Volume 5 No. 2 (July - December 2025), pp. 168-187 | ISSN 2962-2360 (online) | ISSN 2962-3669 (print)
Arcitech: Journal of Computer Science and Artificial Intelligence
https://journal.iaincurup.ac.id/index.php/arcitech/article/view/14551 | DOI : https://dx.doi.org/10.29240/arcitech.v5i2.14551

Implementasi dan Evaluasi Sistem Failover Otomatis Berbasis Netwatch pada Router Mikrotik Dual-ISP untuk Meningkatkan Ketersediaan Jaringan Apotek Farmaku

Boy Yuliadi[1], Rasto[2]
[1,2] Program Studi Teknik Informatika, Universitas Dian Nusantara, Jakarta, Indonesia
Email : boy.yuliadi@undira.ac.id, 411211232@mahasiswa.undira.ac.id

Article Information

Article history

Received 1 August 2025
Revised 15 November 2025
Accepted 20 December 2025
Available 30 Desember 2025

Keywords

Failover
Netwatch
Mikrotik
Network
ISP
NDLC

Corresponding Author:

Boy Yuliadi,
Universitas Dian Nusantara,
Email : boy.yuliadi@undira.ac.id

Abstract

This study contributes by proposing and implementing an automated failover–failback mechanism based on Mikrotik Netwatch for multi-homed Internet connectivity, which has not been widely explored in the context of pharmacy information systems, and by validating its effectiveness through empirical testing in a production-like environment. Unlike prior work that is largely conceptual or simulation-oriented, this research evaluates the system in an end-to-end manner at both the control plane (router-level monitoring and switching) and the data plane (client-side traffic continuity). The system is developed following the Network Development Life Cycle (NDLC) methodology, encompassing analysis, design, simulation, simulation testing, and deployment. A dual-ISP architecture is implemented, in which Netwatch continuously probes upstream reachability and triggers automated route switching upon link degradation or failure, as well as automatic restoration upon link recovery. Experimental results indicate that the system achieves an average failover time of approximately 5 seconds, with minimal packet loss and no perceptible service interruption for end users. The failback mechanism also operates autonomously and stably. Overall, router- and client-side performance measurements confirm that the proposed solution effectively enhances network resilience and service availability in environments with high availability requirements.

Keywords : *failover, netwatch, Mikrotik, network, ISP, NDLC*

Abstrak

Penelitian ini berkontribusi dengan mengusulkan dan mengimplementasikan mekanisme failover–failback otomatis berbasis Netwatch yang belum banyak dibahas dalam konteks operasional apotek, serta membuktikan efektivitasnya melalui pengujian langsung pada lingkungan nyata. Berbeda dari penelitian sebelumnya yang umumnya bersifat konseptual atau simulatif, penelitian ini menguji performa sistem secara end-to-end dari sisi router dan klien. Metode pengembangan yang digunakan mengacu pada tahapan Network Development Life Cycle (NDLC), mencakup analisis, desain, simulasi, pengujian simulasi, dan implementasi. Sistem dirancang menggunakan dua jalur koneksi internet dari ISP berbeda, dengan Netwatch sebagai pemantau konektivitas dan pemicu switching otomatis saat terjadi gangguan atau pemulihan jaringan. Hasil pengujian menunjukkan sistem mampu melakukan perpindahan koneksi dalam rata-rata 5 detik dengan tingkat packet loss yang rendah dan tanpa mengganggu aktivitas pengguna. Proses failback juga berjalan otomatis dan stabil. Evaluasi dari sisi router dan client membuktikan sistem ini efektif menjaga keberlanjutan layanan jaringan di lingkungan yang memerlukan ketersediaan tinggi

Kata Kunci : *failover, netwatch, Mikrotik, jaringan, ISP, NDLC*

1. Pendahuluan

Ketersediaan jaringan internet yang cepat dan stabil merupakan kebutuhan esensial dalam mendukung kelancaran operasional perusahaan, guna meningkatkan efisiensi dan produktivitas. (Khudori et al., 2022). Termasuk bisnis ritel dan layanan kesehatan seperti Apotek Farmaku yang menerapkan sistem Point of Sale (POS), Perangkat lunak untuk mengelola transaksi penjualan, yang secara umum dikenal sebagai system kasir (Sulistyawan et al., 2023) dan Sistem Informasi Manajemen Apotek (SIMA) kedua sistem itu berbasis web yang sangat bergantung pada ketersediaan jaringan internet agar saling terkoneksi. Sistem POS, misalnya, memerlukan koneksi yang stabil untuk memproses transaksi dengan cepat dan akurat, sementara sistem manajemen apotek bergantung pada internet untuk mengelola ketersediaan obat dan melakukan proses pesanan secara online. Ketika jaringan internet mengalami downtime, meski hanya sebentar, hal tersebut dapat menghambat operasional apotek, mengakibatkan penundaan pelayanan, dan bahkan menurunkan tingkat kepuasan pelanggan (Azmi et al., 2022).

Tantangan besar terkait downtime dapat terjadi karena gangguan pada jaringan internet yang disebabkan oleh ketidakstabilan koneksi dari Internet Service Provider (ISP), seperti putusnya sambungan secara tiba-tiba, penurunan kecepatan akses, maupun proses pemeliharaan layanan, dapat menjadi hambatan signifikan dalam menunjang kelancaran kegiatan operasional perusahaan. (Rukmana & Suhendi, 2023). Ketergantungan terhadap satu penyedia layanan internet (ISP) saja menyebabkan sistem memiliki risiko tinggi terhadap kegagalan (fail) koneksi, Salah satu alternatif solusi untuk mengatasi permasalahan konektivitas jaringan adalah dengan menyediakan koneksi cadangan dari penyedia layanan internet (ISP) yang berbeda. Dengan memiliki lebih dari satu sumber koneksi internet, apabila terjadi gangguan pada salah satu jalur, koneksi tetap dapat berjalan melalui jalur lainnya (Irman & Anton, 2024). Untuk mewujudkan hal ini, diperlukan metode khusus yang mampu menentukan jalur utama dan jalur cadangan. Melalui mekanisme failover, sistem dapat secara otomatis memilih jalur utama dan beralih ke jalur cadangan saat dibutuhkan (Panggabean & Kuswanto, 2023).

Metode failover memungkinkan memungkinkan sistem melakukan transisi otomatis ke koneksi cadangan apabila konektivitas jaringan utama mengalami gangguan, sehingga kontinuitas layanan tetap terjaga. (Putra et al., 2023). Ketersediaan koneksi internet yang andal menjadi aspek penting bagi perusahaan untuk menunjang aktivitas operasional harian secara berkelanjutan. (Saputra & Ariyadi, 2023). Dalam penelitian ini, implementasi failover dilakukan dengan memanfaatkan fitur Netwatch pada perangkat router Mikrotik, Sistem ini berperan dalam memantau koneksi jaringan secara real-time serta menginisiasi proses pemulihan secara otomatis apabila terdeteksi adanya gangguan pada jaringan. Penerapan failover pada jaringan menggunakan Netwatch memungkinkan waktu henti (downtime) selama proses perpindahan dari koneksi

internet utama ke koneksi cadangan menjadi lebih singkat, sehingga gangguan akibat terputusnya koneksi internet dapat dikurangi secara signifikan (Rahman et al., 2022).

Penelitian ini bertujuan untuk merancang dan implementasi solusi redundansi jaringan internet menggunakan metode failover pada perangkat Mikrotik dengan memanfaatkan fitur Netwatch guna meminimalkan downtime dan meningkatkan ketersediaan jaringan di Apotek Farmaku. Melalui pendekatan ini, perusahaan dapat memperoleh gambaran pengelolaan jaringan yang lebih efektif dalam menghadapi gangguan koneksi dari berbagai sumber, seperti masalah ISP, kendala infrastruktur jaringan, atau kegagalan jalur utama.

