BAB IV

ANALISA JARINGAN USULAN

4.1. Jaringan Usulan

Berdasarkan hasil analisis terhadap infrastruktur jaringan yang saat ini digunakan di PT. ABB Sakti Industri ditemukan sejumlah permasalahan yang berdampak pada performa dan keandalan sistem jaringan, seperti tidak optimalnya pemanfaatan dua jalur ISP, ketiadaan sistem *failover* otomatis, serta belum diterapkannya metode *load balancing.* Dengan demikian, pada bab ini akan dipaparkan rancangan jaringan yang diusulkan sebagai solusi untuk mengatasi permasalahan yang telah diidentifikasi. Rancangan jaringan usulan dirancang dengan pendekatan yang lebih efisien, stabil, dan aman. Fokus utama dari rancangan ini adalah penerapan metode *load balancing* dan *failover* otomatis menggunakan perangkat Mikrotik*,* sehingga kedua jalur ISP dapat dimanfaatkan secara optimal dan koneksi internet tetap tersedia meskipun salah satu jalur mengalami gangguan. Selain itu, rancangan ini juga mencakup peningkatan aspek keamanan jaringan, penggunaan sistem *monitoring,* serta dokumentasi dan manajemen jaringan yang lebih terstruktur. Dengan implementasi jaringan usulan ini, diharapkan sistem jaringan di PT. ABB Sakti Industri dapat mendukung operasional perusahaan secara lebih andal dan berkelanjutan.

4.1.1. Topologi Jaringan

Topologi jaringan yang diusulkan untuk PT. ABB Sakti Industri tetap mengadopsi pendekatan *hybrid*, yaitu kombinasi antara topologi *star* dan *extended*

star. Optimalisasi dilakukan melalui pemanfaatan dua jalur ISP dengan penerapan konfigurasi *load balancing* serta mekanisme *failover otomatis* pada *router* Mikrotik.

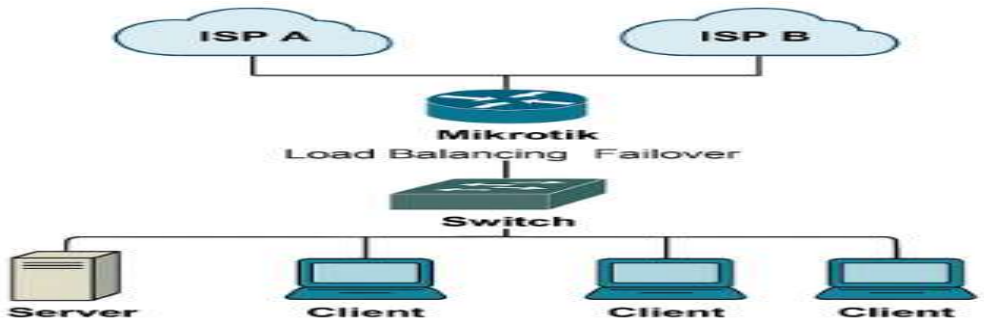
Dalam rancangan topologi ini, kedua jalur ISP (ISP A dan ISP B) terhubung langsung ke *router* Mikrotik. *Router* dikonfigurasi dengan metode PCC (*Per Connection Classifier*) untuk mendistribusikan beban trafik secara proporsional berdasarkan koneksi pengguna. Selain itu, fitur *Netwatch* akan digunakan untuk memantau konektivitas masing-masing ISP dan secara otomatis mengalihkan *trafik* ke jalur cadangan jika salah satu ISP mengalami gangguan.

Dari *router* Mikrotik, koneksi diteruskan ke *switch* utama yang berfungsi mendistribusikan jaringan ke seluruh perangkat klien dan server di lingkungan perusahaan. Dengan pendekatan ini, jaringan akan memiliki dua keunggulan utama, yaitu:

1. *Redundansi* koneksi internet melalui *failover* otomatis.

2. Efisiensi penggunaan *bandwidth* melalui *load balancing.*

Topologi ini juga memungkinkan pengembangan lebih lanjut, seperti segmentasi jaringan menggunakan VLAN, penambahan *access point* untuk koneksi *wireless,* serta integrasi sistem *monitoring* jaringan. Berikut adalah diagram visual dari topologi jaringan usulan untuk PT. ABB Sakti Industri:



Sumber: Hasil Penelitian

Gambar IV.1 Topologi Jaringan Usulan

Penjelasan Gambar:

1. Dua ISP (ISP A dan ISP B) terhubung ke router Mikrotik.
2. *Router* Mikrotik diatur dengan konfigurasi yang mendukung metode *load balancing* serta mekanisme *failover otomatis*.
3. *Router* terhubung ke *switch* utama yang mendistribusikan koneksi ke Server internal (untuk file *sharing* dan ERP) dan beberapa *client* di lingkungan kantor dan produksi.

Berikut adalah informasi konfigurasi IP *address* pada perangkat Mikrotik yang digunakan dalam penelitian adalah sebagai berikut:

Tabel IV.1 informasi konfigurasi IP *address*

Interface	**Koneksi**	**IP Address**	**Keterangan**
ether1	ISP 1	11.11.11.1/30	Jalur internet utama
ether2	ISP 2	12.12.12.1/30	Jalur backup / *load balancing*
ether3	LAN	192.168.10.1/24	*Gateway* jaringan internal

Sumber: Hasil Penelitian

Mikrotik menggunakan mekanisme *recursive routing* untuk melakukan *failover* otomatis. Pemeriksaan koneksi dilakukan dengan melakukan ping ke DNS publik seperti:

1. 8.8.8.8
2. 1.1.1.1

Failover akan aktif apabila:

1. Mikrotik tidak dapat merespons *gateway* ISP 1
2. Atau tidak dapat mengakses target *ping recursive*

Ketika kondisi ini terjadi, semua trafik internet dari LAN secara otomatis dialihkan ke jalur ISP 2 sehingga konektivitas tetap terjaga.

4.1.2. Skema Jaringan

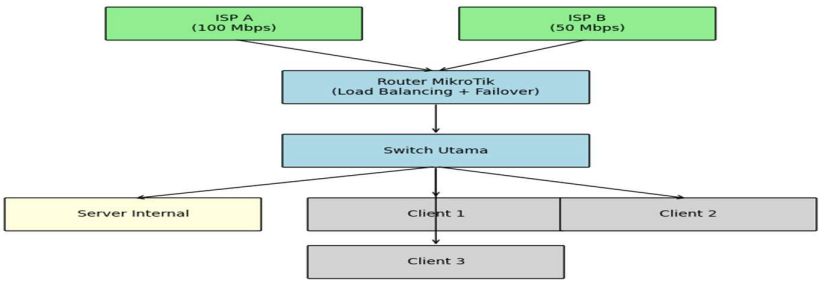
Skema jaringan yang diusulkan merepresentasikan struktur konektivitas antar perangkat serta jalur komunikasi data yang dirancang untuk meningkatkan efisiensi dan keandalan jaringan di PT. ABB Sakti Industri. Dalam skema ini, dua jalur ISP (ISP A dan ISP B) terhubung langsung ke *router* Mikrotik yang telah dikonfigurasi dengan metode *load balancing* dan *failover* otomatis.

