



Optimizing the Internet of Things Lab Network Using the Failover Method

Putri Ariza Ardani¹, Husaini^{2*}, Fachri Yanuar Rudi F³

^{1,2,3}Jurusan Teknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe
Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA

*Penulis Korespondensi : husaini@pnl.ac.id

INFORMASI ARTIKEL

Riwayat artikel:

Diajukan pada 00 Maret 00

Direvisi pada 00 April 00

Publikasi pada 00 Juni 00

Kata kunci:

Failover

Netwatch

Internet Service Provider

Quality of Service

Keywords:

Failover

Netwatch

Internet Service Provider

Quality of Service

ABSTRAK

Pada era digital yang semakin berkembang pesat, keberlanjutan operasional pendidikan sangat bergantung pada kestabilan dan keamanan jaringan komputer. Masalah utama yang dihadapi adalah gangguan koneksi internat yang dapat menghambat produktivitas. Penelitian ini bertujuan untuk mengoptimalkan penggunaan jaringan di Lab Gedung TIK Politeknik Negeri Lhokseumawe. Metodologi yang digunakan melibatkan implementasi Netwatch pada MikroTik untuk memonitor dan mengalihkan jalur koneksi secara otomatis ketika terjadi kegagalan koneksi. Data dikumpulkan melalui pengujian langsung di laboratorium, dan analisis QoS dilakukan dengan mengukur parameter seperti *throughput*, *packet loss*, *delay*, dan *jitter* sebelum dan sesudah penerapan metode *Failover*. Hasil penelitian menunjukkan bahwa penerapan metode *Failover* berhasil meningkatkan efisiensi pengelolaan jaringan dan mengurangi *downtime* secara signifikan dengan waktu selama 2 detik saat perpindahan ISP. Sebelum penerapan *Failover*, *throughput* rata-rata adalah 1678.35 kbps, dengan *packet loss* 0%, *delay* 4 ms, dan *jitter* 16ms. Setelah penerapan *Failover*, *throughput* meningkat menjadi 1776.34 kbps, dengan *packet loss* 0%, *delay* 5 ms, dan *jitter* 6 ms. Hasil keseluruhan dari penggunaan metode *Failover* efektif dalam menjaga ketersediaan jaringan dan meningkatkan kualitas layanan di Lab .

ABSTRACT

In the rapidly developing digital era, the continuity of educational operations is highly dependent on the stability and security of computer networks. The main problem faced is internet connection disruptions that can hinder productivity. This study aims to optimize network usage in the Lab of the Lhokseumawe State Polytechnic ICT Building. The methodology used is to implement Netwatch on MikroTik to monitor and redirect connection paths automatically when a connection failure occurs. Data collection was carried out through direct testing in the laboratory, and QoS analysis was carried out by measuring parameters such as throughput, packet loss, delay, and jitter before and after the implementation of the Failover method. The results showed that the implementation of the Failover method succeeded in increasing network management efficiency and significantly reducing downtime by 2 seconds when switching ISPs. Before the implementation of Failover, the average throughput was 1678.35 kbps, with 0% packet loss, 4 ms delay, and 16 ms jitter. After implementing Failover, the throughput increased to 1776.34 kbps, with 0% packet loss, 5 ms delay, and 6 ms jitter. The overall results of using the Failover method are effective in maintaining network availability and improving service quality in the Lab.

1. Pendahuluan

Internet merupakan jaringan global yang menghubungkan berbagai komputer di seluruh dunia menggunakan protokol standar TCP/IP, memungkinkan miliaran pengguna untuk saling bertukar informasi. Proses penghubungan jaringan ini dikenal sebagai internetworking atau antar jaringan [1]. Seiring dengan perkembangan teknologi, jaringan internet telah mencakup hampir seluruh dunia, memfasilitasi akses yang mudah bagi berbagai kalangan, termasuk dosen, mahasiswa, dan masyarakat umum.

Pada Lab *Internet of Things* (IoT) Gedung TIK Politeknik Negeri Lhokseumawe, sering terjadi gangguan koneksi internet akibat masalah pada *Internet Service Provider* (ISP) utama. Hal ini mengakibatkan *downtime* yang menghambat kegiatan belajar mengajar di laboratorium. Salah satu solusi yang efektif untuk mengatasi masalah ini adalah penerapan metode *Failover*, di mana lebih dari satu ISP digunakan. Metode *Failover* memungkinkan koneksi internet secara otomatis dialihkan ke ISP cadangan ketika ISP utama mengalami gangguan, sehingga konektivitas tetap terjaga [2]. Implementasi metode *Failover* di Lab IoT ini diharapkan dapat membantu administrator jaringan mengelola jaringan dengan lebih efisien. Selain itu, penggunaan fitur Netwatch pada MikroTik memungkinkan pemantauan dan pengalihan koneksi secara otomatis antara jalur utama dan cadangan, yang memperlancar pengelolaan sistem jaringan [3].

