JURNAL LITEK : Jurnal Listrik Telekomunikasi Elektronika, Vol. 19, No. 2, September 2022, pp. 48~56
pISSN: 1693-8097; eISSN: 2549-8762

ANALISIS DAN SIMULASI *ROUTING BORDER GATEWAY PROTOCOL* (BGP) ANTAR *AUTONOMOUS SYSTEM* MENGGUNAKAN *FREE RANGE ROUTING* (FRR)

Muhammad Sahal Nurhidayah[1], Dadiek Pranindito[2], Reni Dyah Wahyuningrum[3]

[1,2,3]Fakultas Teknik Telekomunikasi dan Elektro, Institut Teknologi Telkom Purwokerto
Email: 18101201@ittelkom-pwt.ac.id[1], dadiek@ittelkom-pwt.ac.id[2], reni@ittelkom-pwt.ac.id[3]

Abstrak – Perkembangan dunia teknologi yang begitu pesat membuat pertukaran data dalam komunikasi global sangatlah penting. Agar pertukaran data antar perusahaan dapat berkomunikasi satu dengan lainnya menggunakan perangkat yang memiliki nilai biaya rendah dan kehandalan yang tinggi, maka menerapkan metode *routing Border Gateway Protocol* (BGP) menggunakan *Free Range Routing* (FRR). FRR merupakan *software* yang dibuat dari kolaborasi antara cumulus foundation dan linux foundation yang difungsikan berjalan di layer *network* dan dapat menjalankan *routing protocol* BGP. Penelitian ini menggunakan protokol *User Datagram Protocol* (UDP) untuk memeriksa kualitas jaringan topologi 1 (4 FRR) dan topologi 2 (6 FRR) di berbagai ukuran data, yaitu 10 MB, 20 MB, 30 MB, 40 MB, dan 50 MB dengan menggunakan skenario tanpa *failover* dan *failover*. Pengujian topologi 1 dengan skenario tanpa *failover* menunjukan nilai rata-rata *throughput* 10,805 Mbps, rata-rata *delay* 3,441 ms, rata-rata *jitter* 0,747 ms, rata-rata *packet loss* 0%, pada skenario *failover* nilai rata-rata *throughput* 10,754 Mbps, rata-rata *delay* 100,039 ms, rata-rata *jitter* 0,928 ms, rata-rata *packet loss* 0,349%. Pengujian topologi 2 dengan skenario tanpa *failover* menunjukan nilai rata-rata *throughput* 10,797 Mbps, rata-rata *delay* 124,786 ms, rata-rata *jitter* 1,132 ms, rata-rata *packet loss* 0%, pada skenario *failover* dengan rute *failover* terbaik menunjukkan nilai rata-rata *throughput* 10,734 Mbps, rata-rata *delay* 445,864 ms, rata-rata *jitter* 1,096 ms, rata-rata *packet loss* 0,341%. Pada dua topologi pengujian, hasil dari parameter *Quality of Service* (QoS) menggunakan topologi 1 lebih baik daripada topologi 2. Hasil pengujian dikategorikan performa "sangat baik" pada skenario tanpa *failover* dan dikategorikan performa "sangat baik" hingga "sedang" pada skenario *failover*.

Kata-kata kunci: BGP, FRR, QoS, UDP, Failover

Abstract – The rapid development of the world of technology makes data exchange in global communication very important. In order for data exchange between companies to communicate with each other using devices that have low cost and high reliability, the Border Gateway Protocol (BGP) routing method uses Free Range Routing (FRR). FRR is software created from a collaboration between cumulus foundation and linux foundation which is enabled to run at the network layer and can run the BGP routing protocol. This study uses the User Datagram Protocol (UDP) protocol to check the network quality of topology 1 (4 FRR) and topology 2 (6 FRR) in various data sizes, namely 10 MB, 20 MB, 30 MB, 40 MB, and 50 MB using scenarios without failover and failover. The test of topology 1 with scenario without failover shows the average throughput value is 10.805 Mbps, the average delay is 3.441 ms, the average jitter is 0.747 ms, the average packet loss is 0%, in the failover scenario the average throughput is 10.754 Mbps, the average the average delay is 100.039 ms, the average jitter is 0.928 ms, the average packet loss is 0.349%. Testing topology 2 with scenarios without failover shows an average throughput value of 10,797 Mbps, an average delay of 124,786 ms, an average jitter of 1,132 ms, an average packet loss of 0%, in a failover scenario with the best failover route, the average value shows throughput 10,734 Mbps, average delay 445.864 ms, average jitter 1.096 ms, average packet loss 0.341%. In the two test topologies, the results of the Quality of Service (QoS) parameter using topology 1 are better than topology 2. The test results are categorized as "very good" performance in the scenario without failover and categorized as "very good" to "moderate" performance in the failover scenario.

Key words: BGP, FRR, QoS, UDP, Failover

I. PENDAHULUAN

Perkembangan dunia teknologi yang begitu pesat membuat pertukaran data dalam komunikasi sangatlah penting, agar pertukaran data antar perusahaan dapat berkomunikasi satu dengan lainnya menggunakan perangkat yang memiliki nilai biaya rendah dan kehandalan yang tinggi, maka menerapkan metode *routing Border Gateway Protocol* (BGP) menggunakan *Free Range Routing* (FRR).

BGP merupakan salah satu jenis *routing protocol* yang berfungsi untuk menghubungkan jaringan antar AS yang berbeda. *Routing protocol* yaitu algoritma yang digunakan untuk mengatur proses *routing*. *Routing* yaitu proses memilih rute yang akan ditempuh oleh sebuah paket data dalam suatu jaringan komputer dan

perangkat yang digunakan untuk melakukan *routing* yaitu router [1].

AS yaitu sekelompok router yang membentuk jaringan yang masih berada dalam satu administrasi atau satu kepemilikan yang sama dan dikonfigurasi menggunakan aturan yang sama [2]. FRR merupakan *project open source* yang dibuat dari kolaborasi antara cumulus foundation dan linux foundation yang berperan sebagai router untuk melakukan *routing*. FRR hanya dapat berjalan di sistem operasi linux dan dapat menerapkan routing protocol seperti: BGP, OSPF, IS-IS, EIGRP [3]. QoS yaitu metode pengukuran tentang seberapa baik jaringan dan suatu usaha untuk mendefinisikan karakteristik dan sifat dari satu layanan serta berfungsi untuk mengukur kemampuan sebuah jaringan dalam menyediakan layanan lalu lintas komunikasi data [4].