Manfaat yang diharapkan mencakup kontribusi praktis berupa peningkatan keandalan infrastruktur jaringan Apotek Farmaku, serta manfaat teoritis dalam memperkaya kajian ilmiah mengenai manajemen redundansi jaringan. Ruang lingkup penelitian ini terbatas pada implementasi sistem failover dengan dua ISP dan evaluasi performanya di salah satu cabang Apotek Farmaku.

Berdasarkan kajian terhadap penelitian terdahulu, penelitian mengenai failover jaringan umumnya masih berfokus pada perancangan atau simulasi sistem, sementara pengujian implementasi di lingkungan operasional nyata, pengujian mekanisme failback, serta evaluasi performa dari sisi router dan klien secara bersamaan masih relatif terbatas. Selain itu, uraian mengenai detail implementasi teknis pada perangkat jaringan juga belum banyak disajikan secara komprehensif.

Sejalan dengan hal tersebut, penelitian ini berupaya melengkapi kajian yang ada melalui pendekatan integratif yang mencakup implementasi langsung sistem failover–failback berbasis Netwatch pada perangkat Mikrotik, disertai dengan evaluasi performa end-to-end di lingkungan operasional apotek. Pendekatan ini diharapkan dapat memberikan kontribusi empiris yang lebih aplikatif terhadap pengembangan sistem redundansi jaringan.

2. Kajian Terdahulu

Penelitian mengenai implementasi failover menggunakan perangkat Mikrotik, khususnya dengan memanfaatkan fitur Netwatch, telah banyak dilakukan sebagai solusi untuk menjaga ketersediaan konektivitas jaringan ketika terjadi gangguan pada jalur utama (Putra et al., 2023). Keunggulan utama penelitian Putra et al. (2023) terletak pada keberhasilannya menunjukkan bahwa mekanisme failover berbasis Netwatch dapat diimplementasikan secara stabil pada lingkungan jaringan operasional. Namun demikian, penelitian tersebut belum mengevaluasi mekanisme pemulihan koneksi (failback).

Panggabean dan Kuswanto (2023) mengkaji implementasi sistem failover berbasis Netwatch di PT Pancamagran Wisesa. Kontribusi utama penelitian ini adalah

pembuktian bahwa sistem mampu menjaga kontinuitas layanan jaringan tanpa gangguan signifikan terhadap aktivitas pengguna. Akan tetapi, pengujian masih terbatas pada skenario kegagalan jalur utama, sehingga reliabilitas sistem dalam siklus penuh failover–failback belum dapat dievaluasi.

Raharjo et al. (2024) meneliti penerapan failover pada router Mikrotik dalam lingkungan dengan satu penyedia layanan internet berbasis SIM card. Keunggulan penelitian ini adalah relevansinya terhadap lingkungan dengan keterbatasan infrastruktur jaringan. Namun demikian, penelitian ini tidak membahas skenario multi-ISP, sehingga implikasinya terhadap sistem redundansi jaringan masih terbatas.

Sandi et al. (2021) mengkaji optimalisasi sistem failover berbasis Netwatch untuk meningkatkan stabilitas jaringan akibat gangguan ISP. Kekuatan penelitian ini terletak pada fokusnya terhadap stabilitas koneksi dan minimalisasi gangguan terhadap pengguna akhir. Akan tetapi, penelitian tersebut tidak menyajikan uraian konfigurasi teknis Netwatch secara rinci, sehingga menyulitkan proses replikasi.

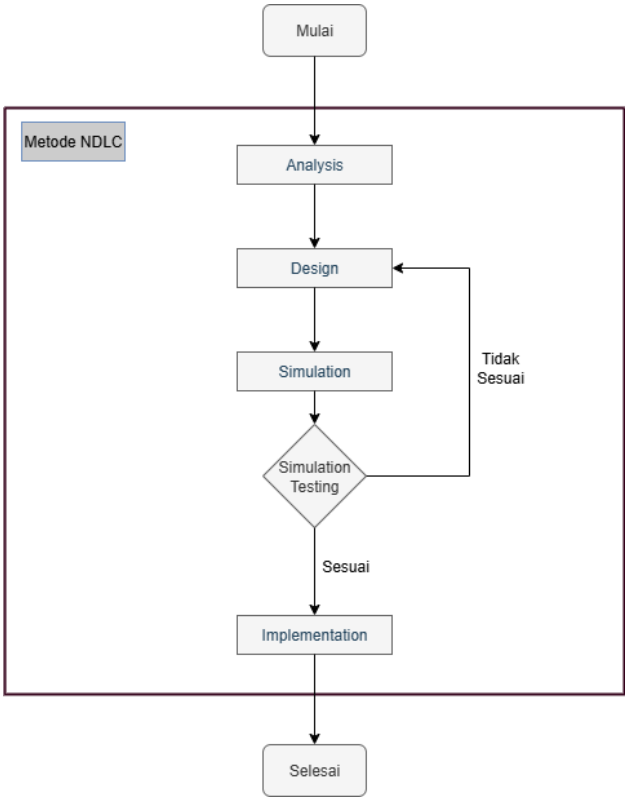
Secara konseptual, Netwatch berfungsi untuk memantau konektivitas jaringan secara real time dan menginisiasi perpindahan otomatis ke jalur alternatif ketika terjadi kegagalan koneksi (Khudori et al., 2022; Rukmana & Suhendi, 2023).

Secara komparatif, dapat disimpulkan bahwa penelitian-penelitian terdahulu sepakat mengenai efektivitas Netwatch dalam mendukung mekanisme failover. Namun demikian, perbedaan terletak pada fokus analisis, ruang lingkup pengujian, serta kedalaman dokumentasi teknis. Aspek pengujian failback, evaluasi performa end-to-end, dan dokumentasi konfigurasi sistem masih relatif terbatas. Oleh karena itu, penelitian ini diarahkan untuk melengkapi celah tersebut melalui pendekatan yang lebih komprehensif.

3. Metodologi Penelitian

Penelitian ini termasuk dalam penelitian terapan dengan menggunakan pendekatan metode campuran (mixed methods) yang bertujuan menghasilkan solusi praktis terhadap permasalahan koneksi internet di Apotek Farmaku melalui implementasi sistem failover otomatis berbasis Netwatch pada Mikrotik. Pendekatan kualitatif digunakan untuk mengidentifikasi kebutuhan jaringan melalui wawancara dan observasi, sementara pendekatan kuantitatif digunakan untuk mengukur kinerja sistem melalui parameter latency, packet loss, dan waktu switching menggunakan Winbox dan Command Prompt. Kombinasi ini memberikan analisis yang komprehensif terhadap keandalan dan fungsionalitas sistem.

Tahapan dalam penelitian ini disusun berdasarkan acuan Metode NDLC (Network Development Life Cycle) yang berperan sebagai metode dalam proses pengembangan jaringan yang adaptif, dan dapat disesuaikan untuk implementasi pada jaringan berskala kecil maupun besar. (Syahrani & Yuliadi, 2023).



Gambar 1. Tahapan Metode Penelitian

Pada tahap analisis, diawali dengan mengidentifikasi permasalahan utama yang dihadapi Apotek Farmaku, khususnya berkaitan dengan ketersediaan jaringan internet dan potensi terjadinya downtime yang berdampak pada kelancaran operasional harian. Tahap ini dilakukan melalui pendekatan kualitatif berupa wawancara langsung dengan pemangku kepentingan, seperti apoteker, tim IT, dan data analyst, serta observasi terhadap kondisi jaringan di lapangan.

Pada tahap desain, dalam penelitian ini mencakup perencanaan teknis sistem jaringan dengan metode failover pada Mikrotik. Berdasarkan hasil observasi terhadap infrastruktur jaringan Apotek Farmaku saat ini, akan dilakukan perancangan ulang topologi jaringan untuk memastikan koneksi tetap stabil meski terjadi gangguan pada jalur utama. Desain ini mencakup design topologi yang akan diterapkan, pengaturan rute failover, pemilihan perangkat keras yang sesuai, serta sistem otomatis agar proses peralihan koneksi berjalan lancar.

