

Quality of Service Gateway Load Balancing Protocol Message Digest Algorithm 5 Authentication untuk Peningkatan Kualitas Jaringan

Firmansyah¹, Sari Dewi², Rachmat Adi Purnama³

Abstract—Gateway Load Balancing Protocol (GLBP) Message-Digest algorithm 5 (MD5) is a Cisco's proprietary protocol. GLBP used to enhance the Quality of Service(QoS) on a network. It applies the IP Address Gateway Virtual that redundancy on the local network. GLBP run all used routers in time because of load balancing itself, there is no router used as a standby/backup only. Using the GLBP protocol, all network loads are shared equally to all connected routers. The way the GLBP network works is different from how the HSRP and VRRP networks work, which will run the standby/backup router if the active / master router experiences a problem (failover). The average time needed to redundancy the master to router backup router is 7.6 ms. While the average time needed to change from standby router redundancy to master router redundancy or the master router reused is 33.4 Ms. The average packet loss obtained when the redundancy of the active router change to standby router is 1.7 packet, and The average packet loss obtained when the redundancy of the active router change to standby router is 1.7 packet and 0.5 packets in opposite ways.

Intisari— Gateway Load Balancing Protocol (GLBP) Message Digest algorithm 5 (MD5) merupakan sebuah protokol Cisco proprietary. GLBP dibentuk untuk meningkatkan Quality of Service (QoS) terhadap jaringan komputer dikarenakan menggunakan IP Address Gateway Virtual yang bersifat redundancy pada jaringan lokal. GLBP menjalankan semua router yang digunakan secara bersamaan dikarenakan sifatnya Load Balancing itu sendiri, sehingga tidak ada router yang bersifat hanya standby/backup saja. Dengan menggunakan protokol GLBP, semua beban jaringan dibagi sama rata kepada semua router yang terhubung. Cara kerja jaringan GLBP berbeda dengan cara kerja jaringan HSRP dan VRRP yang akan menjalankan router standby/backup jika router active/master mengalami sebuah permasalahan (fail over). Adapun waktu rata-rata yang dibutuhkan untuk melakukan redundancy router master to router backup adalah 7,6 Ms. Sedangkan waktu rata-rata yang dibutuhkan untuk melakukan redundancy router standby to router master ataupun ketika router master telah dapat digunakan kembali adalah 33,4 Ms. Sedangkan hasil rata-rata packet loss yang didapat saat redundancy router active to router standby adalah 1,7 packet loss dan packet loss yang didapat saat terjadi redundancy router standby to router master sebesar 0,5 packet.

Kata Kunci — Gateway Load Balancing Protocol, Quality of Service, Redundancy, Packet Loss

¹Sistem Informasi, STMIK Nusa Mandiri, Jl. Kramat Raya No. 18 Jakarta Pusat (e-mail: firmaryah.fmy@bsi.ac.id)

^{2,3}Sistem Informasi, Fakultas Teknologi Informasi Universitas Bina Sarana Informatika, Jl. Kamal Raya No. 18 Ring Road Barat Cengkareng, Jakarta Barat (e-mail: sari.sre@bsi.ac.id, rachmat.rap@bsi.ac.id)

I. PENDAHULUAN

Kestabilan jaringan komputer saat ini merupakan sebuah aspek yang begitu penting dalam penentuan transfer data. Tidak hanya perangkat jaringan saja yang menjadi faktor utama dalam penentuan stabilnya sebuah jaringan komputer. Software, implementasi jaringan juga mengambil alih dalam penentuan stabil atau tidaknya jaringan yang digunakan.

Semakin terus berkembangnya teknologi informasi akan terus berdampak dengan kebutuhan manusia terhadap informasi tersebut. Dengan meningkatnya kebutuhan jaringan, maka akan mengakibatkan kompleksitas jaringan yang sangat padat dan diharapkan memiliki jaringan yang handal dengan dukungan Quality of Service (QoS) yang baik. Untuk melakukan penanganan terhadap QoS pada jaringan komputer, kita dapat menggunakan perangkat jaringan, dan software yang sesuai dengan kebutuhan. Dan yang tidak kalah pentingnya adalah bagaimana cara melakukan implementasi terhadap perangkat jaringan yang digunakan. QoS merupakan kemampuan suatu jaringan untuk menyediakan layanan yang lebih baik pada traffic data tertentu pada berbagai jenis platform teknologi [8].

