Jurnal Minfo Polgan
Volume 12, Nomor 1, Juli 2023
DOI : https://doi.org/10.33395/jmp.v12i1.12663
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Terbit : 01 Juli 2023

Failover Performance Analysis on Redundancy Link using Gateway Load Balancing Protocol

[1] Tri Sari D. N. B. Mira, [2] Fajar Hariadi
[1, 2]Program Studi Teknik Informatika, Universitas Kristen Wira Wacana Sumba

[1]tri@unkriswina.ac.id, [2]fajar@unkriswina.ac.id

ABSTRACT

Universitas Kristen Wira Wacana carries out various activities using an internet connection. Realizing the importance of this internet connection, the campus provides two different sources of internet connection. The first internet source (ISP1) has a speed of 100 Mbps, while the second internet source (ISP2) has a speed of 20 Mbps. The configuration that is currently used is less than optimal because if one of the internet sources used is disconnected, the internet connection for some campuses will be cut off, causing activities to be disrupted. In addition, the distribution of network loads is still not optimal where the second internet source (ISP2) is not used optimally due to the lack of activities that use this internet source. To overcome these two problems, a design was made by implementing the Gateway Load Balancing Protocol (GLBP) which can act as a redundancy link as well as load balancing. The simulation results of the implementation of GLBP can continue to provide internet connections to all local networks even though one internet line is disconnected and is able to divide the network load with a weight scale of 5 to 1, 5 weights for 100 Mbps internet connections and 1 weight for 20 Mbps internet connections. The failover and recovery process can be done in 1.36 seconds and 1.57 seconds if the path that is interrupted is the path to the internet, while if the path that is disconnected is the path to the local network, the failover and recovery process takes 7.70 seconds and 8.15 seconds, respectively.

Keywords: GLBP; Redundancy Link; Load Balancing; Failover; Recovery

INTRODUCTION

Internet connectivity is one of the important components that must be owned at this time. Problems in internet connection can cause problematic business process within an organization. Universitas Kristen Wira Wacana Sumba is an organization in the form of a university that carries out various activities using an internet connection. Realizing the importance of this internet connection, the campus provides two different sources of internet connection. The first internet source (ISP1) has a speed of 100 Mbps, while the second internet source (ISP2) has a speed of 20 Mbps. The first internet source (ISP1) is used to provide internet connection to Building A and Building B because these two buildings have more activity. The second internet source (ISP2) is used to provide internet connection in Buildings C and D which are new buildings with lower activity levels because they used as laboratories and libraries as well as activity hall rooms.

The configuration that is currently used is less than optimal because if one of the internet sources used is disconnected, the internet connection for some campuses will be interrupted which causes activities to be disrupted. In addition, because the activities of buildings A and B are denser than buildings C and D, the network load will be concentrated on the source of the first internet connection (ISP1) while the network load on the second internet connection (ISP2) will be less used because the activities are not congested.

To overcome the first problem Redundancy Link can be used, which the process of providing alternative paths to maintain network functionality when network problems occur

Jurnal Minfo Polgan
Volume 12, Nomor 1, Juli 2023 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v12i1.12663 p-ISSN : 2089-9424

(Shahriar, Newaz, Rashid, Rahman, & Rahman, 2018). If there is only one internet access and the path is experiencing any problems, then the internet connection is no longer available. A second or third internet connection needed as a backup or alternative, so if one of the paths experiencing any problems, the internet connection still can be provided using other paths that have been reserved (Khaing Khaing Wai, 2019). The second problem can be solve by Load Balancing to distribute network load over several available paths (Syaputra & Assegaff, 2017). This aims to balance network load so that network load does not accumulate on one line (Dewi & Purnama, 2019).

Redundancy links for internet connections can be formed with the First Hop Redundancy Protocol (FHRP). This protocol was designed to protect the main gateway used in the network by configuring several other gateway routers to become a backup when a problem occurs with the main gateway router. If there is a problem with the main router, within a few seconds the backup router will take over the role of the main router to be able to continue the existing network traffic (Sahoo & Goswami, 2014).

