JUNIF: Jurnal Nasional Informatika

p-ISSN: 2774-3497
e-ISSN: 2774-3500

Vol. 4 No. 2, 15 Oktober 2025, pp. 1-13

DESAIN DAN IMPLEMENTASI MANAJEMEN KONEKSI INTERNET DENGAN METODE LOAD BALANCING DAN FAILOVER PADA KANTOR PUSAT TRANS COFFEE

PENULIS [1)]**Muhammad Nabawi,** [2)]**Dwi Sidik Permana** [3)]**Rino Subekti**

ABSTRAK

Di era digitalisasi, konektivitas internet yang stabil dan berkecepatan tinggi menjadi faktor penting dalam mendukung operasional bisnis. PT. Trans Coffee, perusahaan di sektor makanan dan minuman dengan banyak cabang, membutuhkan sistem jaringan yang andal untuk mendukung penerapan sistem Enterprise Resource Planning (ERP). Penelitian ini bertujuan untuk merancang dan menerapkan sistem manajemen koneksi internet menggunakan metode load balancing dan failover pada router MikroTik guna meningkatkan efisiensi dan keandalan jaringan. Metode Per-Connection Classifier (PCC) digunakan untuk mendistribusikan beban koneksi secara optimal di antara dua gateway ISP, sedangkan teknik failover diterapkan untuk memastikan koneksi tetap berjalan ketika salah satu ISP mengalami gangguan. Selain itu, sistem monitoring berbasis NetWatch dan Telegram bot diimplementasikan untuk memberikan notifikasi otomatis terhadap perubahan status jaringan. Hasil penelitian menunjukkan bahwa penerapan metode PCC dan failover berhasil meningkatkan stabilitas koneksi, mengurangi downtime, serta mendukung kelancaran operasional bisnis PT. Trans Coffee

Kata Kunci *load balancing; failover; PCC; MikroTik; jaringan internet; monitoring;*

AFILIASI

Prodi, Fakultas [1,2)] Program Studi Sistem Informasi, Fakultas Ilmu Komputer.
[3)] Program Studi Teknik Informatika, Fakultas Ilmu Komputer.

Nama Institusi [1,2,3)] Institut Bisnis dan Informatika Kosgoro 1957.

Alamat Institusi [1,2,3)] Jl. Moh Kahfi II, Srengseng Sawah, Jagakarsa, Jakarta Selatan, DKI Jakarta.

KORESPONDENSI

Penulis Muhammad Nabawi

Email Nabawiawi257@gmail.com

DOI : https://doi.org/10.55122/junif.v4i2.1810

I. PENDAHULUAN

Di era digitalisasi saat ini, konektivitas Internet telah menjadi salah satu aspek penting yang mendukung berbagai operasi bisnis, komunikasi, dan pertukaran informasi di banyak organisasi, termasuk kantor pusat perusahaan. Internet sudah menjadi kebutuhan primer bagi semua kalangan, tidak terkecuali bagi bisnis dan perusahaan. Internet telah menjadi kebutuhan utama bagi berbagai kalangan, termasuk sektor bisnis dan perusahaan. Sebagai jaringan komunikasi global, internet menghubungkan komputer serta jaringan komputer di seluruh dunia. Internet menggunakan protokol TCP/IP untuk mengintegrasikan serta mengomunikasikan jaringan [1].PT. Trans Coffe sebagai salah satu perusahan F&B penyedia kopi yang memiliki kebutuhan yang tinggi akan koneksi internet. Hal ini dikarenakan Trans Coffee sudah menerapkan ERP (*Enterprise Resource Planning*) sehingga membutuhkan konektivitas untuk proses internal, dan juga untuk interaksi dengan pelanggan, pemasok, dan kantor cabang yang terseb ar di berbagai lokasi. Dalam upaya meningkatkan kinerja akses internet, perusahaan mengimplementasikan penggunaan lebih dari satu ISP (Internet Service Provider). Strategi ini bertujuan untuk memastikan stabilitas kualitas koneksi internet, meminimalkan risiko terputusnya layanan, serta menyediakan koneksi cadangan yang dapat diandalkan apabila terjadi gangguan jaringan. Dengan demikian, aktivitas operasional perusahaan dapat terus berjalan tanpa hambatan.

Salah satu teknologi yang dapat memecahkan masalah penggabungan dua atau lebih link internet adalah teknik *load balancing* dan *failover* yang meningkatkan *throughput* dan meminimalkan potensi *downtime*. *Load balancing* adalah teknik yang mendistribusikan trafik antara dua atau jalur koneksi sehingga trafik berjalan optimal, meminimalkan waktu respon, dan menghindari terjadinya *overload* pada salah satu jalur koneksi [2]. *Load balancing* memungkikan distribusi trafik di beberapa link internet dan memastikan penggunaan optimal setiap *link* internet yang tersedia. Sedangkan *failover* merupakan teknik dari sebuah sistem untuk dapat berpindah secara manual maupun otomatis jika salah satu sistem mengalami kegagalan sehingga menjadi backup bagi sistem yang gagal tersebut. Jika *gateway* utama terputus, maka *gateway* cadangan akan menggantikan *gateway* utama [3].

Menerapkan metode *load balancing* dan *failover* sangat penting dalam penelitian di kantor pusat TransCoffe. metode *load balancing* yang paling umum dan efisien adalah metode PCC (*Per Connection Classifier*) dari *router* MikroTik. *Per Connection Classifier* (PCC) adalah metode yang menentukan *packet* ke *gateway* untuk koneksi tertentu. PCC mengklasifikasikan lalu lintas koneksi ke dalam dan ke luar *router* ke dalam beberapa kelompok. Pengelompokan ini dapat dibedakan berdasarkan *source address, destination address, source port*, dan *destination port*. Mikrotik mencatat jalur *gateway* yang diambil pada awal lalu lintas koneksi. Artinya, *packet* data berikutnya yang masih terkoneksi akan dirutekan melalui jalur *gateway* yang sama dengan *packet* data yang dikirim sebelumnya, sehingga menghasilkan distribusi trafik yang seimbang dan efisien [4]. Selain itu, untuk mengoptimalkan konfigurasi *load balancing* dan *failover*, penulis juga mengimplementasikan sistem monitoring berupa pesan informasi status jaringan menggunakan *tools* Netwatch yang akan mengirimkan status jaringan ke *bot* Telegram jika salah satu ISP down, sehingga jika terjadi kegagalan koneksi internet pada salah satu ISP tim IT dapat mengetahui lebih cepat untuk melakukan *troubleshooting*.