Beberapa penelitian terkait *routing* BGP sudah dilakukan, penelitian [1] membahas mengenai simulasi interkoneksi antara *Autonomous System* (AS) menggunakan *Border Gateway Protocol* (BGP), dengan menggunakan *software* cisco packet tracert 7.0. Dasar dari penggunaan *routing protocol* BGP yaitu untuk interkoneksi antar kampus yaitu karena masing-masing kampus menggunakan AS yang berbeda. Kampus I menggunakan AS 100 dan kampus II menggunakan AS 200. Agar kedua kampus tersebut dapat interkoneksi satu sama lain, maka menggunakan penerapan *routing protocol* BGP. Pada penelitian [5] membahas mengenai implementasi penerapan jaringan *Multihome* menggunakan *routing protocol* BGP di Fakultas Hukum Universitas Udayana (UNUD). Dalam penjelasannya, jaringan komputer pada Fakultas hukum UNUD memiliki koneksi ke GDLN Udayana. Ketika Fakultas Hukum melakukan akses internet, harus melalui jalur GDLN sebagai jalur keluarnya untuk menuju internet. Jika jalur GDLN terjadi *down* atau gangguan koneksi, maka Fakultas Hukum tidak dapat mengakses internet. Oleh karena itu, jaringan komputer Fakultas Hukum menerapkan jaringan *Multihoming* menggunakan *routing protocol* BGP agar jika jalur GDLN terjadi *down*, Fakultas Hukum tetap bisa mengakses internet melalui jalur alternatif yaitu jalur ISP. Penelitian [6] membahas mengenai simulasi teknologi DMVPN pada *routing protocol* BGP menggunakan perangkat lunak *Free Range Routing* (FRR). Dalam penjelasanya, DMVPN merupakan salah satu jenis teknologi dari VPN. Pada DMVPN, komunikasinya secara *point to multipoint* di jalur tunnel yang artinya dapat menghubungkan beberapa *site* yang jumlahnya banyak dengan menggunakan 1 jalur tunnel. Metode penerapan DMVPN menggunakan *routing protocol* BGP di FRR. Dari penelitian tersebut, menjelaskan bahwa DMVPN menggunakan *routing protocol* BGP di FRR.

Berdasarkan literatur tersebut, maka penelitian ini akan melakukan simulasi ro*uting protocol* BGP antar AS menggunakan FRR. Penelitian ini berbeda pada 3 penelitian literatur tersebut, yang menjadi pembeda yaitu menggunakan perangkat router berbasis *open source* yaitu FRR. Penelitian ini bertujuan untuk menguji performansi *Quality of Service* (QoS) pada topologi 1 dan 2 dengan menggunakan skenario tanpa *failover* (rute utama) dan *failover* (rute backup). Parameter QoS yang diujikan yaitu *throughput*, *delay*, *jitter*, dan *packet loss*. Pengiriman paket data menggunakan protokol *User Datagram Protocol* (UDP).

II. METODOLOGI

Penelitian ini melakukan simulasi *routing protocol* BGP antar AS menggunakan FRR. Terdapat 2 skenario topologi yang digunakan yaitu topologi 1 (4 router FRR) dengan 1 rute *failover* atau *backup* dan topologi 2 (6 router FRR) dengan 3 rute *failover* atau *backup*, serta kedua topologi tersebut menerapkan skema *Exterior Border Gateway Protocol* (EBGP). Metode pengiriman paket data yaitu pengirim (*Client-Core*) mengirimkan paket data menuju penerima (*Client-Tech*) menggunakan protokol UDP sebanyak 30 kali percobaan untuk mendapatkan hasil data yang akurat. Besar data yang dikirimkan yaitu 10 MB, 20 MB, 30 MB, 40 MB, dan 50 MB. Simulasi yang diterapkan dalam penelitian ini menggunakan *Graphical Network Simulator* (GNS3), *Software Disributed Internet Traffic Generator* (D-ITG) digunakan untuk mengukur nilai parameter *Quality of Service* (QoS), dan Wireshark digunakan untuk menganalisis data dan *capture packet*.

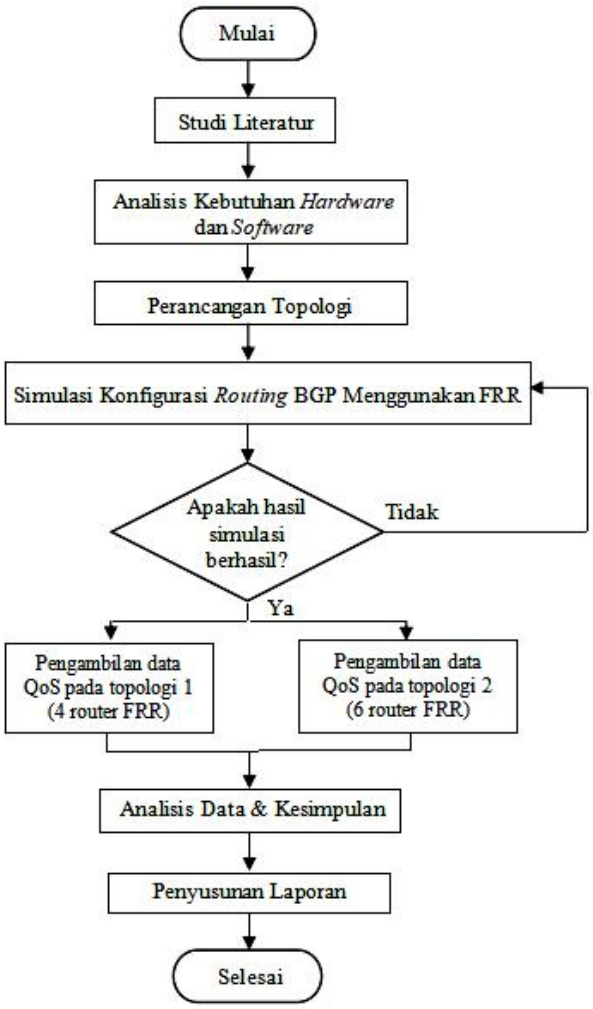
A. Alur Penelitian

Gambar 1 merupakan alur kerja penelitian. Tahap pertama yaitu memahami studi literatur dari penelitian sebelumnya yang akan dijadikan tinjauan pustaka penelitian ini. Adanya tinjauan pustaka digunakan untuk memahami konsep dasar yang menjadi rujukan penelitian. Tahap kedua yaitu menjelaskan tentang kebutuhan *hardware* dan *software* yang digunakan dalam penelitian ini.

Tahap selanjutnya yaitu melakukan perancangan topologi jaringan yang akan digunakan. Penelitian ini menggunakan topologi jenis *partial mesh* yaitu topologi 1 menggunakan 4 router FRR dan 2 client sebagai pengirim dan penerima dengan 1 rute *failover*, sedangkan topologi 2 menggunakan 6 router FRR dan 2 client sebagai pengirim dan penerima dengan 3 rute *failover*. Perangkat router menggunakan sistem operasi linux Ubuntu Server 18.04 LTS yang telah terinstal FRR dan perangkat *client* menggunakan sistem operasi Ubuntu Desktop 18.04 LTS yang telah terinstall D-ITG.

