Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th October 2025. Vol. 5. No. 1; e-ISSN: 2808-4519

Design and Implementation of Internet Failover with Automated Email Notification for Network Continuity

Husni[1]*, Nurdin[2], Al Khaidar[3]

[1,2,3,] *Master of Information Technology Program, Malikussaleh University, Batam Street, Bukit Indah Campus, Lhokseumawe, Aceh.*
husniabda7@gmail.com[1*], nurdin@unimal.ac.id[2], alkhaidarkutablang@gmail.com[3]

Abstract

Rapid developments in telecommunications have increased the need for reliable and efficient communications networks. With the shift in information exchange from physical documents to digital formats, computer networks connected to the internet play a crucial role in sharing resources. In Indonesia, with internet penetration reaching 79.5% in 2024, internet network stability is very important. Disruptions to the network, such as bad weather or hardware failure, require failover solutions to maintain connection continuity. This research discusses the implementation of the failover method on Mikrotik routers to maintain a stable internet connection. Through IP configuration, DHCP Server, DNS, and firewall, the system can prioritize the primary path and provide a backup path. Monitoring is done with Netwatch for fast detection of intrusions, while mangle and firewall rules support automatic data traffic redirection. An automatic notification system via email, integrated with Mikrotik and Netwatch email servers, provides real-time information about connectivity status. Evaluation of network quality using the TIPHON method shows very good performance with throughput of 1,039,143.50 bps, packet loss of 0.77%, delay of 12.88 ms, and jitter of 0.00004 ms. These results show that the failover and notification system implemented is effective in maintaining network speed, stability and consistency.

Keywords: *Network Failover, Mikrotik Router and Email Notification*

1. Introduction

The rapid development of telecommunications today is driven by ever-increasing technological advances, resulting in an increasing need for reliable and efficient communication networks. Initially, information exchange was limited to physical documents such as handwritten and printed documents. However, with technological advancements, exchanges have shifted to digital forms through information networks that connect various nodes using cables or wireless media [1].

Computer networks, as part of a telecommunications system, enable nodes to share resources. Computer networks connected to the internet today facilitate the efficient and effective exchange of information between computers [2]. Indonesia, one of the countries with the highest number of internet users in the world, is experiencing a significant increase in internet penetration. According to data from the Indonesian Internet Service Providers Association (APJII), the number of internet users reached 221,563,479 in 2024 out of a total population of 278,696,200 in 2023, with a penetration rate of 79.5% [3].

The availability of a stable and reliable internet network is crucial for supporting operations and productivity. However, internet network disruptions are unavoidable and can be caused by various factors such as bad weather, hardware failure, or issues with service providers. To address this issue, the use of backup or failover connections is necessary. Failover allows alternative connections to automatically take over the primary connection when an outage occurs, ensuring business continuity without significant disruption [4]. Managing network outages requires real-time notification to the IT team or responsible parties. One effective method for providing notification is through an instant messaging platform integrated with email.

2. Literature Review

2.1 Computer Networks

A computer network is a system consisting of computers designed to share resources (such as printers and CPUs), communicate (via email and instant messaging), and access information (via web browsers). The purpose of a computer network is to enable each part of the network to request and provide services. The computer requesting or receiving services is called a client, while the computer providing or

sending services is called a server. This design is known as a client-server system and is applied to almost all computer network applications [5].

Based on its characteristics, it can be divided into four types, including [6]:

