Quality of Service Gateway Load Balancing Protocol Message Digest algorithm 5 Authentication For Network Quality Enhancement

[1]**Firmansyah,** [2] **Rachmat Adi Purnama,** [3] **Mustofa,** [4] **Sari Dewi**
[1,3] System Information, STMIK Nusa Mandiri Jakarta
[2] Informatics Management, AMIK BSI Tegal
[4] Informatics Management, AMIK BSI Pontianak
021-7500680
e-mail: sari.sre@bsi.ac.id

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.

Keywords*: : Gateway Load Balancing Protocol, Quality of Service, Redundancy, Packet Loss*

1. Introduction

The stability of computer networks presently is an important aspect in determining the data transfer. Not only network devices are the main factor in determining the stability of a computer network. Software, network implementation also takes over in determining whether the network is stable or not.

The development of information technology will have an impact on human needs for information. Increasing network requirements, it will lead to network complexity and is expected to have a reliable network with good Quality of Service (QoS) support. To handle QoS on computer networks, we can use network devices, and software that suits our needs. And no less important is how to implement network devices that are used. QoS is the ability of a network to provide better services on certain data traffic in various types of technology platforms [8].

In this case, there are techniques to overcome the failure of QoS on the network. Technology that has good optimization capabilities that can be applied to the network is the Gateway Load Balancing Protocol (GLBP). GLBP is able to automatically redundancy against gateway addresses used on local networks when experiencing link problems.

2. Research Method

Gateway Load Balancing Protocol (GLBP) itself was born from the concept of load balancing, which is a useful concept for balancing loads or multiple links to the same remote network [1]. The results of the obtained throughput can occur due to the GLBP protocol as gateway redundancy [3].

***Gateway Load Balancing Protocol* (GLBP)**

GLBP is Cisco's propriertary protocol. GLBP provides different features wich the VRRP Protocol and the HSRP protocol do not have, named dynamic load balancing [7]. The difference between GLBP and VRRP and HSRP is the load balancing properties that are owned by the GLBP protocol itself. When using the GLBP protocol the network traffic at each gateway will be balanced, in contrast to the working concept of the VRRP and HSRP protocols that will run the standby / backup router if the active / master router experiences a problem. The redundancy group distributes forwarding addresses to hosts which turn out to be distributed forwarding addresses to send packets to the redundancy group [7]

Table 1. Deference beetwen 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*

In Table 1, the differences between the HSRP, VRRP and GLBP protocols are explained. Although HSRP, VRRP and GLBP have in common, it is important for you to know the problem solving as efficiently and effectively as possible [4]

***Active Virtual Gateway* (AVG)**

AVG is a router that acts as the chairman of all routers joined in a GLBP group. The GLBP router will choose AVG as the highest priority [6]. Routers with AVG status will be used as active routers / master routers. In general, GLBP specifies the rules and encoding specifications for sending data to and from the server farm. Members of a GLBP elect one gateway group to be the active virtual gateway (AVG) for that group [9].

***Active Virtual Forwarder* (AVF)**

AVF is useful as a representative of AVG, when the AVG router experiences problems, this AVF router will detect and replace the position of the AVG router. The AVF router acts as a router backup / standby.

***Standby Virtual Gateway (*SVG)**

The SCG router is the representative of the AVF router when the router experiences problems.

Load Balancing

Load Balancing is a technique used to distribute traffic loads on two or more connectivity paths in a balanced manner, with the aim of optimizing the network, maximizing throughput, and minimizing network delays and minimizing overloading of one connection path. Load Balancing and Fail Over methods use more than one gateway device in a group of gateway devices to communicate directed to a LAN network [2]

MD5 *Authentication*

MD 5 Authentication is used to provide security against the GLBP protocol. By using MD5 Authentication security, it is expected that the legality and security of data packets that will pass through the router has validated the password used

3. Results and Analysis

In this section, it is explained the results of research and at the same time is given the comprehensive discussion. Results can be presented in figures, graphs, tables and others that make the reader understand easily [2], [5]. The discussion can be made in several sub-chapters.