Selanjutnya menerapkan simulasi konfigurasi *routing protocol* BGP antar AS menggunakan FRR. Jika penerapan simulasi konfigurasi berhasil, maka akan dilanjutkan dengan pengambilan data QoS. Namun jika penerapan simulasi konfigurasi tidak berhasil, maka melakukan penerapan simulasi konfigurasi routing protocol BGP lagi sampai berhasil. Proses pengambilan data QoS pada topologi 1 dan topologi 2 dengan skenario tanpa *failover* dan *failover* dilakukan dengan pengujian protokol UDP, dengan menggunakan *software* D-ITG untuk menguji nilai parameter

throughput, *delay*, *jitter*, dan *packet loss* dan Wireshark untuk menganalisis data. Tahap selanjutnya yaitu dilakukan proses penyusunan laporan dengan tujuan untuk pembukuan penelitian dan dokumentasi penelitian.



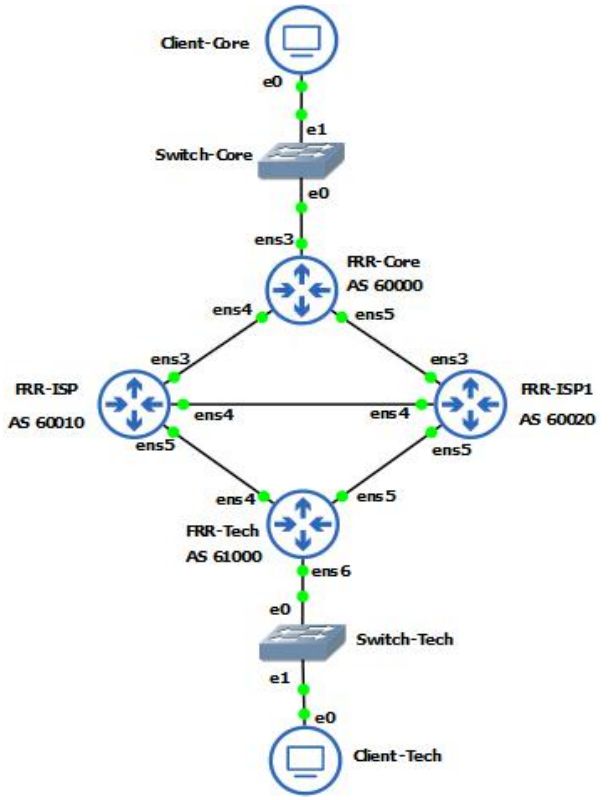
Gbr.1 Alur Penelitian

B. Skenario Topologi Jaringan

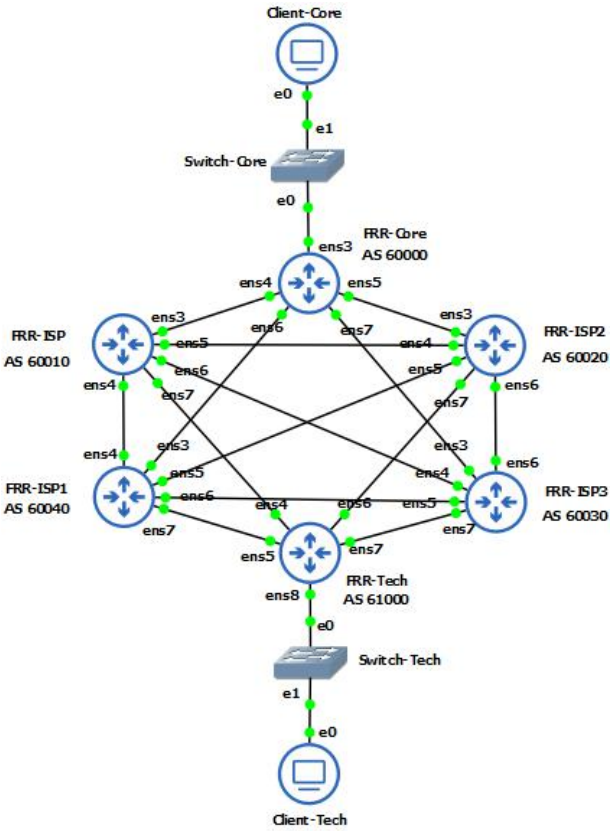
Topologi 1 pada Gambar 2, dilakukan simulasi *routing protocol* BGP menggunakan 4 router FRR. FRR-Core menggunakan ASN 60000, FRR-ISP menggunakan ASN 60010, FRR ISP1 menggunakan ASN 60020, dan FRR-Tech menggunakan ASN 61000 dengan rute utama menuju FRR-ISP dan rute *backup* menuju FRR-ISP1. Kemudian dilakukan pengujian QoS.

Topologi 2 pada Gambar 3 dilakukan simulasi *routing protocol* BGP menggunakan 6 router FRR. FRR-Core menggunakan ASN 60000, FRR-ISP menggunakan ASN 60010, FRR ISP1 menggunakan ASN 60040, FRR-ISP2 menggunakan ASN 60020, FRR-ISP3 menggunakan ASN 60030, dan FRR-Tech menggunakan ASN 61000 dengan rute utama menuju FRR-ISP dan rute *backup* menuju FRR-ISP1, FRR-ISP2, dan FRR-ISP3. Kemudian dilakukan pengujian QoS.

Pengujian QoS berfungsi untuk mengetahui performansi kinerja dan kualitas layanan protokol UDP pada kedua topologi tersebut, apakah sesuai dengan standarisasi TIPHON atau tidak.



Gbr. 2 Topologi 1 (4 router FRR)



Gbr. 3 Topologi 2 (6 router FRR)

C. Instalasi dan Konfigurasi FRR

Peneliti melakukan instalasi perangkat lunak FRR pada virtual OS Linux-Ubuntu Server 18.04 LTS. Pembuatan virtual OS menggunakan aplikasi *Virt-Manager* karena format *disk/image* yang dihasilkan *Virt-Manager* berbentuk ekstensi *QEMU copy-on-write format* (*.qcow2*). Dengan format *image* .qcow2, virtual OS yang sudah dibuat dapat berjalan pada QEMU VMs yang terdapat di GNS3 pada GNS VMWare. Instalasi perangkat lunak FRR dapat dilakukan setelah selesai melakukan instalasi Linux-Ubuntu Server 18.04 LTS. Versi FRR yang digunakan yaitu 7.5.1. Gambar 4 yaitu tahap instalasi FRR.

```
$ curl -s https://deb.frrouting.org/frr/keys.asc | sudo apt-key
add -

$ FRRVER="frr-stable"

echo deb https://deb.frrouting.org/frr $(lsb_release -s -c)
$FRRVER | sudo tee -a /etc/apt/sources.list.d/frr.list

$ sudo apt update && sudo apt install frr frr-pythontools
```