1) LAN Networks: Computer networks that cover only a small area, such as computer networks on campuses, buildings, offices, homes, schools, or smaller. Currently, most LANs are based on IEEE 802.3 Ethernet technology using switch devices, which have data transfer speeds of 10, 100, or 1000 Mbit/s. In addition to Ethernet technology, 802.11b technology (commonly known as Wi-Fi) is also frequently used to form LANs. Places that provide LAN connections with Wi-Fi technology are commonly called hotspots. In a LAN, each node or computer has its own computing power, unlike the concept of a dump terminal. Each computer can also access resources on the LAN according to predetermined access rights. These resources can be data or devices such as printers. On a LAN, a user can also communicate with other users using appropriate applications [6].
2) WAN is an abbreviation for Wide Area Network, which is a computer network that covers a wide area, such as between cities, regions, or even countries. A WAN can be defined as a computer network that requires routers and public communication channels. The primary function of a WAN is to connect one local network to another, allowing users or computers in one location to communicate with users or computers in other locations [6].
3) MAN Network: Metropolitan area network, or MAN for short. A network within a city with high-speed data transfer, connecting various locations such as campuses, offices, government offices, and so on. A MAN network is a combination of several LANs. The range of this MAN is between 10 to 50 km, this MAN is the right network Metropolitan area network or abbreviated as MAN. A network in a city with high-speed data transfer, which connects various locations such as campuses, offices, government, and so on. The MAN network is a combination of several LANs. The range of this MAN is between 10 to 50 km, this MAN is the right network to build a network between offices in one city between factories/agencies and head offices within its range [6].

2.2 Network Address Translation

Network Address Translation (NAT) is a technique used in computer networking to modify network address information in the IP header of packets as they pass through a traffic routing device [7]. NAT is typically used to improve security and reduce the number of IP addresses required by an organization. Here's a detailed explanation of how NAT works and its types.

NAT allows multiple devices on a local network to be mapped to a single public IP address. This is particularly useful for conserving the limited number of IPv4 addresses. When a device on an internal network sends a packet to an external network, the NAT device (usually a router or firewall) converts the source's private IP address to a public IP address. When a response arrives, the NAT device translates the public IP address back to a private IP address and forwards the packet to the appropriate device on the internal network. Here are the types of NAT [8].

1. Static NAT: Maps a single private IP address to a single public IP address. This is often used when a device within a private network needs to be accessed from the outside, such as a web server.

   Example: 192.168.1.10 (private) ↔ 203.0.113.10 (public)

2. Dynamic NAT: Maps a private IP address to a public IP address from a public IP address pool. The mapping is temporary and can change over time.

   Example: 192.168.1.10 (private) ↔ 203.0.113.10 (public)

at one point, and 203.0.113.11 at the next.

3. Port Address Translation (PAT): Also known as NAT overload, maps multiple private IP addresses to a single public IP address (or multiple addresses) but uses different ports to distinguish each connection. This is the most common form of NAT.

Example: 192.168.1.10:1234 (private) ↔ 203.0.113.10:5678 (public), 192.168.1.11:1234 (private) ↔ 203.0.113.10:5679 (public).

2.3 Failover Method

Failover is generally implemented to improve the availability of the services provided. Cluster elements operate with redundant nodes, which are then used to provide services when one of the cluster elements fails. The most common size for this category is two nodes, which is the minimum requirement for redundancy. This type of cluster implementation attempts to utilize the redundancy of cluster components to eliminate a single point of failure [9].

Failover can simplify network management for network administrators, eliminating the need for network configuration if the primary network goes down. Failover also ensures high availability and a reliable network. Implementing Failover and Autoscaling of Nginx Web Server Containers on Docker Using Kubernetes [10]. The similarities in this study are that both use Kubernetes, Docker containers, and an Nginx Web Server. The differences in this study lie in the implementation of failover, which is specifically carried out on the Nginx web server and the autoscaling process.

3. Research Methodology

3.1 Block Diagram Design

The design of this stage explains the configuration carried out by the network administrator or user as in Figure 1.