Router Mikrotik berperan sebagai pusat pengendali lalu lintas jaringan. Dengan memanfaatkan metode PCC (*Per Connection Classifier*), *router* mengatur distribusi beban trafik secara proporsional ke kedua jalur ISP. Selain itu, fitur *Netwatch* digunakan untuk memantau konektivitas ISP dan secara otomatis mengalihkan *trafik* ke jalur cadangan jika terjadi gangguan pada salah satu ISP.

Koneksi dari *router* diarahkan ke *switch* utama yang berfungsi mendistribusikan jaringan ke seluruh perangkat klien dan server internal. Server digunakan untuk layanan *file sharing,* sistem ERP, dan *backup* data. Sementara itu, *client* mencakup komputer pengguna di berbagai divisi seperti produksi, logistik, dan administrasi.

Skema ini juga memungkinkan pengembangan lebih lanjut seperti segmentasi jaringan menggunakan VLAN, penambahan *access point* untuk koneksi *wireless,* serta integrasi sistem *monitoring* jaringan menggunakan aplikasi seperti *The Dude*.

Berikut adalah diagram visual dari skema jaringan usulan:



Sumber: Hasil Penelitian

Gambar IV.2 Diagram Topologi Jaringan Usulan

Penjelasan Diagram:

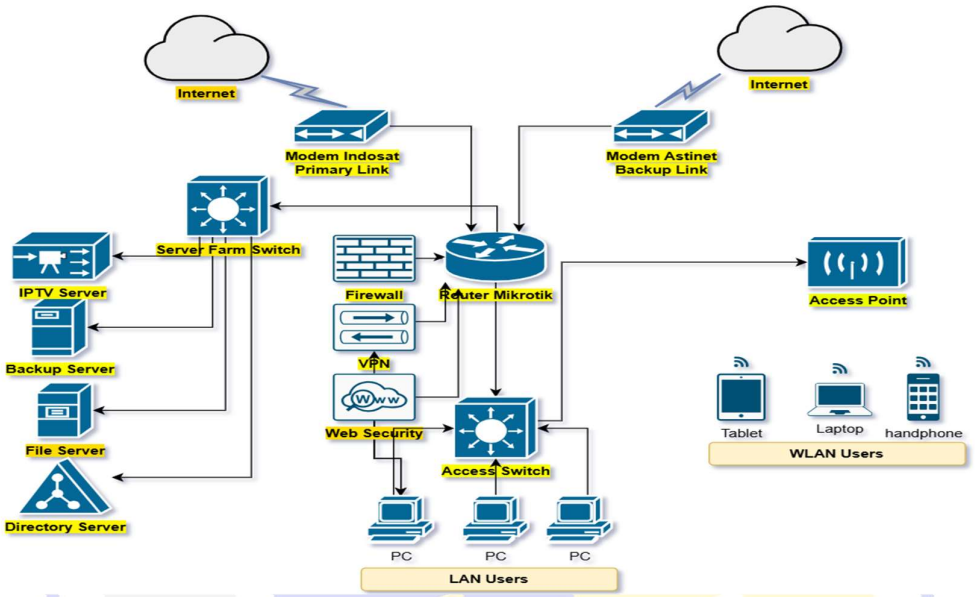
1. Dua ISP (ISP A dan ISP B) terhubung ke *router* Mikrotik.

2. Router Mikrotik dikonfigurasi dengan *load balancing* dan *failover* otomatis.

3. Router terhubung ke switch utama.

4. Switch mendistribusikan koneksi ke server internal dan beberapa client.

Dengan skema ini, diharapkan jaringan komputer di PT. ABB Sakti Industri dapat beroperasi secara lebih stabil, efisien, dan siap menghadapi gangguan koneksi tanpa mengganggu aktivitas operasional perusahaan.



Sumber: Hasil Penelitian

Gambar IV.3 Skema Jaringan Usulan

4.1.3. Keamanan Jaringan

Dalam implementasi manajemen jaringan pada PT. ABB Sakti Industri, aspek keamanan menjadi salah satu komponen penting untuk menjaga integritas, kerahasiaan, dan ketersediaan layanan jaringan. Sistem keamanan jaringan yang diusulkan mencakup beberapa lapisan proteksi, baik dari aspek perangkat keras maupun perangkat lunak, optimalisasi dilakukan dengan memanfaatkan fitur-fitur yang tersedia pada Mikrotik *RouterOS*.

Adapun langkah-langkah keamanan jaringan yang diterapkan adalah sebagai berikut:

1. *Firewall Filter Rules*

   Konfigurasi *firewall* digunakan untuk membatasi akses antar subnet, memblokir *port* yang tidak digunakan, serta mencegah akses dari IP *address* yang mencurigakan. Beberapa aturan yang diterapkan antara lain:

a. Drop semua koneksi dari luar kecuali yang diizinkan.

b. Allow akses hanya untuk port tertentu seperti HTTP (80), HTTPS (443), dan Winbox (8291) dari IP internal.

c. Blokir akses remote dari luar kecuali melalui VPN.

Tabel IV.2 ***Firewall* Filter *Rules***

Rule No.	Chain	Protocol	Port	Source Address	Destination Address	Action	Description
1	input	tcp	8291	0.0.0.0/0	192.168.100.1	drop	Block Winbox access from external sources
2	input	udp	500,1701,4500	0.0.0.0/0	192.168.100.1	accept	Allow L2TP/IPSec VPN connections
3	forward	tcp	any	192.168.10.0/24	192.168.20.0/24	drop	Block traffic from Production to Finance
4	forward	tcp	any	192.168.20.0/24	192.168.10.0/24	accept	Allow traffic from Finance to Production
5	input	icmp	-	0.0.0.0/0	192.168.100.1	accept	Allow ping to router

Sumber: Hasil Penelitian

2. *Port Knocking.*

Untuk menghindari serangan *brute force* terhadap *port* manajemen Mikrotik, digunakan teknik *port knocking*. Hanya pengguna yang mengetahui urutan port tertentu yang dapat membuka akses ke *port* manajemen.

3. VPN (*Virtual Private Network*)

Akses *remote* ke jaringan internal hanya diperbolehkan melalui koneksi VPN. Mikrotik dikonfigurasi sebagai VPN server menggunakan protokol L2TP/IPSec untuk menjamin keamanan data yang ditransmisikan.