Pada tahap simulasi, peneliti mulai melakukan pengujian terhadap rancangan jaringan yang telah rancang pada tahap desain sebelumnya. Proses ini dilakukan menggunakan jaringan internal Apotek Farmaku guna mendekati kondisi nyata di lapangan. Simulasi mencakup pemasangan berbagai perangkat jaringan seperti dua sumber koneksi internet dari ISP berbeda, perangkat Mikrotik sebagai pengatur lalu

lintas jaringan, kabel LAN, beserta perangkat Orbit yang berfungsi sebagai koneksi cadangan. Salah satu aspek krusial dalam tahap ini adalah konfigurasi Mikrotik yang berperan sebagai pusat pengendali sistem failover. Dalam proses konfigurasi ini, diterapkan mekanisme failover menggunakan fitur Netwatch yang cukup kompleks, karena melibatkan pemantauan koneksi secara real-time serta otomatisasi perpindahan jalur koneksi saat gangguan terjadi.

Pada tahap simulation testing, peneliti menggunakan jaringan internal sebagai lingkungan uji coba. Pada tahap ini, dilakukan pengujian dan evaluasi secara menyeluruh terhadap sistem yang telah dikonfigurasi pada tahap simulasi sebelumnya. dengan fokus utama pada pemantauan stabilitas jaringan, kecepatan respon saat terjadi perpindahan koneksi (failover), serta kualitas koneksi internet selama sistem failover aktif. Temuan dari hasil pengujian ini akan menjadi dasar untuk melakukan perbaikan maupun penyesuaian terhadap desain yang telah dirancang, apabila ditemukan kekurangan atau potensi masalah, sebelum tahap implementasi langsung di lingkungan operasional.

Analisis Data Kuantitatif, Pengukuran performa jaringan dilakukan sebelum dan sesudah implementasi sistem failover untuk memperoleh gambaran perbandingan kinerja yang objektif. Parameter yang dianalisis meliputi latency, packet loss, dan waktu perpindahan koneksi (switching time). Latency dihitung sebagai nilai rata-rata round-trip time (RTT) dari hasil perintah ping ke target eksternal, packet loss dihitung sebagai persentase paket yang tidak mendapat balasan dibandingkan dengan jumlah paket yang dikirim, sedangkan switching time dihitung sebagai selisih waktu antara terdeteksinya gangguan pada koneksi utama hingga koneksi cadangan aktif kembali dan dapat digunakan. Setiap parameter diukur secara berulang pada kondisi normal dan saat terjadi failover. Data yang diperoleh dianalisis menggunakan statistik deskriptif berupa nilai rata-rata, nilai minimum, nilai maksimum, dan simpangan baku untuk menggambarkan kecenderungan dan stabilitas performa sistem. Analisis difokuskan pada perbandingan deskriptif antar kondisi tanpa menggunakan uji statistik inferensial, karena tujuan penelitian bersifat evaluatif dan kontekstual.

Pada tahap implementasi, tahap ini merupakan proses penerapan hasil rancangan dan pengujian sistem jaringan yang telah dilakukan pada tahap sebelumnya ke dalam lingkungan operasional yang sesungguhnya di Apotek Farmaku.

4. Hasil dan Pembahasan

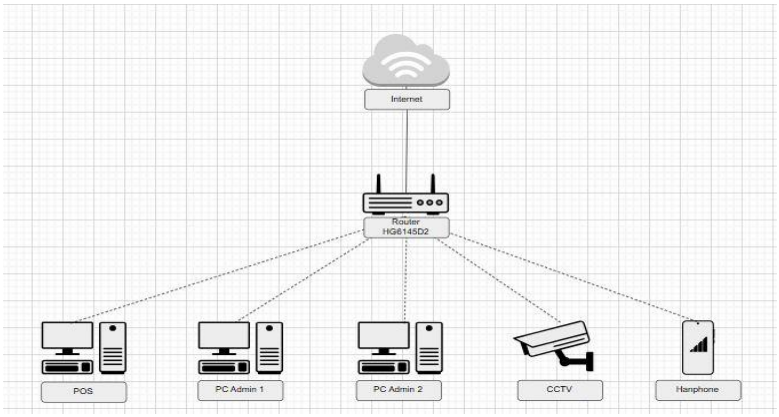
4.1 Analysis (Analisis)

Dari hasil analisis pada tahap awal ini mengacu pada hasil wawancara dan hasil observasi langsung di lingkungan operasional Apotek Farmaku. Pendekatan ini bertujuan untuk memperoleh gambaran faktual mengenai kondisi infrastruktur jaringan

yang ada, serta mengidentifikasi permasalahan utama yang berkaitan dengan kestabilan koneksi internet.

Wawancara dipilih untuk mencari informasi yang mendalam dari para pemangku kepentingan, Apoteker sebagai penanggung jawab Apotek, IT Infrastructure, serta Data Analyst dimana hasil wawancara tersebut menunjukan bahwa gangguan koneksi internet terjadi 2–3 kali per bulan dengan durasi 2–3 jam. Dampaknya mencakup keterlambatan transaksi, pencatatan manual, serta kerugian materiil hingga 20–30 transaksi tertunda per hari dan beban kerja tambahan. Meskipun telah berganti ISP, masalah konektivitas belum terselesaikan. Dari hasil tersebut menilai bahwa sistem failover sangat dibutuhkan sebagai solusi teknis untuk menjaga kestabilan jaringan dan mendukung kelancaran operasional.

Sedangkan observasi dilakukan dengan fokus memahami infrastruktur jaringan, catatan dokumentasi pengelolaan jaringan, pemantauan ketersediaan bandwidth dan penanganan masalah koneksi jaringan di Apotek Farmaku. Hasil dari observasi ini peneliti mendapatkan gambaran infrastruktur jaringan yang diimplementasikan saat ini seperti pada Gambar 2 yang merupakan Implementasi sederhana dengan penggunaan router bawaan ISP sebagai tumpuan operasional yang terkoneksi ke beberapa komputer untuk menjalankan kegiatan operasional sehari-hari.



Gambar 2. Topologi Existing

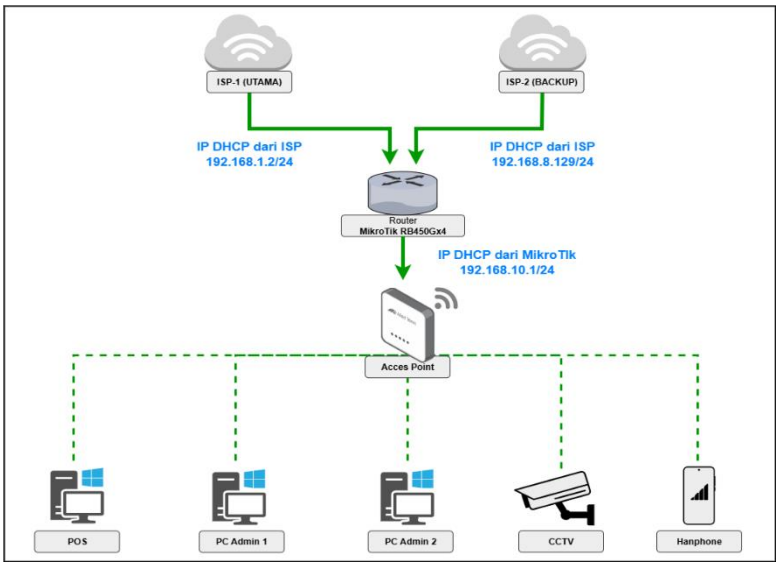
Berdasarkan hasil observasi mengenai ketersediaan bandwith diperoleh nilai kecepatan unduh (download) sebesar 70 Mbps dan unggah (upload) sebesar 78 Mbps.

