JOURNAL INFORMATIC, EDUCATION AND MANAGEMENT
Vol 7 No 2 (2025): March 2025 - August 2025, pp. 336 ~ 349
ISSN: 2716-0696, DOI : 10.61992/jiem.v7i2.150

Optimizing Network Uptime Through Dual ISP Failover Implementation Using Netwatch

Hoesiin[1], **Boy Yuliandi**[1*]
[1] Universitas Dian Nusantara

Article Info
Article history:
Received 2 August 2025
Revised 5 August 2025
Accepted 9 August 2025

Keywords:
Failover, Dual ISP, MikroTik, Netwatch, NDLC.

ABSTRACT
Stable internet connectivity is a crucial aspect in supporting company operations, especially for businesses that rely on Point of Sale (POS) systems such as PT. XYZ. A common issue encountered is the loss of internet connection due to disruptions from the primary Internet Service Provider (ISP), which results in the POS system becoming inoperable and transactional activities being disrupted. To address this problem, this study proposes and implements a failover solution using two ISP connections with the help of MikroTik devices and the Netwatch feature. The methodology employed follows the Network Development Life Cycle (NDLC) approach, consisting of six phases: analysis, design, simulation, implementation, monitoring, and management. The analysis phase is conducted to identify network needs and issues. In the design phase, a dual ISP topology is created along with NAT configuration, static routing, and Netwatch as the connection detection system. The implementation phase involves setting the primary and backup routes using distance parameters and automated Netwatch scripts to switch connections during disruptions. Testing results show that failover occurs automatically in under five seconds without significantly affecting the internet connection. The results demonstrate that the dual ISP system with failover configuration effectively minimizes downtime and enhances overall network availability. This solution is also flexible and can be adapted for other branches with cost efficiency and good scalability.

Corresponding Author:
Boy Yuliandi | Universitas Dian Nusantara
Email: boy.yuliadi@undira.ac.id

1. Introduction

Network availability plays a vital role in daily activities, especially in the digital era. Its function goes beyond personal communication—it facilitates transactions, education, and work processes. A network enables computer devices to connect with each other, allowing for efficient data and information exchange. According to the Indonesian Internet Service Providers Association (APJII), internet users in Indonesia have reached over 221 million out of a total population of nearly 280 million an increase of 1.4% compared to the previous survey period. This indicates the growing necessity of internet connectivity.

A stable internet connection is a universal necessity. Relying on a single Internet Service Provider (ISP) poses significant risks for organizations, particularly in terms of potential downtime (Syahrani & Yuliadi, 2023). Many businesses and institutions operate with systems that heavily depend on consistent internet access. One such system is the Point of Sale (POS), used to manage sales and customer transactions at each company branch. To support its performance, a stable internet network is crucial, ensuring that transactional data is stored and integrated with the central server in real-time. Minimizing downtime in customer transactions, which are dependent on internet access, is critical. A stable network ensures uninterrupted business operations and smooth data processing. Conversely, any disruption such as an ISP outage can hinder operational activities, delay customer service, and risk the loss of transaction data.

Previously relying on a single ISP makes the system vulnerable to failure, whether due to technical issues or excessive load on the provider. As a result, branches experiencing such disruptions are unable to access the POS system, which in turn affects services and overall business activities. Therefore, optimizing network availability requires designing a system capable of managing connectivity issues effectively (Almakhi et al., 2022).

A failover mechanism allows the network system to automatically switch to a backup ISP when the primary one fails (Almakhi et al., 2023). By implementing such a simulation, organizations can gain clearer insights into how to manage their networks more efficiently, particularly in emergency situations such as ISP infrastructure failures. The failover method enables uninterrupted operations without being solely dependent on a single internet connection (Zaen & Tantoni, 2023). Moreover, this approach presents a cost-effective alternative to full-scale implementation across all branches, which is especially beneficial for companies with limited budgets.

The proposed simulation serves as a practical starting point before deploying physical devices in the field, helping organizations ensure that the selected solution aligns with their technical needs and capacities. Through this study, it is expected that PT. XYZ will be able to continuously develop its network infrastructure and be better prepared to face potential network disruptions in the future.

2. Research Methodology

This study employs the Network Development Life Cycle (NDLC) method, which is considered suitable for the design, implementation, and evaluation processes of computer networks. NDLC is a systematic approach consisting of several stages, including analysis, designs planning, hardware and software selection, installation, testing, maintenance, and documentation. By applying this method, network design can be carried out in a structured and comprehensive manner, ensuring that the implementation results are optimized and aligned with the needs of the users or organization. The workflow of this process is illustrated in the following figure.