FHRP can be made using Virtual Router Redundancy Protocol (VRRP), Hot Standby Redundancy Protocol (HSRP) and Gateway Load Balancing Protocol (GLBP) (Pramawahyudi, Syahputra, & Ridwan, 2020). VRRP is a standard protocol of the Internet Engineering Task Force (IETF) and is an open standard that can be used by everyone by working by enabling several routers in one group to create a default gateway that is used to provide services to every host connected to that gateway (Mahdi & Hussain, 2013). HSRP is a protocol that works like VRRP but has standards that can only be used by Cisco devices, where the way it works is that several routers joined in one group will form one virtual router that is used as a gateway for each connected host, VRRP and HSRP will choose one of the physical routers in the group as the main router to forward all packets to be sent out of the network. If the main router is experiencing problems, then its role will be replaced by one of the router members in the same group (Mansour, 2020). However, VRRP and HSRP do not have Load Balancing capabilities, so if load balancing is needed, load balancing can be made manually, while GLBP support load balancing capabilities in the configuration (Singh & Raju, 2012). Load Balancing Algorithm in GLBP can be set as none or no load balancing used, weighted so each internet connection can be given some weight to provide more or less traffic, host dependent so traffic can be chosen based on the host, and the last one is round robin which each internet connection take turn as a sequence to provide the internet connectivity to the host (Cisco, 2008). Therefore, in the case faced by Universitas Kristen Wira Wacana Sumba, GLBP was chosen to be used as a redundancy link as well as load balancing.

RESEARCH METHOD

The research was carried out following the stages as shown in Figure 1. The research stages:

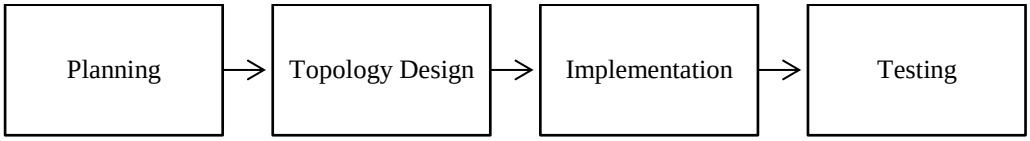

Figure 1. Research Stages

A. Planning

Planning starts from deciding the number and configuration of VLANs. There are 4 VLANs used with the configuration in Table 1. VLAN Design.

Table 1. VLAN Design

VLAN ID	VLAN Name	Network	Gateway
10	DOSEN	192.168.10.0 /24	192.168.10.254
20	PEGAWAI	192.168.20.0 /24	192.168.20.254
30	MAHASISWA	192.168.30.0 /24	192.168.30.254
40	TAMU	192.168.40.0 /24	192.168.40.254

Jurnal Minfo Polgan
Volume 12, Nomor 1, Juli 2023
DOI : https://doi.org/10.33395/jmp.v12i1.12663
e-ISSN : 2797-3298
p-ISSN : 2089-9424

This VLAN design will be implemented on switches SW1 and SW2 with VLAN access configurations to the hub and VLAN trunk configuration to the router. The configurations for both are made the same to make it easier to remember and implement. The configuration can be seen in Table 2. Port Types Configuration on SW1 and SW2:

Table 2. Port Types Configuration on SW1 and SW2

Port	VLAN	Type
G0/1	-	Trunk
G1/1	10	Access
G2/1	20	Access
G3/1	30	Access
G4/1	40	Access
G5/1	-	Trunk

GLBP also need to be planned with a load balancing weighted mode configuration because the bandwidth of the two gateways used is different, where the first gateway (GW1) is on the first router (R1) has a bandwidth of 100 Mbps and the second gateway (GW2) on the second router (R2) has a bandwidth of 20 Mbps. Since the GW1 bandwidth on R1 is 5 times the GW2 bandwidth on R2 the weight is 5 to 1 for each VLAN.

Tabel 3. Weighted Load Balancing

Group	VLAN	Weight on R1	Weight on R2
10	10	5	1
20	20	5	1
30	30	5	1
40	40	5	1

Preempt for each group is activated and tracking is carried out on the path to the internet with the configuration in Table 4. Configuration of GLBP Tracking Group:

Table 4. Configuration of GLBP Tracking Group:

Router	Group	Tracking
R1	10	G1/0
	20	G1/0
	30	G1/0
	40	G1/0
R2	10	G2/0
	20	G2/0
	30	G2/0
	40	G2/0

Tracking is used for changing the traffic route if the path from the switch to the router is good, but it is the Internet or ISP (Internet Service Provider) that is experiencing problems.