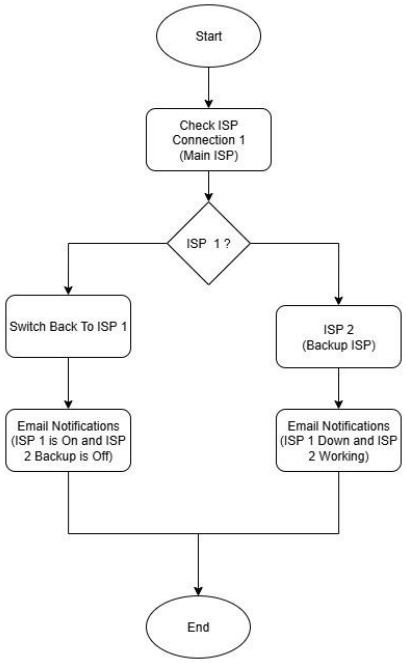

Fig. 1: Network Backup Flowchart

Figure 1 illustrates the process of checking an internet connection using two ISPs (Internet Service Providers). First, the program checks the connection to ISP 1, the primary ISP. If ISP 1's connection is active, the program will terminate immediately. If ISP 1's connection is down, the program will check the connection to ISP 2, the backup ISP. If ISP 2's connection is active, the program will send an email notification that ISP 1 is down and ISP 2 is working. If ISP 2's connection is also down, the program will send an email notification that ISP 1 and ISP 2 are down. After that, the program will check the connection to ISP 1 again. This process will continue until ISP 1's connection is active.

3.2 Network Topology Design

Network topology design functions as a mapping of the tools and materials used to connect to each other, which can be seen in Figure 2.

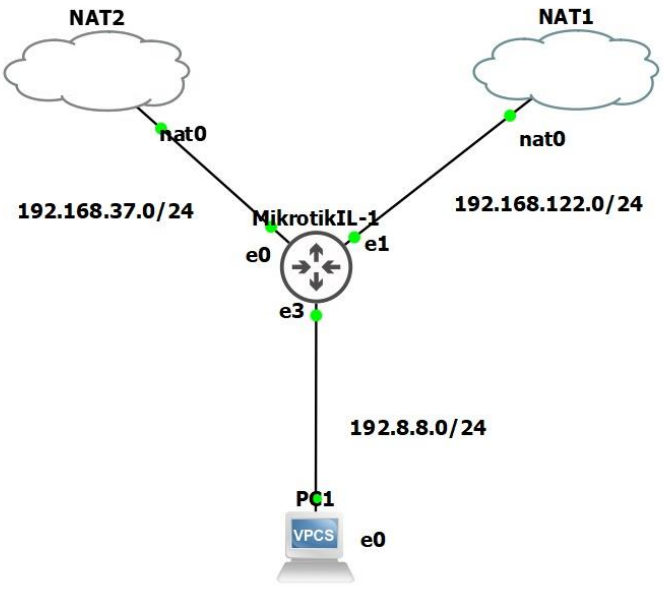

Fig. 2: Network Topology

Figure 1 shows a network topology configured using a Mikrotik router labeled "MikrotikIL-1." This router connects three different network segments, namely NAT1, NAT2, and PC1, each with a corresponding IP address range. The NAT1 segment is a private network with the address range 192.168.122.0/24. This segment is connected to the Mikrotik router through the e1 interface, which has been configured with Network Address Translation (NAT) mechanism labeled nat0. The NAT2 segment, similar to NAT1, is a private network with the address range 192.168.37.0/24. This segment is connected to the Mikrotik router through the e0 interface, which also uses NAT with the same configuration label nat0. This indicates the possibility of implementing similar or shared NAT rules between different segments. The PC1 segment is another network segment connected to the Mikrotik router through the e3 interface. The IP address range for this segment is 192.8.8.0/24, and most likely represents a local area network (LAN) or a dedicated subnet for end-user devices. PC1 is shown as being directly connected to the Mikrotik router via interface e0.

3.4 Testing Methods

In research on Internet Network Backup with the implementation of failover and email notification methods, QoS testing can be conducted by examining several important aspects. First, evaluation of network availability and performance is carried out by monitoring parameters such as response time, data transfer speed, latency, jitter, and packet loss both before and after a failover. Second, testing the reliability of the failover system is carried out through failure simulations to ensure that the backup system can function effectively, as well as verifying that email notifications are sent in a timely manner. Third, evaluation of QoS implementation must be carried out to ensure that the priority policy for important traffic remains consistently applied across both networks, namely the main network and the backup network.

4. Result and Discussion

This chapter discusses the implementation of the method for internet network backup using the failover method, as well as the results and testing of the system that was built. The results of this research and testing of the system will be explained in more detail as follows.

4.1 Topologi

This network topology consists of two NATs (InternetMain and InternetBackup) as ISPs, one Mikrotik router, and one Ubuntu client. InternetMain connects to Mikrotik via IP 192.168.37.130/24, while InternetBackup connects via IP 192.168.122.175/24. The Ubuntu client gets a dynamic IP from Mikrotik via DHCP on the 192.8.8.1/24 network as a LAN segment. The results of this topology are shown in Figure 3.