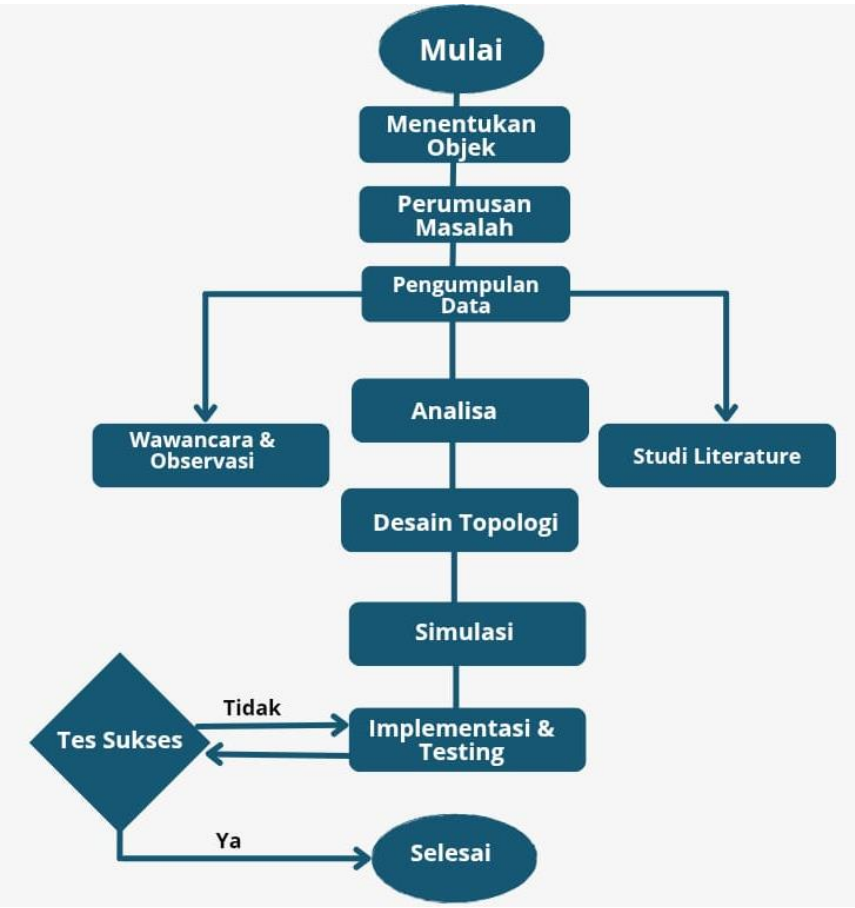


Figure 1. Flowchart

Analysis

The initial phase in the Network Development Life Cycle (NDLC) is initiation, which involves identifying the network requirements to be developed. This stage includes analyzing existing problems and defining the objectives of the network development. For example, ensuring continuous internet connectivity despite disruptions in the primary connection (failover) is one such objective. The outcome of this phase is a preliminary

understanding of the project scope, stakeholders involved, and the overall network coverage to be designed.

Design

The design phase aims to develop the network topology based on the analysis results. This includes the technical design of the system, such as selecting network devices (e.g., MikroTik routers and Orbit modems), configuring IP addresses, determining the connection methods, and specifying the failover configuration. The design also incorporates automatic connection switching scenarios using features such as Netwatch and distance-based routing configurations. The resulting design serves as a reference for the simulation and implementation stages.

Simulation

Simulation or prototyping is conducted to test the network design before full-scale deployment. At this stage, network configurations are tested in a simulated environment, either through virtual devices or limited physical setups. This phase is critical for verifying that the network design functions as expected, particularly regarding the failover mechanism and connection status detection. Simulation also helps identify potential errors prior to actual implementation.

Implementation

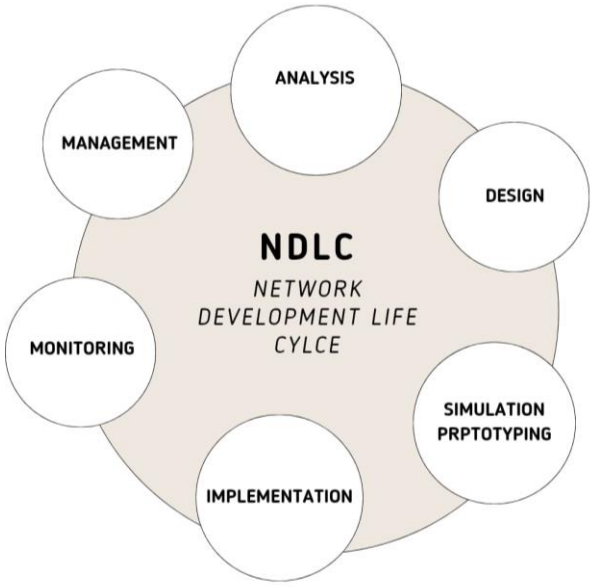
The implementation phase involves deploying the network design into a real environment. All hardware components are installed and configured according to the simulated design. In this study, for instance, the implementation includes installing and configuring the MikroTik router, setting up both primary and backup connections, and applying Netwatch scripts to detect connection failures. The main objective of this phase is to ensure that the network operates functionally and is ready for use.