Gbr. 4 Tahap instalasi FRR

Konfigurasi daemons berfungsi untuk mengaktifkan atau menonaktifkan *routing protocol* dan *service* yang akan digunakan pada FRR. Untuk mengaktifkan *service* FRR yang akan digunakan, dapat dilakukan pada file "/etc/frr/daemons". Peneliti mengaktifkan BGP sebagai *routing protocol* dalam melakukan simulasi penelitian ini. Mengaktifkan *service routing protocol* BGP dengan mengatur menjadi "bgpd=yes". Gambar 5 yaitu mengaktifkan *service daemons* BGP.

```
 GNU nano 2.9.3                  /etc/frr/daemons                    Modified

# This file tells the frr package which daemons to start.
#
# Sample configurations for these daemons can be found in
# /usr/share/doc/frr/examples/.
#
# ATTENTION:
#
# When activating a daemon for the first time, a config file, even if it is
# empty, has to be present *and* be owned by the user and group "frr", else
# the daemon will not be started by /etc/init.d/frr. The permissions should
# be u=rw,g=r,o=.
# When using "vtysh" such a config file is also needed. It should be owned by
# group "frrvty" and set to ug=rw,o= though. Check /etc/pam.d/frr, too.
#
# The watchfrr, zebra and staticd daemons are always started.
#
bgpd=yes
ospfd=no
ospf6d=no

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

Gbr. 5 Mengaktifkan *service daemons* BGP

D. Konfigurasi BGP

Pada topologi 1 dan topologi 2 bertujuan untuk mengirimkan paket data protokol UDP dari sisi pengirim (*Client*-Core) menuju sisi penerima (*Client*-Tech) menggunakan metode *routing protocol* BGP. Topologi 1 dan 2 pada router FRR, masing-masing memiliki *Autonomous System Number* (ASN) yang berbeda-beda. Jadi, semua router interkoneksi menggunakan jenis EBGP. Konfigurasi *routing protocol* BGP dilakukan pada file konfigurasi *bgpd.conf* dengan letak file pada "/etc/frr/bgpd.conf".

Gambar 6 yaitu salah satu konfigurasi BGP pada router FRR-Core. Pada FRR-Core, menggunakan ASN yaitu 60000. Perintah *no bgp ebgp-requires-policy* berfungsi untuk memfilter paket data yang masuk dan keluar dari FRR-Core. Rute router tetangga digunakan sebagai rute paket data menuju penerima yaitu 11.11.11.2 (FRR-ISP) dan 12.12.12.12 (FRR-ISP1). Perintah *network* 1.1.1.1/32, *network* 11.11.11.0/30, *network* 12.12.12.0/30, dan *network* 192.168.10.0/24 berfungsi untuk menentukan *network address* yang di-*advertise* oleh *routing protocol* BGP pada FRR-Core.

```
 GNU nano 2.9.3                  /etc/frr/bgpd.conf

router bgp 60000
 no bgp ebgp-requires-policy
 neighbor 11.11.11.2 remote-as 60010
 neighbor 12.12.12.2 remote-as 60020
 network 1.1.1.1/32
 network 11.11.11.0/30
 network 12.12.12.0/30
 network 192.168.10.0/24
```

Gbr. 6 Konfigurasi BGP Router FRR

E. Konfigurasi Attribute BGP

Attribute BGP berfungsi untuk menentukan rute terbaik pengiriman paket data dari *Client*-Core menuju *Client*-Tech. *Attribute* BGP yang digunakan pada topologi 1 dan topologi 2 yaitu *local preference*. Pada *attribute local preference*, lebih memilih rute *local preference* yang lebih tinggi daripada rute *local preference* yang rendah untuk menentukan rute terbaiknya.

Gambar 7 yaitu salah satu konfigurasi *attribute* BGP pada router FRR-Core. Pada FRR-Core, *route-map* berfungsi untuk memfilter paket data yang masuk dan keluar dengan menerapkan tindakan pada rute.

```
 GNU nano 2.9.3                  /etc/frr/bgpd.conf

router bgp 60000
 bgp router-id 192.168.10.1
 no bgp ebgp-requires-policy
 neighbor 11.11.11.2 remote-as 60010
 neighbor 12.12.12.2 remote-as 60020
 neighbor 11.11.11.2 route-map localpref in
 neighbor 12.12.12.2 route-map localprefe in
 network 1.1.1.1/32
 network 11.11.11.0/30
 network 12.12.12.0/30
 network 192.168.10.0/24
!
route-map localpref permit 10
 set local-preference 200
!
route-map localprefe permit 20
 set local-preference 150
!
```

Gbr. 7 Konfigurasi *attribute local preference*

Perintah *route-map localpref* permit 10 berfungsi untuk mengkonfigurasi nama *route*-map rute utama yaitu *localpref* dan dizinkan. Perintah *set local preference* 200 berfungsi untuk menentukan rute *local-preference* untuk nilai *localperf* yaitu 200. Perintah

neighbor 11.11.11.2 *route-map localpref in* berfungsi sebagai rute utama (FRR-ISP) dan *in* untuk menetapkan *localpref* ke rute masuk FRR-Core. Perintah *route-map localprefe* permit 20 berfungsi untuk mengkonfigurasi nama *route*-map rute *backup* yaitu *localprefe* dan dizinkan. Perintah *set local preference* 150 berfungsi untuk menentukan rute *local-preference* untuk nilai *localperfe* yaitu 150. Perintah *neighbor* 12.12.12.2 *route-map localprefe in* berfungsi sebagai rute *backup* (FRR-ISP1) dan *in* untuk menetapkan *localprefe* ke rute masuk FRR-Core.

F. Skenario *Failover* dan *Traceroute*

Pada topologi 1, skenario *failover*-nya yaitu jika router FRR-ISP mengalami *down*, maka rute akan dialihkan ke rute *failover* atau *backup* pada FRR ISP1 untuk menuju penerima (*Client*-Tech). Sedangkan pada topologi 2, skenario *failover*-nya yaitu jika router FRR-ISP mengalami *down*, maka rute akan dialihkan 3 rute *failover* atau *backup* menuju *Client*-Tech yaitu rute *backup* pertama pada FRR-ISP1, rute *backup* kedua pada FRR-ISP2, dan rute *backup* ketiga pada FRR-ISP3. Perintah "*traceroute* <IP tujuan>" digunakan untuk mengetahui rute yang dilewati menuju penerima saat pengiriman protokol paket data UDP.

G. Pengambilan Data QoS

Tahap pengujian QoS pada topologi 1 dan topologi 2 menggunakan *software* D-ITG. Metode yang digunakan yaitu sisi pengirim (*Client*-Core) mengirimkan paket data protokol UDP menuju sisi penerima (*Client*-Tech) sebanyak 30 kali pengujian, untuk mendapatkan hasil data yang akurat dari setiap besar data yang dikirimkan yaitu 10 MB, 20 MB, 30 MB, 40 MB, dan 50 MB.

III. HASIL DAN PEMBAHASAN

A. Pengujian QoS

Pengujian QoS dilakukan untuk menentukan performansi kinerja terbaik dari topologi 1 (4 router FRR) dan topologi 2 (6 router FRR) dalam menerapkan protokol UDP sebagai pengiriman paket data menggunakan *software* D-ITG. Terdapat 5 besaran data yang diujikan pada topologi 1 dan 2 yaitu 10 MB, 20 MB, 30 MB, 40 MB, dan 50 MB.

Pengujian QoS dilakukan dengan 2 skenario yaitu saat tidak terjadi *failover* (menggunakan rute utama) dan terjadi *failover* (menggunakan rute *backup*). Perintah *./ITG-CORE.sh* berfungsi untuk menjalankan atau mengeksekusi *script ITG-CORE.sh* yang bertujuan untuk menguji QoS dan mengirimkan paket data protokol UDP kepada penerima (*Client*-Tech). Perintah *ITG-Recv* berfungsi untuk menerima paket data dari *Client*-Core dan file *log receiver* berfungsi untuk menampilkan informasi hasil pengujian parameter QoS sebanyak 30 kali. Gambar 8 yaitu pengujian QoS pada *Client*-Core dan Gambar 9 yaitu pengujian QoS pada *Client*-Tech.