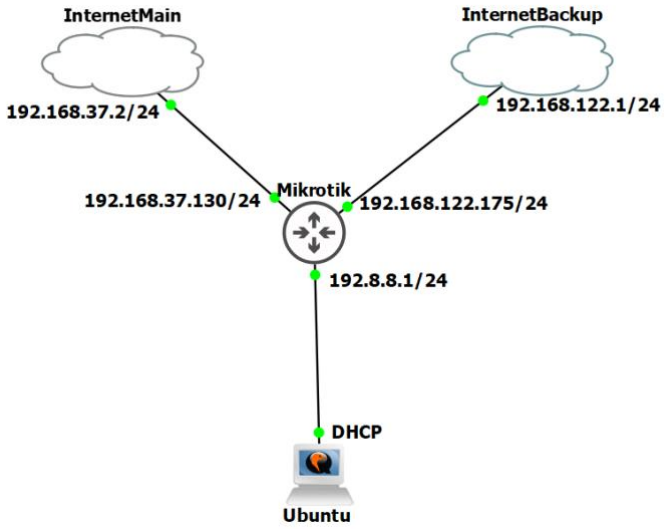

Fig. 3: Network Topology Creation

4.2 IP Configuration on Mikrotik

Basic configuration on a Mikrotik router by assigning IP addresses to each ethernet interface. Address List configuration on a Mikrotik router that includes three different network segments: Client, Main ISP, and Backup ISP. The Client segment uses the IP address 192.8.8.1/24 connected via the ether4 interface, indicating that this is the local network for client devices. The Main ISP, with the IP address 192.168.37.130/24, is connected via the ether1 interface and serves as the primary connection to the internet. Meanwhile, the Backup ISP uses the IP address 192.168.122.175/24 via the ether2 interface, which serves as a backup path if the main ISP experiences problems. The Configuration Results can be seen in Figure 4.