Monitoring

Following implementation, the monitoring phase is conducted to regularly observe the network's performance. Monitoring aims to assess connection conditions, system stability, and ensure that the failover feature functions properly when disruptions occur in the primary connection. Tools such as MikroTik's logging features and monitoring scripts are used to record real-time network status. The monitoring results serve as the basis for evaluating the reliability of the network system.

Management

The final stage in the NDLC is network management. This includes ongoing system maintenance, reconfiguration when necessary, technical documentation, and troubleshooting operational issues. It also covers user access control, configuration backups, and system upgrades to support network scalability. With effective management, the network can continue to operate optimally over the long term.



Source: Akbar et al, 2023

Figure 2: Development Methods

During the analysis phase, the primary network issue identified was frequent downtime caused by the absence of a backup connection. In the subsequent design phase, a failover network topology was developed using two ISPs, configured through a MikroTik device. Following this, the proposed solution was implemented in the company's external network environment. However, during the management phase, regular monitoring could not be conducted due to time constraints and limited access to the research site. As a result, the process was concluded at the implementation phase.

3. Results and Discussion

PT. XYZ is a company engaged in the food and beverage (F&B) industry and utilizes a Point of Sale (POS) system to support sales transactions at each of its outlets. One of the main challenges faced by the company is its dependence on a stable internet connection. When disruptions occur with the Internet Service Provider (ISP), the internet network is completely disconnected due to the absence of a backup link, rendering the POS system inoperable and halting transaction processes.

A temporary solution has been implemented by using employees' smartphones as mobile hotspots. However, this approach has proven ineffective due to the high data consumption—used continuously for 6 to 10 hours—which results in financial strain for both employees and the company. This issue highlights a critical weakness in the network infrastructure, particularly the lack of an adequate failover system. Furthermore, the absence of real-time network monitoring slows down the response to network failures, negatively affecting customer satisfaction and store operations. To address this, a failover

system using Netwatch was implemented, applying the Network Development Life Cycle (NDLC) as the development methodology.

Analysis

In the Analysis phase of the NDLC cycle, the primary issues within PT. XYZ's network infrastructure were identified, particularly the frequent occurrences of internet downtime. Based on interviews with the operations team and direct observation, it was found that the company's reliance on a single internet connection was the main cause of Point of Sale (POS) service disruptions and operational disturbances during network outages. Additionally, the absence of a backup network system or failover solution further exacerbated the impact of these downtimes. Therefore, at this stage, the need for implementing a failover system using MikroTik devices was established, with the aim of maintaining connection stability and minimizing service interruptions during network failures.

Design

In this phase, a network topology was planned for implementation at PT. Inspirasi Bisnis Nusantara to enhance the reliability and availability of internet connectivity at the store. As illustrated in Figure 4.6.1, the proposed topology utilizes two Internet Service Providers (ISPs) to reduce the risk of downtime and ensure smooth operational continuity. With the integration of two ISPs, the store will have both a primary and a backup internet connection, allowing the backup link to be activated automatically in the event of a failure in the primary connection.

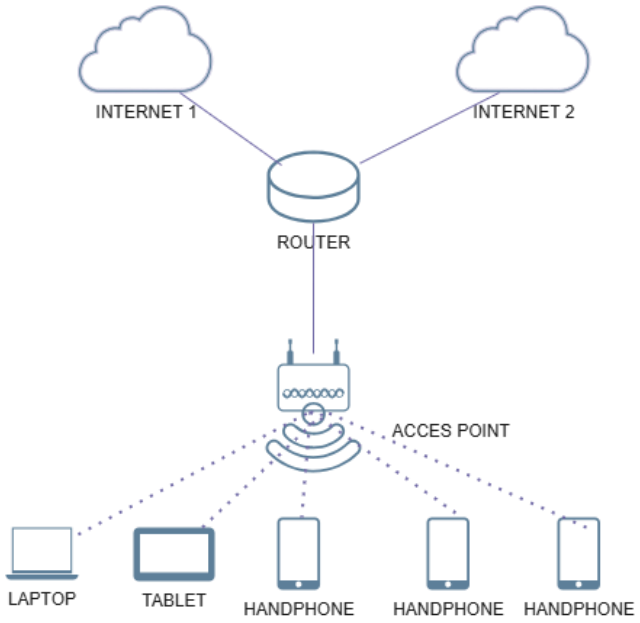


Figure 3. Topology Design

Simulation

In this phase, a simulation was conducted to test the failover script that would be implemented. The steps involved are as follows:

1. NAT Configuration for Clients

A NAT masquerade rule was added to enable clients to connect to the internet.