Dalam hal ini, terdapat teknik yang mampu untuk menanggulangi kegagalan terhadap QoS pada jaringan. Salah satu teknologi baru yang mempunyai kemampuan optimalisasi yang baik yang dapat diterapkan pada jaringan adalah Gateway Load Balancing Protocol (GLBP). GLBP mampu melakukan redundancy secara otomatis terhadap alamat gateway yang digunakan pada jaringan lokal ketika mengalami permasalahan link.

II. METODOLOGI PENELITIAN

Gateway Load Balancing Protocol (GLBP) sendiri lahir dari konsep load balancing, yang merupakan konsep yang gunanya untuk menyeimbangkan beban atau muatan pada beberapa link yang menuju network remote yang sama [1]. Hasil throughput yang didapat dapat terjadi dikarenakan adanya protokol GLBP sebagai gateway redundancy [3].

1. Gateway Load Balancing Protocol (GLBP)

GLBP merupakan protokol proprietary dari Cisco. GLBP menyediakan fitur yang berbeda yang tidak dimiliki oleh Protokol VRRP maupun protokol HSRP, yaitu dynamic load balancing [7]. Perbedaan GLBP dengan VRRP dan HSRP adalah sifat load balancing yang dimiliki oleh protokol GLBP itu sendiri. Ketika menggunakan

protokol GLBP lalu lintas jaringan pada setiap gateway akan seimbang, berbeda dengan konsep kerja dari protokol VRRP dan HSRP yang akan menjalankan router *standby/backup* jika router *active/master* mengalami sebuah permasalahan. The redundancy group distributes forwarding addresses to hosts which in turn use the distributed forwarding addresses to send packets to the redundancy group [7]

TABEL 1. PERBEDAAN HSRP, VRRP DAN GLBP

Characteristic	HSRP	VRRP	GLBP
Cisco proprietary.	Yes	No	Yes
Interface IP address can act as virtual IP address.	No	Yes	No
More than one router in a group can simultaneously forward traffic for that group.	No	No	Yes
Hello timer default value.	3 seconds	1 seconds	3 seconds
Hold timer default value.	10 seconds	3 seconds	10 seconds
Preemption enabled by default.	No	Yes	No for AVG, Yes for AVFs
Default priority.	100	100	100

Pada Tabel 1, dijelaskan perbedaan dari protokol HSRP, VRRP dan GLBP. Meskipun HSRP, VRRP dan GLBP memiliki kesamaan, penting bagi Anda untuk mengetahui pemecahan permasalahan seefisien dan seefektif mungkin [4].

2. Active Virtual Gateway (AVG)

AVG merupakan router yang bertindak sebagai ketua dari seluruh router yang tergabung didalam satu group GLBP. Router GLBP akan memilih AVG sebagai prioritas tertinggi [6]. Router dengan status AVG akan dijadikan sebagai router *active/router master*. In general, GLBP specifies the rules and encoding specifications for sending data to and from the server farm. Members of a GLBP group elect one gateway to be the active virtual gateway (AVG) for that group [9].

3. Active Virtual Forwarder (AVF)

AVF berguna sebagai wakil dari AVG, ketika router AVG mengalami permasalahan maka router AVF ini akan mendeteksi dan menggantikan posisi dari router AVG. Router AVF berperan sebagai router *backup/standby*.

4. Standby Virtual Gateway (SVG)

Router SCG merupakan wakil dari router AVF ketika router tersebut mengalami permasalahan.

5. Load Balancing

Load Balancing merupakan sebuah teknik yang digunakan untuk melakukan distribusi beban traffic pada dua ataupun lebih jalur konektivitas secara seimbang, dengan tujuan mengoptimalkan jaringan, memaksimalkan

throughput, serta memperkecil terjadinya delay pada jaringan dan meminimalisir terjadinya overload terhadap salah satu jalur koneksi. Metode Load Balancing dan Fail Over menggunakan lebih dari satu perangkat gateway dalam kelompok perangkat gateway untuk berkomunikasi yang diarahkan ke jaringan LAN [2].