II. METODE PENELITIAN

2.1. Wawancara

Penulis melakukan wawancara kepada staff bagian IT yang bertanggung jawab dibagian tersebut untuk mendapat informasi dan data yang benar dan akurat.

2.2. Observasi

Penulis melakukan pengamatan secara langsung dan cermat yang bertujuan untuk mendapatkan data yang berkaitan dengan penggunaan jaringan internet secara langsung di kantor pusat PT Trans Coffee.

2.3. Studi Pustaka

Studi pustaka dapat melengkapi informasi yang dibutuhkan dalam melakukan penelitian. Informasi yang berkaitan dengan topik atau masalah yang dapat mendukung penyelesaian masalah yang dibahas seperti metode *Load Balancing*, *Failover*, Mikrotik, algoritma *Per Connection Classifier* (PCC), dan teori pendukung lainnya. Dengan mencari data melalui buku-buku, jurnal, penelitian terdahulu, situs-situs internet, dan berbagai sumber lainnya.

2.4. Analisa dan Perancangan

Analisa diperlukan untuk dapat mengidentifikasi kebutuhan kantor pusat Trans Coffe terkait manajemen dan ketersediaan koneksi internet. Selanjutnya dibuat rancangan konsep solusi berdasarkan analisis kebutuhan dan tinjauan literatur dengan membuat *blue print* atau skema topologi yang mencakup konfigurasi MikroTik dalam infrastruktur jaringan yang ada.

2.5. Implementasi

Tahap implementasi akan menerapkan desain solusi pada lingkungan jaringan internet kantor pusat Trans Coffe. Serta melakukan Konfigurasi perangkat *router* MikroTik sesuai dengan desain atau topologi yang telah dirancang.

2.6. Pengujian

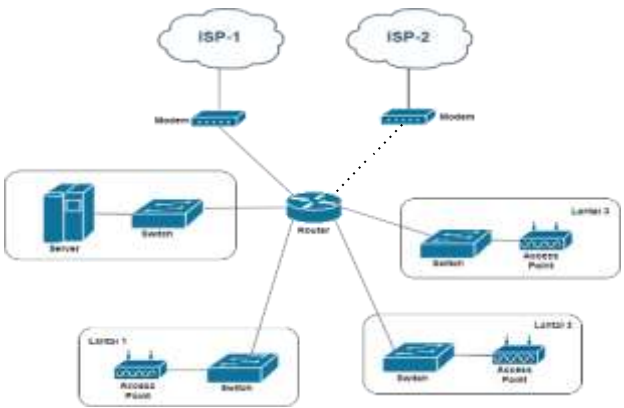
Pengujian yang akan dilakukan terhadap konfigurasi yang telah dilakukan, termasuk pengujian load balancing dan simulasi failover dengan tujuan untuk mengetahui apakah konfigurasi dan sistem monitoring berjalan dengan baik.

III. HASIL DAN PEMBAHASAN

3.1. Analisa Permasalahan

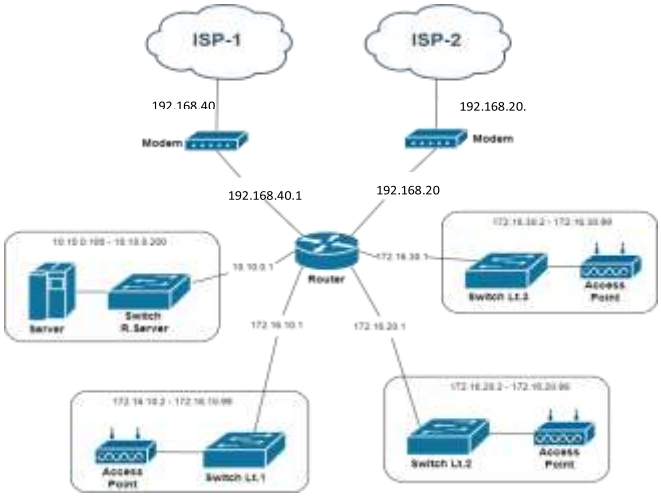
Terdapat beberapa masalah yang ada infrastruktur jaringan PT. Trans Coffee sudah bisa dibilang baik, yaitu Kurang maksimalnya penggunaan 2 ISP dengan hanya menggunakan 1 ISP sebagai jalur koneksi aktif. Hal itu dapat memperlambat kecepatan koneksi internet dan membuat internet mengalami gangguan / *down* yang dapat menyebabkan gangguan pada produktivitas karyawan dalam bekerja yang disebabkan karena banyak nya user yang melakukan request ke internet hanya pada satu jalur koneksi. Masalah lain ketika jaringan internet down hal itu mengakibatkan *Downtime* yang cukup lama disebabkan perubahan setinggan antara ISP yang aktif dan ISP cadangan dilakukan secara manual oleh Tim IT. Langkah yang dilakukan bisa lebih memburuk jika divisi Infrastruktur IT sedang tidak berada di kantor yang tentu nya akan mengakibatkan *downtime* internet akan menjadi lebih lama. Dalam mendukung konfigurasi *Load Balancing* dan *Failover* maka akan di implementasikan sistem monitoring dengan menggunakan *tools* Netwatch pada *router* Mikrotik.

3.2. Rancangan Topologi



Gambar 1. Topologi Jaringan Sebelum Implementasi Load Balancing dan Failover

Pada topologi yang ditunjukkan, jalur ISP beroperasi dalam mode aktif dan standby , yang berarti hanya ISP-1 yang aktif secara penuh menerima trafik internet dari client, sementara ISP-2 hanya berfungsi sebagai cadangan. Proses pengalihan koneksi dari ISP yang mengalami gangguan ke ISP lain yang berfungsi masih dilakukan secara manual, sehingga kurang efisien. Oleh karena itu, dirancang sebuah arsitektur jaringan yang mengintegrasikan implementasi load balancing dan failover untuk meningkatkan efisiensi dan keandalan sistem.