Gambar 3. Ketersediaan Bandwith

Hasil ini menunjukkan bahwa kinerja koneksi internet yang tersedia masih berada dalam kisaran yang optimal yang ditawarkan oleh pihak ISP.

4.2 Design (Desain)

Topologi jaringan yang dikembangkan dalam penelitian ini dirancang untuk menjamin kestabilan koneksi internet melalui sistem failover otomatis berbasis Mikrotik menggunakan fitur Netwatch. Sistem ini menggunakan dua jalur ISP, yakni Biznet sebagai koneksi utama dan Telkomsel Orbit sebagai cadangan, yang keduanya terhubung langsung ke router Mikrotik. Router mendistribusikan koneksi ke Accesspoint dan perangkat operasional seperti POS, komputer admin, CCTV, dan perangkat mobile.

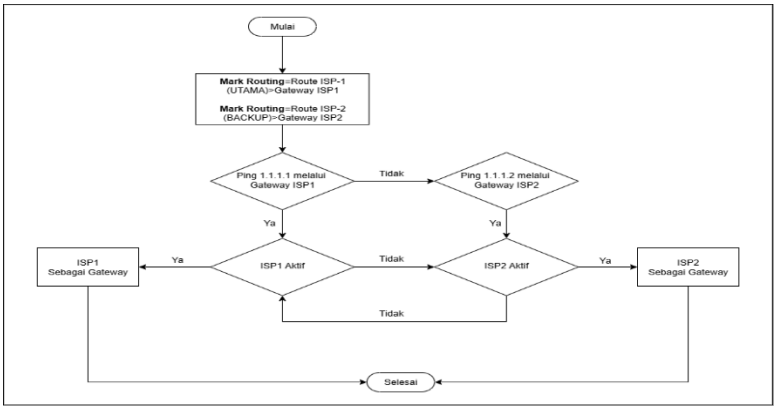


Gambar 3. Topologi Jaringan Usulan

Failover Netwatch digunakan untuk memantau koneksi secara berkala, saat gateway utama tidak merespon, sistem secara otomatis mengalihkan koneksi ke jalur cadangan tanpa intervensi manual. Setelah koneksi utama pulih, sistem akan kembali ke jalur gateway utama melalui proses failback. Mekanisme ini dijelaskan secara sistematis dalam Gambar 4 yang menampilkan alur kerja logika failover Netwatch dalam menentukan jalur aktif berdasarkan hasil pemantauan konektivitas.

Tabel 1. Rute Koneksi Internet

No	ISP 1	ISP 2	Rute
1.	Hidup	Hidup	Melalui Gateway ISP 1
2.	Mati	Hidup	Melalui Gateway ISP 2
3.	Hidup	Mati	Melalui Gateway ISP 1
4.	Mati	Mati	Koneksi Terputus



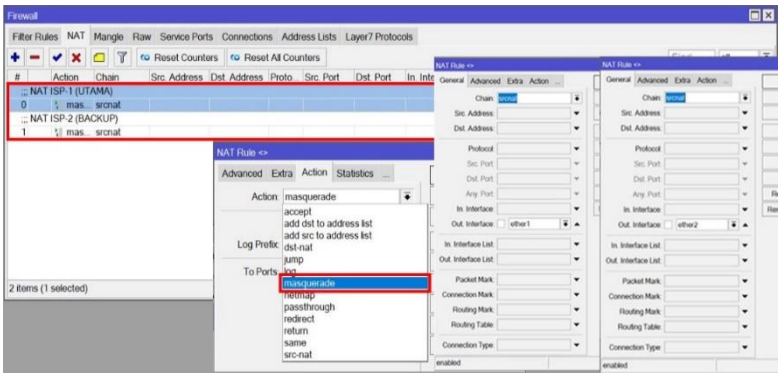
Gambar 4. Flowchart Failover Netwatch

4.3 Simulation (Simulasi)

Tahapan ini mengkaji penerapan dan konfigurasi sistem failover otomatis menggunakan fitur Netwatch pada perangkat Mikrotik RB450Gx4 melalui aplikasi Winbox, yang terhubung ke 2 jalur sumber internet yaitu ISP 1 dan ISP 2, Serta diteruskan ke access point agar jaringan internet dapat diakses oleh end user seperti pada desain topologi jaringan usulan.

4.3.1 Konfigurasi NAT (Network Address Translation)

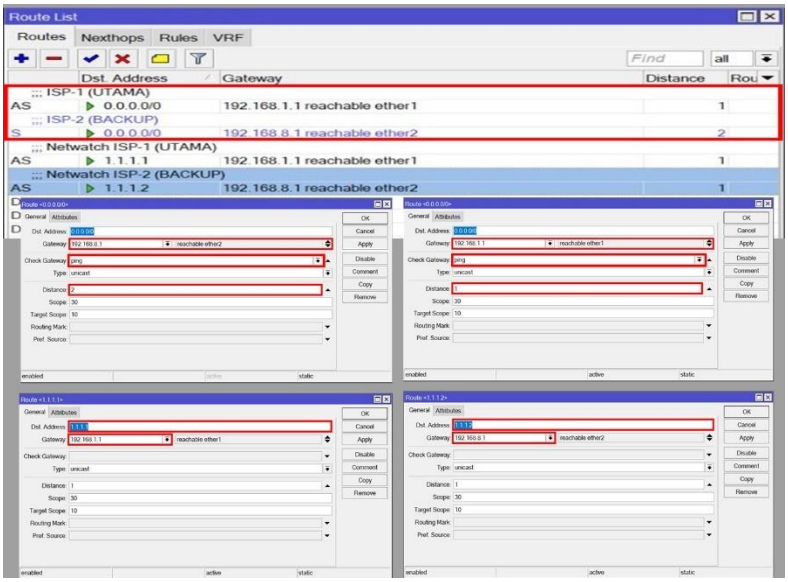
Pada penelitian ini menggunakan 2 ISP maka harus di tambahakn 2 buah NAT yang nantinya konfigurasi ini digunakan dalam skenario failover, di mana kedua WAN akan dipantau menggunakan fitur Netwatch. Saat koneksi utama misalnya ether1 terdeteksi down, router secara otomatis mengalihkan trafik ke jalur cadangan yaitu ether2, untuk memastikan koneksi tetap aktif. Pada Gambar 5 terlihat bahwa konfigurasi NAT masquerade diterapkan pada antarmuka ether1 dan ether2 yang berfungsi sebagai jalur koneksi internet. Untuk rule NAT ISP-1 out interfacenya di arahkan ke ether1 serta chain diisi srcnat, kemudian untuk ISP-2 di arahkan ke ether2 serta chain diisi srcnat, dengan masing – masing action disisi masquerade.



Gambar 5. Konfigurasi NAT ISP 1 dan NAT ISP 2

4.3.2 Konfigurasi Routing

Routing dalam sistem ini menerapkan pendekatan berbasis jarak prioritas atau distance, di mana ISP-1 dengan gateway 192.168.1.1 dikonfigurasi sebagai jalur utama dengan nilai distance 1 dan metode pemeriksaan gateway menggunakan ping. Sementara itu, ISP-2 dengan gateway 192.168.8.1 diatur sebagai jalur cadangan dengan nilai distance 2 dan metode pemeriksaan serupa. Jalur utama akan tetap digunakan selama koneksi aktif, Apabila koneksi utama terputus atau tidak dapat diakses, sistem secara otomatis mengalihkan trafik ke koneksi alternatif yang telah dikonfigurasi. Untuk mendukung pemantauan konektivitas, ditambahkan dua rute statis yang mengarahkan ping ke IP tujuan 1.1.1.1 dan 1.1.1.2 melalui fitur Netwatch. Apabila koneksi ke IP utama tidak merespons, Netwatch akan mengeksekusi skrip untuk menonaktifkan rute ISP-1 dan mengaktifkan ISP-2 secara otomatis, serta mengembalikannya ke ISP-1 saat koneksi pulih (failback). Skema ini digambarkan secara rinci pada Gambar 6 dan memungkinkan mekanisme failover berjalan secara dinamis berdasarkan status koneksi aktual.