4. *Address* List dan Layer 7 *Protocol*

Address list digunakan untuk mengelompokkan IP *address* berdasarkan kategori *(trusted, untrusted, blacklist)*. Sementara itu, Layer 7 *Protocol*

digunakan untuk mendeteksi dan memblokir trafik aplikasi tertentu seperti *torrent* atau aplikasi yang tidak diizinkan.

5. DNS *Static* dan *Cache*

   Untuk mencegah DNS *spoofing,* digunakan konfigurasi DNS *static* dan *cache* DNS lokal. Hal ini juga membantu mempercepat proses resolusi nama domain.

6. *Monitoring* dan *Logging*

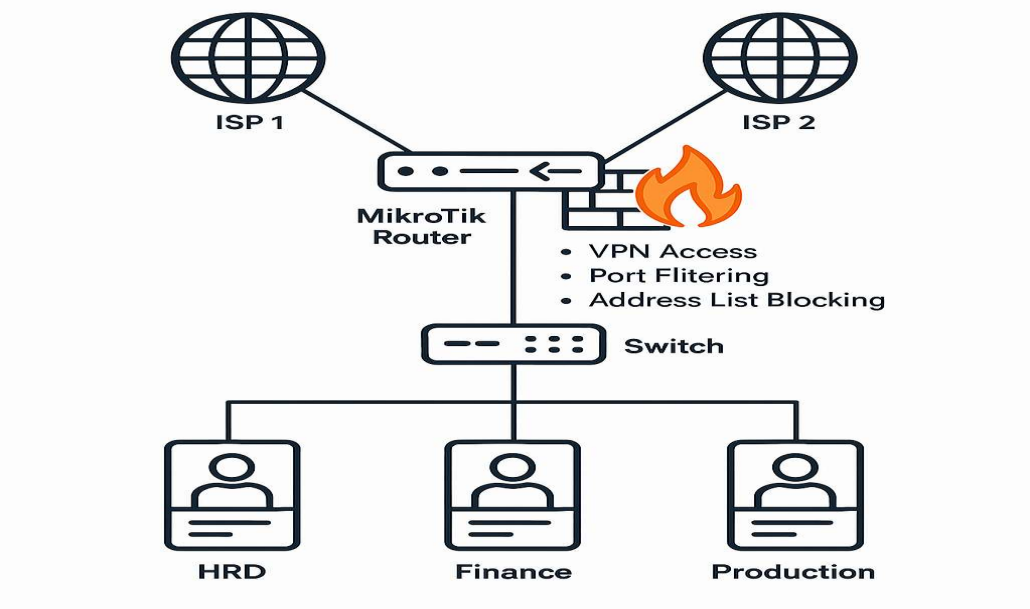
   Aktivitas jaringan dimonitor secara *real-time* menggunakan *The Dude* dan fitur *log* pada Mikrotik. Semua aktivitas penting seperti *login*, perubahan konfigurasi, dan trafik mencurigakan dicatat untuk keperluan audit dan *troubleshooting.*

7. *Backup* konfigurasi berkala

   Konfigurasi Mikrotik di *backup* secara berkala dan disimpan di lokasi yang aman. Hal ini penting untuk pemulihan cepat jika terjadi kerusakan atau serangan terhadap perangkat.

Dengan penerapan sistem keamanan ini, diharapkan jaringan PT. ABB Sakti Industri dapat terlindungi dari berbagai ancaman internal maupun eksternal, serta mendukung kelangsungan operasional perusahaan secara optimal.

Diagram ini menggambarkan arsitektur jaringan PT. ABB Sakti Industri dengan dua ISP, *router* Mikrotik, switch utama, dan tiga departemen. *Firewall* dikonfigurasi pada Mikrotik untuk mengatur akses dan keamanan.



Sumber: Hasil Penelitian

Gambar IV.4 Diagram Arsitektur Jaringan PT ABB

Arsitektur jaringan merupakan komponen penting dalam mendukung keamanan dan ketersediaan layanan di PT ABB Sakti Industri. Desain arsitektur yang baik memungkinkan pengendalian akses, segmentasi jaringan, serta penerapan kebijakan keamanan yang efektif untuk meminimalkan risiko serangan.

1. Desain Topologi

Jaringan PT ABB menggunakan topologi *star* dengan *hierarki* tersegmentasi. Perangkat pengguna terhubung ke *switch* utama, yang kemudian terhubung ke *router* MikroTik sebagai pengendali lalu lintas dan keamanan. *Router* ini bertugas mengelola koneksi ke dua ISP (*Internet Service Provider*) guna menjamin *redundansi* dan mendukung mekanisme *failover.*

2. Komponen Utama

a. *Router* MikroTik: Berfungsi sebagai *gateway* utama dengan fitur keamanan seperti:

1) *VPN Access* untuk koneksi aman dari luar.

2) *Port Filtering* untuk membatasi akses layanan tertentu.

3) *Address List Blocking* untuk memblokir alamat IP yang terindikasi berbahaya.

b. *Switch*: Menghubungkan perangkat dari berbagai departemen (HRD, *Finance*, *Production*) dan mendukung VLAN untuk *segmentasi*.

c. ISP 1 dan ISP 2: Menyediakan jalur koneksi internet dengan konfigurasi *failover* untuk menjaga ketersediaan.

3. *Segmentasi* Jaringan

Segmentasi dilakukan menggunakan VLAN untuk memisahkan lalu lintas antar departemen:

a. VLAN 10 – HRD

b. VLAN 20 – Finance

c. VLAN 30 – Production

d VLAN 99 – Manajemen VLAN untuk perangkat jaringan

Segmentasi ini mendukung penerapan kebijakan *firewall* dan ACL (*Access Control List*) yang lebih ketat antar *segmen*.

4. Keamanan Perimeter

Di sisi perimeter, *router* MikroTik dilengkapi dengan *firewall* dan mekanisme *filtering* untuk mencegah akses tidak sah. Selain itu, terdapat konfigurasi VPN untuk akses remote yang aman.

5. *Redundansi* dan *Failover*

Untuk menjamin ketersediaan layanan, arsitektur jaringan menggunakan dua ISP dengan konfigurasi *failover*. Apabila salah satu jalur mengalami gangguan, sistem akan secara otomatis mengalihkan koneksi ke jalur cadangan.

4.1.4. Rancangan Aplikasi

Rancangan aplikasi dalam implementasi manajemen jaringan ini berfokus pada konfigurasi dan pemanfaatan fitur-fitur yang tersedia pada perangkat Mikrotik *RouterOS* untuk mendukung metode *Load Balancing* dan *Failover.* Aplikasi yang digunakan bukan berupa *software* tambahan, melainkan konfigurasi internal Mikrotik yang dijalankan melalui *Winbox* atau terminal CLI.

1. Tujuan Rancangan

a. Mengoptimalkan distribusi *trafik* internet melalui beberapa jalur ISP.

b. Menjamin ketersediaan koneksi internet dengan mekanisme *failover* otomatis.

c. Menyediakan *monitoring* dan *logging trafik* untuk analisis performa jaringan.

