Jurnal Infortech
Volume 4 No. 2 Desember 2022
E-ISSN: 2715-8160

Implementasi Load Balancing Dan Failover Menggunakan IP SLA Pada PT Pan Pacific Insurance

Riyan Almakhi[1], Anton[2], Fitra Septia Nugraha[3]

[1,2,3] Universitas Nusa Mandiri
e-mail: [1]riyanalmakhi@gmail.com, [2]anton@nusamandiri.ac.id, [3]fitra.fig@nusamandiri.ac.id

Diterima	Direvisi	Disetujui
06-08-2022	18-10-2022	30-11-2022

Abstrak - Perkembangan jaringan komputer dan internet begitu pesat pada era industry 4.0, khususnya internet sebagai media informasi tentunya harus memiliki kualitas koneksi yang baik. Begitu juga pada PT Pan Pacific Insurance yang sangat bergantung pada koneksi internet untuk menunjang berjalannya operasional perusahaan. Sebelumya PT Pan Pacific Insurance hanya menggunakan satu *Internet Service Provider* (ISP) dan jika terjadi gangguan pada koneksi internet maka operasional perusahaan menjadi tidak berfungsi dengan baik. Untuk mengatasi hal tersebut maka dilakukan penambahan koneksi ISP baru yang dapat digunakan secara bersamaan sehingga tidak bergantung pada satu ISP, teknik tersebut disebut dengan *load balancing*. Penerapan teknik *failover* juga dilakukan untuk mengantisipasi bila salah satu koneksi pada jaringan ini mati, karyawan tetap mendapatkan koneksi internet dari ISP lainnya. Perangkat yang digunakan untuk menerapkan teknik teknik *load balancing* dan *failover* adalah cisco router. Selain itu dibuat juga *Internet protocol Service Level Agreement* (IP SLA) untuk melakukan pengecekan *Round Trip Time* (RTT) yaitu waktu yang dibutuhkan untuk paket kembali, konfigurasi pada router dengan ketentuan untuk melakukan ping selama 10 detik sekali dan jika round trip timenya mencapai 5000 milisecond maka hal tersebut dianggap sudah melanggar ketentuan IP SLA dan dikatakan koneksi internet tidak bagus. Setelah menggunakan dan mengimplementasikan konfigurasi teknik *load balancing* dan *failover* menggunakan IP SLA koneksitas operasional pada PT Pan Pacific Insurance dapat berjalan dengan baik dan lancar, hal ini dapat mengatasi permasalahan yang sering terjadi pada saat jam sibuk kemudian salah satu ISP mengalami kendala, pengguna akan tetap mendapatkan koneksi internet dari ISP yang lain sehingga pekerjaan dapat terselesaikan.

Kata Kunci : Load Balancing, Failover, Cisco

Abstract *- The development of computer networks and the internet is so rapid in the current era, especially the internet as a medium of information, of course, must have a good connection quality. Likewise, PT Pan Pacific Insurance relies heavily on internet connections to support the company's operations. Previously, PT Pan Pacific Insurance only used one ISP (internet service provider) and if there was a problem with the internet connection, the company's operations would be disrupted. To overcome this, the addition of a new internet connection that can be used simultaneously so that it does not depend on one ISP, this technique is called load balancing. A failover technique will also be applied to this network, ie if one internet connection dies, employees will still get internet connections from other ISPs. One device that can use load balancing and failover techniques is a Cisco router. And also made an IP SLA (Service Level Agreement) to check the Round Trip Time (RTT), which is the time it takes for the packet to return. The Cisco router will be configured to ping every 10 seconds and if the Round Trip Time reaches 5000 milliseconds then it is a violation of the SLA (Service Level Agreement) and it says the internet connection is not good. Configuration and implementation of load balancing and failover using the IP SLA that has been implemented went well. This can solve the problem when there is interference with one ISP, the user will still get an internet connection from another ISP.*

Keywords: Load Balancing, Failover, Cisco

PENDAHULUAN

Pemanfaatan teknologi jaringan komputer dan internet sebagai media komunikasi sangat dibutuhkan untuk menjalankan operasional perusahaan dan untuk membantu mempermudah pertukaran data. Saat ini semakin banyak kegiatan usaha, lembaga, dan organisasi yang proses bisnisnya bergantung pada keberadaan jaringan komputer. (Primartha, 2019)

Pada PT Pan Pacific Insurance yang penulis lakukan *observasi*, sudah terdapat jaringan komputer

yang sedang berjalan saat ini. Akan tetapi terdapat permasalahan pada jaringan internet yang sering muncul seriring berjalannya waktu, sering terjadinya gangguan pada koneksi internet yang digunakan saat ini dikarenakan beberapa faktor yang terjadi disisi penyedia layanan internet diantaranya FO *cut* dan masalah *routing* antar ISP, masalah *routing* antar ISP mengakibatkan koneksi antar cabang graha panfic dan tempat penyimpanan *server* di gedung *cyber* mengalami gangguan. Tuntutan kestabilan jaringan komputer dan internet tanpa *down time* sangat diperlukan untuk menjaga layanan prima perusahaan ini yang begerak pada bidang asuransi untuk melayani pelanggan. Untuk mengatasi hal itu, diperlukan koneksi internet tambahan dan penambahan NIC pada perangkat cisco *router*.