Gambar 6. Konfigurasi Routing

4.3.3 Konfigurasi Netwatch

Pada proses konfigurasi ini fitur Netwatch dimanfaatkan untuk melakukan pemantauan konektivitas secara real-time. Sistem ini dikonfigurasi untuk mengirim ping secara berkala ke dua alamat IP. Jika ping ke gateway ISP-1 tidak mendapatkan respons dalam jangka waktu tertentu, Netwatch secara otomatis menjalankan skrip failover yang mengaktifkan jalur cadangan dan mengubah rute trafik ke ether2 sebagai jalur cadangan. Ketika koneksi ISP-1 kembali aktif, Netwatch akan mengeksekusi skrip failback, yang mengembalikan rute koneksi ke ether1 sebagai jalur utama, Pada Gambar 7

menunjukkan dua entri Netwatch yang masing-masing memantau konektivitas terhadap host 1.1.1.1 untuk ISP-1 dan 1.1.1.2 untuk ISP-2. Setiap entri dikonfigurasi dengan interval ping setiap 3 detik dan timeout selama 1000 ms untuk mendeteksi status koneksi secara cepat dan akurat. Pada host 1.1.1.1 ISP-1, bagian Down diatur untuk menonaktifkan route utama menggunakan perintah:

```
/ip route disable [find comment="ISP-1 (UTAMA)"];
/log error "Koneksi ISP-1 (UTAMA) Down"
```

Artinya, ketika koneksi ke ISP-1 terputus, sistem akan menonaktifkan rute tersebut dan mencatat kejadian di log. Sebaliknya, pada bagian Up route akan kembali diaktifkan secara otomatis dengan perintah:

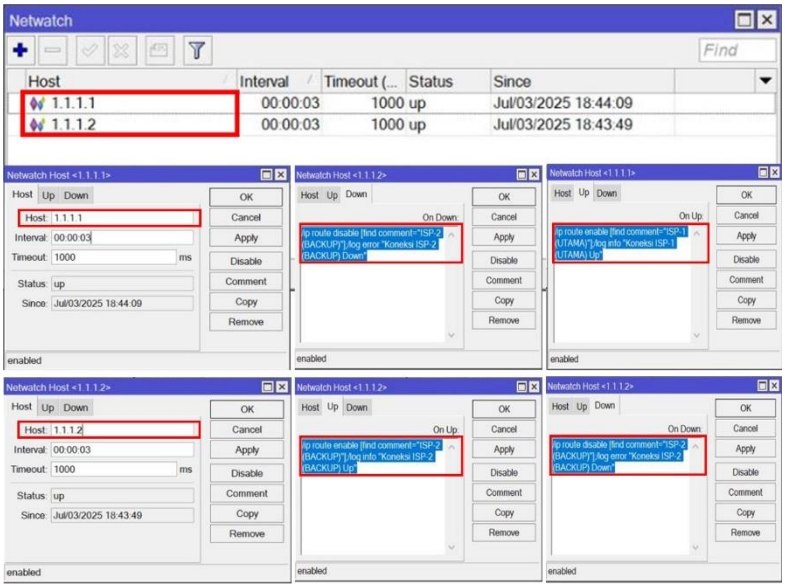
```
/ip route enable [find comment="ISP-1 (UTAMA)"];
/log info "Koneksi ISP-1 (UTAMA) Up"
```

Konfigurasi serupa juga diterapkan pada host 1.1.1.2 ISP-2, yang berfungsi sebagai koneksi cadangan atau backup, ketika ISP-1 gagal dan ISP-2 terdeteksi aktif, maka route untuk ISP-2 akan diaktifkan dengan perintah:

```
/ip route enable [find comment="ISP-2 (BACKUP)"];
/log info "Koneksi ISP-2 (BACKUP) Up"
```

Dan jika ISP-2 kembali tidak aktif, route akan dimatikan secara otomatis dengan perintah:

```
/ip route disable [find comment="ISP-2 (BACKUP)"];
/log error "Koneksi ISP-2 (BACKUP) Down"
```



Gambar 7. Konfigurasi Netwatch

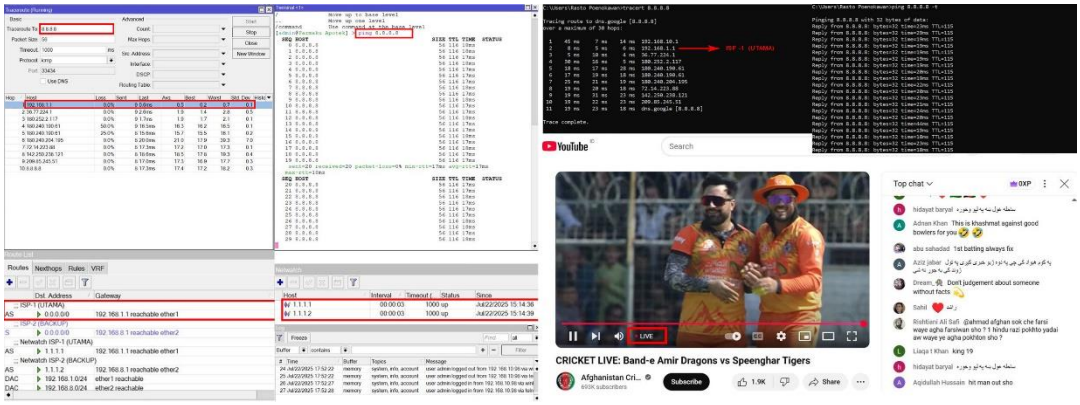
4.4 Testing Simulation (Pengujian Simulasi)

Pengujian dilakukan untuk mengevaluasi efektivitas konfigurasi failover Netwatch menggunakan perangkat Router Mikrotik serta PC client yang memanfaatkan aplikasi Winbox dan Command Prompt melalui mekanisme traceroute dan ping ke alamat IP target eksternal, yaitu 8.8.8.8 milik Google Public DNS.

4.4.1 Kondisi Awal (Kedua ISP Aktif)

Pada tahap pengujian konektivitas saat kedua ISP aktif, dilakukan pengujian dengan perintah traceroute dan ping ke 8.8.8.8 yaitu DNS Google melalui perangkat Mikrotik dan PC client. Hasil traceroute menunjukkan bahwa jalur koneksi yang digunakan adalah melalui ISP-1 dengan gateway 192.168.1.1. Uji ping dari Mikrotik menunjukkan rata-rata waktu respons sekitar 17 ms tanpa mengalami packet loss, yang menandakan koneksi berjalan stabil, Hasil lengkap dari pengujian ini dapat dilihat pada Gambar 8, yang menampilkan tangkapan layar traceroute dan ping.

Hal ini juga diperkuat oleh uji coba streaming YouTube di sisi client yang berjalan lancar tanpa buffering. Dari sisi PC klien, hasil traceroute juga mengarah ke ISP-1 dengan respons yang konsisten, serta uji ping menunjukkan waktu rata-rata sekitar 19 ms tanpa packet loss.