```
eve@Client-Core:~$ ./ITG-CORE.sh
Pengambilan data UDP 10MB
ITGSend version 2.8.1 (r1023)
Compile-time options: sctp dccp bursty multiport
Started sending packets of flow ID: 1
Finished sending packets of flow ID: 1

Pengambilan data UDP 10MB
ITGSend version 2.8.1 (r1023)
Compile-time options: sctp dccp bursty multiport
Started sending packets of flow ID: 1
Finished sending packets of flow ID: 1
```

Gbr. 8 Pengujian QoS pada *Client*-Core

```
eve@Client-Tech:~$ ITGRecv
ITGRecv version 2.8.1 (r1023)
Compile-time options: sctp dccp bursty multiport
Press Ctrl-C to terminate
Listening on UDP port : 8999
Finish on UDP port : 8999
eve@Client-Tech:~/QOS/udp/10mb/receiver$ ls
receiver_udp_10mb_Data-1   receiver_udp_10mb_Data-19  receiver_udp_10mb_Data-28
receiver_udp_10mb_Data-10  receiver_udp_10mb_Data-2   receiver_udp_10mb_Data-29
receiver_udp_10mb_Data-11  receiver_udp_10mb_Data-20  receiver_udp_10mb_Data-3
receiver_udp_10mb_Data-12  receiver_udp_10mb_Data-21  receiver_udp_10mb_Data-30
receiver_udp_10mb_Data-13  receiver_udp_10mb_Data-22  receiver_udp_10mb_Data-4
receiver_udp_10mb_Data-14  receiver_udp_10mb_Data-23  receiver_udp_10mb_Data-5
receiver_udp_10mb_Data-15  receiver_udp_10mb_Data-24  receiver_udp_10mb_Data-6
receiver_udp_10mb_Data-16  receiver_udp_10mb_Data-25  receiver_udp_10mb_Data-7
receiver_udp_10mb_Data-17  receiver_udp_10mb_Data-26  receiver_udp_10mb_Data-8
receiver_udp_10mb_Data-18  receiver_udp_10mb_Data-27  receiver_udp_10mb_Data-9
eve@Client-Tech:~/QOS/udp/10mb/receiver$
```

Gbr. 9 Pengujian QoS pada *Client*-Tech

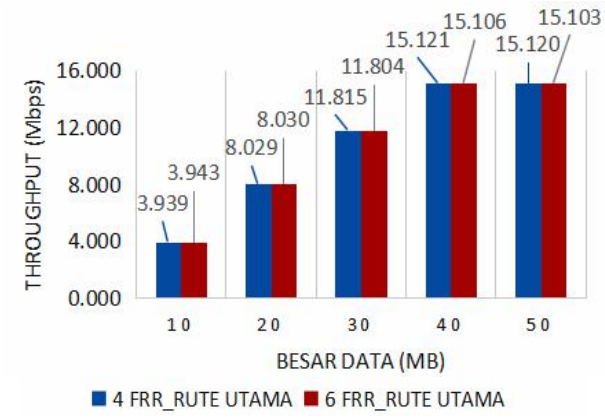
B. Analisis *Throughput*

Pada pengukuran protokol UDP dengan skenario tanpa *failover* (rute utama) di topologi 1 (4 router FRR), besar data 10 MB diperoleh nilai rata-rata *throughput* yaitu 3,939 Mbps, sedangkan pada skenario *failover* (rute *failover* atau *backup*) diperoleh nilai rata-rata *throughput* yaitu 3,931 Mbps. Peningkatan nilai *throughput* sejalan dengan peningkatan besar ukuran data yag diujikan pada skenario tanpa *failover* dan *failover*. Pada skenario tanpa *failover*, nilai *throughput* terjadi peningkatan tertinggi pada besar data 40 MB dengan nilai rata-rata yaitu 15,121 Mbps, sedangkan pada skenario *failover* terjadi peningkatan tertinggi pada besar data 40 MB dengan nilai rata-rata yaitu 15,037 Mbps.

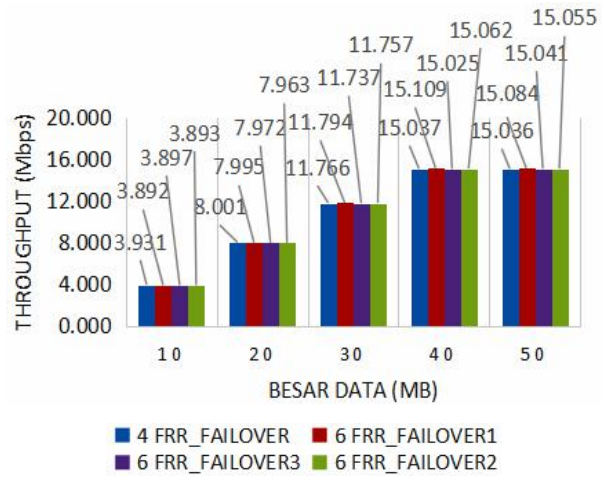
Pada pengukuran protokol UDP dengan skenario tanpa *failover* di topologi 2 (6 router FRR), besar data 10 MB diperoleh nilai rata-rata *throughput* yaitu 3,943 Mbps. Sedangkan pada skenario *failover*, diperoleh nilai rata-rata *throughput failover1* yaitu 3,892 Mbps, nilai rata-rata *throughput failover2* yaitu 3,893 Mbps, dan nilai rata-rata *throughput failover3* yaitu 3,897 Mbps. Pada skenario tanpa *failover*, Nilai *throughput* terjadi peningkatan tertinggi pada besar data 50 MB dengan nilai rata-rata yaitu 15,113 Mbps. Sedangkan pada skenario *failover*, terjadi peningkatan tertinggi pada besar data 40 MB dengan nilai rata-rata *throughput failover1* yaitu 15,109 Mbps, nilai rata-rata *throughput failover2* yaitu 15,062 Mbps, dan nilai rata-rata *throughput failover3* yaitu 15,041 Mbps.

Oleh karena itu, pengukuran *parameter throughput* pada topologi 1 dan topologi 2 dapat dikategorikan memiliki kualitas optimalisasi yang sangat baik, serta kualitas yang dihasilkan stabil untuk