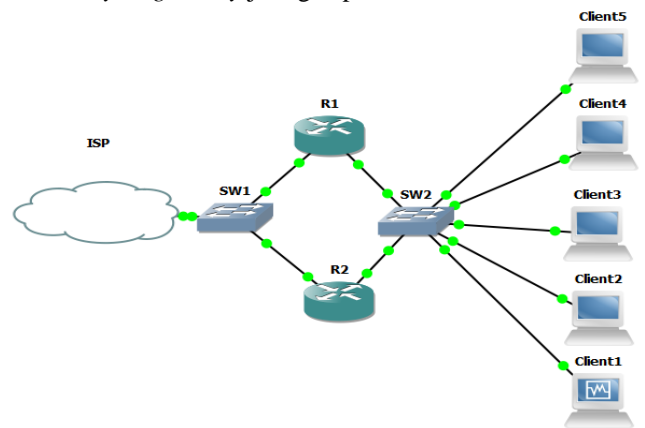
6. MD5 Authentication

MD 5 Authentication digunakan untuk memberikan keamanan terhadap protokol GLBP. Dengan menggunakan keamanan MD5 Authentication diharapkan legalitas dan keamanan paket data yang akan melewati router telah melakukan validasi terhadap password yang digunakan.

III. HASIL DAN PEMBAHASAN

A. Desain Jaringan

Topologi jaringan komputer yang digunakan dalam penelitian ini dapat dilihat pada Gambar 1. Dengan menggunakan 2 buah router yang akan dijadikan sebagai redundancy IP gateway jaringan pada lokal.



Gbr 1. Topologi Jaringan

TABEL 2. SPESIFIKASI IP ADDRESS ROUTER 1

Interface	IP Address	Gateway
Ether 1	192.168.137.254	192.168.137.1
Ether 2	192.168.1.1	-
GLBP	192.168.1.254	-

TABEL 3. SPESIFIKASI IP ADDRESS ROUTER 1

Interface	IP Address	Gateway
Ether 1	192.168.137.253	192.168.137.1
Ether 2	192.168.1.2	-
GLBP	192.168.1.254	-

Jika melihat pada tabel 2 dan tabel 3, terdapat dua buah alamat gateway yang dapat digunakan untuk jaringan lokal. Jika jaringan lokal menggunakan alamat gateway 192.168.1.1 maka router yang melayani jaringan lokal hanya router 1 saja. Sedangkan, jika jaringan lokal menggunakan alamat gateway 192.168.1.2 maka router yang melayani jaringan lokal hanya router 2 saja. Hal ini akan mengakibatkan salah satu router tidak digunakan semaksimal mungkin. Untuk memaksimalkan kinerja

jaringan lokal kita dapat menggunakan *virtual gateway* untuk menjalankan kedua router secara bersamaan. Jaringan komputer yang terbentuk pada Gambar 1 akan menggunakan alamat *virtual gateway* 192.168.1.254 dengan tujuan mendapatkan *redundancy gateway* dari router 1 dan router 2.

TABEL 4. SPESIFIKASI GLBP

Spesifikasi	R1	R2
Interface	FastEthernet1/0	FastEthernet1/0
Group	GLBP 1	GLBP 1
IP Address	192.168.1.254/24	192.168.1.254/24
Priority	200	90
Load Balancing	Round-robin	Round-robin

Jika melihat pada tabel 4, router 1 digunakan sebagai router *active/master* dengan nilai *priority* 200 yang lebih besar dibandingkan dengan nilai *priority* yang digunakan terhadap router 2 dengan nilai 90.

GLBP terhadap kedua router menggunakan *group* yang sama, yaitu *group* 1. Sedangkan IP *Virtual* yang digunakan terhadap kedua router adalah 192.168.1.254/24. Nilai *group* ataupun IP *Virtual* yang akan digunakan haruslah memiliki nilai yang sama. *Interface* yang akan digunakan sebagai GLBP sama-sama menggunakan *interface* *FastEthernet1/0*.