Failover adalah proses otomatis yang mengalihkan koneksi ke ISP cadangan saat ISP utama gagal menyediakan layanan internet. Pada router MikroTik, pengaturan *Failover* dapat dilakukan dengan menambahkan rute *default* dengan parameter jarak lebih tinggi, sehingga rute dengan jarak lebih rendah diprioritaskan [4]. Dalam konteks jaringan, *Failover* memungkinkan sistem beralih secara otomatis atau manual ke koneksi cadangan, sehingga fungsi jaringan tetap berjalan meskipun terjadi kegagalan pada ISP utama. Sistem ini juga dapat dikonfigurasi untuk bekerja dengan lebih dari dua ISP.

Netwatch adalah fitur MikroTik yang memungkinkan pemantauan kondisi host dalam jaringan melalui berbagai jenis *probe* seperti ICMP (ping), TCP, dan HTTP GET. Setiap entri Netwatch dapat dikonfigurasi dengan alamat IP, interval ping, dan skrip untuk menjalankan perintah otomatis saat status host berubah [2]. Keunggulan utama Netwatch adalah kemampuannya menyesuaikan konfigurasi secara otomatis sesuai kondisi jaringan. Netwatch pada MikroTik berfungsi memantau host dengan mengirimkan pesan ICMP secara berkala. Jika balasan diterima, koneksi dianggap aktif (*Up*), sementara tidak adanya balasan menunjukkan koneksi terputus (*Down*). Berdasarkan hasil ini, skrip dapat dijalankan secara otomatis untuk menanggapi perubahan status koneksi [5].

Penelitian ini berfokus pada tiga masalah utama: pertama, seberapa efektif metode *Failover* dapat mengurangi *downtime* pada jaringan Lab Internet of Things; kedua, apa dampak penerapan metode *Failover* menggunakan Netwatch terhadap kualitas layanan (QoS) jaringan, yang diukur dari parameter *throughput*, *packet loss*, *delay*, dan *jitter*; dan ketiga, berapa lama waktu yang dibutuhkan oleh Netwatch untuk mendeteksi gangguan pada ISP utama sebelum berhasil mengalihkan koneksi ke ISP cadangan.

Adapun tujuan dari penelitian ini adalah untuk mengukur efektivitas penerapan metode *Failover* dalam meminimalkan *downtime* di jaringan Lab Internet of Things. Selain itu, penelitian ini bertujuan mengevaluasi dampak implementasi *Failover* menggunakan Netwatch terhadap kualitas layanan (QoS)

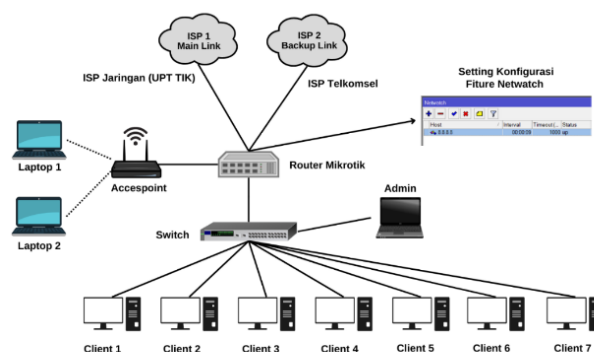
jaringan melalui pengukuran parameter *throughput*, *packet loss*, *delay*, dan *jitter*, serta untuk menentukan seberapa cepat waktu yang dibutuhkan Netwatch untuk mendeteksi kegagalan ISP utama dan mengalihkan koneksi ke ISP cadangan.

2. Metode

Penelitian ini menggunakan metode *Failover* untuk memantau dan mengelola koneksi internet di Lab Internet of Things, Gedung TIK Politeknik Negeri Lhokseumawe. Sistem kerja *Failover* melibatkan pemantauan ISP 1 (*UPT TIK*) sebagai provider utama, dengan ISP 2 (*Orbit Telkomsel*) sebagai cadangan yang akan aktif secara otomatis jika ISP utama mengalami gangguan. Fitur Netwatch pada MikroTik digunakan untuk mendeteksi kondisi koneksi dan mengalihkan jalur internet sesuai kebutuhan. Tahapan dalam penerapan metode *Failover* ini adalah sebagai berikut:

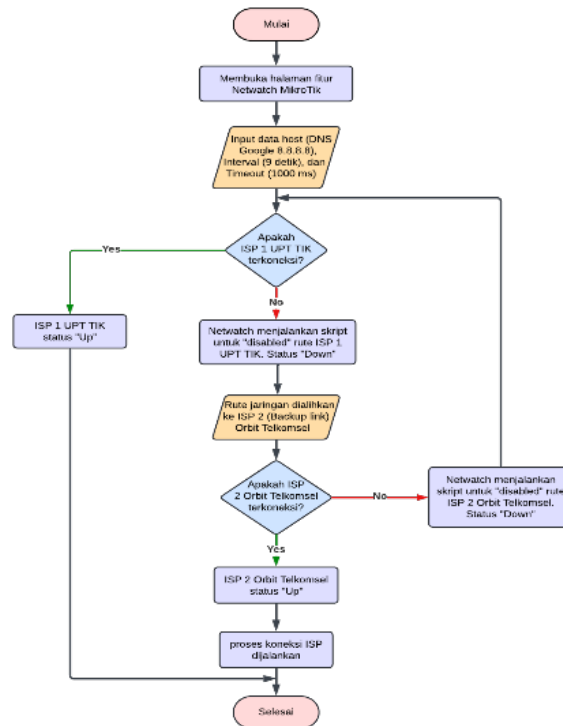
1. Pemantauan koneksi dengan Netwatch, Netwatch mengirimkan permintaan ping secara berkala untuk memeriksa respons perangkat jaringan pada Lab Internet of Things.
2. Konfigurasi skrip Netwatch, skrip atau aturan dibuat untuk mendeteksi kondisi saat koneksi terputus atau tidak responsif. Ambang batas atau threshold ditetapkan untuk menentukan kapan *Failover* harus diaktifkan.
3. Penyiapan sumber daya cadangan, ISP 2 (*Orbit Telkomsel*) diatur sebagai jalur *backup* yang akan diaktifkan secara otomatis ketika Netwatch mendeteksi kegagalan pada ISP 1 (*UPT TIK*).
4. Pengalihan Layanan, Konfigurasi memastikan bahwa layanan internet secara otomatis beralih ke ISP cadangan saat diperlukan dan kembali ke ISP utama setelah kondisinya normal.
5. Pemantauan dan manajemen pasca-*Failover*, tahap akhir melibatkan pencatatan kejadian *Failover*, pemantauan sistem secara terus-menerus, serta manajemen sumber daya cadangan dan utama hingga pemulihan. Metode ini memberikan kerangka kerja yang terstruktur untuk mendeteksi gangguan secara proaktif, memastikan ketersediaan layanan, dan mengoptimalkan kinerja jaringan di Lab Internet of Things.

Perancangan topologi digunakan untuk menjelaskan gambaran mengenai perancangan sistem yang akan dibangun pada penelitian ini. Blok diagram sistem secara keseluruhan menjelaskan bagaimana Optimalisasi Jaringan Lab Internet of Things dengan metode *Failover* dapat bekerja. Gambar arsitektur rancangan sistem dapat dilihat pada Gambar 1.



Gambar 1. Rangkaian Sistem Metode *Failover*

Perancangan sistem Netwatch MikroTik digunakan untuk menjelaskan gambaran mengenai cara sistem fitur Netwatch di dalam MikroTik yang akan diterapkan pada penelitian ini. Berikut rancangan sistem kerja Netwatch MikroTik dapat dilihat pada Gambar 2.



Gambar 2. Sistem kerja fitur Netwatch MikroTik

Berdasarkan Gambar 2 tahapan proses penerapan sistem kerja fitur Netwatch MikroTik adalah sebagai berikut:

1. Membuka halaman MikroTik, Halaman antarmuka MikroTik akan dibuka kemudian fitur Netwatch akan dicari melalui menu 'Tools' >> 'Netwatch'
2. Penentuan host monitoring, Pada fitur Netwatch pengaturan dilakukan dengan menentukan *host* yang akan dimonitor, yaitu menghubungkan IP milik DNS Google 8.8.8.8. Selain host, interval pengecekan dan waktu timeout juga diatur. Interval ditetapkan sebagai 00:00:09 (9 detik), dan *timeout* diatur menjadi 1000 ms.
3. Pengaturan kondisi saat *host* tersambung (*Up*), Jika host dalam kondisi *Up* (tersambung), perintah `/ip route set [find comment="isp1"] disabled=no` akan dijalankan. Perintah ini mengaktifkan (*enable*) jalur ke ISP 1.
4. Pengaturan kondisi saat *host* tidak tersambung (*Down*), Jika host tidak terhubung atau *down*, maka perintah `/ip route set [find comment="isp1"] disabled=yes` akan dijalankan. Perintah ini menonaktifkan (*disable*) jalur ke ISP 1.
5. Perubahan status pada routing, Ketika ISP 1 tidak terhubung atau *down*, jalur routing ke ISP 1 akan otomatis dinonaktifkan (*disabled*). Akibatnya, *backup* link melalui ISP 2 akan diaktifkan dan digunakan oleh router MikroTik sebagai jalur utama. Sebaliknya, ketika ISP 1 kembali terhubung atau *Up*, jalur routing ke ISP 1 akan otomatis diaktifkan (*enabled*), dan ISP 1 akan kembali menjadi jalur utama.

Rangkaian sistem *flowchart* ini menjelaskan mengenai proses saat Netwatch MikroTik berjalan pada penelitian ini dengan metode *Failover*.

Teknik pengujian dilakukan setelah data terkumpul pada saat pengujian alat adalah menggunakan teknik pengujian QoS (*Quality of Service*). Adapun teknik pengujian dilakukan sebagai berikut :

1. Perhitungan *Throughput*, digunakan untuk mengukur kecepatan data yang dapat dikirim dan diterima oleh jaringan dalam menilai kinerja jaringan metode *Failover*.
2. Perhitungan *Delay*, digunakan untuk mengukur waktu yang diperlukan untuk data berpindah dari sumber ke tujuan dalam menilai kinerja jaringan metode *Failover*.
3. Perhitungan *Jitter*, digunakan untuk mengukur variasi dalam waktu *delay* data saat berpindah melalui jaringan.
4. Perhitungan *Packet Loss*, digunakan untuk mengukur persentase data paket yang hilang selama transmisi melalui kinerja jaringan metode *Failover*.