pengiriman paket data protokol UDP dalam kondisi jaringan menggunakan rute utama dan rute *failover*. Dari hasil pengujian yang sudah dilakukan, maka diperoleh data nilai rata-rata *throughput* sebagai bahan analisa untuk mengetahui performansi pada topologi 1 dan topologi 2. Performansi kinerja penggunaan protokol UDP antara topologi 1 dan 2 pada skenario rute utama dan rute *failover*, nilai *throughput* pada topologi 1 lebih unggul daripada topologi 2. Pengujian menggunakan 4 router FRR dan 6 router FRR dapat dikategorikan memiliki performa yang baik dan stabil, seiring dengan meningkatnya nilai *throughput* berdasarkan peningkatan ukuran besaran data yang digunakan. Berdasarkan standarisasi TIPHON, dapat dikatakan performansi kinerja topologi 1 dan 2 dalam kondisi optimal karena nilai *throughput* yang diperoleh tergolong sangat baik yaitu > 2,1 Mbps. Gambar 10 yaitu grafik nilai rata-rata *throughput* rute utama dan Gambar 11 yaitu grafik nilai rata-rata *throughput* rute *failover*.



Gbr. 10 Grafik nilai rata-rata *throughput* rute utama



Gbr. 11 Grafik nilai rata-rata *throughput* rute *failover*

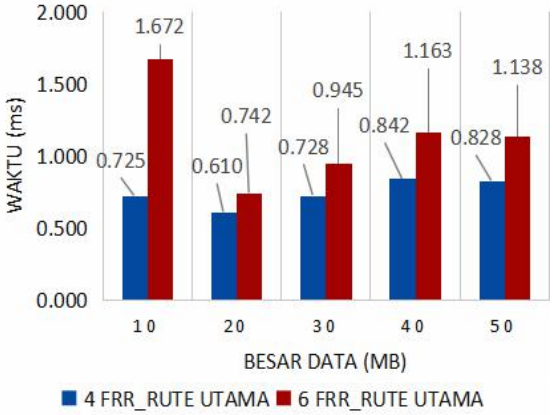
C. Analisis *Jitter*

Pada pengukuran protokol UDP dengan skenario tanpa *failover* (rute utama) di topologi 1 (4 router FRR), besar data 10 MB diperoleh nilai rata-rata *jitter* yaitu 0,725 ms, sedangkan pada skenario *failover* (rute *backup*) diperoleh nilai rata-rata *jitter* yaitu 0,658 ms. Pada skenario tanpa *failover* (rute utama), peningkatan tertinggi nilai *jitter* terjadi pada besar data 40 MB dengan nilai rata-rata yaitu 0,842 ms, sedangkan pada skenario *failover* dengan nilai rata-rata yaitu 1,155 ms.

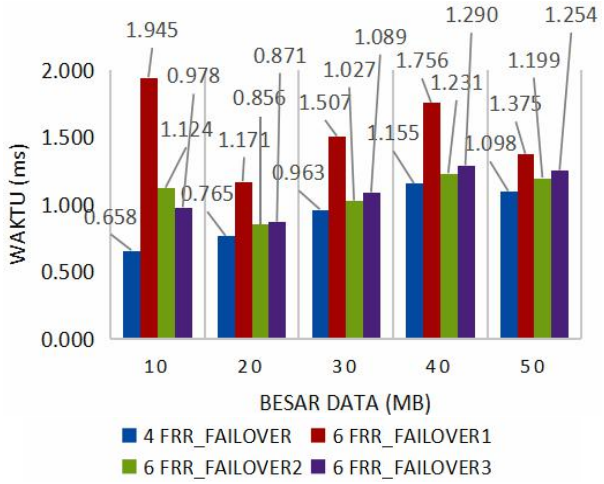
Pada pengukuran protokol UDP dengan skenario tanpa *failover* di topologi 2 (6 router FRR), besar data 10 MB diperoleh nilai rata-rata *jitter* yaitu 1,672 ms, sedangkan pada skenario *failover* diperoleh nilai rata-rata *jitter failover1* yaitu 1,945 ms, nilai rata-rata *jitter failover2* yaitu 1,124 ms, dan nilai rata-rata *jitter failover3* yaitu 0,978 ms.

Pada skenario tanpa *failover*, peningkatan tertinggi nilai *jitter* terjadi pada besar data 10 MB dengan nilai rata-rata yaitu 1,672 ms, sedangkan pada skenario *failover* terjadi peningkatan tertinggi pada besar data 10 MB untuk *failover1* dengan nilai rata-rata yaitu 1,945 ms, peningkatan tertinggi pada besar data 40 MB untuk *failover2* dengan nilai rata-rata yaitu 1,231 ms, dan peningkatan tertinggi pada besar data 40 MB untuk *failover3* dengan nilai rata-rata yaitu 1,290 ms. Dari hasil pengujian yang dilakukan, nilai rata-rata *jitter* pada topologi 1 lebih rendah dibandingkan dengan topologi 2 pada skenario tanpa *failover* dan *failover*.

Berdasarkan standarisasi TIPHON, dapat dikatakan performansi kinerja topologi 1 dan 2 dalam kondisi optimal dengan menerapkan skenario rute utama karena dengan bertambahnya ukuran besar data hingga pengujian terakhir yaitu 50 MB, memperoleh nilai rata-rata *jitter* untuk topologi 1 yaitu 0,747 ms dan topologi 2 yaitu 1,132 ms. Pada skenario rute *failover*, performansi kinerja topologi 1 dan 2 dalam kondisi optimal karena dengan bertambahnya ukuran besar data hingga pengujian terakhir yaitu 50 MB, memperoleh nilai rata-rata *jitter failover* untuk 4 router FRR yaitu 0,928 ms, nilai rata-rata *jiter failover1* yaitu 1,514 ms, nilai rata-rata *jiter failover2* yaitu 1,075 ms, dan nilai rata-rata *jiter failover3* yaitu 1,096 ms untuk 6 router FRR. Oleh karena itu, nilai rata-rata *jitter* pada topologi 1 dan 2 tergolong baik yaitu < 75 ms. Gambar 12 yaitu grafik nilai rata-rata *jitter* rute utama dan Gambar 13 yaitu grafik nilai rata-rata *jitter* rute *failover*.



Gbr. 12 Grafik nilai rata-rata *jitter* rute utama



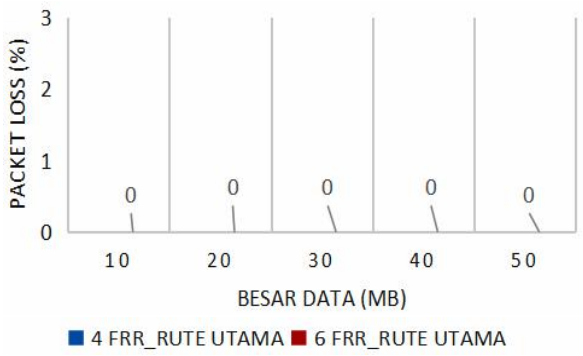
Gbr. 13 Grafik nilai rata-rata *jitter* rute *failover*

D. Analisis *Packet Loss*

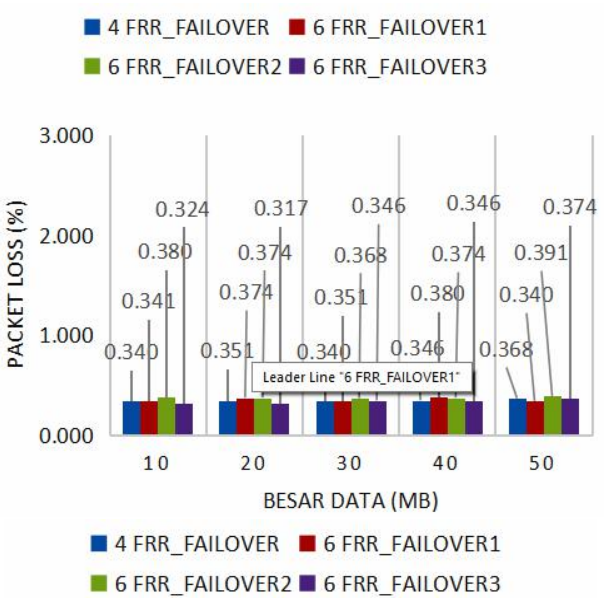