B. Konfigurasi Jaringan

1. Konfigurasi GLBP Router 1

Untuk melakukan konfigurasi GLBP terhadap Router 1, terdapat beberapa hal yang harus diperhatikan. Seperti IP *address* yang akan digunakan terhadap *interface* *FastEthernet0/0* yang nantinya akan terkoneksi dengan akses internet, *FastEthernet1/0* yang akan digunakan sebagai alamat *gateway* jaringan lokal serta pemberian alamat *Virtual* IP yang akan digunakan sebagai *redundancy gateway* pada jaringan lokal.

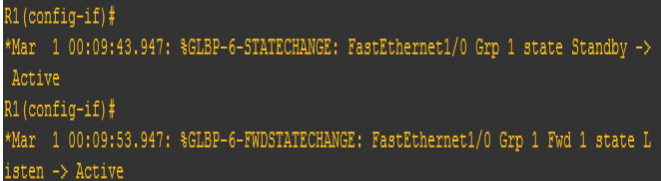
Setelah mengetahui spesifikasi IP *Address* yang akan digunakan terhadap Router 1 terlihat pada Tabel 2, selanjutnya untuk melakukan konfigurasi GLBP terhadap router 1, kita dapat menggunakan perintah:

```
R1(config)#int fa1/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#ip nat inside
R1(config-if)#no shut
```

Perintah tersebut digunakan untuk memberikan IP *Address* terhadap *interface* *fastethernet1/0* dengan alamat IP: 192.168.1.1/24. Selanjutnya membuat *group* GLBP terhadap *interface* *fastethernet1/0*, serta memberikan IP *virtual* dan memastikan router 1 sebagai router AVF.

```
R1(config)#int fa1/0
R1(config-if)#glbp 1 ip 192.168.1.254
R1(config-if)#glbp 1 preempt
R1(config-if)#glbp 1 forward preempt
R1(config-if)#glbp 1 priority 200
R1(config-if)#glbp 1 load-balancing round-robin
```

Perintah *preempt* digunakan untuk mengaktifkan *preemption* terhadap GLBP, yang bertujuan untuk mendapatkan status *active* jika prioritas router lain memiliki nilai prioritas yang lebih kecil.



```
R1(config-if)#
*Mar 1 00:09:43.947: %GLBP-6-STATECHANGE: FastEthernet1/0 Grp 1 state Standby -> Active
R1(config-if)#
*Mar 1 00:09:53.947: %GLBP-6-FWDSTATECHANGE: FastEthernet1/0 Grp 1 Fwd 1 state Listen -> Active
```

Gbr 2. Hasil Aktivasi GLBP

Pada gambar 2 dijelaskan, bahwa router 1 sudah melakukan perubahan *state*-nya yang sebelumnya *standby* kini menjadi *state active*.

2. Konfigurasi GLBP Router 2

Untuk melakukan konfigurasi GLBP terhadap router 2 secara garis besar tidaklah berbeda jauh dengan konfigurasi yang digunakan terhadap router 1, hanya saja terjadi perbedaan terhadap alamat IP yang digunakan, dengan tujuan agar tidak terjadinya konflik IP *Address* antara router 1 dengan router 2. Untuk melakukan konfigurasi terhadap router 2, kita dapat menggunakan perintah:

```
R2(config)#int fa1/0
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#ip nat inside
R2(config-if)#no shut
```

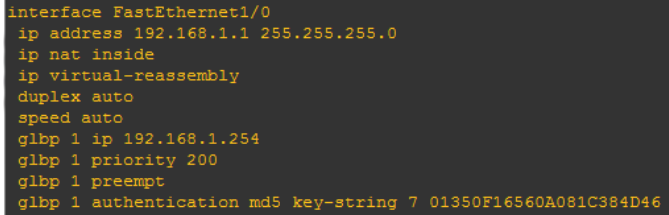
Perintah tersebut digunakan untuk memberikan IP *Address* terhadap *interface* *fastethernet1/0* dengan alamat 192.168.1.2/24. Selanjutnya membuat *group* GLBP terhadap *interface* *FastEthernet1/0*, serta memberikan IP *virtual* dan memastikan router 1 sebagai AVF atau router *standby*.

```
R2(config)#int fa1/0
R2(config-if)#glbp 1 ip 192.168.1.254
R2(config-if)#glbp 1 preempt
R2(config-if)#glbp 1 forward preempt
R2(config-if)#glbp 1 priority 90
R2(config-if)#glbp 1 load-balancing round-robin
```