Untuk mengatasi permasalahan perusahaan dan meningkatkan kualitas jaringan maka perlu dilakukan pembagian beban trafik pada perangkat jaringan agar tidak bergantung pada ISP (*Internet Service Provider*) dan memperoleh keuntungan berupa jaminan internet menjadi stabil. Seperti penelitian yang dilakukan (Armanto, 2017) mengatakan bahwa *load balancing* dan *failover* yaitu mengabungkan dua buah teknik yang mampu digunakan sebagai internet *gateway.*

Karena ada dua jalur koneksi Internet simultan, ketika satu koneksi terputus, koneksi lain tersedia. Untuk mengoptimalkan kinerja suatu jaringan komputer, maka perlu dirancang suatu jaringan yang dapat menangani masalah konektivitas. Pada jaringan komputer, teknik penggabungan 2 link internet yang berbeda (2 *provider*) disebut juga dengan istilah *load balancing*. (Suryanto et al., 2018)

1. Konsep Dasar Jaringan

Menurut (Rachman, 2019) jaringan komputer dapat diklasifikasikan berdasarkan cakupan area dan media penghantarnya.

Jaringan komputer adalah koneksi beberapa komputer otonom yang dapat berbagi informasi satu sama lain. Jaringan komputer menghubungkan beberapa komputer melalui media perantara. Media perantara ini dapat berupa media kabel atau *nirkabel.* Informasi dalam format data mengalir dari satu komputer ke komputer lain, atau dari satu komputer ke perangkat lain, memungkinkan setiap komputer yang terhubung untuk bertukar data. (Primartha, 2019) dan menurut (Ardhiansyah et al., 2020) Jaringan Komputer dalam arti luas adalah sekumpulan dari bebebrapa komputer yang tersambung dan saling terhubung sehingga dapat saling berbagi informasi dan berkomunikasi antara satu perangkat dengan perangkat lainnya.

2. Load Balancing

Dengan adanya penerapan metode *load balancing* ini diharapkan mampu mempermudah pengguna dalam menggunakan fasilitas internet dan internet tidak mengalami *down time*, karena dari teknik *load balancing* ini dapat mendistribusikan beban trafik pada 2 jalur koneksi secara seimbang sehingga traffik bisa berjalan optimal dan juga dapat menghindari *overload* pada salah satu jalur koneksi. *Load balancing* ini digunakan untuk mengurangi waktu eksekusi 2 beban pada *traffic line* dan memastikan bahwa semua sumber daya yang ada dalam sistem dimanfaatkan secara optimal, memaksimalkan *throughput*. (Mustofa & Ramayanti, 2020)

Menurut (Dani & Suryawan, 2017) Load balancing merupakan teknologi untuk melakukan pembagian beban kepada beberapa server, memastikan tidak terjadi kelebihan beban pada salah satu server.

Menurut (Irfan Oktavianto dan et al., 2019) Load balancing sendiri merupakan teknik pembagian beban pada lebih dari satu jaringan secara merata dengan membagi jalur koneksi yang tersedia. Dengan adanya load balancing beban yang ditanggung oleh server akan terbagi ke server yang lain dengan pembagian yang sesuai kapasitas server masing-masing.

3. Failover

Sedangkan untuk menangani masalah jika salah satu isp mati dan dapat di gantikan secara otomatis oleh isp yang lain maka digunakan teknik *failover*. Dalam kasus jaringan komputer, *failover* adalah kemampuan sistem untuk beralih secara manual atau otomatis jika terjadi kegagalan sistem untuk menjadikannya cadangan untuk sistem yang gagal. Selain kelebihan, penggunaan dua link ISP untuk *load balancing* dan *failover* juga memiliki beberapa kelemahan, yaitu ketika kedua ISP *down/down* maka koneksi internet akan *drop.* (Mustofa & Ramayanti, 2020)

Menurut (Gofindo Malau, 2022) *failover* membantu jika terjadi gangguan pada salah satu jalur/ISP. Sebaiknya sistem secara otomatis memindahkan gateway kejalur yang masih tersedia atau aktif.

4. IP SLA

SLA merupakan akronim dari *Service Level Agreement. Service Level Agreement* jika diterjemahkan dalam bahasa Indonesia kurang lebih adalah Perjanjian Tingkat Layanan. SLA banyak dijumpai dalam praktik bisnis umum. Secara umum SLA merupakan kesepakatan formal yang dapat dinegosiasikan guna mengidentifikasi harapan, tanggung jawab, dan memfasilitasi komunikasi antara penyedia produk/layanan (*supplier*) dengan pelanggannya (*costumers*) yang diukur dengan jangka waktu tertentu. SLA dapat diartikan secara sederhana sebagai jaminan kuialitas layanan. (Primartha, 2019)

Sedangkan IP SLA sendiri didalam jaringan komputer yaitu sebuah metode *monitoring service* pada *router* untuk mengetahui *traffic*. Seperti *memonitoring traffic* yang menuju ke sumber koneksi *internet* atau ISP.