3.1 Network Desingn

The computer network topology used in this study can be seen in Figure 1. By using 2 routers that will be used as a redundancy of the network gateway IP on the local.

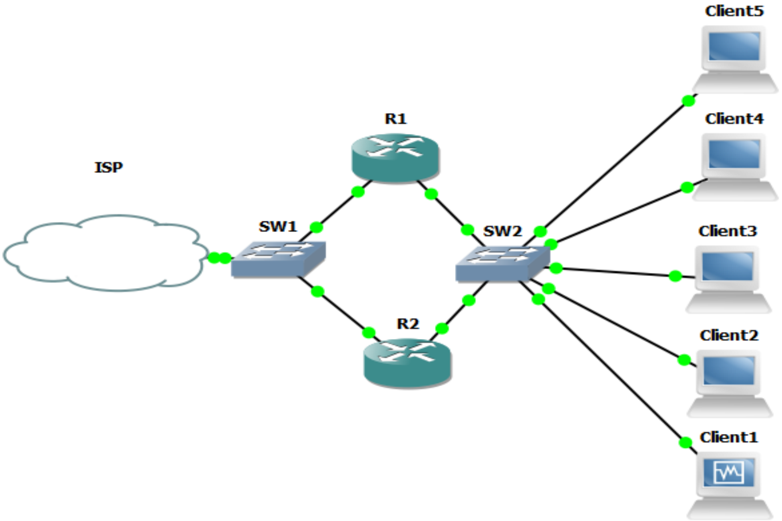


Figure 1. Network Thopology

Table 2. Specification of 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	-

Table 3. Specification of 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	-

If you look at table 2 and table 3, there are two gateway addresses that can be used for local networks. If the local network uses the gateway address 192.168.1.1 then the router that serves the local network is only router 1. Meanwhile, if the local route uses the gateway address 192.168.1.2 then the router that serves the local network is only router 2. This will cause one of the routers to not be used to the maximum extent possible. To maximize local network performance we can use a virtual gateway to run both routers simultaneously. The computer network that is formed in Figure 1 will use the gateway virtual address 192.168.1.254 with the aim of getting the redundancy gateway from router 1 and router 2.

Table 4. Spesifikasi GLBP

Spesifikasi	**R1**	**R2**
Interface	*FastEthernet*1/0	*FastEthernet*1/0
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

If you look at table 4, router 1 is used as an active / master router with the priority 200 value that is greater than the priority value used for router 2 with a value of 90.

GLBP for both routers uses the same group, namely group 1. While the Virtual IP used for both routers is 192.168.1.254/24. The group value or Virtual IP that will be used must have the same value. The interface that will be used as GLBP uses the FastEthernet1 / 0 interface.

3.2 Network Configuration

1. Configuration of GLBP Router 1

To configure GLBP for Router 1, there are several things that must be considered. Like the IP address that will be used on the FastEthernet0 / 0 interface that will be connected to internet access, FastEthernet1 / 0 will be used as the local network gateway address and the provision of Virtual IP addresses that will be used as a redundancy gateway on the local network.

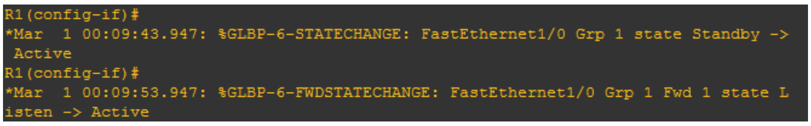
After knowing the specifications of the IP Address that will be used against Router 1, look in Table 2, then to configure GLBP against router 1, we can use the command:

```
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
```

This command is used to give the IP Address to the fastethernet1 / 0 interface with the IP address: 192.168.1.1/24. Next make the GLBP group to the fastethernet1 / 0 interface, and assign a virtual IP and ensure router 1 as the AVG router.

```
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
```

The preempt command is used to activate preemption against GLBP, which aims to get active status if the priority of another router has a smaller priority value.



```
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 L
isten -> Active
```

Figure 2. Activity of GLBP

In Figure 2, it is explained that router 1 has changed its state, which was previously standby and is now active state.