3. Konfigurasi *authentication* md5

Authentication md5 digunakan untuk memberikan autentikasi terhadap *interface* GLBP dengan menggunakan *password* yang telah dienkripsi. Router 1 dan Router 2 harus menggunakan *password* yang sama agar dapat saling berkomunikasi satu dengan lainnya.

```
R1(config-if)#glbp 1 authentication md5 key-string Firmansyah
```



```
interface FastEthernet1/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
glbp 1 ip 192.168.1.254
glbp 1 priority 200
glbp 1 preempt
glbp 1 authentication md5 key-string 7 01350F16560A081C384D46
```

Gbr 3. *Authentication* md5

Setelah melakukan konfigurasi *authentication* md5 terhadap router 1, maka router 2 ataupun router lainnya yang akan melakukan komunikasi GLBP terhadap *Group* 1 harus memasukan *password* yang sama sebagai *Authentication*.

C. Uji Konektifitas

1. GLBP

Pengujian pertama yang dilakukan adalah melakukan pengujian terhadap konektifitas jaringan GLBP dengan cara melakukan pengujian terhadap *interface* router 1 dan router 2 untuk memastikan bahwa router 1 sebagai router *active* dan router 2 sebagai router *standby*.

Cara kerja GLBP berbeda dengan cara kerja VRRP maupun HSRP. GLBP menjalankan kedua router secara bersamaan yang artinya tidak ada router yang bersifat hanya *standby* saja. GLBP bertujuan untuk membagi beban jaringan menjadi sama rata, sehingga ketika didalam jaringan terhubung dengan lima (5) *client*. Maka beban router sebagai *gateway client* dibagi menjadi sama rata antara router 1 dengan router 2. Namun, ketika router 1 (*active*) mengalami permasalahan jaringan maka lalu lintas jaringan secara keseluruhan akan diambil alih oleh router 2 (*standby*).

```
R1#sh glbp brief
Interface Grp Fwd Pri State Address Active router Standby router
Fa1/0 1 - 200 Active 192.168.1.254 local 192.168.1.2
Fa1/0 1 1 - Active 0007.b400.0101 local -
Fa1/0 1 2 - Listen 0007.b400.0102 192.168.1.2 -
```

Gbr 4. GLBP Router 1

Terlihat pada gambar 4, *interface fastethernet1/0* memiliki prioritas 200 dengan *state active* dan menggunakan *group* GLBP 1.

```
R2#sh glbp brief
Interface Grp Fwd Pri State Address Active router Standby router
Fa1/0 1 - 90 Standby 192.168.1.254 192.168.1.1 local
Fa1/0 1 1 - Listen 0007.b400.0101 192.168.1.1 -
Fa1/0 1 2 - Active 0007.b400.0102 local -
```

Gbr 5. GLBP 2

Jika melihat pada gambar 5, *interface fastethernet1/0* menggunakan *group* GLBP 1 dengan nilai prioritas 90 dengan *state standby*. Hal yang menyebabkan router 2 sebagai router *standby* dikarenakan memiliki nilai prioritas yang lebih rendah dibandingkan dengan nilai prioritas yang digunakan oleh router 1 yang bernilai 200.

2. Traceroute

Penguji selanjutnya menggunakan *traceroute* untuk mendapatkan *hops* yang dilalui dari *client* untuk terkoneksi ke jaringan. *Client* pertama yang terkoneksi kedalam jaringan GLBP yang telah terbentuk akan terkoneksi menggunakan *hops* IP *address* 192.168.1.1 terlihat pada gambar 6. Sedangkan *client* kedua yang terkoneksi kedalam jaringan GLBP secara otomatis akan menggunakan *hops* ip *address* 192.168.2.1 terlihat pada gambar 7.

```
C:\Documents and Settings\Client>tracert nusanandiri.ac.id
Tracing route to nusanandiri.ac.id [118.98.72.91]
over a maximum of 30 hops:
  1  15 ms  9 ms  9 ms  192.168.1.1
  2  24 ms  *    22 ms USER-PC.mshome.net [192.168.137.1]
  3  *      *    *    Request timed out.
  4  27 ms  *    500 ms 245.subnet125-160-11.speedy.telkon.net.id [125.1
```