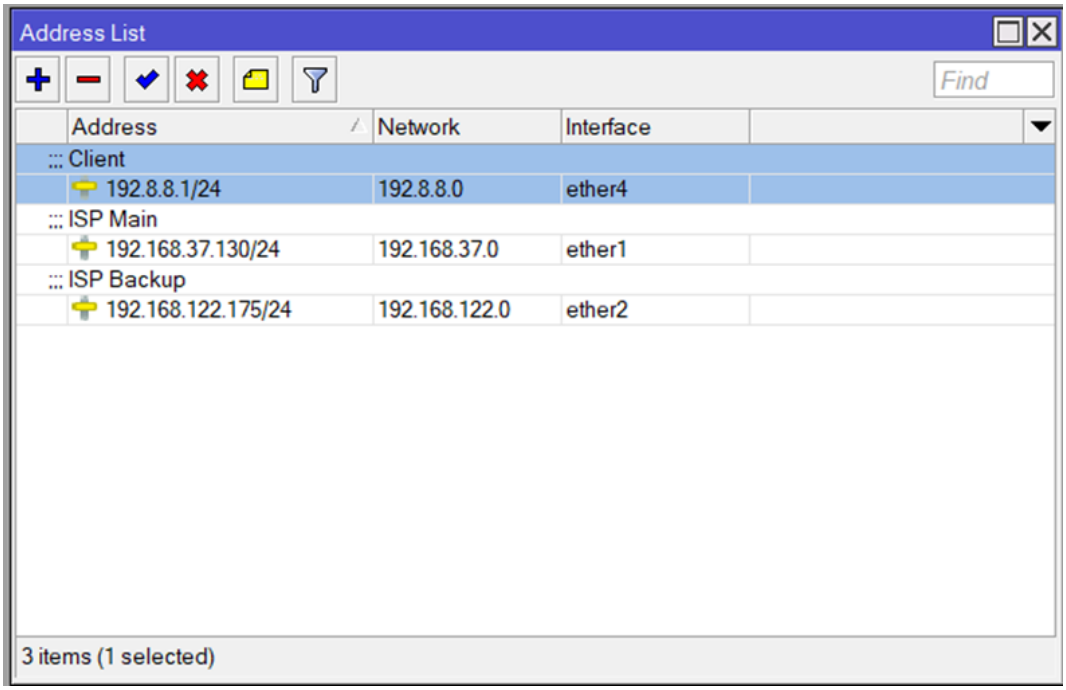

Fig. 4: Mikrotik Configuration

4.2 DNS Server

The DNS configuration on a Mikrotik router is used to define the primary DNS server that the router will use to query domain names and also for ping purposes as a benchmark for internet connectivity. The DNS configuration on the Mikrotik router lists three public DNS servers: Google's 8.8.8.8 and 8.8.4.4, and Cloudflare's 1.1.1.1, which are used for domain name resolution and as a ping benchmark for monitoring internet connectivity. These settings also include technical parameters such as a Max UDP Packet Size of 4096 bytes and a Query Server Timeout of 2 seconds to ensure efficiency and reliability in processing DNS queries. In addition, the router stores query results in a 2048 KiB cache with a maximum TTL of 7 days. The results can be seen in Figure 5.

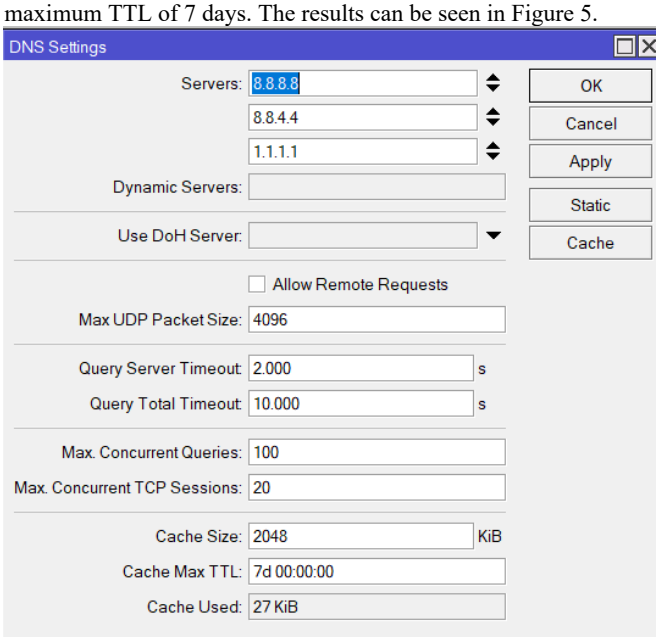

Fig. 5: DNS Server

4.3 ISP Network Monitoring Configuration

Monitor the status of ISP1 (the primary path) by configuring Netwatch on Mikrotik. Netwatch will periodically ping a specific address (e.g., 8.8.8.8) to determine whether ISP1 is active. If there is no response from ISP1, Netwatch will activate the backup path. The results can be seen in Figure 6.

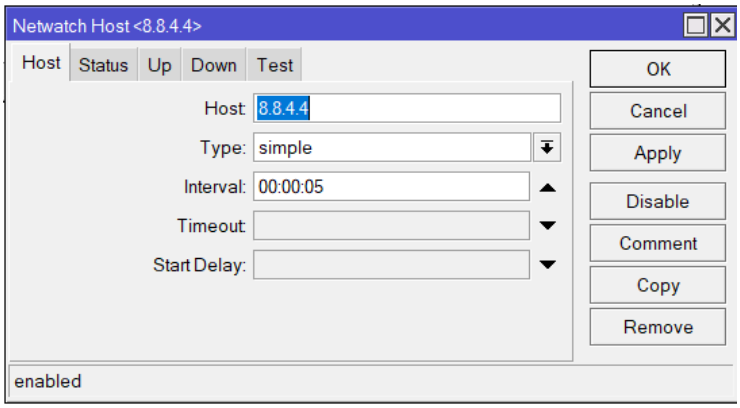

Fig. 6: ISP Monitoring

4.3 Rule Up and Down in Netwatch

Add the Up and Down rules to Netwatch. The Up rule will ensure that the primary path is reused when ISP1 is back online, while the Down rule will redirect connections to the backup path when ISP1 experiences an outage. The results can be seen in Figures 7 and 8.