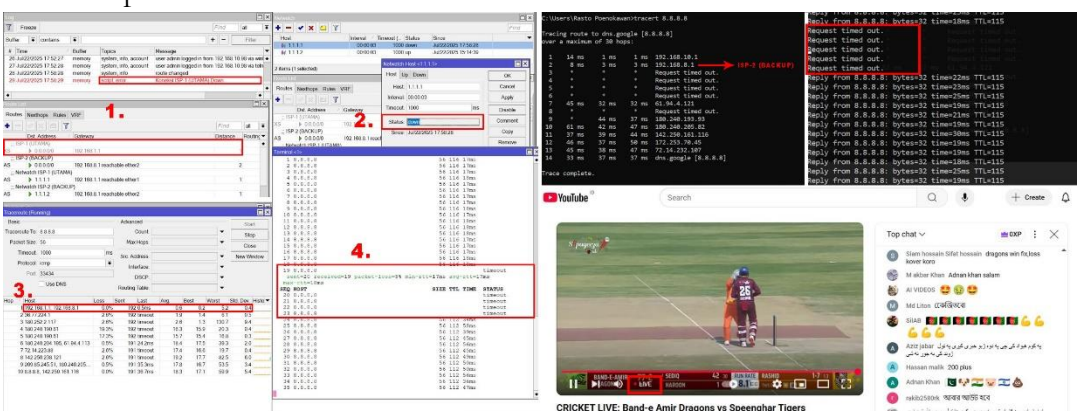


Gambar 8. Pengujian Kondisi Awal

4.4.2 Simulasi Gangguan Pada ISP-1 (Failover Berjalan)

Selanjutnya dilakukan simulasi pemutusan koneksi ISP-1. Hasil pengujian menunjukkan bahwa pada log terdeteksi Koneksi ISP-1 Down serta perubahan status pada Netwatch untuk host 1.1.1.1 dari sebelumnya Up menjadi Down . Skrip Netwatch kemudian menjalankan perintah perubahan route, mengalihkan jalur utama yaitu ISP-1 ke ISP-2 secara otomatis. Berdasarkan hasil traceroute secara otomatis jalur koneksi berpindah ke 192.168.8.1 sebagai gateway dari ISP-2, dalam pengujian terdapat sedikit packet loss saat peralihan berlangsung yaitu 5 detik hasil dari proses ping pada sisi router.

Pada PC Client juga dapat dilihat bahwa dari sisi client hasil dari traceroute secara otomatis jalur koneksi berpindah ke 192.168.8.1 dan terdapat packet loss yaitu 5 detik. Hal ini dibuktikan dengan indikator live streaming YouTube yang tetap berjalan normal pada sisi klien.

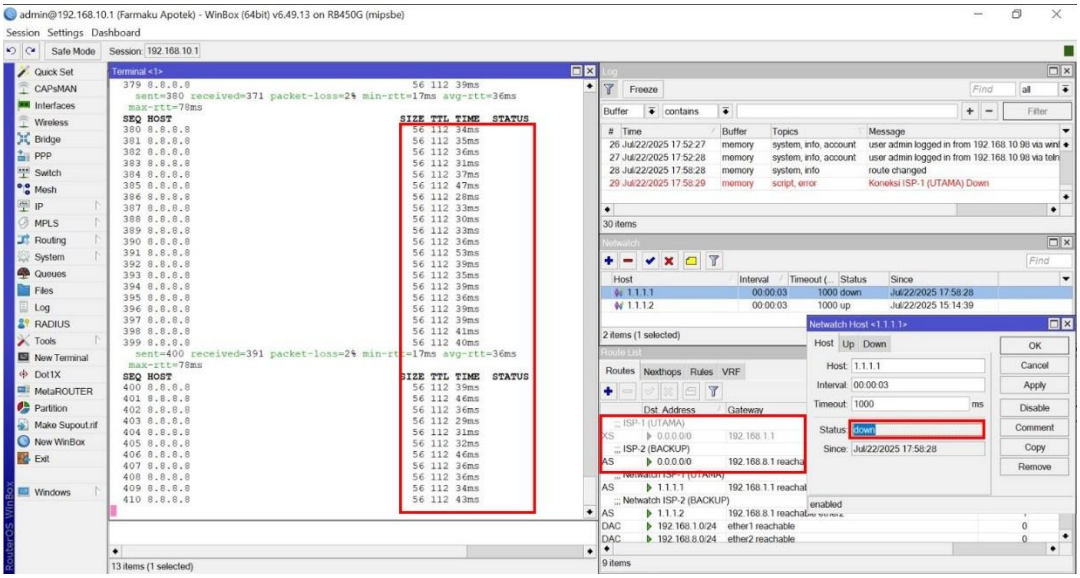


Gambar 9. Pengujian Gangguan Pada ISP 1

4.4.3 Stabilitas Setelah Beralih ke ISP-2

Setelah peralihan berhasil dilakukan, dilakukan pengujian ping secara terus-menerus ke 8.8.8.8 untuk mengamati stabilitas jaringan. Hasil menunjukkan koneksi dari

ISP-2 cukup stabil dengan waktu respons rata-rata 36 ms dan packet loss yang tergolong kecil.

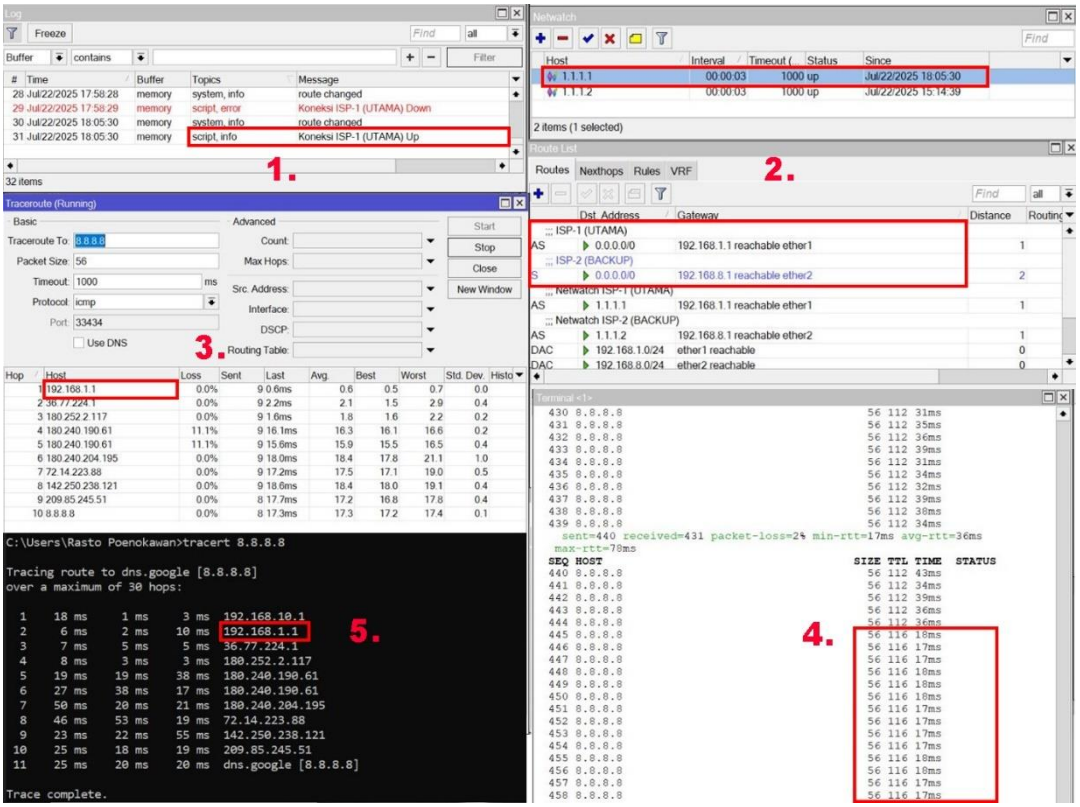


Gambar 10. Pengujian Stabilitas Koneksi ISP 2

4.4.4 Pemulihan Jalur Utama (Failback Berjalan)

Pemulihan jalur utama (failback) dilakukan setelah koneksi berhasil dialihkan ke ISP-2. Saat koneksi ISP-1 kembali normal, Netwatch secara otomatis mendeteksi bahwa host monitoring 1.1.1.1 sudah dapat dijangkau, dan langsung menjalankan skrip untuk mengembalikan rute default ke gateway ISP-1. Hal ini terlihat dari perubahan status Netwatch menjadi "Up" dan log sistem yang mencatat peralihan rute.