Gbr 6. Hasil Tracert Client 1

```
C:\Documents and Settings\Client>tracert nusanandiri.ac.id
Tracing route to nusanandiri.ac.id [118.98.72.91]
over a maximum of 30 hops:
  1  4 ms  9 ms  9 ms  192.168.1.2
  2  22 ms *    17 ms USER-PC.mshome.net [192.168.137.1]
  3  *      *    *    Request timed out.
  4  *      12 ms 30 ms 245.subnet125-160-11.speedy.telkon.net.id [125.1
```

Gbr 7. Hasil Tracert Client 2

TABEL 4. HASIL TRACEROUTE CLIENT

Client	Gateway	Tracert
192.168.1.10	192.168.1.254	192.168.1.1
192.168.1.11	192.168.1.254	192.168.1.2
192.168.1.12	192.168.1.254	192.168.1.1
192.168.1.13	192.168.1.254	192.168.1.2
192.168.1.14	192.168.1.254	192.168.1.1

Client selanjutnya yang terkoneksi kedalam protokol GLBP akan mendapatkan *hops* sesuai dengan kepadatan lalu lintas jaringan terlihat pada tabel 4. Terlihat pada gambar 6 dan gambar 7, beban jaringan dibagi otomatis secara merata ke dua router yang digunakan. Jadi, kedua router yang digunakan sama-sama menjadi *gateway* dari jaringan lokal dengan jumlah *client* yang sama.

3. Redundancy Time Master to Standby

Hasil pengujian terhadap waktu yang dibutuhkan untuk melakukan *redundancy* dari router *master* ke router *standby* dapat dilihat pada Tabel 5. Hasil ini diambil dengan cara melakukan pemutusan akses terhadap *interface FastEthernet1/0* pada router 1 dan akan terjadi *redundancy* secara otomatis lalu lintas jaringan melalui router *standby/router2*.

TABEL 5. REDUNDANCY MASTER TO STANDBY

Percobaan	Router 1 Off	Router 2 On	Time (Ms)
Ke 1	15:12:18	15:12:26	00:00:08
Ke 2	15:16:03	15:16:09	00:00:06
Ke 3	15:18:23	15:18:31	00:00:08
Ke 4	15:25:13	15:25:21	00:00:08
Ke 5	15:40:01	14:40:09	00:00:08
Ke 6	17:41:09	17:41:17	00:00:08
Ke 7	17:45:33	17:45:40	00:00:07
Ke 8	17:53:27	17:53:35	00:00:08
Ke 9	19:08:15	19:08:23	00:00:08
Ke 10	19:13:09	19:13:15	00:00:07

```
R1(config-if)#
.Aug 31 15:25:13.327: %GLBP-6-FWDSTATECHANGE: FastEthernet1/0 Grp 1 Fwd 1 state Active -> Init
.Aug 31 15:25:13.331: %GLBP-6-STATECHANGE: FastEthernet1/0 Grp 1 state Active -> Init
```

Gbr 6. Router Master Off

```
R2#
.Aug 31 15:25:21.591: %GLBP-6-STATECHANGE: FastEthernet1/0 Grp 1 state Standby -> Active
.Aug 31 15:25:21.591: %GLBP-6-FWDSTATECHANGE: FastEthernet1/0 Grp 1 Fwd 1 state Listen -> Active
```

Gbr 7. Router Standby On

Pada tabel 4, telah dilakukan pengujian sebanyak 10 kali dan didapatkan waktu rata-rata yang dibutuhkan untuk melakukan *redundancy* dari router *master* ke router *standby* adalah 7,6 Ms. Dengan waktu tercepat 6 Ms dan waktu terlama sebesar 8 Ms.

Jika melihat pada gambar 6, router 1 mengalami permasalahan jaringan saat 15:25:13, dan router akan melakukan *redundancy* secara otomatis ke router 2 untuk melakukan *backup* lalu lintas jaringan. Waktu yang dibutuhkan oleh router 2 untuk melakukan *redundancy* router 1 ke router 2 sekitar 6 Ms - 8 Ms terlihat pada gambar 7.