METODE PENELITIAN

Metode penelitian yang digunakan adalah metode eksperimental, "Metode eksperimen termasuk dalam metode kuantitatif yang dilakukan dengan adanya perlakuan (*treatment*) (Sugiyono, 2011)". Metode ini merupakan metode penelitian yang digunakan untuk mencari pengaruh perlakuan tertentu terhadap yang lain dalam kondisi yang terkendalikan, meliputi studi literatur, analisa, perancangan, implementasi, pengujian sistem, evaluasi dan dokumentasi. Penulis juga melakukan pengumpulan data sebagai langkah yang tepat untuk mendapatkan solusi dalam menyelesaikan permasalahan diatas. Adapun metode pengumpulan data yang dilakukan adalah:

1. Observasi

Melakukan analisa pada jaringan dan sistem yang dipakai saat ini untuk mengetahui seperti apa kondisi jaringan komputer pada PT. Pan Pacific Insurance, kantor Graha Panfic.

2. Wawancara

Melakukan wawancara dengan pembimbing riset PT. Pan Pacific Insurance, kantor Graha Panfic untuk mendapatkan informasi yang akurat dan dapat dipertanggung jawabkan dengan narasumber yang mengetahui tentang masalah yang sedang diamati mengenai arsitektur jaringan dan topologinya.

3. Studi Pustaka

Mengumpulkan data dengan membaca dan meneliti pengetahuan teoritis yang diperoleh dari buku, artikel dan media *online*. Buku, artikel dan media *online* tersebut membahas atau memuat materi yang berhubungan dengan permasalahan yang dibahas, sebagai bahan pelengkap untuk penulis dan sebagai analisis komparatif

HASIL DAN PEMBAHASAN

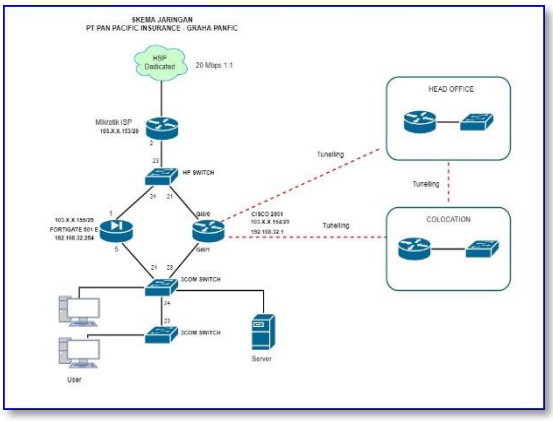
1. Topologi Jaringan

Dari hasil analisa jaringan berjalan yang penulis lakukan pada PT Pan Pacific Insurance kantor Graha Panfic dapat diketahui perusahaan ini menggunakan konfigurasi IP *address static* untuk user yang di priorotaskan dan untuk karyawan lain menggunakan DHCP IP *address*. Semua komputer *user* terhubung langsung ke *switch* menggunakan kabel UTP. Pada perusahaan ini hanya menggunakan koneksi kabel (*wired*)dan tidak ada koneksi tanpa kabel *(wireless*). IP address yang digunakan menggunakan kelas C.

Untuk keamanan jaringan sendiri, PT Pan Pacific Insurance menggunakan firewall fortigate. Lalu untuk pengiriman email menggunakan Microsoft Outlook dan memiliki domain sendiri yaitu panfic.com. Sedangkan untuk penyimpanan data, semua tersimpan di data *center cyber* dan menggunakan Microsoft Azure untuk penyimpanan *cloudn*ya.

a. Jaringan Awal

Dari hasil analisa jaringan berjalan yang penulis lakukan pada PT Pan Pacific Insurance kantor Graha Panfic dapat diketahui perusahaan ini menggunakan konfigurasi IP *address static* untuk user yang di prioritaskan dan untuk karyawan lain menggunakan DHCP IP *address*. Pada perusahaan ini hanya menggunakan koneksi kabel (*wired*) dan



tidak ada koneksi tanpa kabel (*wireless*).
Sumber: (Insurance, 2022)

Gambar 1. Topologi Jaringan Awal

Dari skema jaringan komputer pada gambar 1, penulis dapat menjelaskan sebagai berikut.