Dalam penelitian ini, peneliti menggunakan teknik pengujian QoS (*Quality of Service*) untuk menghitung *throughput*, *delay*, *jitter*, dan *packet loss* guna menguji kinerja metode *Failover*. Pengukuran dilakukan sebelum dan setelah metode *Failover* diterapkan. Perbedaan hasil pengukuran ini digunakan untuk mengevaluasi apakah metode *Failover* dapat mengoptimalkan jaringan internet.

3. Hasil Dan Pembahasan

3.1 Konfigurasi Address List

Mauk ke menu IP>Address dan klik tombol "+", kemudian IP *address* dan *interface* yang digunakan diisi terlebih dahulu. Ether1 diatur untuk ISP 1 UPT TIK, wlan1 diatur untuk ISP 2 Orbit Telkomsel, sementara interface ether4 digunakan untuk koneksi LAN. Berikut ini list setiap IP yang digunakan pada Gambar 3.

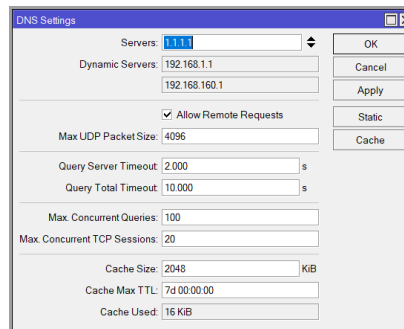
Address	Network	Interface
10.10.1.1/24	10.10.1.0	ether3
20.20.1.1/24	20.20.1.0	ether4
D 192.168.1.100/24	192.168.1.0	ether2
D 192.168.160.12...	192.168.160.0	ether1

Gambar 3. Address List

Pada Gambar 4, dijelaskan bahwa setiap IP akan menunjukkan port yang terhubung dengan perangkatnya. Hal ini menunjukkan bahwa kabel LAN telah terhubung ke router, *access point*, modem MikroTik, dan Orbit. Secara otomatis, alamat IP dari setiap perangkat akan terdeteksi dan ditampilkan pada layar interface IP. Berdasarkan IP address yang ditampilkan pada *interface* LAN, ether1 dihubungkan dengan ISP 1 UPT TIK, ether2 dihubungkan dengan ISP 2 Orbit Telkomsel, ether3 dihubungkan dengan *access point*, dan ether4 dihubungkan dengan IP yang digunakan untuk perangkat PC dan Switch.

3.2 Konfigurasi DNS

Konfigurasi DNS adalah pengisian Alamat DNS *server* pada router untuk penerjemah nama *domain* menjadi Alamat IP. DNS yang dimasukkan adalah DNS publik yaitu (1.1.1.1) untuk digunakan dalam jaringan. Berikut tampilan setting DNS pada Gambar 4.



Gambar 4. Setting DNS

Pada Gambar 4 dijelaskan bahwa konfigurasi DNS pada router MikroTik menggunakan server IP 1.1.1.1 dan IP *gateway* dinamis dari ether1 dan ether2, yaitu 192.168.1.1 (ISP 2 Orbit Telkomsel) dan 192.168.160.1 (ISP 1 UPT TIK). Jika hanya satu DNS diinput, salah satu link akan mati, menyebabkan router dan klien tidak bisa mengakses website. Alternatif lain yang dapat digunakan adalah DNS publik Google (8.8.8.8 atau 8.8.4.4). Pengaturan ini dapat diakses melalui IP > DNS.

3.3 Konfigurasi Router

Route List pada router MikroTik yang digunakan untuk mengatur jalur koneksi internet dari dua ISP berbeda di jaringan lokal. Berikut tampilan route list pada Gambar 5.

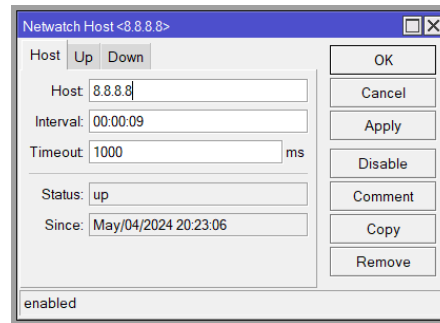
Dst. Address	Gateway	Distance	Routing Mark
AS 0.0.0.0/0	192.168.160.1 reachable ether1	1	
AS 0.0.0.0/0	192.168.1.1 reachable ether2	2	
AS 0.0.0.0/0	192.168.1.1 reachable ether2	1	via-isp1
DC 10.10.10.0/24	ether1 unreachable	255	10
DAC 172.72.72.0/24	ether3 reachable	0	172
DAC 192.168.1.0/24	ether2 reachable	0	192
DAC 192.168.160.0/24	ether1 reachable	0	192

Gambar 5. Tampilan *Route List*

Pada Gambar 5 menunjukkan konfigurasi *default-route* pada router MikroTik, di mana *gateway* 192.168.160.1 melalui ether1 untuk ISP1 UPT TIK dan *gateway* 192.168.1.1 melalui ether2 untuk ISP2 Orbit Telkomsel. *Route* tambahan mencakup *subnet* yang dapat dijangkau seperti 172.72.72.0/24 melalui ether3 dan 192.168.1.0/24 serta 192.168.160.0/24 melalui ether2 dan ether1. Sementara *subnet* 10.10.10.0/24 dinyatakan tidak dapat dijangkau melalui ether4. Konfigurasi ini mengatur lalu lintas jaringan berdasarkan *route* yang ditentukan, jalur utama akan secara otomatis berpindah ke jalur cadangan jika terjadi kegagalan.