2. Komponen Utama

a. Mikrotik *RouterOS* (versi minimal 6.45)

b. *Winbox* sebagai GUI konfigurasi

c. *Tool Netwatch* untuk *monitoring* koneksi ISP

d. *Script* Mikrotik untuk otomatisasi *failover*

e.*Firewall* dan *Mangle Rules* untuk *routing* mark

f. *Routing Table* untuk *load balancing*

3. Langkah Konfigurasi Aplikasi

a. Tujuan konfigurasi

1) *Load balancing* : membagi trafik keluar ke kedua ISP (ISP A dan ISP B) secara proporsional.

2) *Failover* : Jika salah satu ISP terputus, trafik otomatis dialihkan ke ISP yang aktif

b. *Firewall Mangle*

Langkah ini menandai koneksi dan *routing* agar MikroTik tahu paket mana yang harus lewat ISP A atau ISP B.

```
/ip firewall mangle
add action=mark-connection chain=prerouting dst-address-type=!local \
   in-interface=ether3-Lan new-connection-mark="ISP A" passthrough=yes \
   per-connection-classifier=src-address-and-port:2/0
add action=mark-connection chain=prerouting dst-address-type=!local \
   in-interface=ether3-Lan new-connection-mark="ISP B" passthrough=yes \
   per-connection-classifier=src-address-and-port:2/1

add action=mark-routing chain=prerouting connection-mark="ISP A" \
   in-interface=ether3-Lan new-routing-mark="ke ISP A" passthrough=no
add action=mark-routing chain=prerouting connection-mark="ISP B" \
   in-interface=ether3-Lan new-routing-mark="ke ISP B" passthrough=no
```

Sumber: Hasil Penelitian

Gambar IV.5 Firewall Mangle PT ABB

Baris pertama:

```
add action=mark-connection chain=prerouting dst-address-type=!local \
    in-interface=ether3-Lan new-connection-mark="ISP A" passthrough=yes \
    per-connection-classifier=src-address-and-port:2/0
```

Sumber: Hasil Penelitian

Gambar IV.6 *Mangle* Baris Pertama

Artinya:

1) Semua koneksi dari LAN (ether3-Lan) akan diberi tanda "ISP A" untuk sebagian trafik.

2) per-connection-classifier=src-address-and-port:2/0 → membagi koneksi menjadi 2 grup (0 dan 1), grup 0 ke ISP A.

Baris kedua:

```
add action=mark-connection chain=prerouting dst-address-type=!local \
    in-interface=ether3-Lan new-connection-mark="ISP B" passthrough=yes \
    per-connection-classifier=src-address-and-port:2/1
```

Sumber: Hasil Penelitian

Gambar IV.7 *Mangle* Baris Kedua

Artinya: Grup 1 akan diarahkan ke ISP A

Setelah koneksi ditandai, dibuat *mark-routing:*

```
add action=mark-routing chain=prerouting connection-mark="ISP A" \
    in-interface=ether3-Lan new-routing-mark="ke ISP A" passthrough=no
add action=mark-routing chain=prerouting connection-mark="ISP B" \
    in-interface=ether3-Lan new-routing-mark="ke ISP B" passthrough=no
```

Sumber: Hasil Penelitian

Gambar IV.8 *Mark-Routing*

Artinya:

1) Paket yang sudah ditandai koneksi ISP A akan diarahkan ke *routing table* "ke ISP A".

2) Paket ISP B ke *routing table* "ke ISP B".

c. *Routing Table*

Membuat route untuk masing-masing ISP:

```
/ip route
add check-gateway=ping distance=1 gateway=11.11.11.1%ether1_ispa routing-mark="ke ISPA"
add check-gateway=ping distance=1 gateway=12.12.12.1%ether2_ispb routing-mark="ke ISPB"
```

Sumber: Hasil Penelitian

Gambar IV.9 *Routing Table*

Artinya:

1) *Gateway* ISP A = 11.11.11.1 (*interface ether1*_ispa).

2) *Gateway* ISP B = 12.12.12.1 (*interface ether2*_ispb).

3) *check-gateway=ping* → MikroTik akan *ping gateway*. Jika gagal, route dianggap terputus (*failover* aktif).

4. Monitoring koneksi ISP (*Netwatch*)

Script untuk ISP A

```
/tool netwatch add host=11.11.11.1 interval=00:00:10 timeout=1000ms \
up-script="/ip route set [find comment=\"ISP A\"] distance=1; \
/ip route set [find comment=\"ISP B\"] distance=10" \
down-script="/ip route set [find comment=\"ISP A\"] distance=10; \
/ip route set [find comment=\"ISP B\"] distance=1"
```

Sumber: Hasil Penelitian

Gambar IV.10 *Script* ISP A

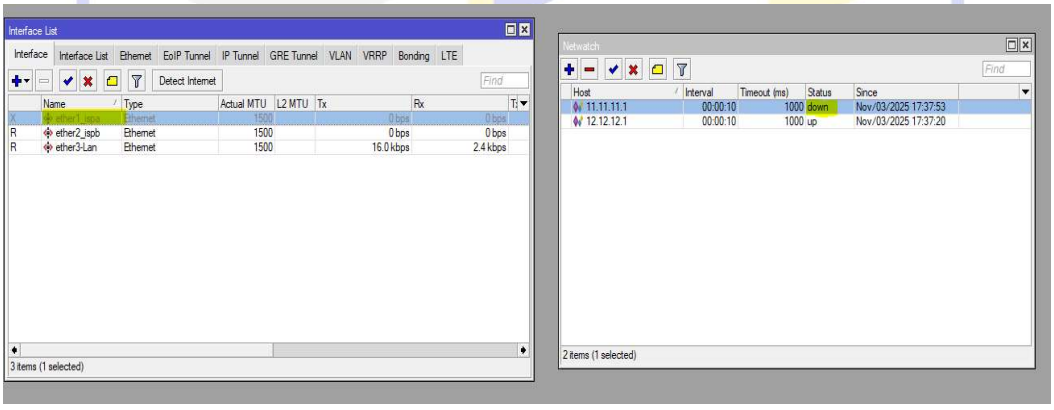
Script untuk ISP B

```
/tool netwatch add host=12.12.12.1 interval=00:00:10 timeout=1000ms \
up-script="/ip route set [find comment=\"ISP B\"] distance=1; \
/ip route set [find comment=\"ISP A\"] distance=10" \
down-script="/ip route set [find comment=\"ISP B\"] distance=10; \
```

Sumber: Hasil Penelitian

Gambar IV.11 *Script* ISP B

Berikut adalah gambar contoh *testing* menggunakan *Netwatch* jika pada koneksi ISP A terputus