Hasil traceroute dari router menunjukkan koneksi kembali melalui gateway 192.168.1.1, dengan latency stabil di kisaran 17–18 ms tanpa packet loss. Dari sisi PC Client, traceroute juga menunjukkan jalur aktif ke ISP-1, membuktikan bahwa failback tidak hanya berhasil di sisi router, tetapi juga efektif dari sisi client seperti pada Gambar 11 Selama proses transisi ini, koneksi tetap stabil dan tidak terjadi gangguan layanan, termasuk saat streaming. Hal ini menunjukkan bahwa failback berlangsung otomatis.



Gambar 11. Pengujian Pemulihan ISP 1

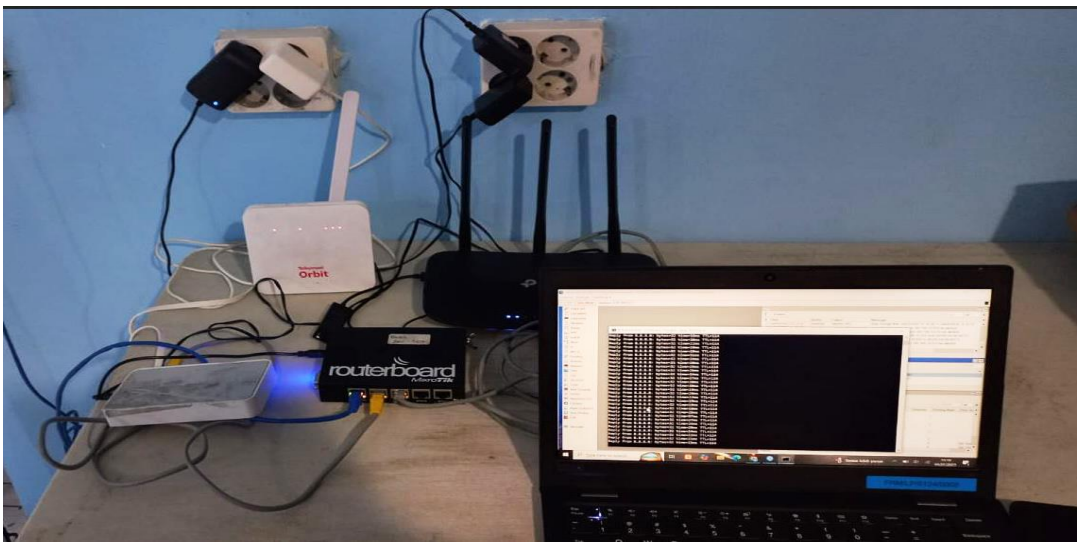
4.4.5 Evaluasi Kinerja Jaringan

Evaluasi kinerja jaringan dilakukan melalui pengujian sistem failover dan failback menggunakan dua jalur ISP pada perangkat Mikrotik RB450Gx4 yang dikonfigurasi dengan fitur Netwatch. Pengujian mencakup analisis latency, packet loss, waktu switching, dan kestabilan koneksi, baik dari sisi router maupun PC Client. Hasil menunjukkan bahwa sistem mampu mempertahankan koneksi internet selama kondisi normal maupun saat ISP utama mengalami gangguan, dengan proses failover otomatis ke ISP cadangan berlangsung cepat (5 detik) dan minim gangguan. Meskipun latensi ISP cadangan sedikit lebih tinggi (36-47ms) dibandingkan ISP utama (17-19 ms), koneksi tetap stabil tanpa buffering, termasuk saat melakukan streaming video. Proses failback juga berjalan otomatis dan efisien ketika koneksi ISP utama pulih, dengan jalur koneksi kembali normal tanpa mengganggu aktivitas pengguna. Secara keseluruhan, konfigurasi ini terbukti efektif dalam menjaga kontinuitas layanan jaringan dan layak diterapkan pada sistem yang membutuhkan konektivitas tinggi dan minim downtime.

Tabel 2. Perbandingan Evaluasi Kinerja ISP 1 dan ISP 2

No	Parameter Evaluasi	ISP 1	ISP 2	Keterangan
1.	**Status Koneksi**	Default / Utama	Backup / Standby	ISP 1 digunakan selama kondisi normal, ISP 2 digunakan saat failover.
2.	**Gateway**	192.168.1.1	192.168.8.1	Tergambar dari hasil traceroute Mikrotik dan PC Client.
3.	**Rata-rata Latency**	17–19 ms	36–47 ms	Pengujian ping ke 8.8.8.8 dari Mikrotik dan PC Client.
4.	**Packet Loss**	0%	<1%	Packet loss hanya muncul saat transisi antar ISP.
5.	**Waktu Deteksi Failover**	5 detik	-	Netwatch mendeteksi host down dan men-trigger skrip peralihan.
6.	**Waktu Failback**	-	5 detik	Netwatch mendeteksi host kembali reachable dan memulihkan jalur ISP 1.
7.	**Streaming YouTube**	Lancar	Lancar	Tidak ada buffering selama perpindahan jalur.
8.	**Log Perubahan Routing**	route changed → ISP 2	route changed → ISP 1	Transisi terekam secara otomatis di system.

4.4 Implementation (Implementasi)



Gambar 12. Proses Implementasi Perangkat Jaringan

Tahap implementasi merupakan proses realisasi dari rancangan sistem jaringan yang telah disusun dan diuji pada tahap sebelumnya, yang kemudian diterapkan secara langsung dalam lingkungan operasional Apotek Farmaku. Pada tahap ini, konfigurasi sistem failover berbasis Netwatch pada perangkat Mikrotik mulai diintegrasikan ke

infrastruktur jaringan yang telah ada, dengan tujuan utama untuk memastikan fungsionalitas sistem berjalan optimal dalam kondisi nyata.

4.5 Diskusi Implikasi

4.5.1 Implikasi Praktis.

Hasil penelitian menunjukkan bahwa sistem failover–failback otomatis berbasis Netwatch mampu menjaga kontinuitas koneksi internet dengan waktu perpindahan rata-rata 5 detik dan packet loss yang minimal. Implikasi praktis dari temuan ini sangat signifikan bagi operasional Apotek Farmaku, khususnya pada sistem Point of Sale (POS) dan Sistem Informasi Manajemen Apotek (SIMA) yang sangat bergantung pada konektivitas jaringan. Dengan adanya sistem ini, risiko keterlambatan transaksi, pencatatan manual, serta gangguan layanan kepada pelanggan dapat diminimalkan secara nyata. Selain itu, sistem ini berpotensi meningkatkan service level agreement (SLA) internal terhadap ketersediaan jaringan dan menurunkan risiko kerugian operasional akibat downtime, yang sebelumnya dilaporkan dapat mencapai puluhan transaksi tertunda per hari.

4.5.1 Implikasi Operasional dan Manajerial.

Dari sisi manajemen TI, implementasi failover otomatis mengurangi ketergantungan pada intervensi manual saat terjadi gangguan koneksi, sehingga beban kerja tim IT menjadi lebih ringan dan respons terhadap gangguan menjadi lebih cepat serta konsisten. Hal ini meningkatkan reliabilitas sistem jaringan sekaligus memperkuat kesiapan infrastruktur terhadap gangguan eksternal seperti gangguan ISP atau pemeliharaan jaringan.

4.5.1 Implikasi Teoretis.

Secara teoretis, penelitian ini memperkuat temuan sebelumnya mengenai efektivitas Netwatch sebagai mekanisme failover, sekaligus melengkapi literatur dengan bukti empiris terkait mekanisme failback dan evaluasi performa end-to-end dalam lingkungan operasional nyata. Dengan demikian, penelitian ini berkontribusi pada pengayaan kajian manajemen redundansi jaringan dengan pendekatan yang lebih aplikatif dan terukur.