3.4 Konfigurasi Netwatch

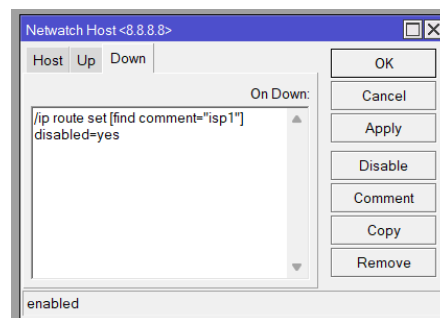
Fitur Netwatch pada MikroTik berfungsi memantau status koneksi jaringan secara otomatis dengan menggunakan *ping* atau protokol khusus. Jika koneksi terputus atau tidak responsif, Netwatch menjalankan perintah yang ditentukan, seperti mengalihkan koneksi ke jalur cadangan atau mengirim notifikasi. Proses konfigurasi Netwatch MikroTik dapat dilihat pada Gambar 6.



Gambar 6. Tampilan *Netwatch Host*

Pada gambar 6, dijelaskan bahwa tahap awal untuk melakukan konfigurasi netwatch yaitu dengan masuk pada halaman netwatch *host* dan menggunakan *host* 8.8.8.8 yang dikarenakan pengguna akan melakukan tes *ping* ke ip 8.8.8.8. Parameter interval pada halaman tersebut tersetting 9 detik (00:00:09) yaitu, waktu untuk router melakukan *ping* ke *host* nya, bagian *timeout* digunakan untuk mengakhiri waktu pengetesan ping ke *host* selama 1000ms, saat pengguna mengeping lebih dari 1000ms maka akan dianggap *timeout*.

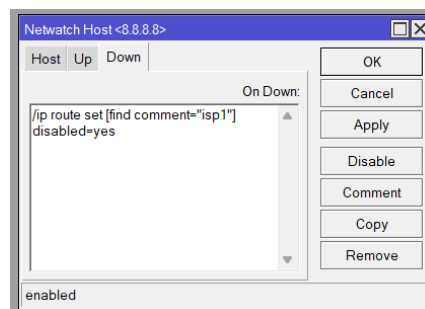
Berikut ini adalah cara mensetting *script* di halaman *UP* fitur Netwatch MikroTik, pada Gambar 7.



Gambar 7. Mensetting *script* pada halaman *UP* Netwatch

Berikutnya pada gambar 8 dijelaskan, halaman *Up* ini menentukan status *Up* dengan melakukan perintah *script* seperti di atas yang artinya ketika ISP1 telah dapat kembali aktif dengan cara melakukan *ping* ke interval yang telah ditentukan. Maka akan dieksekusi sebagai *enabled*/diaktifkan.

Berikut ini adalah cara mensetting *script* di halaman *Down* fitur Netwatch MikroTik, pada Gambar 8.

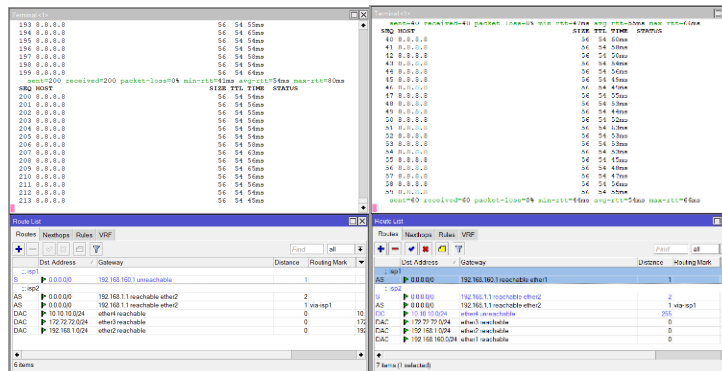


Gambar 8. Mensetting *script* pada halaman *Down* Netwatch

Pada Gambar 8, pengaturan skrip pada tab "Down" di halaman Netwatch digunakan untuk memantau status koneksi ISP1. Skrip tersebut otomatis dijalankan ketika koneksi ISP1 gagal, ditandai dengan ketidakmampuan melakukan *ping* ke IP 8.8.8.8. Perintah `"/ip route set [find comment="isp1"] disabled=yes` menonaktifkan rute ISP1 saat terdeteksi "Down", sehingga lalu lintas jaringan dialihkan otomatis ke ISP2. Pengaturan ini menjaga ketersediaan jaringan dengan memastikan koneksi tetap berjalan meskipun ISP utama tidak berfungsi.

3.5 Pengujian Failover

Pengujian metode *Failover* dilakukan dengan melakukan ping ke IP 8.8.8.8 dan memutus koneksi ISP utama untuk mengamati hasil proses *Failover*, seperti yang ditampilkan pada Gambar 10.