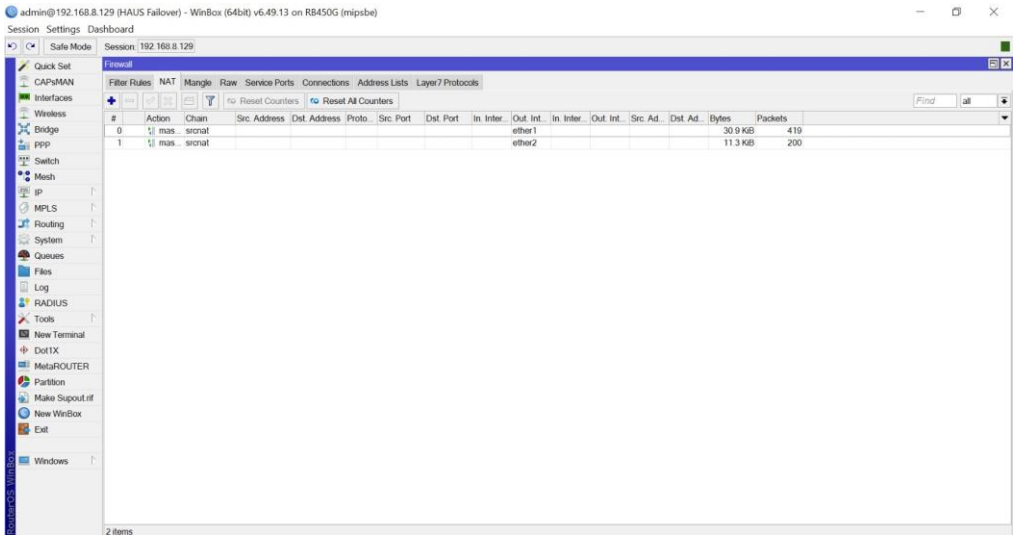


Figure 4. Setting NAT

During the Network Address Translation (NAT) configuration stage, client devices on the local area network (LAN) were granted internet access in the failover setup by configuring the router. NAT was implemented by creating masquerade rules on the MikroTik router for each available ISP uplink. These rules allow local client IP addresses to be translated into the public IP addresses provided by the ISPs, enabling internet access. In a failover system, the NAT rules must be associated with each ISP interface to ensure that network traffic can automatically switch to the backup ISP when the primary connection fails. This configuration ensures uninterrupted client connectivity during the failover process.

2. Netwatch Configuration

Rules for host, up, and down states were created to enable automatic decision-making for switching connection paths, which is essential in ISP failover scenarios.

a. Host Tab

As shown in Figure 5, the Netwatch feature on the MikroTik device was configured to monitor internet connectivity by pinging an external IP address. In this setup, the IP address 1.1.1.1 was selected as the monitoring target due to its high reliability and its common use as a reference for network connectivity checks.

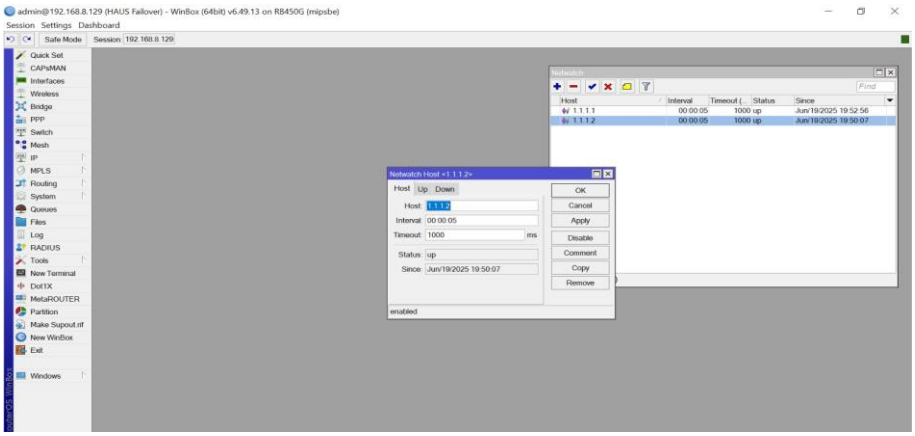


Figure 5. Host Tab

The system performs a connectivity check every 5 seconds, with a response timeout set to 1000 milliseconds. If no response is received from the target IP within this timeframe, the connection is considered down. The “up” status displayed in the configuration indicates that a connection to IP 1.1.1.1 is currently active, meaning that the primary ISP is still functional and in use.

b. Up Tab

Figure 6 shows the script configuration executed when the connection to the target IP becomes active again. The script used is: /ip route enable [find comment="ISP 1"]

This command is designed to re-enable the primary ISP route that was previously disabled due to a connectivity failure.