Gambar 2. Topologi Jaringan Setelah Implementasi Load Balancing dan Failover

Topologi jaringan pada gambar 2 menunjukkan konfigurasi setelah implementasi load balancing, di mana kedua ISP telah beroperasi secara aktif. Dengan demikian, lalu lintas internet secara otomatis didistribusikan secara merata di antara kedua ISP. Selain itu, rancangan teknik failover dapat secara otomatis melindungi jalur yang mengalami gangguan tanpa jeda dan mendukung lalu lintas yang sedang berlangsung dengan mengalihkan ke jalur ISP yang aktif.

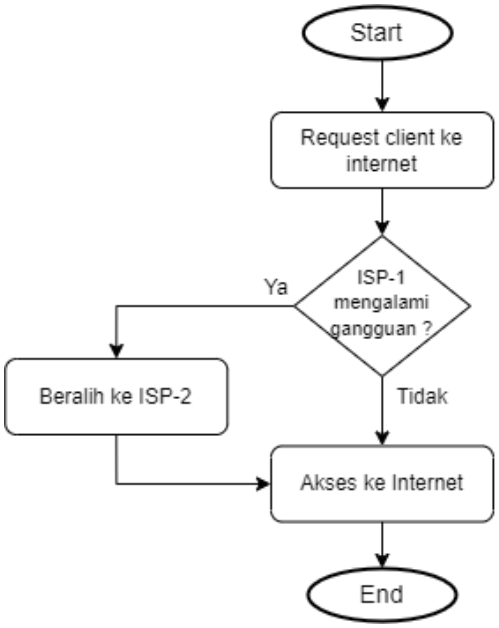
3.3. Rancangan Load Balancing

Rancangan *Load Balancing* menggunakan algoritma PCC akan menggunakan 2 ISP secara aktif, teknik ini bermanfaat untuk membagi *bandwidth* antara jalur internet ISP utama dan jalur Internet ISP cadangan. Oleh karena itu, digunakan jalur internet yang berbeda dari 2 ISP dalam hal *routing*[4]. Selain itu, *load balancing* nantinya dapat meminimalkan *respons time* dan menghindari kelebihan beban (*overload*) pada salah satu jalur koneksi[5].

Gambar 3. Flowchart Load Balancing

3.4. Rancangan Failover

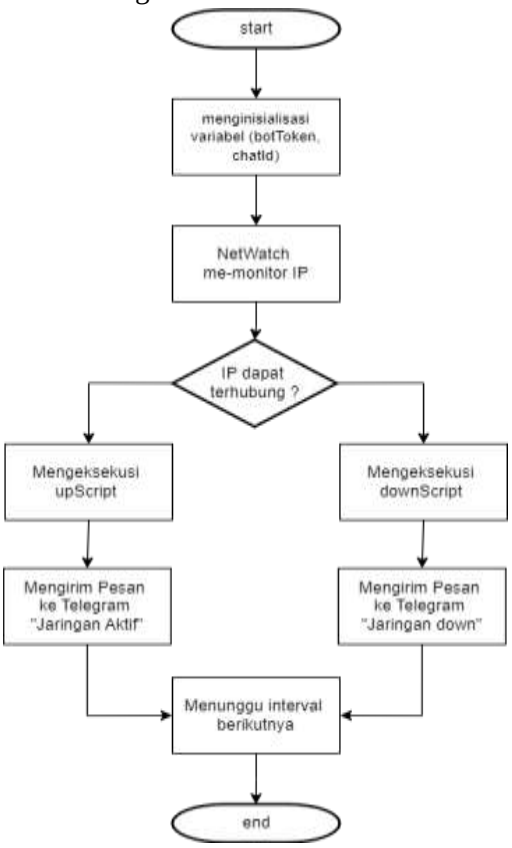
Rancangan *Failover* dapat diterapkan karena jaringan internet kantor pusat Trans Coffee sudah memiliki 2 koneksi internet dari 2 ISP yang berbeda. Failover nantinya akan mengantisipasi putusnya koneksi internet, dengan memindahkan jalur koneksi yang bermasalah baik secara otomatis ke jalur koneksi cadangan [5].



Gambar 4. Flowchart Failover

3.5. Rancangan Monitoring

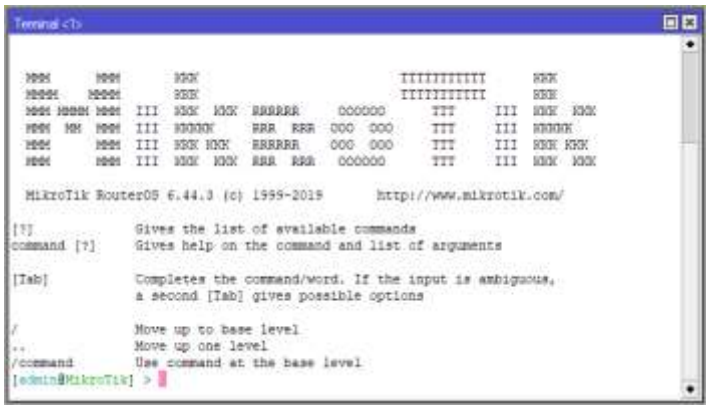
Rancangan Monitoring akan berfungsi memberikan informasi kendala dalam jaringan internet, sehingga memudahkan tim IT dalam menganalisis dan menemukan solusi atas masalah yang terjadi [6].



Gambar 5. Flowchart Monitoring

3.6. Konfigurasi Load Balancing dan Failover

Router MikroTik RouterBoard 1100AHx4 digunakan sebagai perangkat utama yang berfungsi sebagai gateway dalam seluruh konfigurasi yang menjadi fokus penelitian ini. Konfigurasi akan dilakukan melalui software Winbox versi 3.3.8 yang perlu diinstall terlebih dahulu, Winbox merupakan utilitas untuk menghubungkan dan mengkonfigurasi Mikrotik menggunakan MAC address atau protokol IP [7]. Konfigurasi yang dilakukan pada penelitian ini akan menggunakan Command Line Interface (CLI).