Jurnal Minfo Polgan
Volume 12, Nomor 1, Juli 2023
DOI : https://doi.org/10.33395/jmp.v12i1.12663
e-ISSN : 2797-3298
p-ISSN : 2089-9424

B. Topology Design

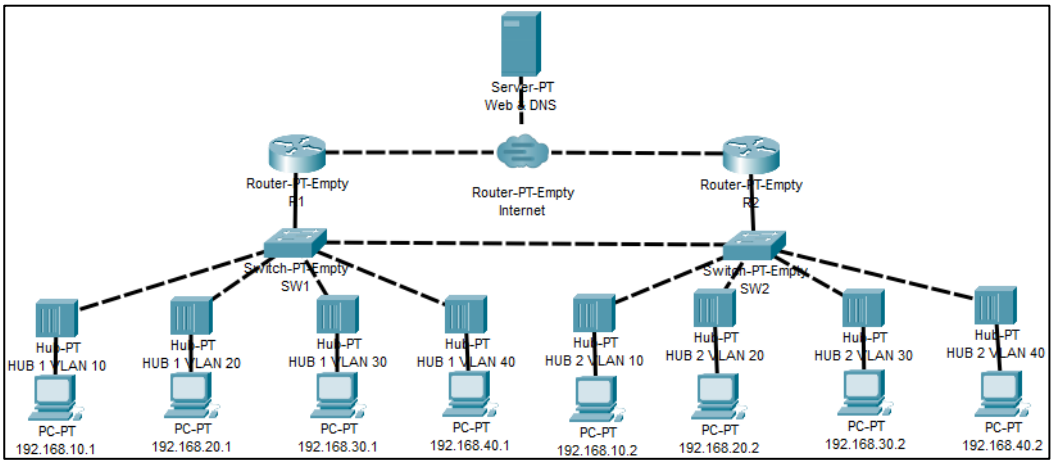

Figure 2. Network Topology

Based on the network topology in Figure 2. Network Topology, IP address configuration for R1 on each layer 3 interface that is connected to other devices shown in table 5. IP Address Configuration on R1.

Table 5. IP Address Configuration on R1

Port	Link	IP Address
G1/0	Internet	20.0.0.2 /8
G0/0.10	SW1	192.168.10.250 /24
G0/0.20	SW1	192.168.20.250 /24
G0/0.30	SW1	192.168.30.250 /24
G0/0.40	SW1	192.168.40.250 /24

In R2, the configuration of the IP addresses on each port interface and sub-interface is shown in Table 6. IP Address Configuration on R2:

Table 6. IP Address Configuration on R2

Port	Link	IP Address
G2/0	Internet	30.0.0.2 /8
G0/0.10	SW2	192.168.10.252 /24
G0/0.20	SW2	192.168.20.252 /24
G0/0.30	SW2	192.168.30.252 /24
G0/0.40	SW2	192.168.40.252 /24

All routers use RIP (Routing Information Protocol) as dynamic routing between all network addresses connected to the router. On routers R1 and R2, each path connected to the switch (SW1 and SW2) is a path with trunk mode to transmit data to each VLAN used.

C. Implementation

The implementation begins with the creation of a VLAN on SW1 which is set using the Command Line Interface (CLI).

Jurnal Minfo Polgan
Volume 12, Nomor 1, Juli 2023
DOI : https://doi.org/10.33395/jmp.v12i1.12663
e-ISSN : 2797-3298
p-ISSN : 2089-9424

```
SW1>ENABLE
SW1#VLAN DATABASE
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

SW1(vlan)#VLAN 10 NAME DOSEN
VLAN 10 added:
    Name: DOSEN
SW1(vlan)#VLAN 20 NAME PEGAWAI
VLAN 20 added:
    Name: PEGAWAI
SW1(vlan)#VLAN 30 NAME MAHASISWA
VLAN 30 added:
    Name: MAHASISWA
SW1(vlan)#VLAN 40 NAME TAMU
VLAN 40 added:
    Name: TAMU
```