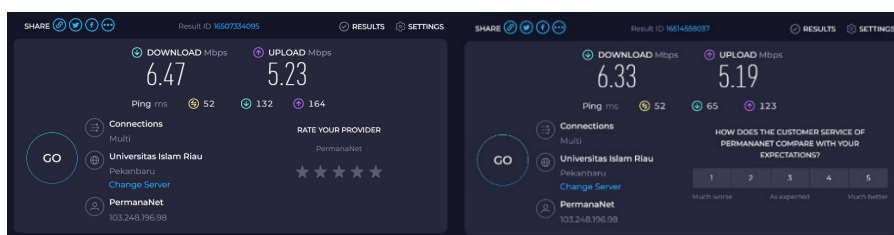


Gambar 9. (A) Saat terjadinya *backup* ke jaringan ISP2 Orbit Telkomsel, (B) Saat ISP1 UPT TIK kembali jalan secara otomatis

Pada Gambar 10 (A), dijelaskan bahwa saat terjadi *downtime* pada ISP1 UPT TIK, koneksi internet otomatis dialihkan ke ISP2 Orbit Telkomsel. *Ping* ke IP 8.8.8.8 menunjukkan "Request Time Out" akibat kegagalan ISP1. Rute utama melalui ether1 (192.168.10.1) dinonaktifkan dan secara otomatis dialihkan ke ether2 (192.168.20.1) yang terhubung ke ISP2, memastikan kontinuitas jaringan melalui proses *Failover*. Berikutnya dijelaskan bahwa *trouble/downtime* pada ISP1 UPT TIK sudah tidak terjadi lagi sehingga jaringan pengaksesan internet akan kembali dialihkan secara otomatis ke *provider* ISP1 UPT TIK, dan ISP2 Orbit Telkomsel akan dinonaktifkan/*disable* secara otomatis.

3.6 Pengujian Kecepatan Internet ISP 1 UPT TIK Pada Speed Test

Dalam pengujian kecepatan *bandwith* internet ISP1 UPT TIK akan dilakukan menggunakan web browser di <https://www.speedtest.net/> . seperti yang dapat dilihat pada Gambar 11.

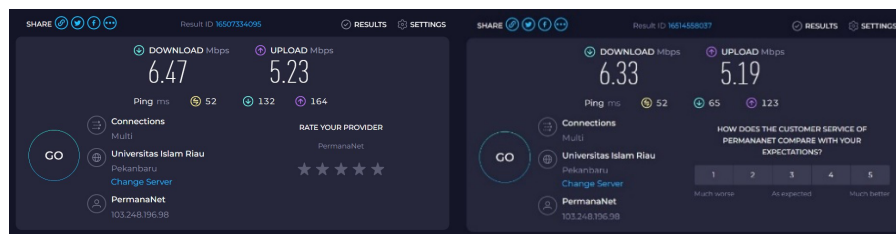


Gambar 10. A) Hasil Speed Test ISP1 UPT TIK Kamis, jam 07:30 pagi, (B) Hasil Speed Test ISP1 UPT TIK Jumat, jam 07:30 pagi

Gambar 10 menunjukkan hasil pengujian koneksi internet dari ISP1 *UPT TIK* (PermanaNet) dengan IP 103.248.196.98. Kecepatan unduh tercatat sebesar 6.54 Mbps dan unggah 5.61 Mbps. Pada pengujian hari Kamis, kecepatan unduh 6.47 Mbps dan unggah 5.23 Mbps, sementara pengujian hari Jumat menunjukkan penurunan kecil dengan unduh 6.33 Mbps dan unggah 5.19 Mbps. Hasil ini menegaskan bahwa ISP1 *UPT TIK* memberikan koneksi internet yang stabil dan andal.

3.7 Pengujian Kecepatan Internet ISP 2 Orbit Telkomsel Pada Speed Test

Selanjutnya adalah hasil *speedtest* dari pengujian kecepatan internet ISP2 Orbit Telkomsel. Seperti pada Gambar 11.



Gambar 11. Hasil Speed Test (A) ISP1 *UPT TIK* kamis, jam 07:40 pagi, (B) Kedua dari Bandwith ISP2 Orbit Telkomsel jumat jam 07:40 pagi

Gambar 11 menampilkan hasil pengujian kecepatan internet menggunakan Speedtest.net dengan layanan Telkomsel Orbit di Universitas Islam Riau, Pekanbaru. Pada pengujian pertama (A), kecepatan unduh mencapai 5.71 Mbps dan meningkat menjadi 6.38 Mbps pada pengujian kedua (B). Kecepatan unggah juga meningkat signifikan dari 0.23 Mbps menjadi 5.22 Mbps, menunjukkan peningkatan kualitas koneksi yang lebih andal.