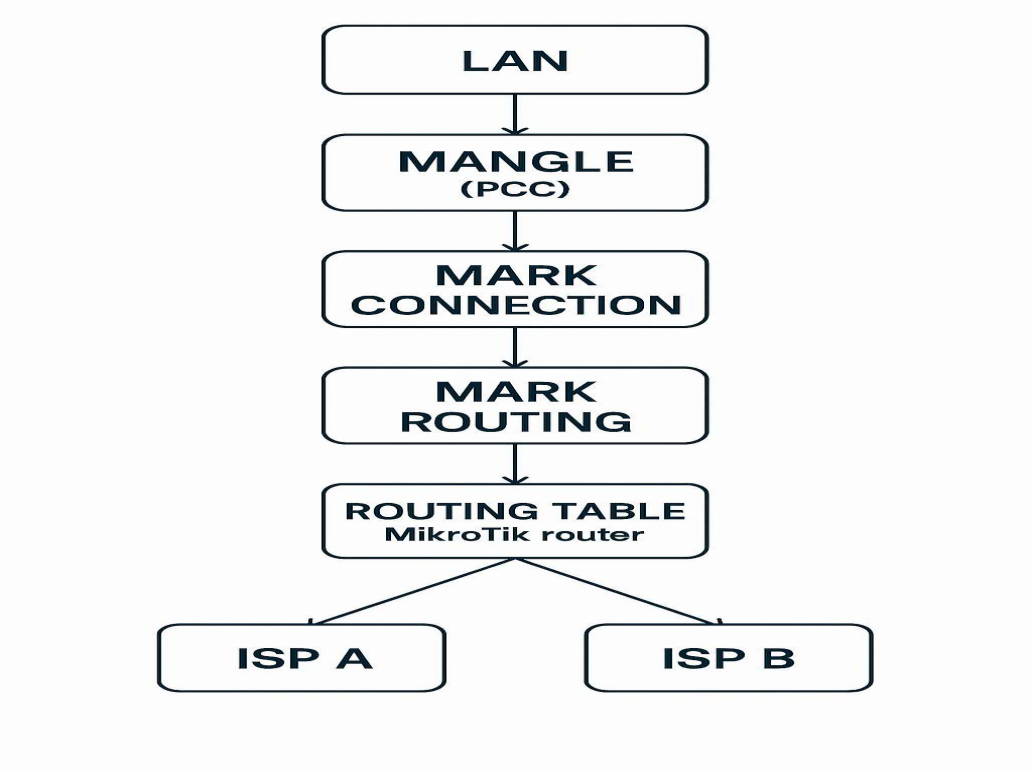


Sumber: Hasil Penelitian

Gambar IV.12 *Testing Netwatch*

5. Diagram alur konfigurasi

Berikut adalah diagram alur konfigurasi aplikasi Mikrotik untuk implementasi *Load Balancing* dan *Failover* yang sesuai dengan bagian Bab IV.1.4 Rancangan Aplikasi:



Sumber: Hasil Penelitian

Gambar IV.13 Diagram Alur Konfigurasi Mikrotik

Berikut adalah flow untuk konfigurasi *Load Balance* 2 ISP dengan PCC dan *Failove*r:

a. LAN → sumber trafik.

b. *Mangle* (PCC) → membagi koneksi berdasarkan *classifier.*

c. *Mark Connection* → memberi tanda ISP A atau ISP B.

d. *Mark Routing* → menentukan *routing mark.*

e. *Routing Table* (MikroTik) → memilih *gateway* sesuai tanda.

f. ISP A / ISP B → jalur keluar, dengan *failover* aktif.

4.1.5. Manajemen Jaringan

Manajemen jaringan merupakan komponen krusial dalam memastikan kinerja, keamanan, dan ketersediaan layanan. Pada implementasi ini, pengelolaan jaringan dilakukan dengan memanfaatkan fitur Mikrotik *RouterOS* untuk memantau, mengatur, serta mengoptimalkan lalu lintas secara *real-time.*

1. Tujuan Manajemen Jaringan

   a. Memastikan distribusi *trafik* berjalan sesuai kebijakan *routing.*

   b. Mendeteksi dan merespons gangguan koneksi secara otomatis.

   c. Melakukan pemantauan performa jaringan secara berkala.

   d. Menyediakan log aktivitas jaringan untuk keperluan audit dan *troubleshooting.*

2. Fitur-Fitur yang Digunakan

   a. *Netwatch* – untuk *monitoring* status koneksi ISP.

   b. Log System – mencatat *event* penting seperti *failover, reboot,* dan *error.*

   c. Queue Tree / *Simple Queue* – untuk manajemen *bandwidth* per user atau per *interface.*

   d. *Torch* – untuk analisis *trafik real-time.*

e. SNMP *(Simple* Network Management *Protocol)* – untuk integrasi dengan sistem *monitoring* eksternal seperti *Zabbix* atau *The Dude*.

f. Email *Notification* (opsional) – untuk mengirimkan peringatan jika terjadi gangguan.

3. Contoh Konfigurasi *Monitoring* dan *Logging*

a. Aktifkan *Logging* untuk *Routing* dan *Netwatch*

/system logging

add topics=netwatch action=memory

add topics=route action=memory

b. Monitoring Trafik dengan *Torch*

/tool torch interface=ether1

c. Queue untuk Manajemen *Bandwidth*

/queue simple

add name="Limit-User1" target=192.168.10.10/32 *max-limit*=2M/2M

4. Strategi Pemeliharaan

a. *Backup* konfigurasi secara berkala.

b. *Update firmware* Mikrotik jika diperlukan.

c. Audit log dan *trafik* minimal seminggu sekali.

d. Simulasi *failover* setiap bulan untuk memastikan sistem tetap responsif.

Berikut adalah tabel ringkasan fitur manajemen jaringan yang digunakan dalam implementasi Mikrotik untuk metode *Load Balancing* dan *Failover:*

Tabel IV.3 Ringkasan Fitur Manajemen Jaringan Mikrotik

No.	Fitur Mikrotik	Fungsi Utama	Contoh Penggunaan
1	*Netwatch*	*Monitoring* status koneksi ke IP publik atau *gateway*	Deteksi koneksi ISP dan eksekusi *script failover* otomatis
2	System *Logging*	Mencatat *event* penting dalam sistem	Log aktivitas *routing, Netwatch,* dan *error* sistem
3	*Torch*	Analisis *trafik real-time* per *interface*	Melihat *trafik* masuk/keluar pada *interface* ether1
4	*Queue (Simple/Tree*)	Manajemen *bandwidth* per IP atau *interface*	Membatasi *bandwidth* user tertentu (misal 2 Mbps)
5	SNMP	Integrasi *monitoring* eksternal	*Monitoring* dengan *Zabbix* atau The Dude
6	*Script*	Otomatisasi tindakan berdasarkan kondisi jaringan	Menonaktifkan *route* saat ISP *down*
7	Email *Notification*	Mengirim peringatan otomatis (opsional)	Kirim email saat terjadi *failover* atau *reboot*
8	*Scheduler*	Menjadwalkan eksekusi *script* secara berkala	*Backup* konfigurasi setiap minggu

Sumber: Hasil Penelitian

4.2 Pengujian Jaringan

Pengujian jaringan dilakukan untuk memastikan bahwa *konfigurasi Load Balancing dan Failover* pada perangkat Mikrotik telah berjalan sesuai dengan rancangan. Pengujian ini dibagi menjadi dua tahap, yaitu pengujian awal (sebelum implementasi) dan pengujian akhir (setelah implementasi).