Figure 3. Implementation of VLAN on SW1

The same VLAN is also applied to SW2, shown in Figure 4. Implementation of VLAN on SW2.

```
SW2(vlan)#VLAN 10 NAME DOSEN
VLAN 10 added:
    Name: DOSEN
SW2(vlan)#VLAN 20 NAME PEGAWAI
VLAN 20 added:
    Name: PEGAWAI
SW2(vlan)#VLAN 30 NAME MAHASISWA
VLAN 30 added:
    Name: MAHASISWA
SW2(vlan)#VLAN 40 NAME TAMU
VLAN 40 added:
    Name: TAMU
SW2(vlan)#
```

Figure 4. Implementation of VLAN on SW2

VLAN implementation on SW1 and SW2 follows the configuration in Table 1. VLAN Design in the planning section. After the VLAN has been successfully created, the next step is to configure the port type used for each outgoing path. Starting from SW1 which can be seen in Figure 5. Port Types Configuration on SW1:

```
SW1>ENABLE
SW1#CONFIGURE TERMINAL
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#INTERFACE G0/1
SW1(config-if)#SWITCHPORT MODE TRUNK
SW1(config-if)#INT G1/1
SW1(config-if)#SWITCHPORT ACCESS VLAN 10
SW1(config-if)#INT G2/1
SW1(config-if)#SWITCHPORT ACCESS VLAN 20
SW1(config-if)#INT G3/1
SW1(config-if)#SWITCHPORT ACCESS VLAN 30
SW1(config-if)#INT G4/1
SW1(config-if)#SWITCHPORT ACCESS VLAN 40
SW1(config-if)#INT G5/1
SW1(config-if)#SWITCHPORT MODE TRUNK
```

Figure 5. Port Types Configuration on SW1

The same configuration is also applied on SW2 as in Figure 6. Port Types Configuration on SW2:

Jurnal Minfo Polgan
Volume 12, Nomor 1, Juli 2023
DOI : https://doi.org/10.33395/jmp.v12i1.12663
e-ISSN : 2797-3298
p-ISSN : 2089-9424

```
SW2>ENABLE
SW2#CONFIGURE TERMINAL
Enter configuration commands, one per line.  End with CNTL/Z.
SW2(config)#INTERFACE G0/1
SW2(config-if)#SWITCHPORT MODE TRUNK
SW2(config-if)#INTERFACE G1/1
SW2(config-if)#SWITCHPORT ACCESS VLAN 10
SW2(config-if)#INTERFACE G2/1
SW2(config-if)#SWITCHPORT ACCESS VLAN 20
SW2(config-if)#INTERFACE G3/1
SW2(config-if)#SWITCHPORT ACCESS VLAN 30
SW2(config-if)#INTERFACE G4/1
SW2(config-if)#SWITCHPORT ACCESS VLAN 40
SW2(config-if)#INTERFACE G5/1
SW2(config-if)#SWITCHPORT MODE TRUNK
```

Figure 6. Port Types Configuration on SW2

Each layer 3 devices are assigned an IP address. Starting with the provision of IP addresses on the interface and sub-interface on R1. On sub-interfaces, before being given an IP address, Dot1Q encapsulation will be activated with the appropriate VLAN number. The process of assigning IP addresses can be seen in Figure 7. IP Address Configuration on R1:

```
R1>ENABLE
R1#CONFIGURE TERMINAL
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#INTERFACE G1/0
R1(config-if)#IP ADDRESS 20.0.0.2 255.0.0.0
R1(config-if)#INTERFACE G0/0.10
R1(config-subif)#ENCAPSULATION DOT1Q 10
R1(config-subif)#IP ADDRESS 192.168.10.252 255.255.255.0
R1(config-subif)#INTERFACE G0/0.20
R1(config-subif)#ENCAPSULATION DOT1Q 20
R1(config-subif)#IP ADDRESS 192.168.20.252 255.255.255.0
R1(config-subif)#INTERFACE G0/0.30
R1(config-subif)#ENCAPSULATION DOT1Q 30
R1(config-subif)#IP ADDRESS 192.168.30.252 255.255.255.0
R1(config-subif)#INTERFACE G0/0.40
R1(config-subif)#ENCAPSULATION DOT1Q 40
R1(config-subif)#IP ADDRESS 192.168.40.252 255.255.255.0
```