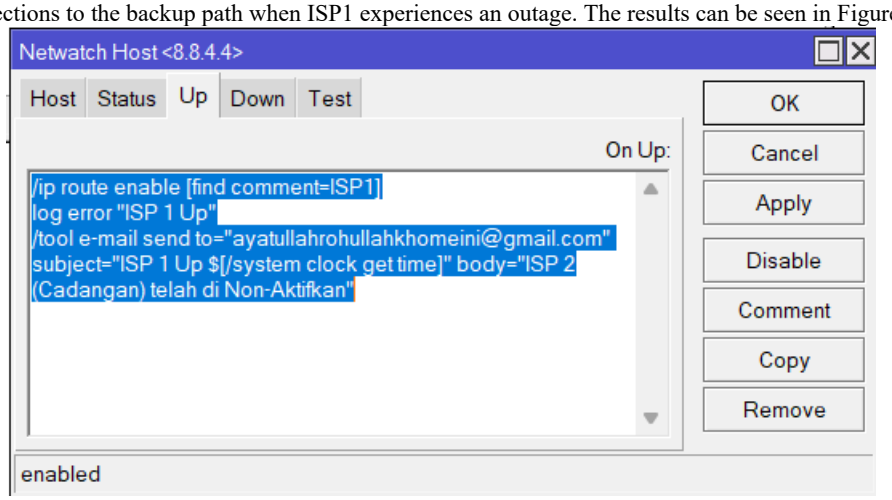

Fig. 7: Rule Up

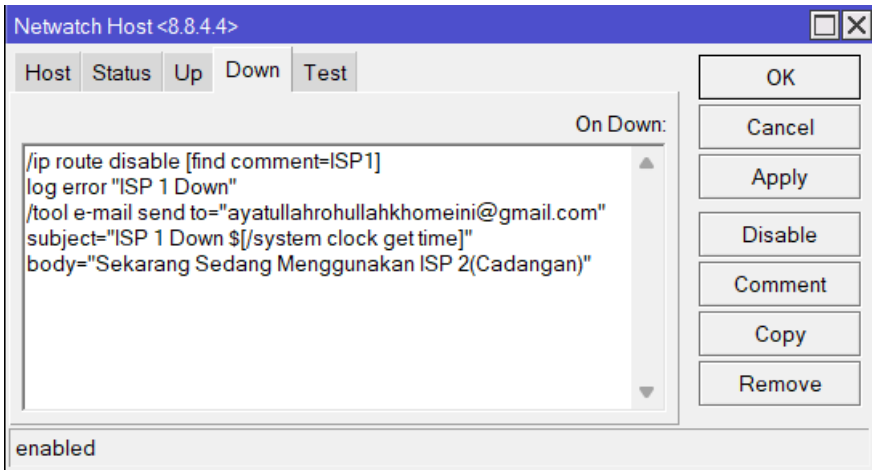

Fig. 8: Rule Down

4.4 Email Notification Configuration

Configure email notifications on Mikrotik. These notifications will be sent via email when there is a change in ISP connectivity status. Users will receive a notification when ISP1 is down or back up, allowing them to take the necessary action immediately. The results can be seen in Figure 9.

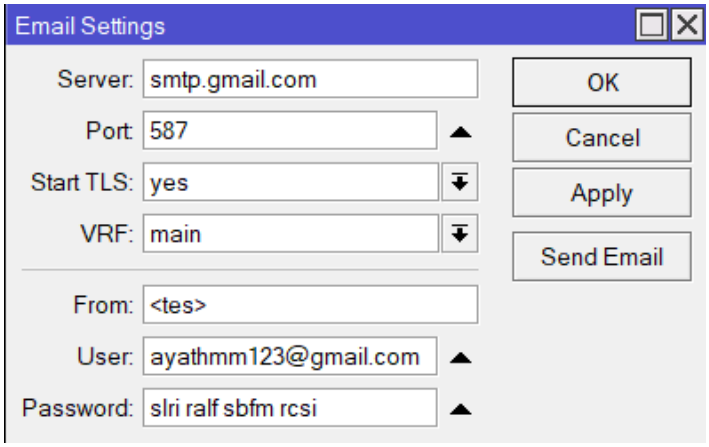

Fig. 9: Email Notification Configuration

4.5 Failover Testing With ISP Disconnection

The ISP disconnection failover test aims to evaluate the system's ability to detect failures in the primary ISP connection and automatically redirect network traffic to the backup ISP. The test results show that no data traffic is running through ether1, while the backup connection on ether3 is active with a transmit speed of 47.3 kbps and a receive speed of 5.4 kbps. This indicates that the system successfully redirects network traffic to the backup ISP via ether3, ensuring that connectivity is maintained even if the primary ISP fails. The results can be seen in Figure 10.