Gambar 6. Tampilan New Terminal Winbox

3.6.1. Inisialisasi Interface

Inisialisasi *interface* akan memberkian nama dan fungsi dari setiap *port ethernet* pada *router* Mikrotik yang menghubung jaringan Internet dari ISP, beberapa jaringan LAN, dan juga server. Inisialisasi interface menjadi penting karena dapat dengan mudah mengidentifikasi dan mengelola koneksi yang berbeda pada *router*.

```
[admin@MikroTik] > interface ethernet
[admin@MikroTik] /interface ethernet> set ether1 name=ISP1 comment="Fiberstar"
[admin@MikroTik] /interface ethernet> set ether2 name=ISP2 comment="Maxindo"
[admin@MikroTik] /interface ethernet> set ether6 name=LAN-Lt.1 comment="LAN Lantai 1"
[admin@MikroTik] /interface ethernet> set ether7 name=LAN-Lt.2 comment="LAN Lantai 2"
[admin@MikroTik] /interface ethernet> set ether8 name=LAN-Lt.3 comment="LAN Lantai 3"
[admin@MikroTik] /interface ethernet> set ether9 name=LAN-Server comment="LAN Ruangan Server"
```

Gambar 7. Command Inisialisasi Interface

3.6.2. Konfigurasi IP Address

Tahap konfigurasi IP address akan menjelaskan beberapa konfigurasi, yaitu melakukan konfigurasi IP address untuk setiap ISP menggunakan tools DHCP Client untuk mendapat IP secara dinamis dari ISP-1 dan ISP2. Setelah itu mengkonfigurasi IP Address untuk setiap interface jaringan LAN yang akan menjadi gateway. Lalu akan ditambahkan konfigurasi DNS dengan menambahkan DNS google, langkah terakhir adalah melakukan konfigurasi DHCP Server untuk masing-masing jaringan LAN. Konfigurasi ini bertujuan untuk memberikan alamat IP secara otomatis kepada setiap perangkat yang terhubung ke jaringan LAN, sehingga mempermudah pengelolaan jaringan.

```
[admin@MikroTik] > ip dhcp-client
[admin@MikroTik] /ip dhcp-client> add interface=ISP1 disabled=no
[admin@MikroTik] /ip dhcp-client> add interface=ISP2 disabled=no
```

Gambar 8. Command Konfigurasi IP DHCP Client untuk ISP

```
[admin@MikroTik] > ip address
[admin@MikroTik] /ip address> add address=172.16.10.1/24 interface=LAN-Lt.1
[admin@MikroTik] /ip address> add address=172.16.20.1/24 interface=LAN-Lt.2
[admin@MikroTik] /ip address> add address=172.16.30.1/24 interface=LAN-Lt.3
[admin@MikroTik] /ip address> add address=10.10.0.1/24 interface=LAN-Server
```

Gambar 9. Command Konfigurasi IP untuk Interface Jaringan LAN

```
[admin@MikroTik] > ip dns
[admin@MikroTik] / ip dns> set servers=8.8.8.8,8.8.4.4
```

Gambar 10. Command Konfigurasi DNS

```
[admin@MikroTik] > ip dhcp-server-setup
```

Gambar 11. Command Konfigurasi DHCP Server untuk Jaringan LAN

Setelah menjalankan perintah di atas, maka akan ada beberapa pertanyaan yang berhubungan dengan konfigurasi DCHP Server.

```
Select interface to run DHCP server on
dhcp server interface: LAN-Lt.1

Select network for DHCP addresses
dhcp address space: 172.16.10.0/24

Select gateway for given network
gateway for dhcp network: 172.16.10.1

Select pool of ip addresses given out by DHCP server
addresses to give out: 172.16.10.2-172.16.10.254

Select DNS servers
dns servers: 192.168.20.1,192.168.40.1

Select lease time
lease time: 10m
```

Gambar 12. Konfigurasi DHCP Server

3.6.3.Konfigurasi Firewall dan PCC

Tahap konfigurasi *firewall* dan PCC akan menjelaskan bagaimana konfigurasi dalam implementasi *Load Balancing* PCC pada *router* Mikrotik, yang akan meliputi konfigurasi *Firewall* NAT *masquerade* digunakan untuk melakukan translasi alamat jaringan (*Network Address Translation*) dari LAN ke masing-masing ISP, konfigurasi Mangle merupakan fitur *firewall* yang digunakan untuk menandai *packet-packet* jaringan dari ISP1 dan ISP2, konfigurasi *mangle* dengan metode PCC (*Per Connection Classifier*), penandaan *packet* didasarkan pada *source IP*, *destination IP*, dan *port*. Dengan parameter tersebut maka *connection mark* dan *routing mark* dapat dibuat.

```
[admin@MikroTik] > ip firewall nat
[admin@MikroTik] /ip firewall nat> add chain=srcnat out-interface=ISP1 action=masquerade
[admin@MikroTik] /ip firewall nat> add chain=srcnat out-interface=ISP2 action=masquerade
```

Gambar 13. Command Konfigurasi Firewall NAT Masquerade

```
[admin@MikroTik] > ip firewall mangle
[admin@MikroTik] /ip firewall mangle> add chain=prerouting dst-address=192.168.20.0/24 action=accept
[admin@MikroTik] /ip firewall mangle> add chain=prerouting dst-address=192.168.40.0/24 action=accept
[admin@MikroTik] /ip firewall mangle> add chain=prerouting dst-address=172.16.10.0/24 action=accept
[admin@MikroTik] /ip firewall mangle> add chain=prerouting dst-address=172.16.20.0/24 action=accept
[admin@MikroTik] /ip firewall mangle> add chain=prerouting dst-address=172.16.30.0/24 action=accept
[admin@MikroTik] /ip firewall mangle> add chain=prerouting dst-address=10.10.0.0/24 action=accept
```

Gambar 14. Command Konfigurasi Mangle Bypass

```
[admin@MikroTik] > ip firewall mangle
[admin@MikroTik] /ip firewall mangle> add chain=prerouting in-interface=ISP1
action=mark-connection new-connection-mark=ISP-1
[admin@MikroTik] /ip firewall mangle> add chain=prerouting in-interface=ISP2
action=mark-connection new-connection-mark=ISP-2
```