Figure 7. IP Address Configuration on R1

The configurations that are applied in R2 are shown in Figure 8. IP Address Configuration on R2:

```
R2>ENABLE
R2#CONFIGURE TERMINAL
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#INTERFACE G2/0
R2(config-if)#IP ADDRESS 30.0.0.2 255.0.0.0
R2(config-if)#INTERFACE G0/0.10
R2(config-subif)#ENCAPSULATION DOT1Q 10
R2(config-subif)#IP ADDRESS 192.168.10.253 255.255.255.0
R2(config-subif)#INTERFACE G0/0.20
R2(config-subif)#ENCAPSULATION DOT1Q 20
R2(config-subif)#IP ADDRESS 192.168.20.253 255.255.255.0
R2(config-subif)#INTERFACE G0/0.30
R2(config-subif)#ENCAPSULATION DOT1Q 30
R2(config-subif)#IP ADDRESS 192.168.30.253 255.255.255.0
R2(config-subif)#INTERFACE G0/0.40
R2(config-subif)#ENCAPSULATION DOT1Q 40
R2(config-subif)#IP ADDRESS 192.168.40.253 255.255.255.0
R2(config-subif)#
```

Figure 8. IP Address Configuration on R2

The last router that is configured is the router that acts as the internet. The configuration process can be seen in Figure 9. IP Address Configuration on Router Internet

```
Internet>ENABLE
Internet#CONFIGURE TERMINAL
Enter configuration commands, one per line.  End with CNTL/Z.
Internet(config)#INTERFACE G0/0
Internet(config-if)#IP ADDRESS 10.0.0.1 255.255.255.0
Internet(config-if)#INTERFACE G1/0
Internet(config-if)#IP ADDRESS 20.0.0.1 255.255.255.0
Internet(config-if)#INTERFACE G2/0
Internet(config-if)#IP ADDRESS 30.0.0.1 255.255.255.0
```

Jurnal Minfo Polgan
Volume 12, Nomor 1, Juli 2023
DOI : https://doi.org/10.33395/jmp.v12i1.12663
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Figure 9. IP Address Configuration on Router Internet

After all interfaces and sub-interfaces have IP addresses, the next step is to activate routing. The routing used is Routing Information Protocol (RIP) version 2. This step starts from R1 where the implementation process can be seen in Figure 10. RIP on R1:

```
R1>
R1>ENABLE
R1#CONFIGURE TERMINAL
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ROUTER RIP
R1(config-router)#VERSION 2
R1(config-router)#NETWORK 20.0.0.0
R1(config-router)#NETWORK 192.168.10.0
R1(config-router)#NETWORK 192.168.20.0
R1(config-router)#NETWORK 192.168.30.0
R1(config-router)#NETWORK 192.168.40.0
R1(config-router)#
```

Figure 10. RIP on R1

RIP is one of the dynamic routings, where we register each network address that is directly connected to the router. The same thing is done on router R2 where every directly connected network address is registered in the RIP.

```
R2>ENABLE
R2#CONFIGURE TERMINAL
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ROUTER RIP
R2(config-router)#VERSION 2
R2(config-router)#NETWORK 30.0.0.0
R2(config-router)#NETWORK 192.168.10.0
R2(config-router)#NETWORK 192.168.20.0
R2(config-router)#NETWORK 192.168.30.0
R2(config-router)#NETWORK 192.168.40.0
```

Figure 11. RIP on R2

The last implementation of RIP on routers was carried out on Internet routers which can be seen in Figure 12. RIP on the Internet.

```
Internet>ENABLE
Internet#CONFIGURE TERMINAL
Enter configuration commands, one per line.  End with CNTL/Z.
Internet(config)#ROUTER RIP
Internet(config-router)#VERSION 2
Internet(config-router)#NETWORK 10.0.0.0
Internet(config-router)#NETWORK 20.0.0.0
Internet(config-router)#NETWORK 30.0.0.0
```