	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet
	;;; ISP Main							
X	ether1	Ethernet	1500		0 bps	0 bps	0	
	;;; ISP Backup							
R	ether2	Ethernet	1500		0 bps	0 bps	0	
R	ether3	Ethernet	1500		47.3 kbps	5.4 kbps	10	
	;;; Cliet							
R	ether4	Ethernet	1500		0 bps	0 bps	0	

Fig. 10: ISP disconnection

The disconnection result is indicated by an email notification sent to inform the user that ISP 1's connection was down at 17:54:24. The system automatically switches to using ISP 2 as a backup. This notification is part of a network monitoring mechanism designed to immediately inform administrators when the primary connection fails. The results can be seen in Figure 11.

Fig. 11: Email Down Notification

4.6 ISP Connection Reactivation Failover Testing

The purpose of ISP connection reactivation failover testing is to ensure the system can automatically switch to a backup ISP connection when the primary ISP connection fails, and revert to the primary connection once it is restored. Once the primary connection is restored, the system should automatically revert to the primary ISP. The results are shown in Figure 12 below.

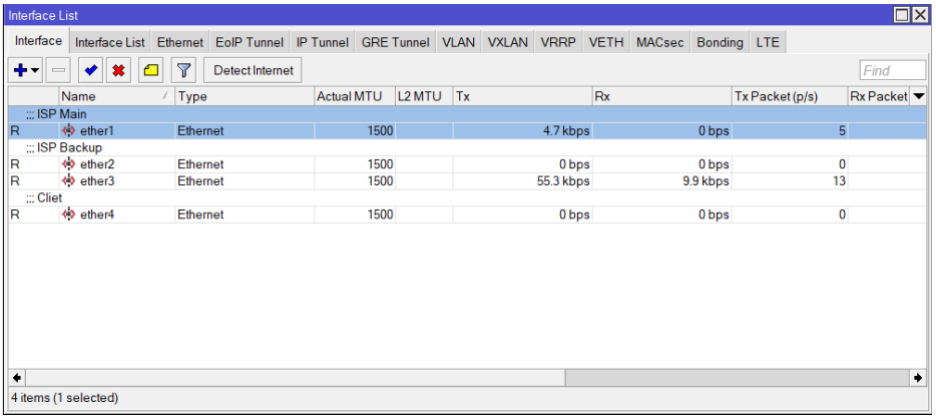

Fig. 12: ISP Activation

The result of the ISP connection reactivation is shown through an email notification sent at 17:59:19, which informs that ISP 1 connection has been reactivated (Up), but ISP 2 as a backup has been disabled. Although ISP 1 connection was successfully restored, this notification indicates that the backup ISP connection is unavailable because it has been disabled, which means the system no longer has an active backup to face the next failure. The results can be seen in Figure 13..

Fig. 13: Email Notification Up

4.7 Testing Using the Tiphon Method

Network testing using the TIPHON method is performed to evaluate various network performance parameters, including throughput, packet loss, delay, and jitter. This method provides a clear picture of network quality and stability by measuring data transmission speed, packet loss, delay time, and variability in packet delivery times.

Table 1: Typhon Method Testing

Parameters	Values	Result
Throughput	7,154,503 bytes : 55,080 seconds	1.039.143,50 bps
Packet Loss	(4.278 - 4.245) : 4.278 x 100	0,77%
Delay	Total Delay: 55.079,88246 ms	Average: 12.88 ms
Jitter	Total Jitter: 0,170284884 ms	Average: 0.00004 ms

Table 1 shows the results using the TIPHON method. The high throughput value of 1,039,143.50 bps indicates good network performance in terms of data transmission speed. Packet loss of 0.77% indicates that only a few packets are lost, indicating fairly good network stability. The average delay of 12.88 ms indicates low latency, meaning data delivery time is relatively fast. In addition, the very small jitter with an average of 0.00004 ms indicates that the delivery time between data packets is consistent without significant fluctuations. Overall, the quality of this network is good and reliable for data transmission needs.