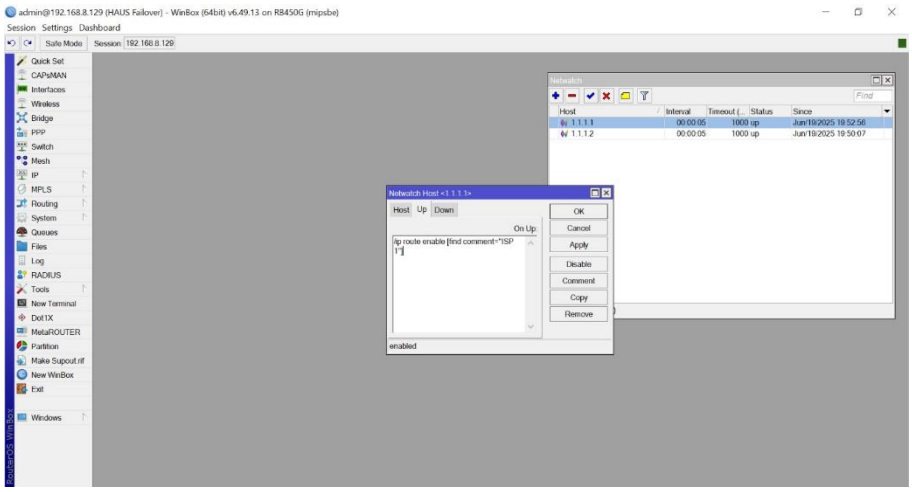


Figure 6. Up Tab

The use of the comment "ISP 1" in the route configuration allows the system to easily identify which route should be reactivated. As a result, when the MikroTik device detects that the connection has been restored, network traffic is automatically redirected back through the primary ISP without requiring manual intervention.

c. Down Tab

Figure 7 displays the script executed when the connection to the target IP address is disrupted or unresponsive.

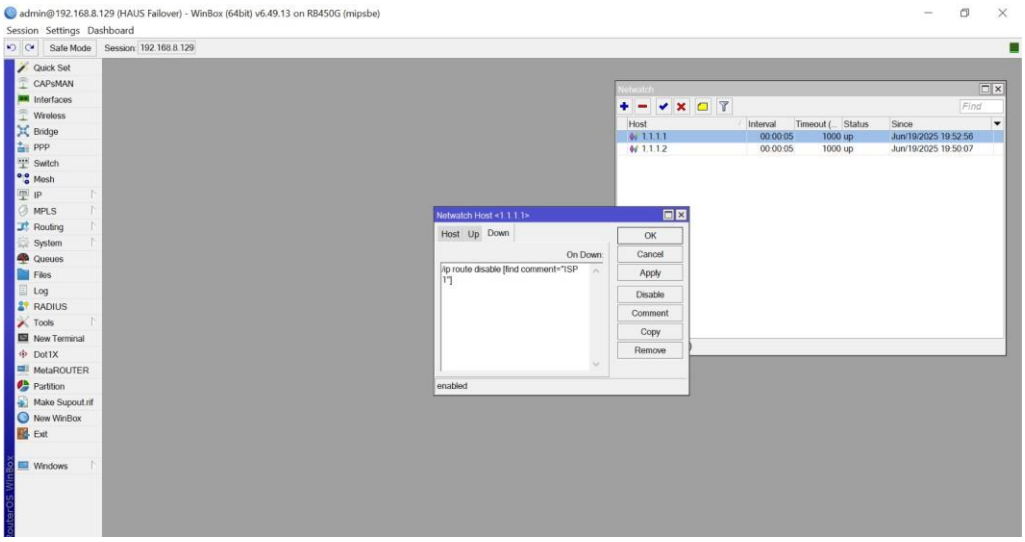


Figure 7. Down Tab

In this configuration, the command:

/ip route disable [find comment="ISP 1"]
is used to disable the route to the primary ISP. This step is intended to allow the system to automatically perform a failover to the backup ISP route that has been preconfigured. By disabling the primary route when the connection is unavailable, the router redirects network traffic through the alternative path, ensuring that internet connectivity remains available.

This mechanism is crucial for maintaining continuous network service automatically during disruptions in the primary ISP connection.

Static Route Configuration

The primary ISP is configured with a lower administrative distance value of 1, while the backup ISP is assigned a higher distance value of 2. MikroTik automatically uses the route with the lowest distance as long as the associated gateway is reachable. In the event of a failure in the primary ISP when the gateway becomes inaccessible the system will automatically switch to the backup route via the secondary ISP.