Figure 12. RIP on the Internet

After RIP is installed on all three routers and all routers have shared routing tables. The Configuration of GLBP started using load balancing groups according to Table 3. Weighted Load Balancing, the weight given is 5 because the bandwidth on R1 is 100 Mbps.

```
R1(config-subif)#INT G0/0.10
R1(config-subif)#GLBP 10 IP 192.168.10.254
R1(config-subif)#GLBP 10 LOAD-BALANCING WEIGHTED
R1(config-subif)#GLBP 10 WEIGHT 5
R1(config-subif)#INT G0/0.20
R1(config-subif)#GLBP 20 IP 192.168.20.254
R1(config-subif)#GLBP 20 LOAD-BALANCING WEIGHTED
R1(config-subif)#GLBP 20 WEIGHT 5
R1(config-subif)#INT G0/0.30
R1(config-subif)#GLBP 30 IP 192.168.30.254
R1(config-subif)#GLBP 30 LOAD-BALANCING WEIGHTED
R1(config-subif)#GLBP 30 WEIGHT 5
R1(config-subif)#INT G0/0.40
R1(config-subif)#GLBP 40 IP 192.168.40.254
R1(config-subif)#GLBP 40 LOAD-BALANCING WEIGHTED
R1(config-subif)#GLBP 40 WEIGHT 5
```

Jurnal Minfo Polgan
Volume 12, Nomor 1, Juli 2023
DOI : https://doi.org/10.33395/jmp.v12i1.12663
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Figure 13. Implementation of GLBP Weighted 5 in R1

The same steps are carried out on R2 by giving a weight of 1 because the bandwidth on R2 is 20 Mbps. The application of GLBP to R2 can be seen in Figure 14.

```
R2(config-subif)#INT G0/0.10
R2(config-subif)#GLBP 10 IP 192.168.10.254
R2(config-subif)#GLBP 10 LOAD-BALANCING WEIGHTED
R2(config-subif)#GLBP 10 WEIGHT 1
R2(config-subif)#INT G0/0.20
R2(config-subif)#GLBP 20 IP 192.168.20.254
R2(config-subif)#GLBP 20 LOAD-BALANCING WEIGHTED
R2(config-subif)#GLBP 20 WEIGHT 1
R2(config-subif)#INT G0/0.30
R2(config-subif)#GLBP 30 IP 192.168.30.254
R2(config-subif)#GLBP 30 LOAD-BALANCING WEIGHTED
R2(config-subif)#GLBP 30 WEIGHT 1
R2(config-subif)#INT G0/0.40
R2(config-subif)#GLBP 40 IP 192.168.40.254
R2(config-subif)#GLBP 40 LOAD-BALANCING WEIGHTED
R2(config-subif)#GLBP 40 WEIGHT 1
```

Figure 14. Implementation of GLBP Weighted 1 in R2

Up to this stage, all configurations have been checked by ensuring that all VLAN configurations are in accordance with the design, and all PCs have been assigned the appropriate IP Address, Subnet Mask and Gateway. If everything is appropriate, the GLBP implementation process has been completed.

D. Testing

There are three types of tests used, the first is to observe the load balancing packet delivery path, the second test is used to observe the redundancy link failover timing when problems occur on the main line and the third test is used to observe the timing of the redundancy link returning to the main line when the main line is reconnected.

RESULTS

The first test results acquired by looking at the hops that are made when sending packets. The testing process can be seen in Figure 15. Example of a Traceroute:

```
Packet Tracer PC Command Line 1.0
C:\>TRACERT 10.0.0.2

Tracing route to 10.0.0.2 over a maximum of 30 hops:

  1    0 ms      1 ms      0 ms      192.168.10.252
  2    0 ms      0 ms      0 ms      20.0.0.1
  3    0 ms      1 ms      0 ms      10.0.0.2

Trace complete.
```

Figure 15. Example of a Traceroute

The traceroute from a PC with IP Address 192.168.10.1 which is VLAN 10 and Group HSRP 10 passing through line 192.168.10.252 on interface R1 which is the main route. The data obtained during the test based on the test scenario is shown in Table 9. Traceroute Data in Normal Conditions:

Table 7. Traceroute Data in Normal Conditions

VLAN	Source IP	Destination IP	Hop
10	192.168.10.1	10.0.0.2	R1
	192.168.10.2		R1
20	192.168.20.1	10.0.0.2	R1

Jurnal Minfo Polgan
Volume 12, Nomor 1, Juli 2023
DOI : https://doi.org/10.33395/jmp.v12i1.12663
e-ISSN : 2797-3298
p-ISSN : 2089-9424

VLAN	Source IP	Destination IP	Hop
	192.168.20.2		R1
30	192.168.30.1	10.0.0.2	R1
	192.168.30.2		R2
40	192.168.40.1	10.0.0.2	R1
	192.168.40.2		R1

From this table can be seen that load balancing has succeeded in dividing 5 to 1 packet delivery paths. Every time there is a request from the host 6 times, 5 packets will pass through R1, and the sixth packet will pass through R2. This treatment is repeated every time a new packet is sent.

