Manual Load Balancing pada *Redundancy Link* Menggunakan *Multi-Group Hot Standby Router Protocol*

http://dx.doi.org/10.28932/jutisi.v7i1.3403
Riwayat Artikel
Received: 14 Februari 2021 | *Final Revision*: 12 Maret 2021 | *Accepted*: 29 Maret 2021

Fajar Hariadi✉#1

Program Studi Teknik Informatika, Fakultas Sains dan Teknologi,
Universitas Kristen Wira Wacana Sumba
Jl. R. Suprapto No. 35 - Waingapu, Sumba Timur, NTT
fajar@unkriswina.ac.id

***Abstract* — Redundancy Link is an effort to prevent network problems by providing a backup path to the main line used. Redundancy link for layer 3 network has several methods, one of which is Hot Standby Router Protocol (HSRP). HSRP itself does not have a load balancing feature, therefore in this paper we will discuss the implementation of load balancing using several HSRP Groups that created manually on four VLANs. The result is that the transition process of failover and recovery handling goes smoothly and there is rarely a loss of packets or time out, but there is an increase in the delay for a while before finally returning to normal. In addition, it was found that there was a significant difference between the failover and recovery times required when there was a network problem on one physical interface and the interface with four sub-interfaces representing the four HSRP groups for each VLAN. Where the failover handling between the two has a time difference of 6.35 seconds, while the recovery time has a time difference of 6.58 seconds.**

***Keywords* — HSRP, Load Balancing, Redundancy Link**

I. PENDAHULUAN

Akses internet merupakan infrastruktur pendukung yang sangat penting. Hampir setiap aktivitas, baik aktivitas rumahan, perkantoran maupun pendidikan memanfaatkan koneksi internet. Terputusnya koneksi internet akan menjadi masalah yang menghambat jalannya aktivitas. Untuk meminimalisir terjadinya hal ini, dapat digunakan dua jalur sumber internet. Satu jalur merupakan jalur utama dan jalur satunya merupakan jalur alternatif apabila jalur utama terputus. Konsep ini dikenal dengan istilah *redundancy link* [1]. Ada tiga buah jenis *redundancy link* yaitu *Virtual Router Redundancy Protocol* (VRRP), *Hot Standby Router Protocol* (HSRP), dan *Gateway Load Balancing Protocol* (GLBP) [2].

Redundancy link menggunakan VRRP dan HSRP tidak disertai dengan fitur *load balancing* [2]. Sedangkan *redundancy link* yang menggunakan GLBP sudah langsung disertai dengan fitur *load balancing* [3]. Sehingga pada GLBP beban jaringan dapat dibagi ke beberapa jalur yang ada, dengan jumlah maksimal 4 jalur [4].

VRRP merupakan sebuah *Protocol multi-vendor* sehingga banyak perangkat dapat menggunakan VRRP, sedangkan HSRP dan GLBP merupakan milik *Cisco*, sehingga hanya dapat digunakan pada perangkat *Cisco* [5]. Hal ini membuat GLBP dapat menggunakan beberapa *gateway* fisik secara bersamaan, pemilihan jalur fisik aktif otomatis dan perubahan jalur otomatis apabila terjadi kesalahan pada salah satu jalur *gateway* [6].

GLBP sendiri memiliki performa yang lebih baik dibandingkan VRRP dan HSRP dalam hal penggunaan CPU pada *router*, penggunaan *bandwidth* untuk komunikasi antar *router* fisik dan kecepatan dalam mengaktifkan jalur cadangan pada saat jalur utama terputus [7]. GLBP juga memiliki kinerja *traffic flow* yang lebih baik dari VRRP dan HSRP [8]. Bahkan dengan adanya fitur *load balancing* bawaan GLBP jarang didapati terjadi *packet missing* walaupun salah satu jalur yang digunakan terputus [9]. Walaupun pada kasus spesifik dalam hal layanan *video streaming* GLBP memiliki kinerja yang lebih rendah dibandingkan HSRP [2]. Tapi dari semua hasil penelitian di atas didapati bahwa VRRP memiliki kinerja yang paling lebih rendah dibandingkan dengan HSRP dan GLBP.