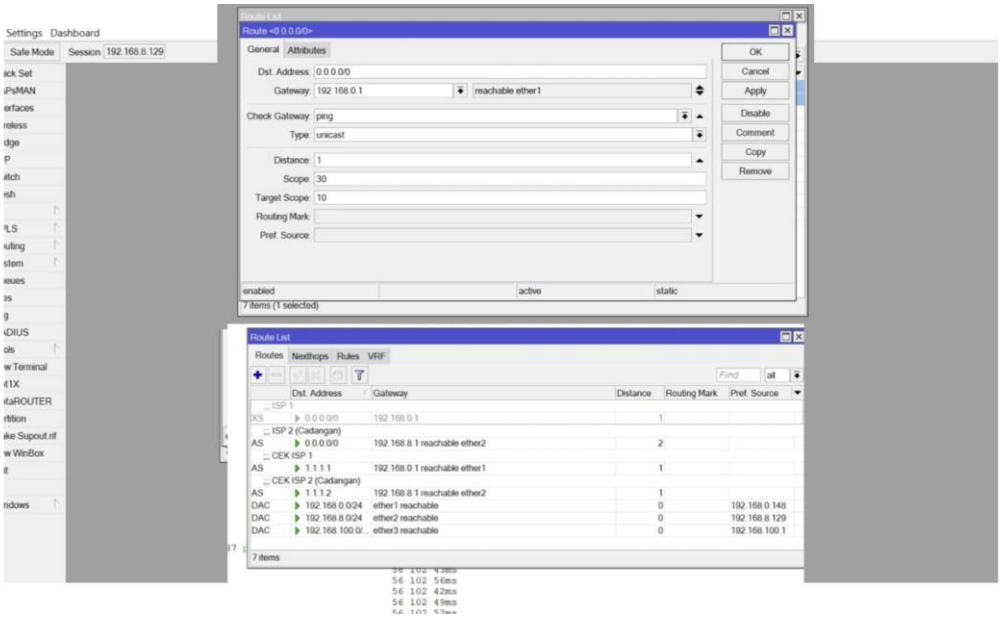


Figure 8. Static Route Configuration

As shown in the figure, the menu path IP > Routes displays multiple routing entries, specifically two main routes with destination address 0.0.0.0/0, which serve as the default gateways for internet connectivity. The first route uses gateway 192.168.0.1 via ether1, while the second route uses 192.168.8.1 via ether2. Each route is assigned a different distance value—1 for the primary route and 2 for the backup route—indicating the order of priority. The route with the lowest distance value is preferred as long as the corresponding gateway remains reachable.

The Check Gateway feature with the ping method is enabled to verify the responsiveness of the gateway. If the primary gateway fails to respond, the system will automatically redirect traffic through the backup route. Although Netwatch is commonly used to monitor specific IP addresses and execute automated scripts based on the monitoring results, in this configuration, the failover mechanism is triggered directly based on the ping response to the gateway.

Implementation

After all configuration and implementation stages were completed accurately and in accordance with the established procedures, the next step involved conducting a failover test to ensure the reliability of the system. The test was performed by intentionally disabling one of the internet connections—ISP1, which had been configured as the primary connection. Upon disconnecting ISP1, the system automatically switched to ISP2, which was set as the backup link.

a. Ping Test to Google

To verify the stability of the primary internet connection, a continuous ping to google.com was executed from the MikroTik terminal. This allowed monitoring of

response time (latency), the number of packets sent and received, as well as detection of any packet loss or timeouts.

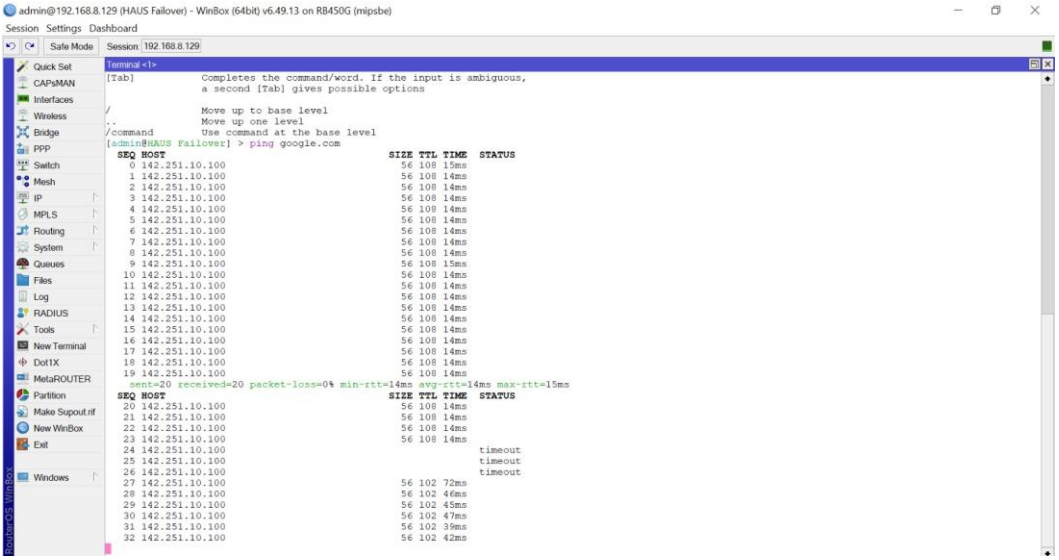


Figure 9. Test Ping

During normal operation, the internet connection functioned properly, indicated by consistent response times between 14–15ms. When the primary ISP connection was disconnected, response timeouts began to appear, indicating a disruption or failure in the main connection. This triggered the failover mechanism, whereby the MikroTik device detected the loss of connectivity and subsequently redirected internet access through the preconfigured backup route, ensuring uninterrupted network connectivity.

b. Connection Status Monitoring

Monitoring was conducted by observing the connectivity status of specific target IP addresses (e.g., 1.1.1.1 and 1.1.1.2). When the primary IP address becomes unreachable (down status), Netwatch executes an automated script to switch the internet route to the backup connection.