3.8 Hasil Pengujian Downtime

Pada tahap ini, akan dilakukan pengujian terhadap *downtime* saat perpindahan ISP 1 *UPT TIK* ke ISP 2 Orbit Telkomsel yang telah diterapkan, berikut Gambar 12.

```

Reply from 8.8.8.8 bytes=32 time=55ms TTL=54
Reply from 8.8.8.8 bytes=32 time=51ms TTL=54
Reply from 8.8.8.8 bytes=32 time=44ms TTL=54
Reply from 8.8.8.8 bytes=32 time=60ms TTL=54
Reply from 8.8.8.8 bytes=32 time=49ms TTL=54
Reply from 8.8.8.8 bytes=32 time=56ms TTL=54
Reply from 8.8.8.8 bytes=32 time=59ms TTL=54
Reply from 8.8.8.8 bytes=32 time=59ms TTL=54
Reply from 8.8.8.8 bytes=32 time=54ms TTL=54
Reply from 8.8.8.8 bytes=32 time=56ms TTL=54
Reply from 8.8.8.8 bytes=32 time=42ms TTL=54
Reply from 8.8.8.8 bytes=32 time=54ms TTL=54
Reply from 20.20.1.1: Destination net unreachable.
Request timed out.
Reply from 8.8.8.8 bytes=32 time=24ms TTL=113
Reply from 8.8.8.8 bytes=32 time=19ms TTL=113
Reply from 8.8.8.8 bytes=32 time=21ms TTL=113
Reply from 8.8.8.8 bytes=32 time=19ms TTL=113
Reply from 8.8.8.8 bytes=32 time=19ms TTL=113
Reply from 8.8.8.8 bytes=32 time=24ms TTL=113

```

Gambar 11. Hasil cmd dari pengetesan *downtime*

Gambar 12, menunjukkan pengujian perpindahan koneksi dari ISP 1 (*UPT TIK*) ke ISP 2 (Orbit Telkomsel) dengan *downtime* tercatat 2 detik. Ping ke 8.8.8.8 sebelum *downtime* menunjukkan waktu respon stabil 42-57 ms tanpa *packet loss*. Selama *Failover*, beberapa *Request timed out* terjadi, tetapi setelah *downtime*, ping kembali normal dengan respon 50-57 ms. Ini menandakan mekanisme *Failover* berjalan efektif dengan *downtime* minimal, menjaga stabilitas konektivitas jaringan.

3.9 Hasil Pengujian QoS (*Quality of Service*)

Pengujian performa jaringan dilakukan tiga kali dengan Wireshark untuk mendapatkan rata-rata parameter QoS (*Throughput*, *Packet Loss*, *Delay*, dan *Jitter*) pada jaringan LAN dan WLAN sebelum *Failover*.

1. Sebelum *Failover*

Tabel 1. Pengujian QoS Sebelum *Failover*

Parameter	Rata-Rata	Kategori QoS	Indeks
Throughput	1678,35 kbps	Memuaskan	3
Packet Loss	0%	Sangat Memuaskan	4
Delay	4 ms	Sangat Memuaskan	4
Jitter	16 ms	Memuaskan	3
Hasil QoS		Memuaskan	3,5

Tabel 1 menunjukkan hasil pengujian kualitas layanan (QoS) untuk jaringan LAN dan WLAN sebelum penerapan metode *Failover*. Pada pengujian ini, *throughput* rata-rata mencapai 1678,35 kbps dengan kategori “memuaskan” dan indeks 3. Tidak terjadi *packet loss*, yang berarti semua data yang dikirimkan berhasil diterima tanpa kehilangan paket, dengan kategori sangat memuaskan dan indeks 4. Rata-rata *delay* tercatat sebesar 4 ms, yang juga dikategorikan sangat memuaskan dengan indeks 4. Namun, *jitter* rata-rata mencapai 16 ms yang termasuk dalam kategori memuaskan dengan indeks 3.

Secara keseluruhan, hasil QoS dari pengujian ini termasuk dalam kategori memuaskan dengan skor rata-rata indeks 3,5. Dalam perhitungan QoS ini terdapat 3 kali pengujian pada jaringan LAN dan WLAN dengan beban 1000 *bytes* serta total paket berjumlah 500.

2. Sesudah *Failover*

Tabel 2. Pengujian QoS Sesudah *Failover*

Parameter	Rata-Rata	Kategori QoS	Indeks
Throughput	1776,34 kbps	Memuaskan	3
Packet Loss	0%	Sangat Memuaskan	4
Delay	5 ms	Sangat Memuaskan	4
Jitter	11 ms	Memuaskan	3
Hasil QoS		Memuaskan	3,5

Tabel 2, menunjukkan hasil pengujian kualitas layanan (QoS) untuk jaringan LAN dan WLAN setelah penerapan metode *Failover*. Dari tabel tersebut, terlihat bahwa *throughput* rata-rata meningkat signifikan menjadi 1776,34 kbps dengan kategori “memuaskan” dan indeks 3. Tidak ada *packet loss* yang tercatat selama pengujian, yang berarti semua data yang dikirimkan berhasil diterima tanpa kehilangan paket, dengan kategori sangat memuaskan dan indeks 4. Rata-rata *delay* juga mengalami penurunan menjadi 5 ms, yang sangat memuaskan dengan indeks 4, menunjukkan respons jaringan yang cepat. *Jitter* rata-rata menurun menjadi 11 ms, masuk dalam kategori memuaskan dengan indeks 3.

Secara keseluruhan, hasil QoS dari pengujian ini termasuk dalam kategori memuaskan dengan skor rata-rata indeks 3,5. Dalam perhitungan QoS ini, juga terdapat 3 kali pengujian pada jaringan LAN dan WLAN dengan beban 1000 *bytes* serta total paket berjumlah 500.