1. Layanan internet yang digunakan di PT Pan Pacific Insurance kantor Graha Panfic menggunakan jasa dari *Internet Service Provider* (ISP) HSP dengan *bandwidth* yang digunakan yaitu dedicated 20 Mbps 1:1 dan mendapatkan IP *Public* prefik /29.
2. Mikrotik ISP digunakan untuk menghubungkan sumber internet dan switch tipe HP.
3. Dari *switch* HP terhubung dengan *router* cisco dan fortigate 501E yang masing-masing memiliki IP *Public* dan IP *Private* sendiri dan masih dalam satu jaringan yang sama. Kemudian dari cisco *router* dan fortigate terhubung dengan *switch* 3Com 1.
4. Dari *switch* 3Com 1 kemudian terhubung dengan *switch* 3Com 2 yang masing menuju ke user dan ke server.
5. Cisco router 2901 digunakan sebagai router utama yang terhubung dengan internet dan melakukan broadcast IP *address* ke jaringan lokal. Selain itu router ini digunakan untuk menguhubungkan daringan di kantor graha panfic dengan jaringan di collocation serta jaringan komputer di kantor utama.
6. Fortigate 501E digunakan untuk memonitoring *bandwitch* dan sebagai *web filter*. Fortigate memiliki IP Public sendiri seperti cisco router, sehingga dapat di akses dari jaringan *public*.

Tabel 1. IP Address

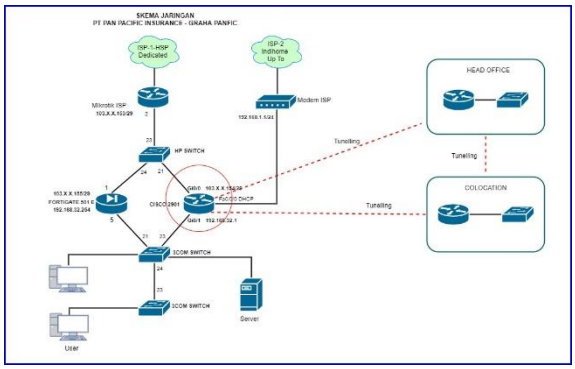
Perangkat	IP Address
Cisco 2901	192.168.32.1/24

Fortigate 501E	192.168.32.254/24
HP-V1410-24	-
3Com Baseline 2024	-
PC User	192.168.32.10 – 239/24

Sumber: (Insurance, 2022)

b. Jaringan Usulan

Rancangan jaringan usulan ini dibuat untuk memenuhi kebutuhan dan menyelesaikan permasalahan yang ada pada jaringan komputer di PT. Pan Pacific Insurance kantor Graha Panfic yang sedang berjalan pada saat ini. Rancangan jaringan ini sebagai alternatif yang dapat di implementasikan dalam meminimalisir permasalahan yang sering terjadi pada jaringan perusahaan.



Sumber: (Riyan, 2022)

Gambar 2. Topologi Jaringan usulan

Pada jaringan usulan, penulis membuat dan mengimplementasikan *load balancing* dengan IP SLA pada cisco *router* 2901, agar dapat menggunakan 2 ISP yang berbeda yang digunakan secara bersamaan dan menentukan jalur terbaik secara otomatis sehingga dapat mengoptimalkan dukungan teknologi informasi terhadap perusahaan. Dalam hal ini penulis menambahkan *Network Interface Card* pada cisco router 2901 dan koneksi internet baru.

2. Konfigurasi Perangkat

a. Konfigurasi Route-map

Fungsi dari *route-map* adalah sebagai *policy besed routing*. Jadi konfigurasi NAT nya nanti akan berdasarkan *route-map* bukan berdasarkan *access list*. Berikut adalah konfigurasi route-map untuk ISP 1 dan ISP 2.

```
RO-DS(config)#route-map ISP-1-HSP permit 10
RO-DS(config-route-map)#match ip address 1
RO-DS(config-route-map)#match interface gi0/0
RO-DS(config-route-map)#exit
RO-DS(config)#
RO-DS(config)#route-map ISP-2-TELKOM permit 10
RO-DS(config-route-map)#match ip address 1
RO-DS(config-route-map)#match interface fa0/0/0
RO-DS(config-route-map)#exit
RO-DS(config)#
```

Sumber: (Riyan, 2022)

Gambar 2. Konfigurasi route-map

Dari gambar 3 dapat dijelaskan sebagai berikut: *route-map* ISP-1-HSP akan mengizinkan IP *address* yang terdaftar pada *list* 1, *list* 1 yaitu *access list* 1 maka akan dikeluarkan melalui *interface GigabitEthernet0/0.* Dan *route-map* ISP-1-TELKOM akan mengizinkan IP address yang terdaftar pada *list* 1, *list* 1 yaitu *access list* 1 maka akan dikeluarkan melalui *interface fastethernet 0/0/0.*