Pada tahap pengujian jaringan ini dilakukan tiga skenario pengujian utama yang sesuai dengan kondisi operasional jaringan PT ABB Sakti Industri, yaitu:

1. Kondisi Normal (dua ISP aktif – *load balancing* berjalan),
2. ISP Utama Mengalami Gangguan (*failover* aktif),
3. Beban Tinggi *Multi-User (stress test).*

Setiap skenario diuji pada dua tahap yaitu pengujian awal (*pra-implementasi*) dan pengujian akhir (*pasca-implementasi*). Parameter performa jaringan yang diukur meliputi *packet loss, delay/latency*, serta *throughput* (opsional). Pengujian dilakukan menggunakan metode *Ping Test*, *Traceroute*, *Torch*, dan simulasi pemutusan koneksi ISP sesuai pedoman pengujian jaringan.

4.2.1. Pengujian jaringan awal

Pengujian awal jaringan dilakukan sebelum penerapan metode *Load Balancing* dan *Failover* untuk mengidentifikasi kondisi serta kelemahan pada sistem jaringan yang sedang digunakan di PT. ABB Sakti Industri. Pengujian ini bertujuan untuk mengidentifikasi titik kegagalan, performa koneksi, dan jalur komunikasi data.

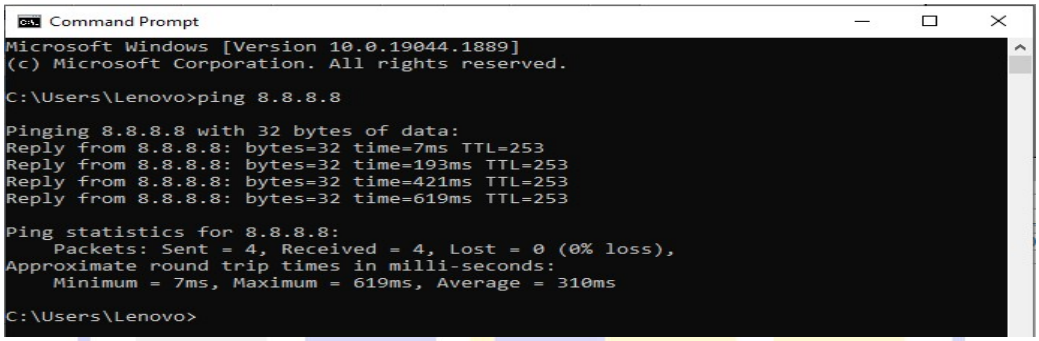
Tabel IV.4 Metode Pengujian Jaringan Awal

Jenis Pengujian	Tujuan
Ping Test	Menguji konektivitas ke gateway dan DNS eksternal (misalnya 8.8.8.8)
Traceroute	Melihat jalur koneksi dari client ke internet
Torch	Menganalisis trafik real-time pada interface Mikrotik
Simulasi ISP Down	Memutus salah satu koneksi ISP untuk melihat dampaknya terhadap jaringan