4. Kesimpulan

Berdasarkan hasil pengujian optimasi jaringan Lab Internet of Things (IoT) di Politeknik Negeri Lhokseumawe menggunakan metode *Failover* dengan dua Internet Service Provider (ISP), yaitu ISP 1 UPT TIK Politeknik sebagai jalur utama dan ISP 2 Orbit Telkomsel sebagai jalur cadangan, serta menggunakan fitur Netwatch untuk memantau status akses jaringan, dapat disimpulkan bahwa metode *Failover* efektif dalam mengurangi *downtime* jaringan. Selama proses *Failover*, *downtime* yang tercatat hanya 2 detik, sehingga konektivitas tetap terjaga meskipun terjadi gangguan pada ISP utama. Pengujian Quality of Service (QoS) tanpa penerapan *Failover* menunjukkan hasil throughput rata-rata sebesar 1.678,35 kbps, delay 4 ms, jitter 16 ms, dan packet loss 0%, dengan skor QoS sebesar 3,5 yang masuk dalam kategori memuaskan. Setelah penerapan *Failover*, throughput meningkat menjadi 1.776,34 kbps, delay sedikit naik menjadi 5 ms, jitter menurun menjadi 11 ms, dan packet loss tetap 0%, dengan skor QoS yang tetap berada di angka 3,5. Ini menunjukkan adanya peningkatan kualitas jaringan internet setelah penerapan *Failover* dibandingkan dengan sebelum penerapan. Netwatch berhasil mendeteksi gangguan pada ISP utama dan secara otomatis mengalihkan koneksi ke ISP cadangan dalam waktu 2 detik, menggunakan metode ping ke DNS Google 8.8.8.8, sesuai dengan interval dan timeout yang telah dikonfigurasi. Kesimpulannya, optimasi jaringan dengan metode *Failover* ini terbukti efektif dalam meningkatkan ketersediaan layanan internet, meminimalkan *downtime*, serta menyediakan solusi efisien terhadap gangguan koneksi. Dengan demikian, jaringan secara otomatis dapat beralih dari ISP utama ke ISP cadangan saat terjadi masalah, memastikan akses internet tetap lancar tanpa gangguan yang signifikan.

Referensi

- [1] D. Kurniawan, W. Wardhana, dan N. A. Ito, "Penggabungan Dua ISP Guna Menstabilkan Koneksi Internet Dengan Metode *Failover*," *J. Komputasi*, vol. 4, no. 2, hal. 1–11, 2016.
- [2] T. Rahman, A. Khudori, H. Nurdin, dan M. Qomaruddin, "Netwatch Mikrotik Pada Jaringan Pt Dinasti Kurnia," *J. Sist. Komput. Musirawas*, vol. 7, no. 2, hal. 106–114, 2022.
- [3] B. E. Putra, T. Panggabean, dan H. Kuswanto, "Implementasi Sistem *Failover* dengan Metode Netwatch Menggunakan Router Mikrotik," *Media J. Inform.*, vol. 15, no. 1, hal. 1–6, 2023, [Daring]. Tersedia pada: <http://jurnal.unsur.ac.id/njinformatika>
- [4] T. Aswin, F. Imansyah, F. T. Pontia W, J. Marpaung, dan R. R. Yacoub, "Analisis Penerapan Access Point Dalam Rentang Frekuensi 2400-2500 MHz di Balmon Kelas II Pontianak," *J. Tek. Elektro*, vol. 2, no. 1, hal. 1–11, 2021, [Daring]. Tersedia pada: <https://jurnal.untan.ac.id/index.php/jteuntan/article/view/51176>
- [5] A. Hidayat, I. P. Saputra, dan A. Bowo, "Bot Monitoring Jaringan Pada BMT Mentari Lampung Timur Menggunakan Mikrotik Dan API Telegram," *JTKSI (Jurnal Teknol. Komput. dan Sist. Informasi)*, vol. 5, no. 3, 2022, doi: 10.56327/jtksi.v5i3.1291.
- [6] Rasudin, "Internet Dengan Metode *Failover*," *Techsi Tek. Inform.*, vol. 6, no. 1, hal. 1–223, 2014.
- [7] M. F. Darmawan dan S. Risnanto, "Implementasi *Failover* Gateway Recursive Dan Load Balancing Menggunakan Metode Per Connection Classifier," *Infotronik J. Teknol. Inf. dan Elektron.*, vol. 8, no. 2, hal. 56, 2023, doi: 10.32897/infotronik.2023.8.2.1887.
- [8] M. Badrul dan Akmaludin, "Implementasi Automatic *Failover* Menggunakan Router Jaringan Mikrotik Untuk Optimalisasi Jaringan," *J. PROSISKO*, vol. 6, no. 2, hal. 82–87, 2019.
- [9] F. Siddiq, "Sistem Monitoring Jaringan Berbasis Netwatch Mikrotik Dengan Integrasi Notifikasi Telegram Pada Laboratorium Komputer SMK Negeri 1 Tanah Jambo Aye," Politeknik Negeri Lhokseumawe, 2023.
- [10] H. Zhahir dan M. Ardiansyah, "Implementasi Manajemen Bandwidth Dengan Menggunakan Metode Load Balancing Dan *Failover* Pada Router MikroTik Dan Switch Cisco (Studi Kasus: Pusat Penguatan Dan Pemberdayaan Bahasa Kemdikbud Ristek)," *Infomatika*, vol. 3, no. 2, hal. 176–193, 2022.