Gambar 15. Command Konfigurasi Mangle untuk Koneksi dari Internet

```
[admin@MikroTik] > ip firewall mangle
[admin@MikroTik] /ip firewall mangle> add chain=prerouting in-interface=LAN-Lt.1
per-connection-classifier=both-addresses-and-port:2/0 action=mark-connection new-connection-mark=ISP-1
[admin@MikroTik] /ip firewall mangle> add chain=prerouting in-interface=LAN-Lt.1
per-connection-classifier=both-addresses-and-port:2/1 action=mark-connection new-connection-mark=ISP-2
[admin@MikroTik] /ip firewall mangle> add chain=prerouting in-interface=LAN-Lt.2
per-connection-classifier=both-addresses-and-port:2/0 action=mark-connection new-connection-mark=ISP-1
[admin@MikroTik] /ip firewall mangle> add chain=prerouting in-interface=LAN-Lt.2
per-connection-classifier=both-addresses-and-port:2/1 action=mark-connection new-connection-mark=ISP-2
[admin@MikroTik] /ip firewall mangle> add chain=prerouting in-interface=LAN-Lt.3
per-connection-classifier=both-addresses-and-port:2/0 action=mark-connection new-connection-mark=ISP-1
[admin@MikroTik] /ip firewall mangle> add chain=prerouting in-interface=LAN-Lt.3
per-connection-classifier=both-addresses-and-port:2/1 action=mark-connection new-connection-mark=ISP-2
[admin@MikroTik] /ip firewall mangle> add chain=prerouting in-interface=LAN-Server
per-connection-classifier=both-addresses-and-port:2/0 action=mark-connection new-connection-mark=ISP-1
[admin@MikroTik] /ip firewall mangle> add chain=prerouting in-interface=LAN-Server
per-connection-classifier=both-addresses-and-port:2/1 action=mark-connection new-connection-mark=ISP-2
```

Gambar 16. Command Konfigurasi Mangle Mark Connection PCC

```
[admin@MikroTik] > ip firewall mangle
[admin@MikroTik] /ip firewall mangle> add chain=prerouting in-interface=LAN-Lt.1
connection-mark=ISP-1 action=mark-routing new-routing-mark=to-ISP1
[admin@MikroTik] /ip firewall mangle> add chain=prerouting in-interface=LAN-Lt.1
connection-mark=ISP-2 action=mark-routing new-routing-mark=to-ISP2
[admin@MikroTik] /ip firewall mangle> add chain=prerouting in-interface=LAN-Lt.2
connection-mark=ISP-1 action=mark-routing new-routing-mark=to-ISP1
[admin@MikroTik] /ip firewall mangle> add chain=prerouting in-interface=LAN-Lt.2
connection-mark=ISP-2 action=mark-routing new-routing-mark=to-ISP2
[admin@MikroTik] /ip firewall mangle> add chain=prerouting in-interface=LAN-Lt.3
connection-mark=ISP-1 action=mark-routing new-routing-mark=to-ISP1
[admin@MikroTik] /ip firewall mangle> add chain=prerouting in-interface=LAN-Lt.3
connection-mark=ISP-2 action=mark-routing new-routing-mark=to-ISP2
[admin@MikroTik] /ip firewall mangle> add chain=prerouting in-interface=LAN-Server
connection-mark=ISP-1 action=mark-routing new-routing-mark=to-ISP1
[admin@MikroTik] /ip firewall mangle> add chain=prerouting in-interface=LAN-Server
connection-mark=ISP-2 action=mark-routing new-routing-mark=to-ISP2
```

Gambar 17. Command Konfigurasi Mangle Mark Routing Chain Prerouting

```
[admin@MikroTik] > ip firewall mangle
[admin@MikroTik] /ip firewall mangle> add chain=output connection-mark=ISP-1
action=mark-routing new-routing-mark=to-ISP1
[admin@MikroTik] /ip firewall mangle> add chain=output connection-mark=ISP-2
action=mark-routing new-routing-mark=to-ISP2
```

Gambar 18. Command Konfigurasi Mangle Mark Routing Chain Output

3.6.4.Konfigurasi Failover

Konfigurasi failover bertujuan untuk memastikan kelangsungan jaringan internet dengan cara mengalihkan jalur koneksi ke ISP cadangan jika ISP utama mengalami kegagalan jaringan atau gangguan. Konfigurasi yang akan diterapkan meliputi konfigurasi *Static Route* yang akan menetapkan *next hop* yang mengarah ke ISP 1 dan ISP 2 pada masing-masing jalur Internet dan konfigurasi *Routing* untuk *Failover* yang memastikan bahwa jika jalur internet (ISP1) mengalami gangguan, *router* akan secara otomatis mengalihkan lalu lintas ke jalur internet (ISP2). Konfigurasi *failover* dengan menetapkan *metric* atau *distance* yang berbeda dari *routing default*. Dengan cara ini, *router* secara otomatis beralih ke jalur dengan distance yang lebih tinggi jika jalur utama tidak tersedia.

```
[admin@MikroTik] > ip route
[admin@MikroTik] /ip route> add dst-address=0.0.0.0/0 gateway=192.168.40.1
check-gateway=ping routing-mark=to-ISP1
[admin@MikroTik] /ip route> add dst-address=0.0.0.0/0 gateway=192.168.20.1
check-gateway=ping routing-mark=to-ISP2
```

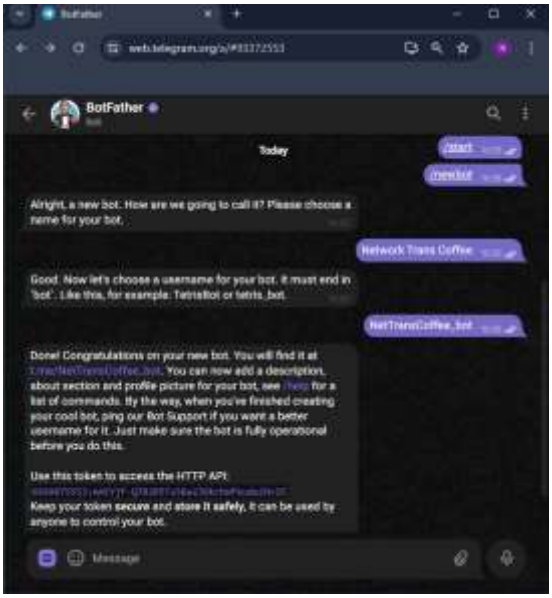
Gambar 19. Command Konfigurasi Static Route

```
[admin@MikroTik] > ip route
[admin@MikroTik] /ip route> add dst-address=0.0.0.0/0 gateway=192.168.40.1 distance=1
[admin@MikroTik] /ip route> add dst-address=0.0.0.0/0 gateway=192.168.20.1 distance=2
```