2. Configuration of GLBP Router 2

To configure GLBP against router 2, it is not much different from the configuration used for router 1, except that there is a difference between the IP address used, so that the IP address does not occur between router 1 and router 2. To configure router 2, we can use the command:

```
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
```

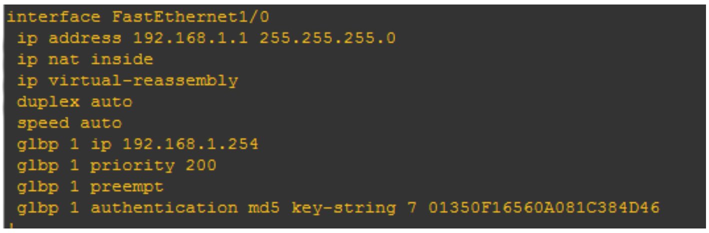
This command is used to give the IP Address to the fastethernet1 / 0 interface with the address 192.168.1.2/24. Then create a GLBP group on the FastEthernet1 / 0 interface, and assign a virtual IP and ensure router 1 as the AVF or router standby.R2(config)#int fa1/0

```
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. Configuration of *authentication* md5

MD5 authentication is used to provide authentication to the GLBP interface by using a password that has been encrypted. Router 1 and Router 2 must use the same password to communicate with each other.

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
```

Figure 3. Authentication of md5

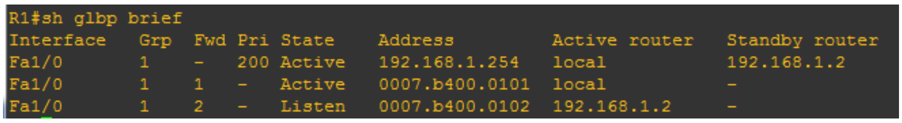
After configuring the md5 authentication for router 1, the router 2 or other router that will do GLBP communication to Group 1 must enter the same password as Authentication.

3.3 Connectivity Testing

GLBP

The first test is to test the connectivity of the GLBP network by testing the router 1 interface and router 2 to ensure that router 1 is the active router and router 2 is the standby router.

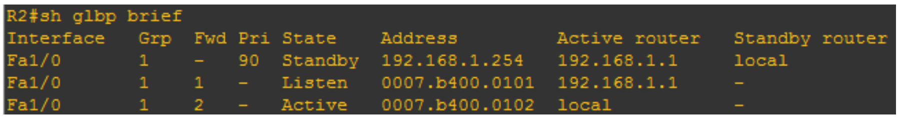
The way GLBP works is different from how VRRP and HSRP work. GLBP runs both routers simultaneously which means there are no routers that are only standby. GLBP aims to divide the network load to be equal, so that when inside the network it is connected to five (5) clients. Then the router load as a client gateway is divided equally between router 1 and router 2. However, when router 1 (active) experiences network problems the overall network traffic will be taken over by 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     -
```

Figure 4. GLBP Router 1

Seen in Figure 4, the Fastethernet1 / 0 interface has a priority of 200 with active state and uses GLBP group 1.



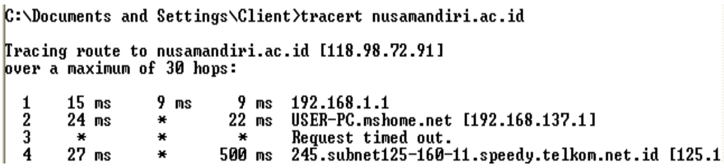
```
R2#sh glbp brief
Interface    Grp  Fwd Pri State    Address         Active router   Standby router
Fa1/0        1    -   90  Standby  192.168.1.254   192.168.1.1     local
Fa1/0        1    1   -   Listen   0007.b400.0101  192.168.1.1     -
Fa1/0        1    2   -   Active   0007.b400.0102  local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

Figure 5. GLBP 2

If you look at Figure 5, the fastethernet1 / 0 interface uses the GLBP 1 group with the priority value 90 with state standby. The thing that causes router 2 as router standby is because it has a lower priority value compared to the priority value used by router 1 which is 200.