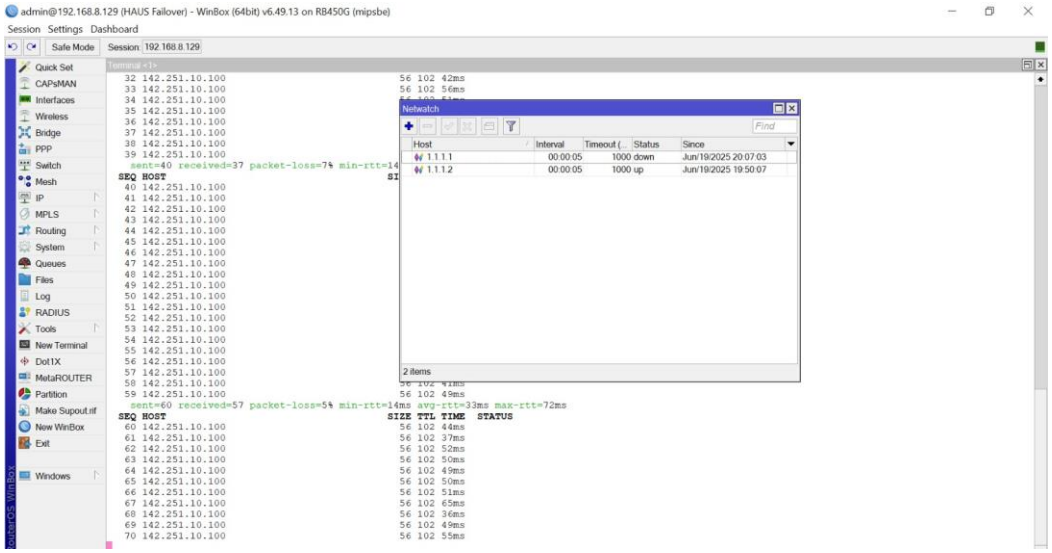


Figure 10. Connection Status Monitoring

The figure above displays the results of a connectivity test to IP 142.251.10.100, along with the Netwatch status window on the MikroTik device. The ping results indicate a 7% packet loss, which reflects degradation in connection quality. Simultaneously, the Netwatch status window shows that IP 1.1.1.1 is in a down state, while IP 1.1.1.2 is detected as up and has been active for some time. This confirms that Netwatch successfully detected the disruption on the primary route and automatically activated the backup route as an alternative path. This process plays a critical role in the failover mechanism, ensuring continuous connectivity even when the primary route becomes unavailable.

c. Disruption and Connection Switching Test

By performing a ping test to a target IP address and monitoring for timeouts or packet loss, the effectiveness of the failover system can be evaluated during a primary link failure—especially during high-bandwidth activities such as YouTube streaming. If the video continues to play without buffering, it indicates that the transition to the backup connection is seamless and does not disrupt the end-user experience.