Gambar 20. Command Konfigurasi Route untuk Failover

3.6.5.Konfigurasi Sistem Monitoring

Konfigurasi sistem monitoring jaringan yang mendukung konfigurasi *load balancing Per Connection Classifier* (PCC) dan *failover* pada *router* Mikrotik. Sistem monitoring ini akan memberikan notifikasi kepada tim IT melalui *bot* Telegram setiap kali terjadi perubahan status jaringan. Konfigurasi ini akan melakukan beberapa tahap diantaranya pemuatan *bot* Telegram dengan mendaftar pada akun *@BotFather* untuk mendapatkan *token* yang dapat digunakan dalam mengakses API telegram yang nantinya digunakan Netwatch untuk mengirimkan informasi status jaringan. Pembuatan *script* untuk status jaringan aktif dan *down*, *Script* digunakan pada *tools* Netwatch mengirimkan pesan notifikasi ke *bot* Telegram yang telah dibuat dengan memanfaatkan API *token* dan chat ID dari *bot*. Dan terakhir Konfigurasi Netwatch pada *router* Mikrotik, untuk memantau status *interface* koneksi internet di jaringan. Netwatch dapat mengirimkan notifikasi ketika terjadi perubahan status *host*, seperti dari Aktif ke Down atau sebaliknya.



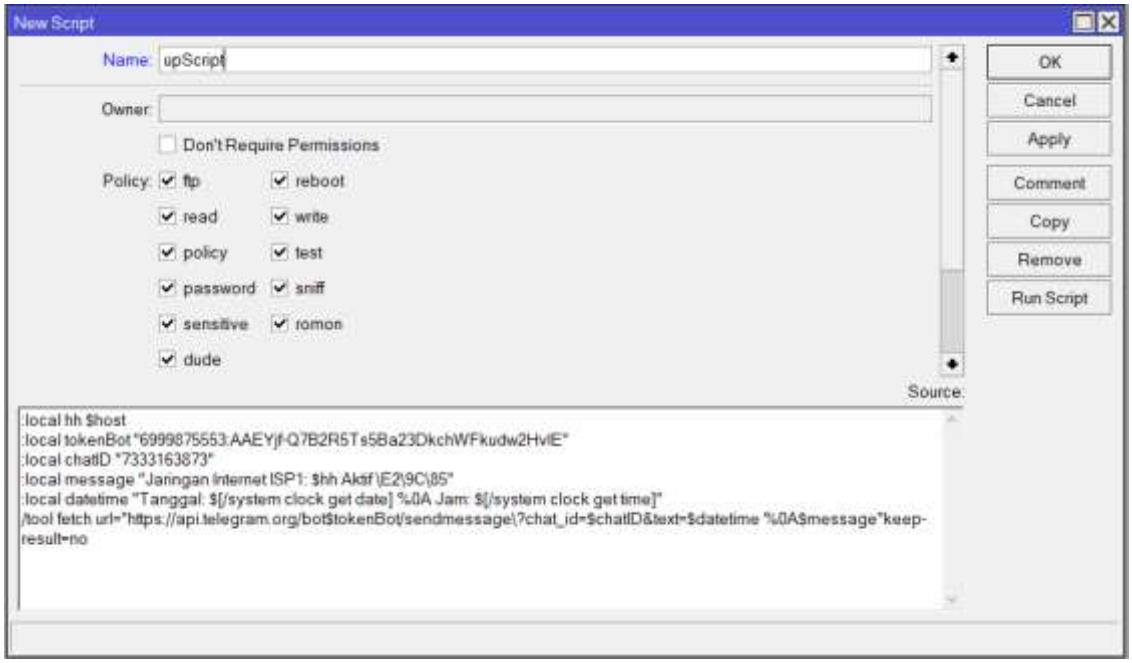
Gambar 21. Pembuatan bot Father

```
:local hh $host
:local tokenBot "6999875553:AAEYjf-Q7B2R5Ts5Ba23DkchWFkudw2HvlE"
:local chatID "7333163825"
:local message "Jaringan Internet ISP1: $hh Aktif \E2\9C\85"
:local datetime "Tanggal: $[/system clock get date] %0A Jam: $[/system clock get time]"
/tool fetch url="https://api.telegram.org/bot$tokenBot/sendmessage\?chat_id=$chatID&text=$datetime %0A$message"keep-result=no
```

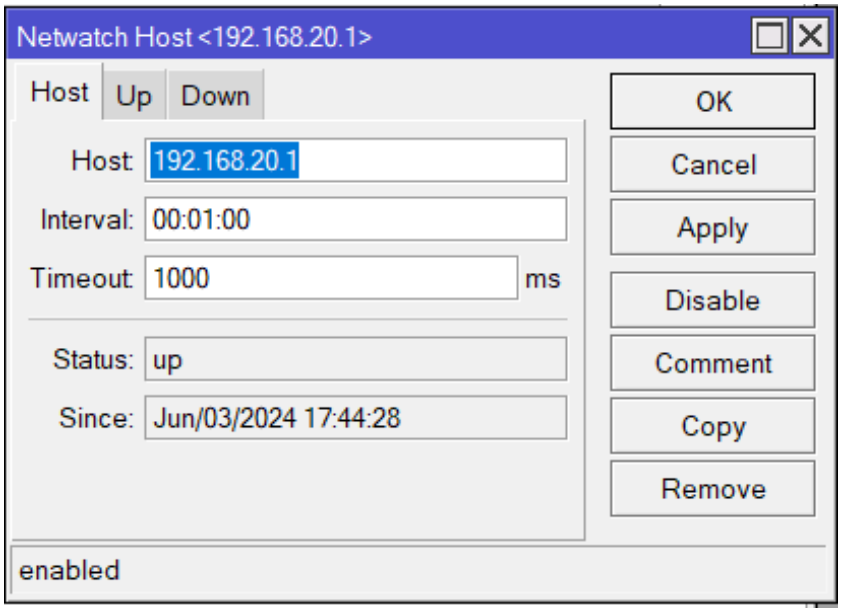
Gambar 22. Script Pesan untuk Jaringan Aktif

```
:local hh $host
:local tokenBot "6999875553:AAEYjf-Q7B2R5Ts5Ba23DkchWFkudw2HvlE"
:local chatID "7333163825"
:local message "Jaringan Internet ISP2: $hh Down \E2\9D\8C"
:local datetime "Tanggal: $[/system clock get date] %0A Jam: $[/system clock get time]"
/tool fetch url="https://api.telegram.org/bot$tokenBot/sendmessage\?chat_id=$chatID&text=$datetime %0A$message"keep-result=no
```