The first test process with the second scenario where R1's internet connection is lost but R2's internet conditions are normal can be seen in Table 10. Traceroute Data on R1 Internet Disconnected:

Table 8. Traceroute Data When R1 Disconnected

VLAN	Source IP	Destination IP	Hop
10	192.168.10.1	10.0.0.2	R2
	192.168.10.2		R2
20	192.168.20.1	10.0.0.2	R2
	192.168.20.2		R2
30	192.168.30.1	10.0.0.2	R2
	192.168.30.2		R2
40	192.168.40.1	10.0.0.2	R2
	192.168.40.2		R2

The first test with the third scenario where R2's internet connection is lost but R1's internet is normal can be seen in Table 11. R2's Internet Traceroute Data Disconnects.

Table 9. Traceroute Data When R2 Disconnected

VLAN	Source IP	Destination IP	Hop
10	192.168.10.1	10.0.0.2	R1
	192.168.10.2		R1
20	192.168.20.1	10.0.0.2	R1
	192.168.20.2		R1
30	192.168.30.1	10.0.0.2	R1
	192.168.30.2		R1
40	192.168.40.1	10.0.0.2	R1
	192.168.40.2		R1

The first test with the fourth scenario where the internet connections R1 and R2 are lost can be seen in Table 12. Data Traceroute Internet R1 and R2 Disconnected.

Table 10. Traceroute Data When R1 and R2 Disconnected

VLAN	Source IP	Destination IP	Hop
10	192.168.10.1	10.0.0.2	Unreachable
	192.168.10.2		Unreachable
20	192.168.20.1	10.0.0.2	Unreachable
	192.168.20.2		Unreachable

Jurnal Minfo Polgan
Volume 12, Nomor 1, Juli 2023
DOI : https://doi.org/10.33395/jmp.v12i1.12663
e-ISSN : 2797-3298
p-ISSN : 2089-9424

VLAN	Source IP	Destination IP	Hop
30	192.168.30.1	10.0.0.2	Unreachable
	192.168.30.2		Unreachable
40	192.168.40.1	10.0.0.2	Unreachable
	192.168.40.2		Unreachable

From the first four test scenarios that have been done, it proves that GLBP is able to provide load balancing. In addition, GLBP is also able to provide backup connection if one of the lines is disconnected. The network will completely disconnect from the internet if both lines are disconnected at the same time. The second test process is done by disconnecting one of the lines on R1 and R2 alternately. The observed data is the length of time the process changes from active to standby status. The delta time between disconnected lines and the status change from standby to active calculated was used to determine the performance of failover capabilities of GLBP.

Table 11. Failover Test Results

Interface	Failover Time (s)			
	Group 10	Group 20	Group 30	Group 40
G1/0 – R1 G2/0 – R2	1.00	1.00	0.00	0.18
	2.00	0.98	2.24	2.24
	0.00	0.00	3.26	2.00
	2.00	1.00	3.00	2.00
	2.00	1.00	1.00	0.30
Average	1.40	0.80	1.9	1.34
G0/0 – R1 & R2	8.01	6.06	7.00	7.00
	9.00	8.00	8.33	8.00
	9.01	8.01	5.65	7.00
	7.00	9.13	7.00	7.00
	8.00	7.00	10.00	7.96
Average	8.20	7.64	7.60	7.39

From the second test, the average failover time results in average are 1.36 seconds if the internet lines disconnected. The average failover time results in average are 7.70 seconds if the local lines the one that disconnected. After the failover test, the next test is to reactivate the disconnected path and observe the time it takes for the router to re-send packets using the main path of each group.