5. Kesimpulan

Penelitian ini berhasil mengimplementasikan sistem failover dengan metode Netwatch pada perangkat Mikrotik RB450Gx4 di lingkungan Apotek Farmaku. Sistem mampu mengatasi permasalahan ketergantungan terhadap satu jalur internet dengan

menyediakan mekanisme otomatis untuk beralih ke jalur cadangan saat ISP utama mengalami gangguan.

Hasil pengujian menunjukkan bahwa proses perpindahan koneksi (failover) ke ISP cadangan terjadi dalam waktu 5 detik dengan tingkat packet loss minimal dan tanpa mengganggu aktivitas pengguna. Proses pemulihan ke jalur utama (failback) juga berlangsung otomatis dan stabil. Baik dari sisi router maupun pengguna (PC Client), koneksi tetap lancar selama transisi berlangsung.

Meskipun hasil penelitian menunjukkan bahwa sistem failover–failback berbasis Netwatch bekerja secara efektif, penelitian ini memiliki beberapa keterbatasan. Pertama, pengujian performa jaringan hanya difokuskan pada metrik dasar berupa latency, packet loss, dan waktu perpindahan koneksi, tanpa mengevaluasi parameter lain seperti jitter, throughput, atau kualitas layanan aplikasi secara lebih mendalam. Kedua, penelitian ini dilakukan pada satu lokasi studi kasus, yaitu salah satu cabang Apotek Farmaku, sehingga hasilnya belum tentu dapat digeneralisasikan ke lingkungan dengan skala jaringan atau karakteristik trafik yang berbeda. Ketiga, metode pengujian konektivitas masih mengandalkan teknik sederhana seperti ping dan traceroute, sehingga belum mencerminkan sepenuhnya variasi beban trafik yang kompleks. Oleh karena itu, penelitian lanjutan diperlukan untuk menguji sistem ini pada lingkungan yang lebih beragam, dengan metrik performa yang lebih komprehensif dan skenario beban jaringan yang lebih kompleks.

Dengan demikian, konfigurasi failover Netwatch terbukti mampu meningkatkan keandalan dan ketersediaan jaringan, serta dapat dijadikan solusi praktis bagi lingkungan yang memerlukan koneksi internet berkelanjutan. Penelitian ini berhasil memenuhi tujuan utama, yakni merancang sistem jaringan yang tangguh dan adaptif terhadap gangguan konektivitas.

6. Ucapan Terima Kasih

Penulis menyampaikan apresiasi kepada Apotek Farmaku atas dukungan, kepercayaan, dan kesempatan yang diberikan dalam mendukung pelaksanaan penelitian ini. Kontribusi dari seluruh jajaran, khususnya apoteker, tim TI, staf operasional, serta analis data, sangat membantu dalam kelancaran proses pengumpulan data, pelaksanaan observasi, hingga tahap implementasi sistem jaringan.

Penulis juga menyampaikan ucapan terima kasih kepada Universitas Dian Nusantara, khususnya Program Studi Teknik Informatika, atas dukungan dan fasilitasi akademik yang telah diberikan sepanjang proses penyusunan penelitian ini. Arahan dari para dosen dan lingkungan pembelajaran yang kondusif turut berperan penting dalam membentuk kemampuan berpikir kritis dan aplikatif dalam merumuskan solusi atas permasalahan nyata melalui pendekatan teknologi.

Ucapan terima kasih disampaikan kepada keluarga dan rekan-rekan atas segala bentuk dukungan moril, motivasi, dan doa yang telah memberikan kekuatan selama berlangsungnya penyusunan penelitian ini.

Sebagai penutup, Penelitian ini diharapkan mampu memberikan nilai tambah dan kontribusi yang bermanfaat bagi Apotek Farmaku dalam meningkatkan keandalan sistem jaringan yang digunakan, maupun bagi pengembangan keilmuan di bidang jaringan komputer, khususnya dalam penerapan sistem failover otomatis yang adaptif dan mudah diimplementasikan. Semoga karya ini dapat menjadi bagian kecil dari kontribusi terhadap kemajuan teknologi informasi di lingkungan praktis maupun akademik.

7. Pernyataan Penulis

Penulis menyatakan bahwa tidak terdapat konflik kepentingan dalam bentuk apa pun terkait dengan publikasi penelitian ini. Seluruh isi dan data yang disajikan dalam artikel ini dijamin bebas dari unsur plagiarisme, dan penulis bertanggung jawab sepenuhnya atas orisinalitas dan keabsahan penelitian ini.

Bibliografi

Panggabean, B. E. P. T., & Kuswanto, H. (2023). Implementasi Sistem Failover dengan Metode Netwatch Menggunakan Router Mikrotik. Media Jurnal Informatika, 15(1), 1. https://doi.org/10.35194/mji.v15i1.2441

Raharjo, P. P., Setiawan, K., & Kastum. (2024). Implementasi Backup Koneksi Jaringan Menggunakan Metode Failover MikroTik pada PT Tiga Kawan Sertifikasi. Jurnal Indonesia : Manajemen Informatika Dan Komunikasi, 5(3), 2899-2914. https://doi.org/10.35870/jimik.v5i3.974

Sandi, T. A. A., Heristian, S., & Leksono, I. N. (2021). Optimalisasi Failover Dengan Netwatch Pada Mikrotik. Content : Computer and Network Technology, 1(1). https://doi.org/10.31294/conten.v1i1.388

Rahman, T., Khudori, A., Nurdin, H., & Qomaruddin, M. (2022). Netwatch Mikrotik Pada Jaringan PT Dinasti Kurnia Sejahtera. Jusikom : Jurnal Sistem Komputer Musirawas, 7(2), 106–114. https://doi.org/10.32767/jusikom.v7i2.1715

Khudori, A., Anton, & Nugraha, F. S. (2022). Implementasi fail over dan load balance untuk grouping jalur koneksi user dan monitoring. Jurnal Infortech, 4(2). https://ejournal.bsi.ac.id/ejurnal/index.php/infortech/article/view/13753

Sulistyawan, R. N., & Priyawati, D. (2023). Implementasi load balancing dan failover recursive pada Mikrotik menggunakan metode PCC (Per Connection Classifier) (Skripsi, Universitas Muhammadiyah Surakarta). Universitas Muhammadiyah Surakarta. https://eprints.ums.ac.id/118367/

Saputra, K., & Ariyadi, T. (2023). Implementasi automatic failover jaringan LAN menggunakan Mikrotik di CV Makmur Abadi. Dalam Seminar Hasil Penelitian Vokasi (SEMHAVOK). Universitas Bina Darma. https://repository.binadarma.ac.id/7765/

Rukmana, I., & Suhendi, H. (2023). Implementasi Load Balancing PCC dan Failover Netwatch Menggunakan Mikrotik di PT. Infomedia Nusantara. 4(1).

Putra, W. P., Robiyanto, R., & Raswa. (2023). Manajemen Jaringan Policy Based Router-Failover Dan Netwatch Pada Router Mikrotik Dalam Membagi Jalur Akses Internet Di SMA-NU Tajanarkidul. Seminar Nasional Teknologi Informasi Dan Komunikasi STI&K (SeNTIK), 7(1). https://ejournal.jak-stik.ac.id/index.php/sentik/article/view/3412

Irman, A., & Anton, A. (2024). Implementasi Load Balance Mikrotik Dual ISP Dengan PCC dan Metode Failover Pada PT. Wahana Ciptasinatria. Jurnal Teknologi Informasi, 10. https://doi.org/10.52643/jti.v10i1.4318

Azmi, K., Syamsul, S., & Razi, F. (2022). Studi penggunaan dua ISP dengan load balancing dan failover untuk meningkatkan kinerja jaringan berbasis router Mikrotik. Jurnal TEKTRO, 6(2). https://e-jurnal.pnl.ac.id/TEKTRO/article/view/3729/2919

Syahrani, A. H., & Yuliadi, B. (2023). Indonesian Scientific Index (SINTA) journal-level of S3. 11(2), 267. https://doi.org/10.33558/piksel.