Sumber: Hasil Penelitian

1. Hasil Pengujian

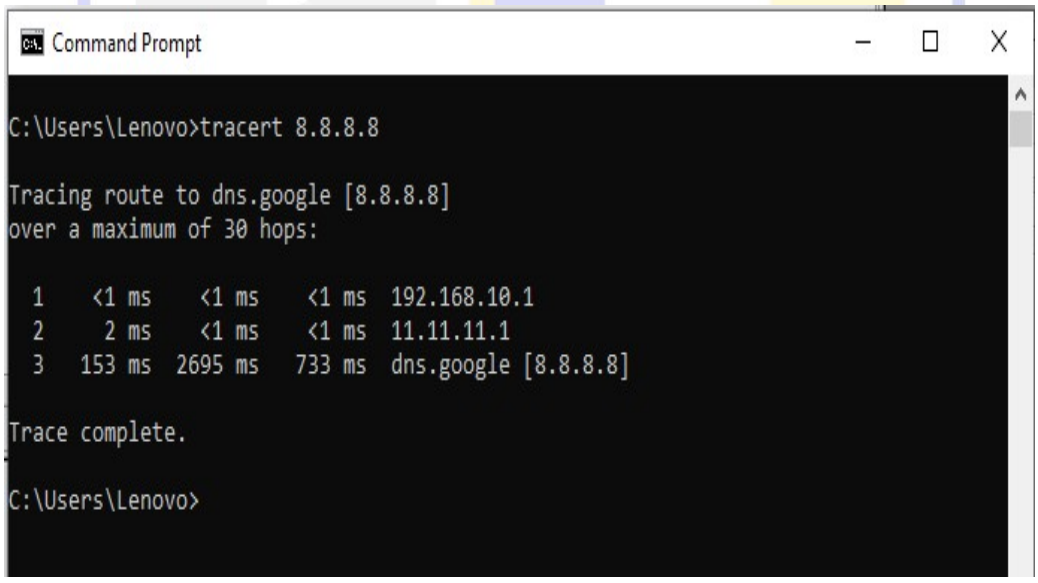
Ping *Test*



Sumber: Hasil Penelitian

Gambar IV.14 Ping *Test* Jaringan Awal

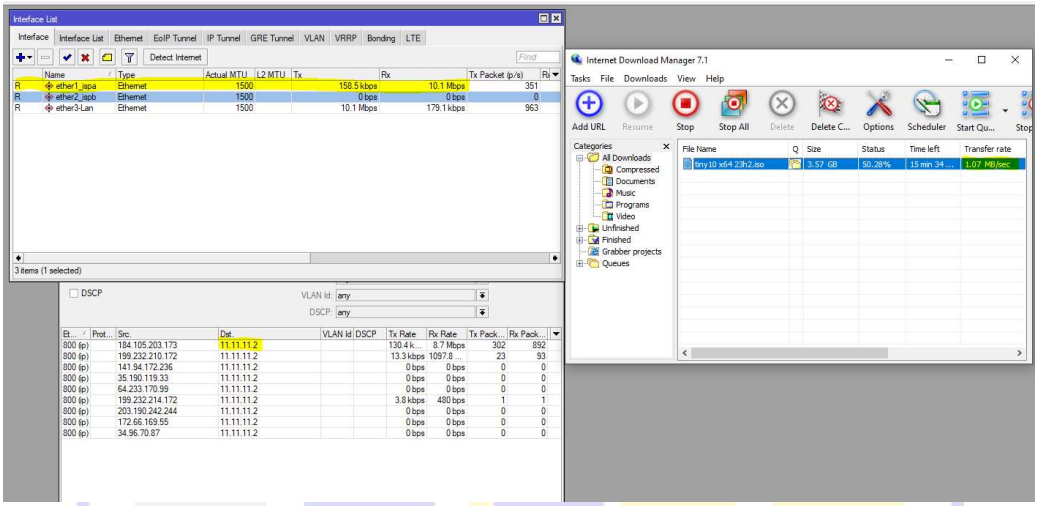
Traceroute Test



Sumber: Hasil Penelitian

Gambar IV.15 *Traceroute Test* Jaringan Awal

2. Analisis *Torch*



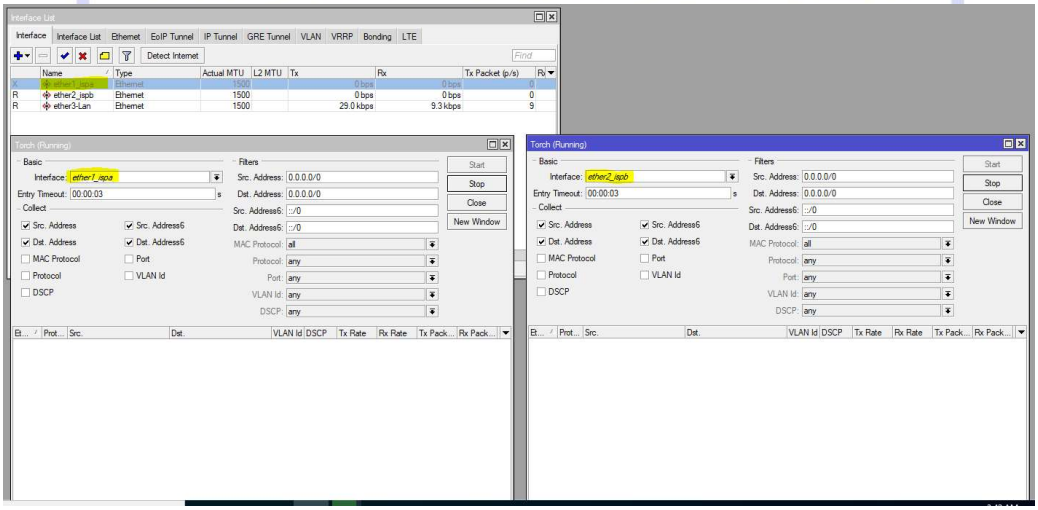
Sumber: Hasil Penelitian

Gambar IV.16 Analisa *Torch* Jaringan Awal

a. *Trafik* hanya mengalir melalui satu *interface* (ISP utama).

b. Tidak ada distribusi *trafik* atau *backup* jalur.

3. Simulasi ISP *Down*



Sumber: Hasil Penelitian

Gambar IV.17 Simulasi ISP *Down* Jaringan Awal

a. Ketika koneksi ISP utama diputus, seluruh koneksi internet terputus.

b. Tidak ada mekanisme *failover* atau *backup* otomatis.

4. Kesimpulan Pengujian Awal

a. Jaringan belum memiliki sistem *redundansi.*

b. Ketergantungan pada satu ISP menyebabkan risiko *downtime* tinggi.

c. Tidak tersedia sistem *monitoring* dan manajemen *trafik* yang memadai.

Untuk memberikan gambaran kondisi dasar jaringan sebelum implementasi metode *load balancing* dan *failover*, maka dicatat parameter performa berupa *packet loss, delay,* dan *throughput*. Ringkasan hasil dapat dilihat pada Tabel IV.X berikut.

Tabel IV.5 Hasil Pengujian Awal

Skenario	**Jalur**	**Sampel**	**Packet Loss (%)**	**Delay min/avg/max (ms)**	**Throughput (Mbps)**	**Catatan**
Normal (1 ISP)	ISP A	200 pkt	…	…	…	Trafik hanya lewat 1 ISP
ISP Down	–	200 pkt	100%	Timeout	–	Tidak ada failover
Beban Tinggi	ISP A	200 pkt	…	…	…	Terjadi bottleneck

Sumber: Hasil Penelitian

4.2.2. Pengujian Jaringan Akhir

Pengujian akhir jaringan dilakukan setelah penerapan metode *Load Balancing* dan *Failover* pada perangkat Mikrotik. Tujuan pengujian ini adalah memastikan sistem mampu mendistribusikan trafik secara optimal serta melakukan *failover* otomatis ketika salah satu jalur ISP mengalami gangguan.

Tabel IV.6 Metode Pengujian Jaringan Akhir

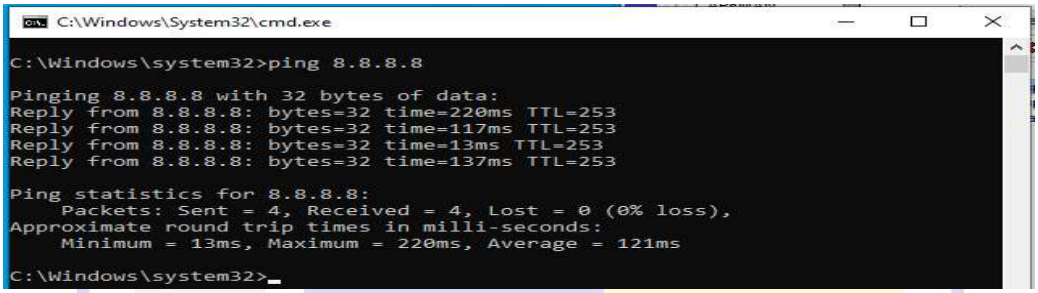
Jenis Pengujian	Tujuan
Ping *Test*	Menguji kestabilan koneksi ke DNS eksternal melalui kedua jalur ISP
Traceroute	Melihat efisiensi jalur koneksi setelah konfigurasi
Simulasi ISP *Down*	Memutus koneksi ISP 1 dan memastikan sistem otomatis beralih ke ISP 2
Simulasi ISP Pulih	Mengaktifkan kembali ISP 1 dan memastikan sistem kembali ke jalur utama

Sumber: Hasil Penelitian

Setelah implementasi metode *Per Connection Classifier* (PCC) untuk *load balancing* serta *Netwatch* dan *recursive routing* untuk *failover,* dilakukan kembali pengujian pada tiga skenario operasional yaitu kondisi normal, ISP *down*, serta beban tinggi *multi-user*. Parameter yang diukur adalah *packet loss, delay*, serta *throughput*. Pengujian ini bertujuan untuk memvalidasi bahwa jaringan telah mampu melakukan distribusi trafik secara seimbang dan beralih otomatis ke ISP cadangan dalam waktu kurang dari 5 detik saat terjadi gangguan.