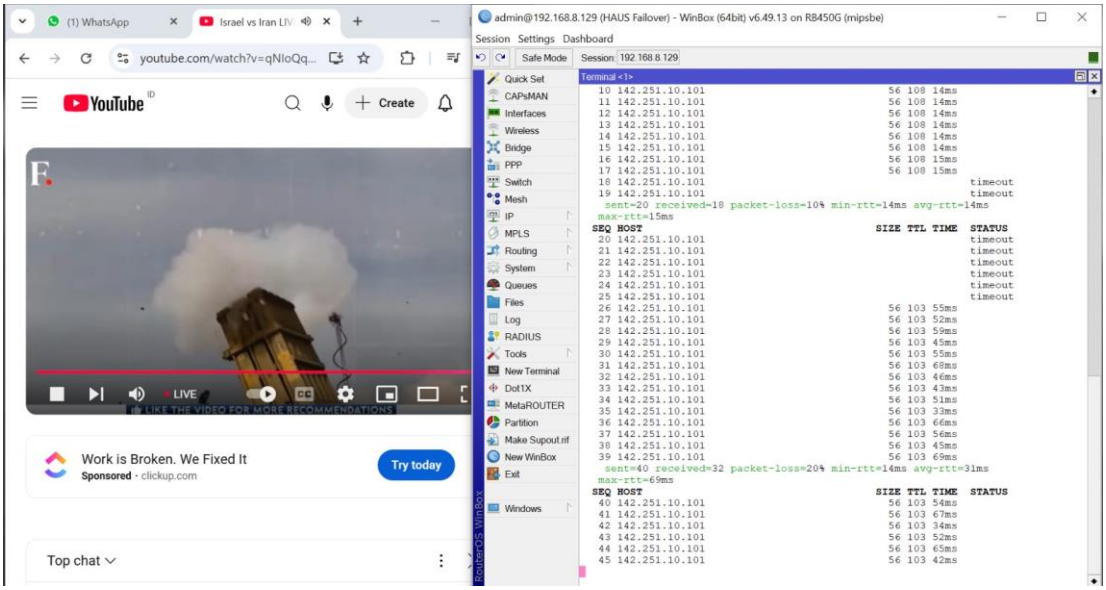


Figure 11. Disruption and Connection Switching Test

As shown in Figure 11, the failover test was conducted in real time while simultaneously streaming a video on YouTube. On the right side of the screen, the Winbox terminal is shown pinging the IP address 142.251.10.101. Multiple response timeouts and an increase in packet loss—ranging from 10% to 20%—can be observed, indicating significant disruption on the primary link. After a short delay, the connection resumes with varying response times, indicating that the system has successfully switched to the backup connection.

Meanwhile, on the left side of the screen, the video stream continues to play smoothly without interruption. This demonstrates that the implemented failover mechanism functions effectively, maintaining service stability even during disruptions in the primary internet connection.

4. Conclusions

Based on the results of the implementation and testing, several limitations were identified in this study, which can serve as a reference for future research. One of the main limitations is that the failover system relies solely on the Netwatch feature of MikroTik. Although effective in basic scenarios, Netwatch has limited flexibility and resilience when dealing with more complex network conditions, such as latency fluctuations, high jitter, or performance degradation without a complete disconnection.

Therefore, future research is recommended to develop a more advanced failover system that considers not only the binary up/down status of the connection, but also integrates Quality of Service (QoS) parameters such as latency, jitter, and packet loss as indicators for triggering failover. This enhancement could be achieved by incorporating additional monitoring scripts or third-party tools that work in parallel with Netwatch.

In addition, future studies may explore the implementation of active load balancing methods (e.g., PCC or ECMP) that allow simultaneous utilization of both ISPs, rather than using one solely as a backup. Such approaches could optimize bandwidth usage and reduce the risk of downtime due to overloading on a single connection. Moreover, implementation and testing could be expanded to larger-scale environments, such as branch offices or inter-location networks, to evaluate how the failover system performs under broader and more complex scenarios. Finally, the integration of configuration automation and documentation tools—such as Ansible or the MikroTik API scripting—may also improve operational efficiency in future network management practices.

References

Anshari, M. I. A. I., & Servenda, Y. (2024). Literatur Review: Sistem Failover Menggunakan Router Mikrotik. Jurnal Sains dan Teknologi (JSIT), 4(2), 195-200.

Khudori, A., Anton, A., & Nugraha, F. S. (2022). Implementasi Fail Over Dan Load Balance Untuk Grouping Jalur Koneksi User Dan Monitoring. Jurnal Infortech, 4(2), 120-125.

Muwajihan, I. I., & Jatikusumo, D. (2021). Perancangan Jaringan Ethernet Link Dengan Menggunakan Teknologi Link Aggregation Dan Auto Failover. IJCIT (Indonesian J. Comput. Inf. Technol, 6(2), 128-137.

Almakhi, R., & Nugraha, F. S. (2022). Implementasi Load Balancing Dan Failover Menggunakan IP SLA Pada PT Pan Pacific Insurance. Jurnal Infortech, 4(2), 98-104.

Zaen, M. T. A., & Tantoni, A. (2023). Analisis dan Implementasi Pengalihan Trafik Data (Failover) Akses Internet Pada Dua ISP. KLIK: Kajian Ilmiah Informatika dan Komputer, 4(3), 1726-1736.

Mawali, A. I., Tantoni, A., & Ashari, M. (2024). Implementasi Load Balancing Dan Failover Pada Jaringan Internet Hotel Puri Indah Dengan Metode NTH. Merkurius: Jurnal Riset Sistem Informasi dan Teknik Informatika, 2(4), 28-38.

Kamelia, Y., & Firdaus, I. C. (2024). Rancangan Dan Implementasi Internet Provider Di Kos–Kosan Jakarta Barat Dengan Metode Load Balance Menggunakan Router D-Link Dan TP-Link. OKTAL: Jurnal Ilmu Komputer dan Sains, 3(07), 1723-1730.

Sabila, K., Rahayu, S., & Sumarni, T. (2024). Peningkatan Efisiensi Penggunaan Sumber Daya Jaringan Melalui Teknik Load Balancing. CEMERLANG: Jurnal Manajemen dan Ekonomi Bisnis, 4(3), 31-41.