b. Konfigurasi IP SLA

Konfigurasi IP SLA yang akan penulis implementasikan yaitu *icmp-echo. Icmp-echo* akan melakukan pengeceka RTT (*Round Trip Time*) yaitu waktu yang dibutuhkan untuk paket kembali, dan satuan RTT *milisecond.*

```
RO-DS(config)#ip sla 1
RO-DS(config-ip-sla)#icmp-echo 103.1      153 source-interface gi0/0
RO-DS(config-ip-sla-echo)#frequency 10
RO-DS(config-ip-sla-echo)#timeout 5000
RO-DS(config-ip-sla-echo)#exit
RO-DS(config)#ip sla schedule 1 start-time now life forever
RO-DS(config)#track 1 ip sla 1 reachability
RO-DS(config-track)#exit
RO-DS(config)#
RO-DS(config)#
RO-DS(config)#ip sla 2
RO-DS(config-ip-sla)#icmp-echo 192.168.1.1 source-interface fa0/0/0
RO-DS(config-ip-sla-echo)#frequency 10
RO-DS(config-ip-sla-echo)#timeout 5000
RO-DS(config-ip-sla-echo)#exit
RO-DS(config)#ip sla schedule 2 start-time now life forever
RO-DS(config)#track 2 ip sla 2 reachability
RO-DS(config-track)#exit
RO-DS(config)#
RO-DS(config)#
```

Sumber: (Riyan, 2022)

Gambar 3. Konfigurasi IP SLA

Dari gambar 4 dapat dijelaskan IP SLA 1 akan selalu memonitoring paket yang dikirimkan dari interface GigabitEthernet0/0 menuju ke IP *gateway* ISP 1 yaitu 103.X.X.153. *Router* akan melakukan ping selama 10 detik sekali dan jika *round trip time*nya atau RTTnya mencapai 5000 *milisecond* maka sudah melanggar SLA dan dikatakan koneksi internet tidak bagus. IP SLA 1 akan aktif mulai dari sekarang dan selamanya. Begitu juga penjelasan IP SLA 2 akan selalu memonitoring paket yang dikirimkan dari *interface fastethernet 0/0/0.*

c. Konfigurasi Default Route

Melakukan konfigurasi ulang *default route* untuk ISP 1 dan ISP 2 dengan *command* seperti pada gambar 5:

```
RO-DS(config)#ip route 0.0.0.0  0.0.0.0  103.1      .153 track 1
RO-DS(config)#ip route 0.0.0.0  0.0.0.0  192.168.1.1 track 2
Jun 20 12:44:00.404: %BGP-5-ADJCHANGE: neighbor 172.17.48.1 Up
RO-DS(config)#
RO-DS(config)#
```

Sumber: (Riyan, 2022)

Gambar 4. Konfigurasi Default Route

d. Konfigurasi NAT

Mengetikan *command* seperti gambar 6 untuk melakukan konfigurasi NAT nya (*ip nat inside source route-map ISP-1-HSP interface gi0/0 overload*) konfigurasi untuk ISP 1. (*ip nat inside source route-map ISP-2-TELKOM interface fa0/0/0 overload)* konfigurasi untuk ISP 2. Dikarenakan *command*nya panjang, maka dalam gambar 6 terlihat tidak *full*.

```
RO-DS(config)#$de source route-map ISP-1-HSP interface gi0/0 overload
RO-DS(config)#$de source route-map ISP-2-TELKOM interface fa0/0/0 overload
RO-DS(config)#
RO-DS(config)#
```

Sumber: (Riyan, 2022)

Gambar 5 Konfigurasi NAT

3. Pengujian

a. Verifikasi Konfigurasi NAT

Lakukan verifikasi dengan perintah do sh ip nat *statistic* untuk memastikan apakah NAT nya sudah benar atau belum.

```
RO-DS(config)#do sh ip nat statistic
Total active translations: 5 (1 static, 4 dynamic; 5 extended)
Peak translations: 28694, occurred 4d16h ago
Outside interfaces:
  GigabitEthernet0/0, FastEthernet0/0/0
Inside interfaces:
  GigabitEthernet0/1
Hits: 113023738  Misses: 0
CEF Translated packets: 112086889, CEF Punted packets: 926520
Expired translations: 4795678
Dynamic mappings:
-- Inside Source
[Id: 7] route-map ISP-1-HSP interface GigabitEthernet0/0 refcount 0
[Id: 8] route-map ISP-2-TELKOM interface FastEthernet0/0/0 refcount 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
RO-DS(config)#
```

Sumber: (Riyan, 2022)

Gambar 6. Verifikasi Konfigurasi NAT

Jika dilihat pada kolom merah gambar 7, konfigurasi NAT sudah benar. *Outside interface*nya yaitu *interface GigabitEthernet 0/0* dan *FastEthernet 0/0/0* yang terhubung dengan ISP 1 dan ISP 2. Dan inside *interface*nya *yaitu interface GigabitEthernet 0/1* yang terhubung ke jaringan lokal. Serta inside mappingnya sudah benar.

b. Verifikasi Default route

Melakukan verifikasi dengan perintah *do sh ip route*. Jika dilihat pada kolom merah gambar 8, maka default routenya sudah benar yaitu lewat IP 192.168.1.1 sebagai *gateway* ISP 2 dan lewat IP 103.X.218.153 sebagai *gateway* ISP 2.

```
RO-DS(config)#do sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.1.1
                [1/0] via 103      .218.153
      103.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
```