4. Redundancy Time Standby to Master

Pengujian selanjutnya adalah melakukan pemulihan terhadap *interface FastEthernet1/0* pada router 1. Hal ini akan berakibat terjadinya perpindahan akses yang sebelumnya di *handle* oleh router 2 akan dialihkan kembali ke router 1. Jika melihat pada tabel 6, waktu rata-rata yang dibutuhkan untuk melakukan *redundancy* dari router 2 ke router 1 sekitar 33,4 Ms.

TABEL 6. REDUNDANCY STANDBY TO MASTER

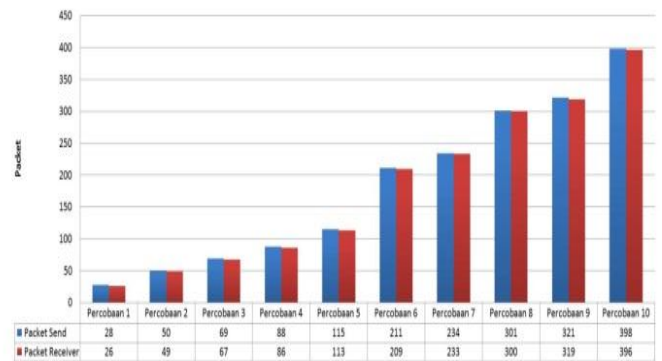
Percobaan	Router 1 On	Router 2 Off	Time
Ke 1	15:13:48	15:14:22	00:00:34
Ke 2	15:17:18	15:17:53	00:00:35
Ke 3	15:20:02	15:20:36	00:00:34
Ke 4	15:28:17	15:28:50	00:00:33
Ke 5	15:45:11	15:45:44	00:00:33
Ke 6	19:13:20	19:13:53	00:00:33
Ke 7	19:17:32	19:18:04	00:00:32
Ke 8	19:18:37	19:19:11	00:00:34
Ke 9	20:40:25	20:40:58	00:00:33
Ke 10	20:51:11	20:51:44	00:00:33

Pada gambar 8 dapat dijelaskan proses *redundancy* yang terjadi terhadap router 1 ketika keadaan *interface fastethernet1/0* telah kembali normal.

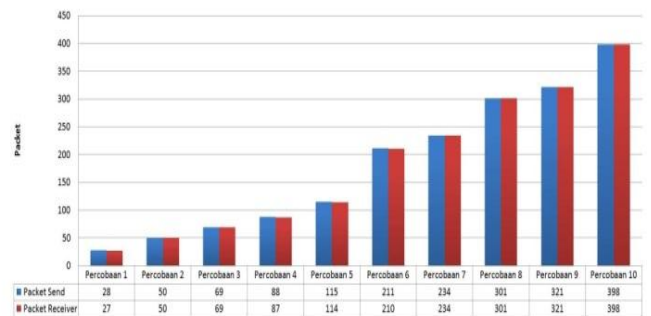
5. Packet Loss

Pengujian terhadap *packet loss* digunakan untuk mengetahui seberapa besar jaringan GLBP mengalami

kegagalan paket saat terjadi *redundancy IP Gateway* dari router 1 ke router 2.



Gbr 9. Packet Loss Active to Standby



Gbr 10. Packet Loss Standby to Active

Setelah melakukan pengujian sebanyak 10 kali terlihat pada gambar 9 dan gambar 10, didapatkan *packet loss* terkecil yang terjadi saat *redundancy* router 1 ke router 2 adalah 1 *packet* yang mengalami kegagalan, sedangkan *packet loss* tertinggi adalah 2 *packet* yang mengalami kegagalan. Rata-rata *packet loss* yang didapat setelah melakukan 10 kali uji coba adalah 1,7 *packet*.

Sedangkan, *packet loss* terkecil yang didapatkan saat terjadi *redundancy* router 2 ke router 1 adalah 0 *packet* dan *packet loss* tertinggi adalah 2 *packet* dengan rata-rata *packet loss* yang didapat sebesar 0,5 *packet*.

```

R1(config-if)#
..Aug 31 15:30:33.375: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
..Aug 31 15:30:34.375: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R1(config-if)#
..Aug 31 15:30:38.715: %GLBP-6-STATECHANGE: FastEthernet1/0 Grp 1 state Speak -> Active
R1(config-if)#
..Aug 31 15:31:06.731: %GLBP-6-FWDSTATECHANGE: FastEthernet1/0 Grp 1 Fwd 1 state Listen -> Active