Traceroute

The examiner then uses traceroute to get the hops passed from the client to connect to the network. The first client connected to the formed GLBP network will be connected using hops IP address 192.168.1.1 shown in figure 6. While the second client connected to the GLBP network will automatically use hops ip address 192.168.2.1 shown in Figure 7.

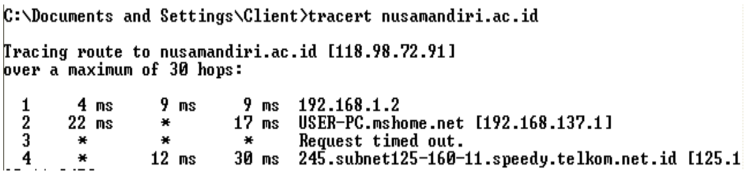


```
C:\Documents and Settings\Client>tracert nusamandiri.ac.id

Tracing route to nusamandiri.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.telkom.net.id [125.1
```

Figure 6. *Tracert Client* 1 Result



```
C:\Documents and Settings\Client>tracert nusamandiri.ac.id

Tracing route to nusamandiri.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.telkom.net.id [125.1
```

Figure 7. *Tracert Client* 2 Rasult

Table 4. Traceroute Client Result

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

The next client that is connected to the GLBP protocol will get hops according to the density of network traffic shown in Table 4. It can be seen in Figure 6 and Figure 7 that the network load is divided automatically into the two routers used. So, the two routers used together become the gateway of the local network with the same number of clients.

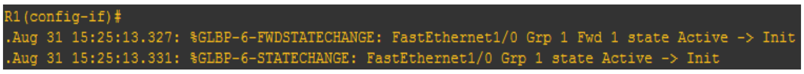
Redundancy Time Master to Standby

The test results on the time needed to do redundancy from the master router to router standby can be seen in Table 5. These results are taken by terminating access to the FastEthernet1 / 0 interface on router 1 and automatic redundancy of network traffic will occur via standby router / router2.

Table 5. *Redundancy Master to Standby*

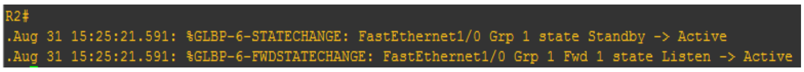
Percobaan	Router 1 *Off*	Router 2 *On*	*Time (Ms)*
1st	*15:12:18*	*15:12:26*	*00:00:08*
2nd	*15:16:03*	*15:16:09*	*00:00:06*
3rd	*15:18:23*	*15:18:31*	*00:00:08*
4th	*15:25:13*	*15:25:21*	*00:00:08*
5th	*15:40:01*	*14:40:09*	*00:00:08*
6th	*17:41:09*	*17:41:17*	*00:00:08*
7th	*17:45:33*	*17:45:40*	*00:00:07*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

In table 4, 10 tests have been carried out and the average time needed to redundancy from the master router to the standby router is 7.6 Ms. With the fastest time of 6 Ms. and the longest time of 8 Ms.



```
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
```