Table 12. Recovery Test Results

Interface	Recovery Time (s)			
	Group 10	Group 20	Group 10	Group 40
G1/0 – R1 G2/0 – R2	2.00	2.00	3.00	2.00
	0.00	0.00	4.25	2.25
	0.00	2.00	0.00	3.00
	2.00	2.03	2.00	1.00
	1.00	1.00	1.00	1.00
Average	1.00	1.41	2.05	1.85
G0/0 – R1 & R2	8.01	8.01	9.00	9.00
	8.90	10.90	8.66	7.00

Jurnal Minfo Polgan
Volume 12, Nomor 1, Juli 2023 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v12i1.12663 p-ISSN : 2089-9424

Interface	Recovery Time (s)			
	Group 10	Group 20	Group 10	Group 40
	7.00	12.89	9.00	8.00
	8.00	8.00	5.97	1.97
	8.00	6.85	8.96	9.01
Average	7.98	9.33	8.32	7.00

Recovery time can be done in 1.57 seconds if the internet line disconnected and then reconnected. If the local lines disconnected and then reconnected, the average time recovery is 8.15 seconds.

CONCLUSION

The overall test results prove that GLBP can be used for load balancing as well as failover. It can be used to share the network traffic and able to handle problems if one of the internet lines used is disconnected, so that the local network can still be connected even if one of the lines is having problems. The process of changing lanes when a failover occurs can be done more quickly if the trouble path is the path that connected to the internet, with an average time of 1.36 seconds. However, if the trouble path is the path that is connected to the local network, the failover process takes longer with an average time of 7.70 seconds. This also applies to the recovery process with the average time results 1.57 seconds and 8.15 seconds respectively.

REFERENCES

Cisco. (2008). Campus Network for High Availability Design Guide Cisco. Cisco Systems, Inc. Cisco Systems, Inc. https://doi.org/10.1002/1097-0142(19880801)62:3<521::AID-CNCR2820620314>3.0.CO;2-F

Dewi, S., & Purnama, R. A. (2019). Quality of Service Gateway Load Balancing Protocol Message Digest Algorithm 5 Authentication untuk Peningkatan Kualitas Jaringan. Jurnal Teknik Informatika STMIK Antar Bangsa, V(1), 45–50.

Khaing Khaing Wai. (2019). Network Level Redundancy for Campus LAN. International Journal of Trend in Scientific Research and Development (IJTSRD) International Journal of Trend in Scientific Research and Development, 3(5), 1738–1743. https://doi.org/https://doi.org/10.31142/ijtsrd26768

Mahdi, A. J., & Hussain, A. A. (2013). Simulation of High Availability Internet Service Provider ' s Network. Iraqi Journal of Computer, Communication, Control and Systems Engineering (IJCCCE), 13(1).

Mansour, M. (2020). Performance evaluation of first hop redundancy protocols. Procedia Computer Science, 177(3), 330–337. https://doi.org/10.1016/j.procs.2020.10.044

Pramawahyudi, Syahputra, R., & Ridwan, A. (2020). Evaluasi Kinerja First Hop Redundancy Protocols untuk Topologi Star di Routing EIGRP. ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika, 8(3), 627. https://doi.org/10.26760/elkomika.v8i3.627

Sahoo, K., & Goswami, J. B. (2014). Redundancy Protocols for Campous Network. International Journal of Science Invention Today, 3(6), 611–624.

Shahriar, F., Newaz, S., Rashid, S. Z., Rahman, M. A., & Rahman, M. F. (2018). Designing a reliable and redundant network for multiple VLANs with Spanning Tree Protocol (STP) and Fast Hop Redundancy Protocol (FHRP). Proceedings of the International Conference on Industrial Engineering and Operations Management, 2018(SEP), 534–540.

Singh, G., & Raju, M. V. (2012). Dual gateway routing protocol. Proceedings: Turing 100 - International Conference on Computing Sciences, ICCS 2012, 350–355. https://doi.org/10.1109/ICCS.2012.27

Syaputra, A. W., & Assegaff, S. (2017). Analisis Dan Implementasi Load Balancing Dengan Metode Nth Pada Jaringan Dinas Pendidikan Provinsi Jambi. Jurnal Manajemen Sistem Informasi, 2(4), 831–844.