Pada pengujian protokol UDP dengan skenario tanpa *failover* (rute utama) di topologi 1 (4 router FRR), dengan ukuran besar data yang digunakan yaitu 10 MB, 20 MB, 30 MB, 40 MB, dan 50 MB diperoleh nilai rata-rata *packet loss* yaitu 0 %. Sedangkan pada skenario *failover* (rute *backup*), besar data 10 MB diperoleh nilai rata-rata *packet loss* yaitu 0,340 %. Nilai *packet loss* diperoleh saat menggunakan skenario *failover*, karena pada saat pengiriman paket data rute dialihkan ke rute *failover*. Selama perpindahan dari rute utama ke rute *failover*, akan terjadi paket data yang hilang saat pengiriman paket data. Rute pengiriman paket data dialihkan ke rute *backup* karena router utama mengalami *down*. Nilai *packet loss* terjadi peningkatan tertinggi pada besar data 50 MB dengan nilai rata-rata yaitu 0,368 %.

Pada pengukuran protokol UDP dengan skenario tanpa *failover* di topologi 2 (6 router FRR), dengan ukuran besar data yang digunakan yaitu 10 MB, 20 MB, 30 MB, 40 MB, dan 50 MB diperoleh nilai rata-rata *packet loss* yaitu 0 %. Sedangkan pada skenario *failover*, besar data 10 MB diperoleh nilai rata-rata *packet loss failover1* yaitu 0,341 %, nilai rata-rata *packet loss failover2* yaitu 0,380 %, dan nilai rata-rata *packet loss failover3* yaitu 0,324 %. Nilai *packet loss* terjadi peningkatan tertinggi pada besar data 40 MB dengan nilai rata-rata *packet loss failover1* yaitu 0,380 %, besar data 50 MB dengan nilai rata-rata *packet loss failover 2* yaitu 0,391 % dan nilai rata-rata *packet loss failover3* yaitu 0,374 %.

Berdasarkan standarisasi TIPHON, performansi kinerja topologi 1 dan topologi 2 dapat dikatakan dalam kondisi optimal karena pengujian *packet loss* pada kedua topologi tersebut dengan skenario tanpa *failover* dan *failover* dikategorikan sangat baik karena nilai rata-rata *packet loss* yaitu diantara 0% - 1%. Gambar 14 yaitu grafik nilai rata-rata *packet loss* rute utama dan Gambar 15 yaitu grafik nilai rata-rata *packet loss* rute *failover*.



Gbr. 14 Grafik nilai rata-rata *packet loss* rute utama



Gbr. 15 Grafik nilai rata-rata *packet loss* rute *failover*

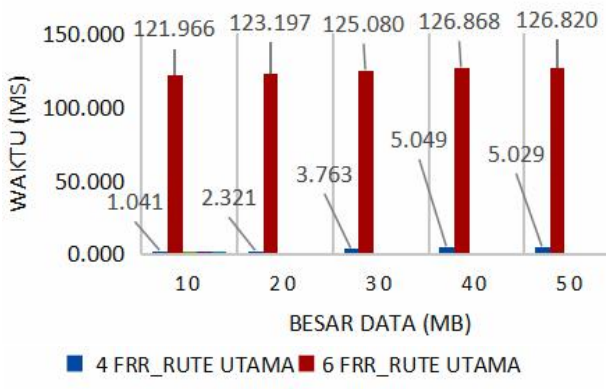
E. Analisis Delay

Pada pengukuran protokol UDP dengan skenario tanpa *failover* (rute utama) di topologi 1 (4 router FRR), besar data 10 MB diperoleh nilai rata-rata *delay* yaitu 1,041 ms, sedangkan pada skenario *failover* (rute *backup*) diperoleh nilai rata-rata *delay* yaitu 97,323 ms. Penggunaan besar data yang bervariasi mempengaruhi nilai rata-rata *delay* yang akan dihasilkan. Pada skenario tanpa *failover*, terjadi peningkatan nilai rata-rata *delay* secara bertahap hingga besar data yang terbesar 50 MB dengan nilainya yaitu 5,029 ms. Sedangkan pada skenario *failover*, juga terjadi peningkatan nilai rata-rata *delay* secara bertahap hingga besar data terbesar 50 MB dengan nilainya yaitu 101,800 ms. Pada skenario tanpa *failover*, nilai rata-rata *delay* tertinggi terjadi pada besar data 40 MB dengan nilai rata-rata yaitu 5,049 ms sedangkan pada skenario *failover*, nilai rata-rata *delay* tertinggi terjadi pada besar data 40 MB dengan nilai rata-rata yaitu 101,831 ms.

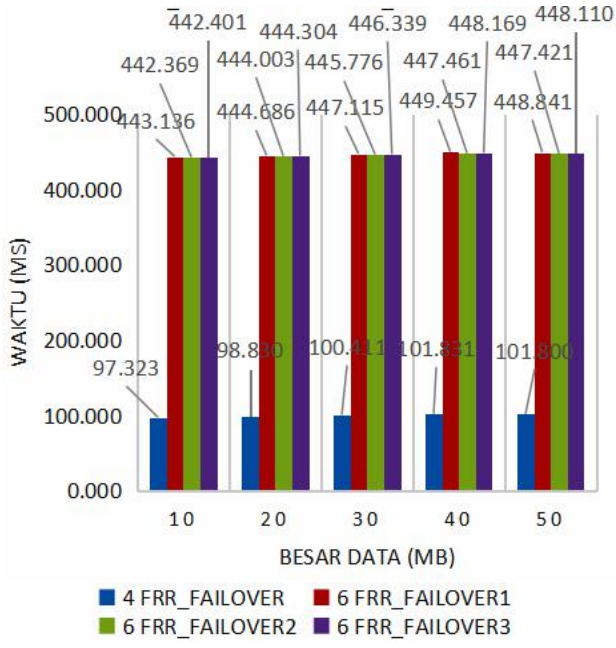
Pada pengukuran protokol UDP dengan skenario tanpa *failover* (rute utama) di topologi 2 (6 router FRR), besar data 10 MB diperoleh nilai rata-rata *delay* yaitu 121,966 ms, sedangkan pada skenario *failover* diperoleh

nilai rata-rata *delay failover1* yaitu 443,136 ms, nilai rata-rata *delay failover2* yaitu 442,369 ms dan nilai rata-rata *delay failover3* yaitu 442,401 ms. Penggunaan besar data yang bervariasi mempengaruhi nilai rata-rata *delay* yang akan dihasilkan. Pada skenario tanpa *failover*, peningkatan nilai rata-rata *delay* secara bertahap hingga besar data yang terbesar 50 MB dengan nilainya yaitu 126,820 ms. Sedangkan pada skenario *failover*, peningkatan nilai rata-rata *delay* secara bertahap hingga besar data terbesar 50 MB dengan nilai rata-rata *delay failover1* yaitu 448,841 ms, nilai rata-rata *delay failover2* yaitu 447,421 ms, dan nilai rata-rata *failover3* yaitu 448,410 ms. Pada protokol paket data UDP, tidak ada jaminan paket yang dikirimkan akan lengkap hingga ke penerima dan memiliki karateristik yaitu pengiriman paket data menuju penerima dilakukan secara terus menerus tanpa adanya proses *handshake*.