Figure 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
```

Figure 7. Router *Standby On*

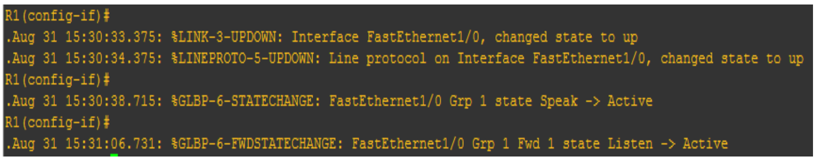
If you look at Figure 6, router 1 experiences network problems at 3:25:13 PM, and the router will automatically redundancy to router 2 to backup network traffic. The time needed by router 2 to redundancy router 1 to router 2 is about 6 Ms - 8 Ms shown in Figure 7.

Redundancy Time Standby to Master

The next test is to recover the FastEthernet1 / 0 interface on the router 1. This will result in the transfer of access that was previously handled by router 2 will be transferred back to the router 1. If you look at table 6, the average time needed to do redundancy from router 2 to router 1 around 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*



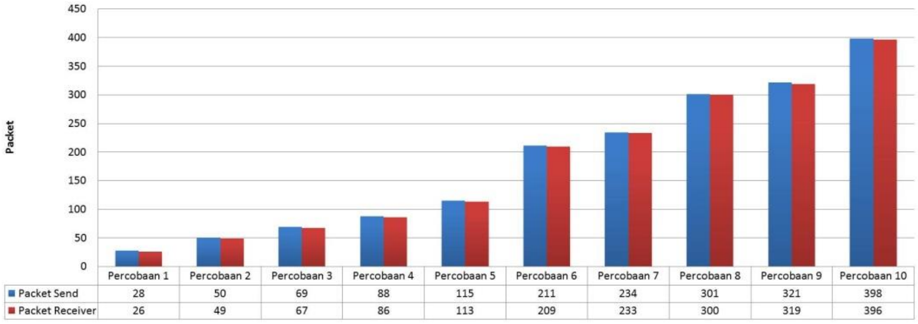
```
R1(config-if)#
.Aug 31 15:30:33.375: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
.Aug 31 15:30:34.375: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R1(config-if)#
.Aug 31 15:30:38.715: %GLBP-6-STATECHANGE: FastEthernet1/0 Grp 1 state Speak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

Gambar 8. *Redundancy* Router 2 ke Router 1

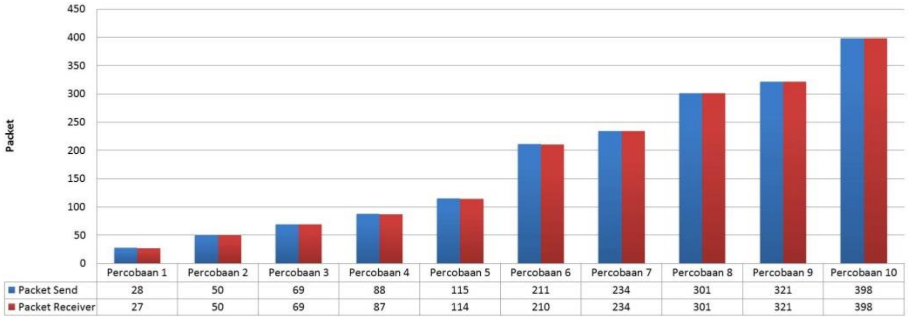
In Figure 8 you can explain the redundancy process that occurs with router 1 when the fastethernet1 / 0 interface state has returned to normal.

Packet Loss

Testing of packet loss is used to find out how much the GLBP network has experienced packet failure when an IP Gateway redundancy occurs from router 1 to the router 2.



Gambar 9. *Packet Loss Active to Standby*



	Percobaan 1	Percobaan 2	Percobaan 3	Percobaan 4	Percobaan 5	Percobaan 6	Percobaan 7	Percobaan 8	Percobaan 9	Percobaan 10
■ Packet Send	28	50	69	88	115	211	234	301	321	398
■ Packet Receiver	27	50	69	87	114	210	234	301	321	398

Gambar 10. *Packet Loss Standby to Active*

After testing 10 times seen in Figure 9 and Figure 10, the smallest packet loss that occurs when redundancy router 1 to router 2 is 1 packet that fails, while the highest packet loss is 2 packets that fail. The average packet loss obtained after 10 trials is 1.7 packets.

Whereas, the smallest packet loss that is obtained when a router 2 redundancy occurs to router 1 is 0 packet and the highest packet loss is 2 packets with an average packet loss obtained as much as 0.5 packet.

4. Conclusion

Based on the results of the analysis and discussion that have been described, the following conclusions that by using GLBP, computer networks will run more balanced. Because the load on the router is divided equally. The redundancy time needed when switching router 1 to router 2 is faster than redundancy router 2 to router 1. *Packet loss obtained when there is less standby to master redundancy than packet loss obtained when redundandy master to standby.* In the GLBP network, you should use two GLBP groups if the network used is very complex.

References

[1] http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glbp.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 (Gataway 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.