Gambar 23. Script Pesan untuk Jaringan Down



Gambar 24. Pembuatan Script pada Router Mikrotik



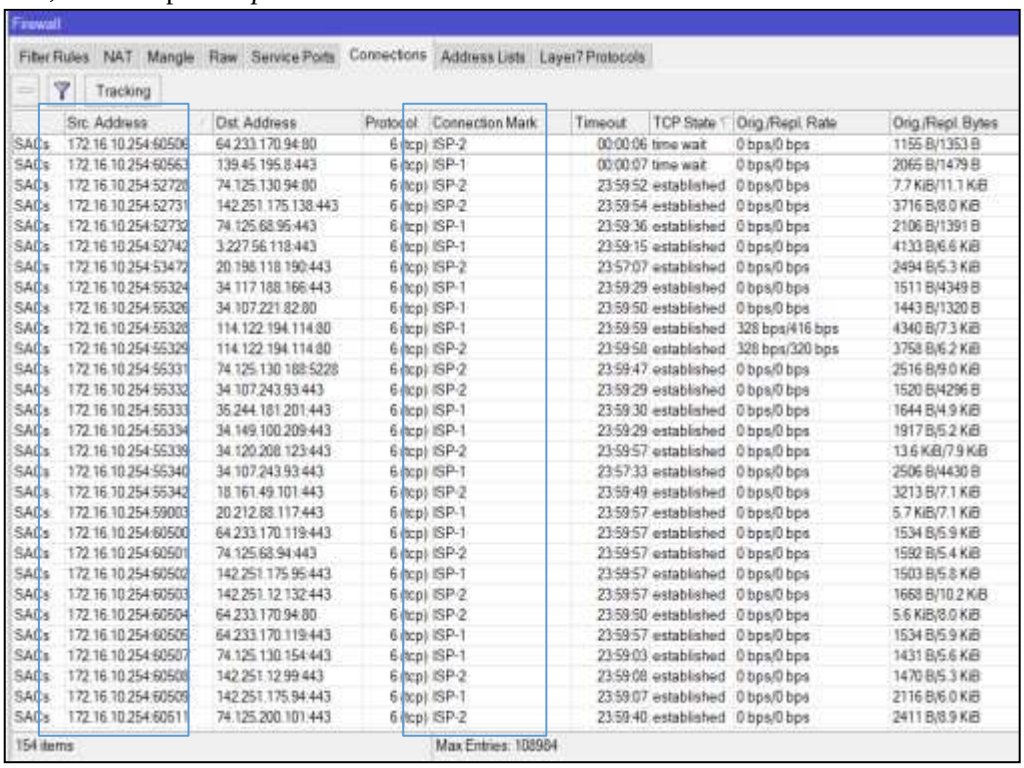
Gambar 25. Konfigurasi Netwatch

3.7. Pengujian Konfigurasi

Pengujian konfigurasi *Load Balancing* PCC dan *Failover* dilakukan untuk memastikan bahwa konfigurasi bekerja dengan optimal dan sesuai dengan tujuan yang diinginkan. Dalam pengujian ini akan dibagi menjadi beberapa bagian pengujian *load balancing*, pengujian *failover*, dan perbandingan pengujian koneksi jaringan.

3.7.1.Pengujian Load Balancing

Pengujian *Load Balancing* dilakukan untuk memastikan bahwa beban jaringan dapat dibagi antara dua jalur koneksi yang tersedia. Pengujian ini akan menggunakan 1 user yang mengakses situs yang sama dari 2 *browser* yang berbeda. Dan akan dilakukan pengujian untuk performa *Load Balancing* menggunakan *tools* berbasi web *speedtest.cbn.id* untuk mengukur *ping*, kecepatan *download*, dan kecepatan *upload*.



Gambar 26. Pengujian Load Balancing

Terlihat pada Gambar 26 jalur koneksi yang dilewatkan oleh IP 172.16.10.254 berhasil didistribusikan bergantian melalui koneksi ISP1 dan ISP2. Hal ini menunjukkan bahwa *load balancing* dapat membagi beban lalu lintas jaringan.

Tabel 1. Pengujian Perfoma Internet sebelum Load Balancing

No	Ping (ms)	Unduh (Mbps)	Unggah (Mbps)
1	20	33,2	30,4
2	15	44,5	35,4
3	17	25,1	35,1
4	15	43,3	33,9
5	16	44,3	35,3
Rata-rata	16,6	38,08	34,02