Gambar 16 yaitu grafik nilai rata-rata *delay* rute utama dan Gambar 17 yaitu grafik nilai rata-rata *delay* rute *failover*.



Gbr. 16 Grafik nilai rata-rata *delay* rute utama



Gbr. 17 Grafik nilai rata-rata *delay* rute *failover*

Berdasarkan standarisasi TIPHON, penggunaan 4 router FRR dengan skenario tanpa *failover* (rute utama) dan *failover* (rute *backup*) lebih baik daripada penggunaan 6 router FRR. Dikarenakan nilai rata-rata *delay* pada topologi 1 (4 router FRR) dengan skenario tanpa *failover* dan *failover* dikategorikan sangat baik yaitu <150 ms. Sedangkan, penggunaan 6 router FRR dengan skenario tanpa *failover* dikategorikan sangat baik yaitu <150 ms dan skenario *failover* dikategorikan sedang yaitu 300 s/d 450 ms. Performansi kinerja topologi 1 dalam kondisi optimal dengan menerapkan skenario rute utama dan rute *failover*. Sedangkan performansi kinerja topologi 2 dalam kondisi optimal dengan menerapkan skenario rute utama.

IV. KESIMPULAN

Berdasarkan dari hasil penelitian dan analisis data simulasi *routing border gateway protocol* (BGP) antar AS menggunakan FRR yang dilakukan, maka dapat diperoleh beberapa kesimpulan yaitu:

1. Simulasi *routing protocol* BGP antar AS menggunakan FRR yaitu mengaktifkan *daemons* BGP menjadi "bgpd=yes" pada file "/etc/frr/daemons" terlebih dahulu. Kemudian, melakukan konfigurasi *routing protocol* BGP di router FRR pada file "/etc/frr/bgpd.conf". Konfigurasi *routing protocol* BGP pada router FRR mudah dilakukan karena konfigurasinya dilakukan dalam file, sehingga memudahkan administrator jaringan untuk menangani saat terjadi kesalahan. Perintah *no bgp ebgp-requires-policy* berfungsi untuk memfilter paket data yang masuk dan keluar dari router FRR. Tanpa adanya perintah tersebut dalam konfigurasi *routing protocol* BGP, BGP tidak dapat diterapkan pada router FRR.
2. Data hasil pengujian QoS pada pengukuran protokol UDP yang diperoleh pada topologi 1 dan topologi 2 dengan skenario tanpa *failover* (rute utama) dan *failover* (rute *backup*) menghasilkan QoS yang baik sehingga performansi kinerja pada topologi 1 dan topologi 2 dalam kondisi optimal. Performansi kinerja topologi 1 lebih baik daripada topologi 2. Hasil pengujian QoS memiliki peningkatan nilai seiring dengan variasi besar data yang dikirimkan dan skenario pengujian. Hasil pengujian dikategorikan performa "sangat baik" pada skenario tanpa *failover* dan dikategorikan performa "sangat baik" hingga "sedang" pada skenario *failover*.

REFERENSI

[1] Musril, H. A. (2017). Simulasi Interkoneksi Antara Autonomous System (AS) Menggunakan Border Gateway Protocol (BGP). *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan*, *2*(1), 1-9.

[2] Sondy C. K. (2014). *Rancang Bangun Jaringan Untuk SMK / MAK Kelas XI Semester 2*. Jakarta: Kementrian Pendidikan & Kebudayaan.

[3] Linux Foundation Collaborative Project. (2017) *FRRouting Project*. Diakses pada 22 Mei 2021, dari Linux Foundation: https://frrouting.org.

[4] Cisco Systems, Inc. (2004). *Internetworking Technologies Handbook*. Cisco Press.

[5] Krisnawijaya, N. N. K., & Paramartha, C. R. A. (2016). Penerapan Jaringan Multihoming Pada Jaringan Komputer Fakultas Hukum. *Jurnal Ilmiah Ilmu Komputer Universitas Udayana*, *9*(1), 23-31.

[6] Iryani, N., & Andika, D. D. (2021). Analisis Performansi Dynamic Multipoint Virtual Private Network pada Routing Protocol BGP dengan FRRouting. *JTERA (Jurnal Teknologi Rekayasa)*, *6* (1), 61-66.