```

Gbr 8. Redundancy Router 2 ke Router 1

IV. KESIMPULAN

Berdasarkan hasil analisa dan pembahasan yang telah diuraikan, dapat diambil kesimpulan sebagai berikut ini:

1. Dengan menggunakan GLBP, jaringan komputer akan berjalan lebih seimbang. Dikarenakan beban pada router dibagi sama rata.
2. Waktu *redundancy* yang dibutuhkan saat perpindahan router 1 ke router 2 lebih cepat dibandingkan dengan *redundancy* router 2 ke router 1.
3. *Packet loss* yang didapat saat terjadi *redundancy standby to master* lebih sedikit dibandingkan *packet loss* yang didapat saat *redundancy master to standby*.
4. Pada jaringan GLBP, sebaiknya menggunakan dua buah *group* GLBP jika jaringan yang digunakan sangat kompleks.

REFERENSI

- [1] Cisco, "GLBP - Gateway Load Balancing Protocol," [Online]. Available: http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glb.html
- [2] Donohue, Denise., Stewart, Brent (2010). CCNP Routing and Switching Quick Reference. USA: Cisco Press.
- [3] Erwin Irwansyah, Rizal., Munadi, Rendy., Mayawari, Ratna. Implementasi Dan Analisa Performansi Glbp (Gateway Load Balancing Protocol) Pada Jaringan Vlan Untuk Layanan Voip. E-Proceeding of Engineering: Vol3, No.1 April 2016 (251-257).
- [4] Ferry Panjaitan, Herman., Ganda Permana, Agus., Mulyono. Analisa Performansi Jaringan Pada Gateway Load Balancing Protokol (GLBP) Dengan Berbagai Mekanisme Anterian. Skripsi. Universitas Telkom Bandung. 2009
- [5] J. Nosella, Thomas., Herbert Wilson, Ian . Gateway Load Balancing Protocol. US7881208B1 (Paten). 2001
- [6] Lacoste, Raymond., Wallace, Kevin (2014). CCNP Routing and Switching TSHOOT 300-135 Official Cert Guide. USA: Cisco Press.
- [7] McLagan, Douglas., Wilson, Ian., Denny., Mark., Williams, Rick. Distributing and balancing traffic flow in a virtual gateway. US20050025179A1 (Paten). 2003.
- [8] Thabratas, Tharom. *Teknologi VoIP*, Jakarta: Elex Media Komputindo, 2001.
- [9] Watts, La Vaughn Ferguson., Jeff Rucker, JR., Wiese, Andreson., Oguri, Roger Wellington. Gateway management using virtual gateways and wildcards. US9888072B2 (Paten). 2014.



Firmansyah, S.Kom, seorang anak yang dilahirkan di Ibu Kota Jakarta, Lulus pendidikan S1 (Teknik Informatika) di STMIK Nusa Mandiri Jakarta tahun 2014, dan saat ini sedang melanjutkan program studi Pasca Sarjana di STMIK Nusa Mandiri Jakarta. Saat ini aktif sebagai tenaga pendidik di AMIK BSI Jakarta. Selain aktif sebagai tenaga pendidik sampai saat ini aktif sebagai assessor kompetensi BNSP dan Instruktur Cisco Networking Academy



Sari Dewi, M.Kom, Lahir di Cirebon 6 Juli 1989. Lulus S1 dari STMIK Nusa Mandiri Jakarta Program Studi Teknik Informatika 2013 dan S2 STMIK Nusa Mandiri Program Studi Ilmu Komputer 2015. Menjadi pengajar di Universitas Bina Sarana Informatika dan Pernah menulis pada jurnal paradigma dan jurnal Techno



Rachmat Adi Purnama M.Kom. Tahun 1997 lulus dari Program Strata Satu (S1) Program Studi Sistem Informasi STMIK BUDI LUHUR Jakarta. Tahun 2010 lulus dari Program Strata Dua (S2) Program Pascasarjana Magister Ilmu Komputer STMIK Nusa Mandiri Jakarta. Tahun 2011 sudah tersertifikasi dosen dengan Jabatan Fungsional Akademik Lektor di AMIK BSI Jakarta.