1. Hasil Pengujian

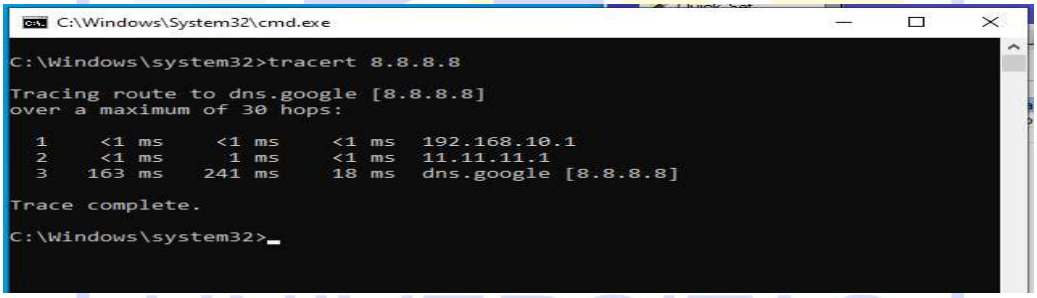
Ping *Test*



Sumber: Hasil Penelitian

Gambar IV.18 Ping *Test* Jaringan Akhir

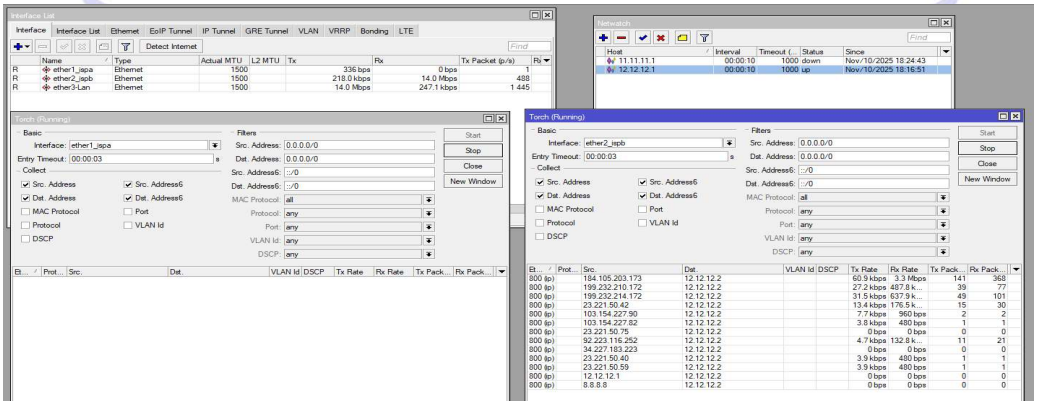
2. *Traceroute*



Sumber: Hasil Penelitian

Gambar IV.19 Traceroute Jaringan Akhir

3. Simulasi ISP *Down*



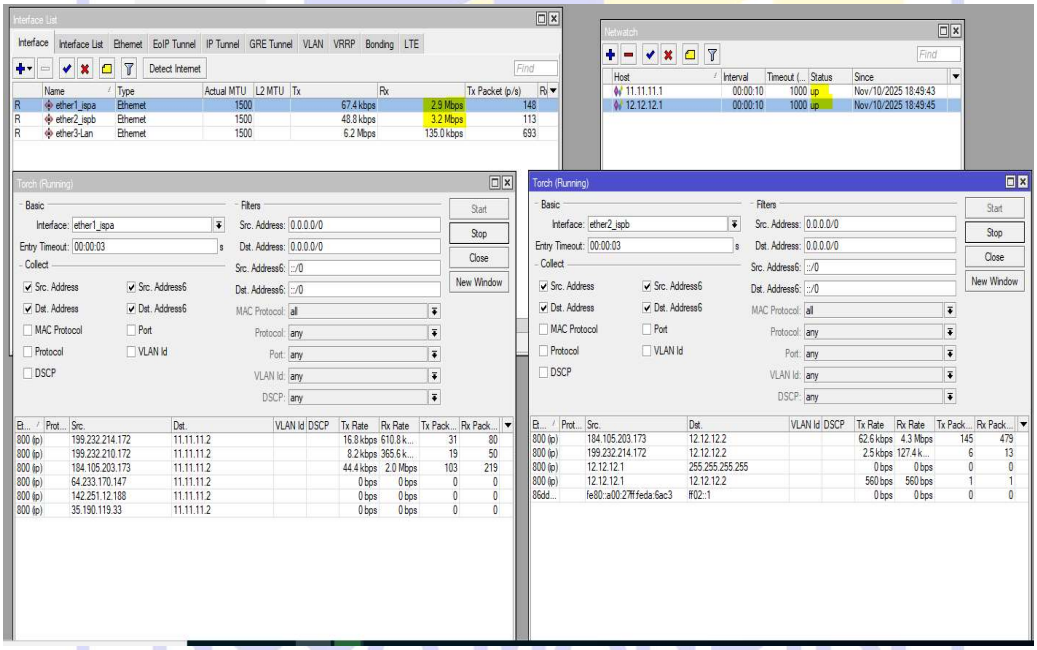
Sumber: Hasil Penelitian

Gambar IV.20 Simulasi ISP *Down* Jaringan Akhir

a. Saat ISP 1 diputus, sistem otomatis mengalihkan *trafik* ke ISP 2 dalam waktu kurang dari 5 detik.

b. Tidak terjadi pemutusan koneksi internet di sisi pengguna.

4. Simulasi ISP Pulih



Sumber: Hasil Penelitian

Gambar IV.21 Simulasi ISP Pulih

a. Setelah ISP 1 aktif kembali, sistem kembali menggunakan jalur utama secara otomatis.

b. *Routing table* menyesuaikan tanpa perlu intervensi manual.

Kesimpulan Pengujian Akhir

1. Sistem berhasil menjalankan *fungsi Load Balancing* dan *Failover* dengan baik.

2. Koneksi internet tetap stabil meskipun salah satu ISP mengalami gangguan.

3. *Monitoring* dan manajemen jaringan berjalan sesuai harapan

Tabel IV.7 Hasil Pengujian Akhir

Skenario	**Jalur**	**Packet Loss (%)**	**Delay min/avg/max (ms)**	**Failover Time (detik)**	**Throughput (Mbps)**	**Catatan**
Normal (2 ISP aktif)	ISP A	…	…	–	…	Trafik terbagi
Normal (2 ISP aktif)	ISP B	…	…	–	…	Trafik terbagi
ISP A Down	ISP B	…	…	< 5 detik	…	Failover otomatis
Beban Tinggi	ISP A/B	…	…	–	…	Sistem stabil