Sumber: (Riyan, 2022)

Gambar 7. Verifikasi Default Route

c. Load Balancing

Melakukan pengujian dengan mengetikan perintah do ping 8.8.8.8 source gi0/1 untuk mengetahui apakah jaringan lokal bisa terhubung dengan dns google. Perintah tersebut maksudnya adalah penulis melakukan ping ke dns google dari *interface* gi0/1, yaitu *interface* dengan IP 192.168.32.1 yang terhubung ke *switch* pada jaringan lokal. Dengan hasil sukses yang bisa dilihat pada kolom hijau pada gambar 9. Artinya jaringan lokal dapat terhubung dengan dns google dan user mendapatkan koneksi internet.

```
RO-DS(config)#do ping 8.8.8.8 source gi0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 192.168.32.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/18/20 ms
RO-DS(config)#
```

Sumber: (Riyan, 2022)

Gambar 8. Ping IP DNS Google

Kemudian mengetikan perintah *do traceroute 8.8.8.8 source gi0/1* untuk mengetahui jalur yang dilewati untuk sampai ke *dns google*. Perintah tersebut maksudnya adalah penulis melakukan pencarian jalur yang dilewati menuju *dns google* dari *interface* gi0/1, yaitu *interface* yang terhubung ke *switch* pada jaringan lokal.

```
RO-DS(config)#do traceroute 8.8.8.8 source gi0/1
Type escape sequence to abort.
Tracing the route to dns.google (8.8.8.8)
VRF info: (vrf in name/id, vrf out name/id)
  1 ip-1   .218.hsp.net (103.   1.218.153) 0 msec
    192.168.1.1 [AS 65001] 0 msec
    ip-1   .218.hsp.net (103.   .218.153) 0 msec
  2 36.83.230.1 4 msec
    10.16.65.237 0 msec
    36.83.230.1 4 msec
  3 ip-129.196.hsp.net.id (103.121.199.129) 0 msec
    180.252.1.178 4 msec
    ip-129.196.hsp.net.id (103.121.199.129) 0 msec
  4 180.252.1.177 4 msec
    103.134.185.4 4 msec
    180.252.1.177 8 msec
  5 72.14.195.20 12 msec *  12 msec
  6 180.240.190.109 16 msec *  *
  7 dns.google (8.8.8.8) 24 msec
    180.240.205.82 16 msec
    dns.google (8.8.8.8) 12 msec
RO-DS(config)#
```

Sumber: (Riyan, 2022)

Gambar 9. Load Balancing

Dari kolom hijau pada gambar 10 dapat dilihat bahwa jalurnya melewati IP 103.X.218.153 yang merupakan *gateway* ISP 1 dan melawati IP 192.168.1.1 yang merupakan *gateway* ISP 2 kemudian sampai ke tujuan yaitu *dns google*. Jadi dari hasil pengujian ini dapat diketahui bahwa *user* yang ada dijaringan lokal dapat terhubung ke internet melalui ISP 1 dan ISP 2 yang artinya bahwa konfigurasi *load balancing* yang diterapkan berhasil. *Load balancing* pada cisco *router* dapat dilihat pada gambar dibawah ini.

d. Failover

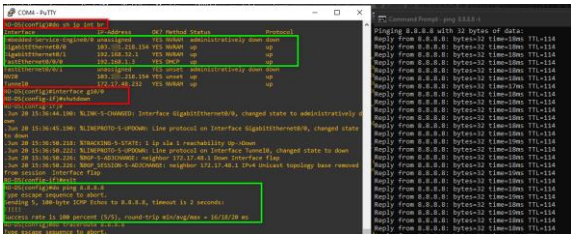
Pada pengujian *failover* ini penulis mematikan koneksi internet antara ISP 1 dan ISP 2 secara bergantian untuk memastikan konfigurasi *failover* berjalan dengan baik. Pertama disimulasikan mematikan koneksi pada ISP 1 dan terakhir mematikan koneksi pada ISP 2.

1) Mematikan koneksi ISP 1

Pertama lakukan verifikasi terlebih dahulu dengan mengetikan perintah *do sh ip int br* untuk mengetahui status pada masing masing *interface*. Jika dilihat pada kolom hijau pada gambar 11 dapat dibaca bahwa status *interface gigabitethernet* 0/0 yang terhubung dengan sumber internet ISP 1 stausnya UP dan *interface fasethernet* 0/0/0 yang terhubung dengan sumber internet ISP 2 statusnya juga UP. Sebelum mematikan koneksi pada ISP 1 penulis melakukan *ping continue* pada laptop penulis ke *dns*

google untuk mengetahui bahwa koneksi internet saat ini sedang berjalan.