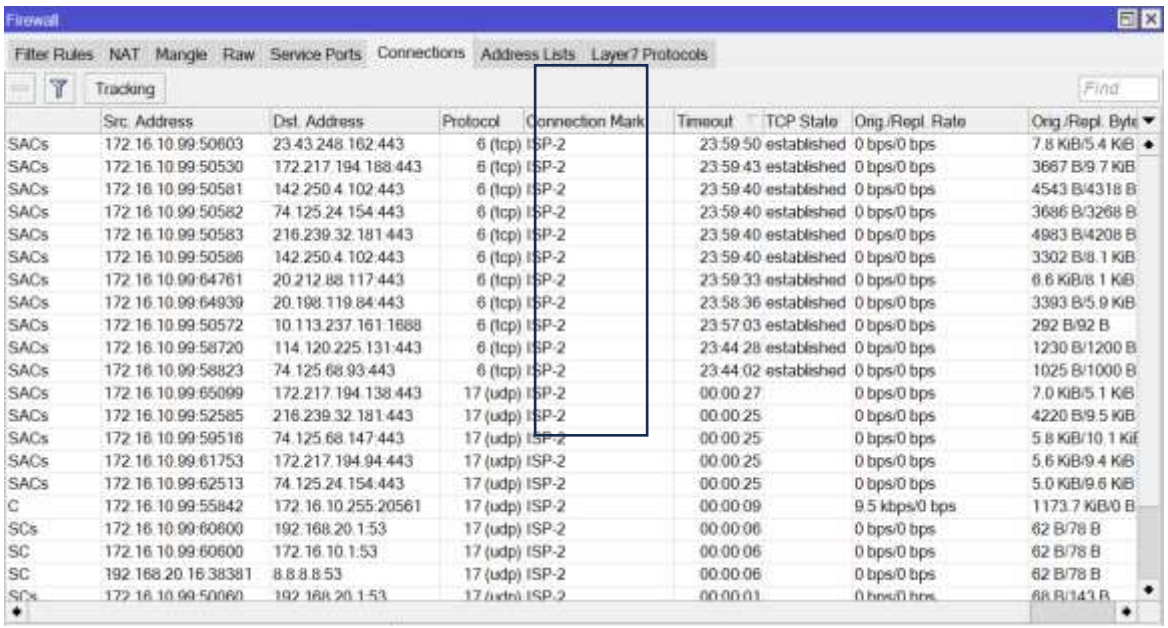
Tabel 2. Pengujian Performa Internet sesudah Load Balancing

No	Ping (ms)	Unduh (Mbps)	Unggah (Mbps)
1	20	33,2	30,4
2	15	44,5	35,4
3	17	25,1	35,1
4	15	43,3	33,9
5	16	44,3	35,3
Rata-rata	16,6	38,08	34,02

Setelah menambahkan konfigurasi *load balancing* terdapat peningkatan pada *ping* sebesar 0,8 Ms yang Menunjukkan *load balancing* membantu mengurangi *latensi* jaringan internet. *Download* sebesar 43,14 Mbps hal ini menandai *load balancing* secara efektif mengalokasikan *bandwith* yang meningkatkan proses unduh. *Upload* sebesar 34,8 Mbps. Peningkatan juga terdapat pada proses *download*.

3.7.2.Pengujian Failover

Pengujian *failover* akan dilakukan untuk memastikan bahwa sistem dapat secara otomatis beralih ke jalur koneksi cadangan jika koneksi *down*. Pengujian ini juga akan mengevaluasi sistem monitoring yang telah diimplementasikan. Pengujian dilakukan dengan me-nonaktifkan *interface* dari setiap ISP secara bergantian.



Gambar 27. Pengujian dengan Me-nonaktifkan ISP1

Terlihat kolom Connection Mark pada Gambar 27. Ketika koneksi ISP1 down maka secara otomatis akan mengalihkan lalu lintas koneksi ke ISP2. Pengujian ini juga akan membuat Netwatch mengirimkan pesan notifikasi ke Telegram bahwa ISP1 down.

Gambar 28. Pesan Informasi bahwa ISP 1 Down

Notifikasi yang diterima menginformasikan bahwa ISP1 down, hal ini akan membantu tim IT untuk segera melakukan troubleshooting. Dan Ketika jalur koneksi dari ISP1 sudah aktif Kembali Netwatch akan mengirimkan notifikasi yang menginformasikan bahwa koneksi jaringan ISP1 sudah aktif.

IV. SIMPULAN

Kesimpulan yang terdapat dari hasil Implementasi *Load Balancing* dan *Failover* adalah sebagai berikut:

1. Implementasi *load balancing* dapat membagi beban trafik pada jalur koneksi pada dua ISP di Kantor Pusat Trans Coffee, sehingga dapat mengoptimalkan penggunaan dua ISP dan tidak membebani satu ISP saja. Pengujian *Speedtest* menunjukkan perubahan nilai yang cukup baik pada *ping, download,* dan *upload* setelah di implementasikan *load balancing.*
2. Implementasi *failover* dapat membuat kinerja jaringan internet tetap berjalan Ketika satu ISP mengalami gangguan atau *down,* dengan otomatis mengalihkan koneksi ke *gateway* ISP yang aktif. Serta implementasi sistem monitoring dengan *tools* Netwatch dapat memberikan informasi status dari dua *interface* ISP, yang berguna jika terjadi masalah sehingga dapat segera dilakukan *troubleshooting*.

REFERENSI

[1] G. Barovih, U. I. Jakarta, M. Mutasar, U. Islam, and K. Indonesia, *Teknologi jaringan komputer*, no. July. 2024.

[2] M. Muzayyin and A. S. Fitrani, “Configuring Load Balancing and Failover Using a Mikrotik Router on RT RW NET (Case Study : Dusun Klatakan Dayurejo) Konfigurasi Load Balancing dan Failover Menggunakan Router Mikrotik Pada RT RW NET (Studi Kasus : Dusun Klatakan Dayurejo),” vol. 2, no. 2, 2022.

[3] J. Generic *et al.*, “Implementasi FTP Server dengan Metode Transfer Layer Security untuk Keamanan Transfer Data Menggunakan,” vol. 9, no. 2, pp. 348–355, 2014.

[4] E. Safrianti, L. O. Sari, and A. Satiarini, “Peer Connection Classifier Method for Load Balancing Technique,” vol. 4, no. 1, pp. 127–133, 2021.

[5] J. Jtik, J. Teknologi, M. Tanujaya, and C. Dewi, “Simulasi Implementasi Load Balancing pada Jaringan Internet dengan Metode Per Connection Classifier (PCC) dan Server dengan Metode IP Hash Menggunakan GNS3,” vol. 8, no. 1, 2024.

[6] M. Wahyu and A. S. Fitrani, “Application of Telegram Bot for Regional Intranet Network Monitoring System in Government Agencies [Penerapan Bot Telegram untuk Sistem Monitoring Jaringan Daerah di Instansi Pemerintahan],” pp. 1–8.

[7] G. F. Krisna and Y. Kurniawan, “SISTEM INFORMASI MANAJEMEN PENGELOLAAN INTERNET UNIVERSITAS MA CHUNG DENGAN PENGGUNAAN MIKROTIK API SERVICES DENGAN AUTENTIFIKASI O365,” vol. 6, pp. 90–107, 2023.