Conclusion

The conclusions after going through the design and testing stages of Internet Network Backup Using the Failover Method and Email Notification are as follows.

1. Implementing the failover method on a Mikrotik router effectively maintains internet connection continuity by configuring various network elements in an integrated manner. By assigning appropriate IP addresses to each interface, configuring a DHCP Server for automatic IP distribution, and configuring DNS and firewalls, the system can prioritize the primary path and provide a backup path ready for use if needed. Monitoring using Netwatch ensures rapid detection of disruptions on the primary ISP, while appropriate mangle and firewall rules support automatic traffic redirection. Email notifications strengthen the system by providing real-time information on changes in connectivity status, allowing for a quick response to disruptions.
2. An automated email notification system for monitoring internet connections using a Mikrotik email server, Netwatch, and email scripts was successfully implemented. Network quality evaluation using the TIPHON method shows excellent performance: high throughput of 1,039,143.50 bps, packet loss of 0.77%, delay of 12.88 ms, and jitter of 0.00004 ms, indicating optimal network speed, stability, and consistency.

Reference

[1] A. Taufik, B. G. Sudarsono, A. Budiyantara, I. K. Sudaryana, and T. T. Muryono, *Pengantar teknologi informasi Sutarman*, vol. 43. 2022. [Online]. Available: http://badanpenerbit.org/index.php/dpipress/article/view/18
[2] E. Yuliansyah, S. Saputra, and I. Ali, "Implementasi redundant link untuk meminimalisir downtime dengan metode failover (studi kasus: PT Kemuning Persada)," *Jurnal Publikasi Ilmu Komputer dan Multimedia*, vol. 1, no. 3, pp. 230–240, 2022.
[3] A.P.J.I.I., "APJII: Jumlah pengguna internet Indonesia tembus 221 juta orang," *APJII*, 2023, [Online]. Available: https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang.
[4] M. Hafizh, "Load Balancing Dengan Metode Per Connection Classifier (Pcc) Menggunakan Proxy Server Sebagai Caching," *Skripsi*, 2011.
[5] Syahputra Ramdhani, Romi mulyadi, Muhammad yusuf, Yogi Pratama, and Adri Yanto, "Analisis dan Implementasi Perbandingan Protokol VRRP dan HSRP pada Jaringan Topologi Star fungsionalitas jaringan terlepas dari kegagalan perangkat atau jalur . Redudansi pada jaringan jaringan apabila terjadi kegagalan pada layanan jaringan . Secara umum," vol. 3, no. 1, 2024.
[6] M. J. N. Yudianto, "Jaringan Komputer dan Pengertiannya," *Ilmukomputer.Com*, vol. Vol.1, pp. 1–10, 2014.
[7] D. Stiawan, D. Jurusan, S. Komputer, and F. Unsri, "Konsep Dasar Internet & Tips Memilih ISP," *Inf. Politek. Indonusa Surakarta*, vol. 1, pp. 1–26, 2016.
[8] H. Hermansyah, A. Khaidar, N. Nurdin, and S. Kurnia, "Implementation of static routing and quality of service for optimization of network traffic management on Cisco routers," *Journal of Artificial Intelligence and Software Engineering*, vol. 5, no. 3, 2025.
[9] Alriza Nuh Hidasaputra, "Mengenal Konsep Gateway Dan Nat (Network Address Translation)," *Teknol. Inf.*, vol. 1, pp. 1–9, 2021.
[10] A. Hakim, M. S. Ridha, S. Heristian, A. Selawati, and P. Paramita, "Implementasi failover clustering server untuk mengurangi risiko downtime pada web server," *Akrab Juara: Jurnal Ilmu-ilmu Sosial*, vol. 9, no. 3, pp. 660–666, 2024.