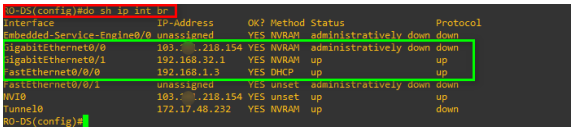
Kemudian penulis mengetikan perintah *interface gi0/0* kemudian *shutdown*, maksud dari perintah ini adalah penulis mematikan *interface* ISP 1. Setelah *interface* mati penulis mengetikan perintah *do ping 8.8.8.8* untuk *ping* ke *dns google* dan hasilnya *success 100 percent* yang artinya berhasil dan ping pada laptop penulis juga masih berjalan.



Sumber: (Riyan, 2022)

Gambar 10. Mematikan ISP 1

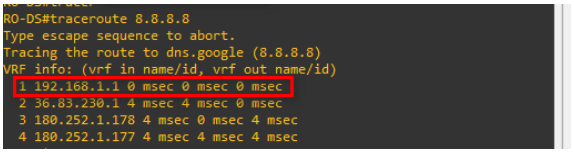
Melakukan pengecekan dengan mengetikan perintah *do sh ip int br* untuk melihat status *interface*. Dapat dilihat pada gambar 12 bahwa *interface gigabitethernet* 0/0 statusnya *down*.



Sumber: (Riyan, 2022)

Gambar 11. Status Interface GigabitEthernet0/0

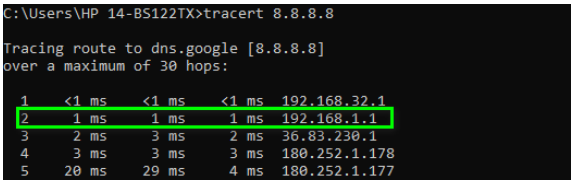
Lalu *traceroute* ke *dns google* dari *router*. Dari gambar 13 dapat dilihat bahwa jalur menuju ke *dns google* melewati IP ISP 2.



Sumber: (Riyan, 2022)

Gambar 12. *Trace route* dari router

Lalu *traceroute* ke *dns google* dari laptop penulis. Dari gambar 14 dapat diketahui bahwa jalur menuju ke *dns google* juga melewati ISP 2.



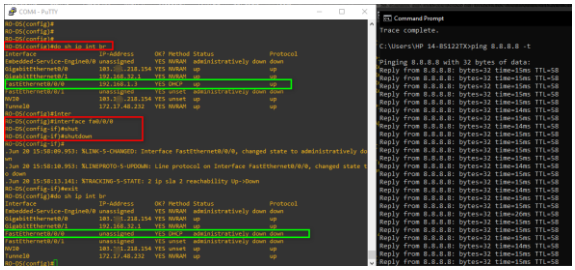
Sumber: (Riyan, 2022)

Gambar 13. Traceroute dari laptop user

Dari hasil pengujian diatas dapat diketahui bahwa teknik *failover* yang diterapkan pada jaringan komputer PT Pan Pacific Insurance berhasil di Jalankan. Selanjutnya pengujian failover terakhir yaitu menghidupkan kembali koneksi ISP 1 dan mematikan koneksi ISP 2.

1) Mematikan Koneksi ISP 2

Langkahnya hampir sama seperti sebelumnya, yang membedakan hanya *interface* yang dimatikan.



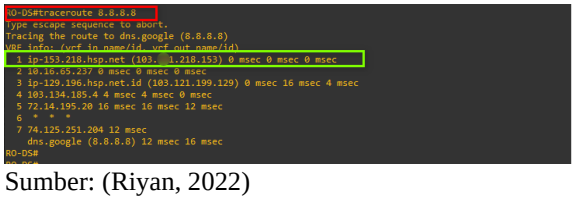
Sumber: (Riyan, 2022)

Gambar 14. Mematikan Koneksi ISP 2

Pertama melakukan verifikasi terlebih dahulu dengan mengetikan perintah *do sh ip int br* untuk mengetahui status pada masing masing *interface*. Jika dilihat pada kolom hijau pada gambar 15 dapat dibaca bahwa status *interface gigabitethernet* 0/0 yang terhubung dengan sumber internet ISP 1 stausnya UP dan *interface fasethernet* 0/0/0 yang terhubung dengan sumber internet ISP 2 statusnya juga UP. Sebelum mematikan koneksi pada ISP 2 penulis melakukan *ping continue* pada laptop penulis ke *dns google* untuk mengetahui bahwa koneksi internet saat ini sedang berjalan.

Kemudian penulis melakukan pengetikan perintah *interface fa0/0/0* kemudian *shutdown*, maksud dari perintah ini adalah penulis mematikan *interface* ISP 2. Setelah *interface* mati penulis mengetikan perintah *do sh ip int br* untuk melihat status semua *interface*, dapat dilihat pada kolom hijau pada gambar paling bawah, bahwa *interface fastethernet* 0/0/0 statusnya *down.* Dan status *ping continue* ke IP DNS *google* masih berjalan.

