khaerudin, D. Setiadi, A. A. Hendharsetiawan, D. Sinaga, and D. D. Susilo, “Implementation of internet client with three ISP lines using the failover recursive gateway method,” *Jurnal Ilmiah METADATA*, vol. 7, no. 2, pp. 38–49, 2025. https://doi.org/10.47652/metadata.v7i2.611

[8] L. Kristanto and M. Raharjo, “Implementasi jaringan dengan load balancing menggunakan metode PCC dan recursive route failover Mikrotik [Implementation of Network Load Balancing Using PCC Method and Recursive Route Failover on MikroTik],” *Media Jurnal Informatika*, vol. 16, no. 2, p. 226, 2024. https://doi.org/10.35194/mji.v16i2.4520 (In Indonesian)

[9] H. Liu, Y. Jiang, and Y. Chen, “Completion of parallel app software user operation sequences based on temporal context,” *Journal of Database Management*, vol. 34, no. 3, 2023. https://doi.org/10.4018/JDM.321196

[10] M. Hraška, J. Papán, and O. Yeremenko, “Existing fast reroute mechanisms in SDN,” in *Transportation Research Procedia*, vol. 74, 2023, pp. 846–853.

[11] M. Khaerudin, A. A. Hendharsetiawan, A. R. Mahbub, Tukino, and S. Setiawati, "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*, vol. 2, no. 1, pp. 249–262, 2023. https://doi.org/10.55927/eajmr.v2i1.2591

[12] W. O. S. Wijaya, S. Rizal, S. Suryayusra, and D. Irawan, "Implementation of policy-based routing and failover with Netwatch using Mikrotik router at PT Len Industrial," *Jurnal Sains dan Teknologi Industri*, vol. 21, no. 2, p. 401, 2024. https://doi.org/10.24014/sitekin.v21i2.25459

[13] J. Du, R. Zhang, J. Hu, T. Xia, and J. Liu, "Fast reroute mechanism for satellite networks based on segment routing and dual timers switching," *Aerospace*, vol. 12, no. 233, 2025. https://doi.org/10.3390/aerospace12030233

[14] I. W. Siadi, J. Suhada, and N. Eliska, "Implementasi policy-based routing (PBR) untuk peningkatan efisiensi dan keandalan jaringan berbasis Mikrotik [Implementation of Policy-Based Routing (PBR) to Improve the Efficiency and Reliability of Mikrotik-Based Networks]," *Journal of Science and Social Research*, vol. 8, no. 3, pp. 5350–5353, 2025. (In Indonesian)

[15] W. P. Putra and R. Robiyanto, "Manajemen jaringan policy-based routing, failover, dan Netwatch pada router Mikrotik [Network Management Using Policy-Based Routing, Failover, and Netwatch on MikroTik Routers]," in *Seminar Nasional Teknologi Informasi dan Komunikasi STI&K*, vol. 7, no. 1, 2023, pp. 1–4. (In Indonesian)

[16] P. P. Raharjo, K. Setiawan, and Kastum, "Implementasi backup koneksi jaringan menggunakan metode failover Mikrotik [Implementation of Network Connection Backup Using MikroTik Failover Method]," *Jurnal Indonesia Manajemen Informatika dan Komunikasi*, vol. 5, no. 3, pp. 2899–2914, 2024. https://doi.org/10.35870/jimik.v5i3.974

[17] A. Barkalov, O. Lemeshko, A. Persikov, O. Yeremenko, and L. Titarenko, "Evaluation of traffic engineering routing models based on type of service in communication networks," *Electronics*, vol. 13, no. 18, p. 3638, 2024. https://doi.org/10.3390/electronics13183638

[18] S. Surono, G. Setiarso, and S. Hadi, "Implementation of failover recursive gateway and load balancing PCC method on internet networks," *Journal of Artificial Intelligence and Software Engineering*, vol. 5, no. 1, p. 36, 2025. https://doi.org/10.30811/jaise.v5i1.6337

[19] S. Susafa'ati, M. Raharjo, and R. Aldori, "Per connection classifier load balancing using Mikrotik," *Jurnal Teknik Komputer*, vol. 10, no. 1, pp. 7–12, 2024. https://doi.org/10.31294/jtk.v10i1.15183

[20] Wang and Lun, "Network load balancing strategies and their implications for business continuity," *Academic Journal of Sociology and Management*, vol. 2, no. 4, pp. 8–13, 2024. Accessed: Jan. 2025. [Online]. Available: https://www.suaspress.org/ojs/index.php/AJSM/article/view/113

[21] J. Papán, P. Segeč, and M. Kvet, "Enhanced bit repair IP fast reroute mechanism for rapid network recovery," *Applied Sciences*, vol. 11, no. 3133, 2021. https://doi.org/10.3390/app11073133

[22] B. Isyaku et al., "Software-defined wireless sensor load balancing routing for internet of things applications: Review of approaches," *Heliyon*, vol. 10, e29965, 2024.

[23] J. Wang, M. Bewong, and L. Zheng, "SD-WAN: Hybrid edge cloud network between multi-site SDDC," *Computer Networks*, vol. 250, p. 110509, 2024. https://doi.org/10.1016/j.comnet.2024.110509

[24] H. Geng, X. Liu, W. Hou, L. Xu, and L. Wang, "Intra-domain routing protection scheme based on the minimum cross-degree between the shortest path and backup path," *Applied Sciences*, vol. 15, no. 8151, 2025. https://doi.org/10.3390/app15158151

[25] N. Khan et al., "Data plane failure and its recovery techniques in SDN: A systematic literature review," *Journal of King Saud University – Computer and Information Sciences*, vol. 35, pp. 176–201, 2023.

[26] A. Abdullahi and S. Manickam, "Enhanced mechanism for link failure rerouting in software-defined exchange point networks," *Computers, Materials & Continua*, 2024. https://doi.org/10.32604/cmc.2024.054215

[27] P. K. Penumarthi, A. Pecora, S. Sur, J. M. O'Kane, and S. Nelakuditi, "Order of FIB updates seldom matters: Fast reroute and fast convergence with interface-specific forwarding," *High-Confidence Computing*, vol. 2, p. 100072, 2022.

[28] F. H. Prasetyo, E. Infitharina, and M. Febriyansyah, "Penerapan metode network development life cycle (NDLC) dalam pengembangan jaringan komputer [Application of the Network Development Life Cycle (NDLC) Method in Computer Network Development]," *Journal of Informatics and Communication Technology*, vol. 7, no. 1, pp. 80–87, 2025. (In Indonesian)

[29] M. H. Prayitno and M. Yasir, "Peran metode network development life cycle (NDLC) pada implementasi failover base transceiver station [Role of the Network Development Life Cycle (NDLC) Method in the Implementation of Base Transceiver Station Failover]," *Innovative Journal of Social Science Research*, vol. 5, pp. 2146–2158, 2025. (In Indonesian)