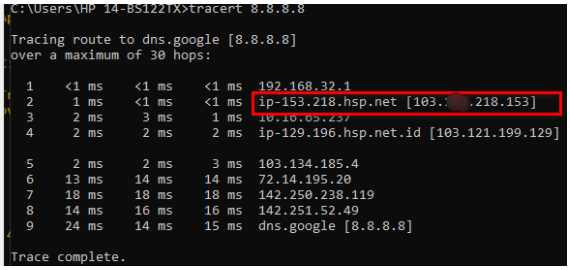
Lalu *traceroute* ke *dns google* dari *router*. Dari gambar 16 dapat dilihat bahwa jalur menuju ke *dns google* melewati IP ISP 1.



Sumber: (Riyan, 2022)

Gambar 15. Traceroute dari router

kemudian *traceroute* ke *dns google* dari laptop penulis. Dari gambar 17 dapat diketahui bahwa jalur menuju ke *dns google* juga melewati ISP 1. hasil tersebut menujukan hasil bahwa dengan diterapkan teknik *load balancing* dan *failover* menggunakan IP SLA berjalan dengan baik.



Sumber: (Riyan, 2022)

Gambar 16. Traceroute dari Laptop Penulis

KESIMPULAN

Berdasarkan data dan informasi tentang jaringan komputer yang telah dilakukan pengecekan, simulasi dan implementasi oleh penulis selama penelitian pada PT Pan Pacific Insurance, didapatkan kesimpulan:

Pada awal penelitian jaringan komputer pada PT Pan Pacific Insurance masih menggunakan satu ISP untuk menunjang berjalannya operasional perusahaan. Saat ini PT Pan Pacific insurance sudah menggunakan dua ISP yang berbeda. ISP 1 dari HSP Net menggunakan layanan internet *dedicated* dan ISP dua dari Telkom Indihome menggunakan layanan internet UP To.

Konfigurasi dan implementasi *load balancing* dan *failover* yang telah diterapkan berjalan dengan baik menggunakan perangkat cisco *router*. Hal ini dapat mengatasi permasalahan apabila terjadi gangguan pada salah satu ISP.

Konfigurasi IP SLA yang dilakukan akan memberi perintah pada *router* untuk melakukan pengecekan *Round Trip* Time (RTT) yaitu waktu yang dibutuhkan paket untuk kembali, dan satuan RTT *milisecond*. *Router* akan melakukan *ping* selama 10 detik sekali dan jika round trip timenya atau RTTnya mencapai 5000 *milisecond* maka sudah melanggar SLA dan dikatakan koneksi internet tidak bagus.

REFERENSI

Ardhiansyah, M., Noris, S., & Andrianto, R. (2020). *Jaringan komputer* (Issue 1). Unpam Press.

Armanto, A. (2017). Perancangan Pengelolahan Jaringan Load Balancing Dan Fileover Menggunakan Router Mikrotik Rb 951 Series Pada Stkip Pgri Lubuklinggau. *Jusikom : Jurnal Sistem Komputer Musirawas*, *2*(2), 87–95.

Dani, R., & Suryawan, F. (2017). Perancangan dan Pengujian Load Balancing dan Failover Menggunakan NginX. *Khazanah Informatika: Jurnal Ilmu Komputer Dan Informatika*, *3*(1), 43. https://doi.org/10.23917/khif.v3i1.2939

Gofindo Malau, B. (2022). Implementasi Load Balancing Mikrotik Jaringan Internet Di Pardamean Sibisa, Ajibata, Toba Samosir, Sumatra Utara. *Journal of Computer Science and Technology (JCS-TECH)*, *2*(1), 20–29. https://doi.org/10.54840/jcstech.v2i1.23

Insurance, P. P. (2022). *Topologi Jaringan dan Spesifikasi Perangkat serta IP Address*. PT Pan Pacific Insurance.

Irfan Oktavianto dan, M., Risah Prayogi, Y., & Raya ITS Sukolilo Surabaya, J. (2019). Sistem Monitoring Jaringan Load balancing Dengan Metode Equal Cost Multipath (ECMP) Menggunakan Media Telegram. *Jurnal Ilmu Komputer Dan Desain Komunikasi Visual*, *4*(2), 18–33.

Mustofa, A., & Ramayanti, D. (2020). Implementasi Load Balancing dan Failover to Device Mikrotik Router Menggunakan Metode NTH (Studi Kasus: PT.GO-JEK Indonesia). *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *7*(1), 139. https://doi.org/10.25126/jtiik.2020701638

Primartha, R. (2019). *Manajemen Jaringan Komputer Teori dan Praktik*. Informatika Bandung.

Rachman, O. (2019). *Panduan Lengkap Instalasi Dan Konfigurasi Jaringan LAN-WAN-Wireless-Fiber Optik - Berbasis IoT Industri 4.0*. Penerbit ANDI.

Suryanto, Prasetyo, T., & Hikmah, N. (2018). Implementasi Load Balancing Menggunakan Metode Per Connection Classifier (PCC) Dengan Failover Berbasis Mikrotik Router. *Seminar Nasional Inovasi Dan Tren (SNIT)*, *1*(1), A230–A238.