Meskipun GLBP memiliki kinerja yang lebih baik, fitur *load balancing* secara otomatis pada beberapa kasus tidak dikehendaki. Misalnya apabila kita menginginkan beberapa VLAN harus melewati suatu *firewall* untuk *filtering traffic* yang lewat, atau apabila salah satu *gateway* memiliki layanan berlangganan berdasarkan kuota seperti VPN atau akses terhadap situs tertentu yang mencatat kuota berdasarkan *IP Public* yang digunakan oleh salah satu *gateway*. Selain itu

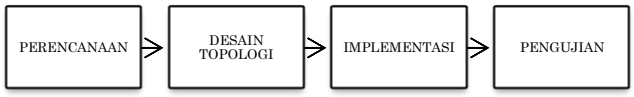
load balancing pada GLBP bekerja dengan cara membagi *traffic* melalui beberapa *Virtual Mac Address*, hal ini berbeda dengan VRRP dan HSRP yang hanya menggunakan satu buah *Virtual Mac Address* [10]. Hal ini memungkinkan terjadinya *hop* tambahan dalam proses pengiriman paket, khususnya apabila menggunakan *switch layer 3* dengan perpaduan *Spanning Tree Protocol* [11]. Penambahan *hop* ini tidak terasa apabila skala jaringan atau jumlah *client* sedikit, tetapi dalam skala besar penambahan *hop* ini membuat pengiriman paket dalam jaringan menjadi tidak optimal.

Load balancing sendiri bisa ditambahkan secara manual pada penerapan VRRP dan HSRP. Sehingga kita dapat membagi *traffic data* yang melalui setiap *gateway* dengan VLAN tertentu saja sesuai dengan kebutuhan, dan hanya membagi *traffic* salah *gateway* apabila *gateway* yang sudah ditetapkan mengalami *trouble*. Disini akan membahas bagaimana menerapkan hal tersebut diatas menggunakan HSRP, karena pada beberapa penelitian sebelumnya, HSRP memiliki kinerja yang lebih baik dibanding VRRP.

Parameter yang akan diamati adalah perbandingan jalur yang dilewati dalam kondisi normal dan kondisi salah satu *gateway* terputus, serta kecepatan perpindahan jalur pada saat jalur pengiriman data dialihkan.

II. METODE PENELITIAN

Penelitian dilakukan mengikuti tahapan seperti terlihat pada gambar 1. Tahapan Penelitian sebagai berikut:



Gambar 1. Tahapan Penelitian

A. Perencanaan

Perencanaan dimulai dari menyusun jumlah dan konfigurasi VLAN. VLAN yang digunakan berjumlah 4 dengan konfigurasi pada Tabel 1. Desain VLAN.

TABEL I
DESAIN VLAN

VLAN	Nama VLAN (*Network* & *Gateway*)	
10	DOSEN	*Net Address* 192.168.10.0 /24
		Gateway 192.168.10.254
20	PEGAWAI	*Net Address* 192.168.20.0 /24
		Gateway 192.168.20.254
30	MAHASISWA	*Net Address* 192.168.30.0 /24
		Gateway 192.168.30.254
40	TAMU	*Net Address* 192.168.40.0 /24
		Gateway 192.168.40.254

Desain VLAN ini akan diimplementasikan kepada *switch* SW1 dan SW2 dengan konfigurasi jalur *access* menuju *hub* dan *trunk* menuju *router*. Konfigurasi pada keduanya dibuat sama persis agar lebih memudahkan mengingat dan melakukan implementasi. Konfigurasi dapat dilihat pada Tabel II. Konfigurasi Tipe *Port* SW1 dan SW2 berikut:

TABEL II
KONFIGURASI TIPE PORT SW1 DAN SW2

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

Selanjutnya perencanaan *group* HSRP berdasarkan VLAN dan pengaturan *load balancing* secara manual pada dua *router* (R1, R2) yang digunakan sebagai jalur internet.

TABEL III
GROUP LOAD BALANCING HSRP

Group	VLAN	Active	Standby
10	10	R1	R2
20	20	R1	R2
30	30	R2	R1
40	40	R2	R1

Setiap *router* yang memiliki status *Active* akan menggunakan nilai priority 105, sedangkan pada *router mode Standby* akan menggunakan nilai *priority* 100.

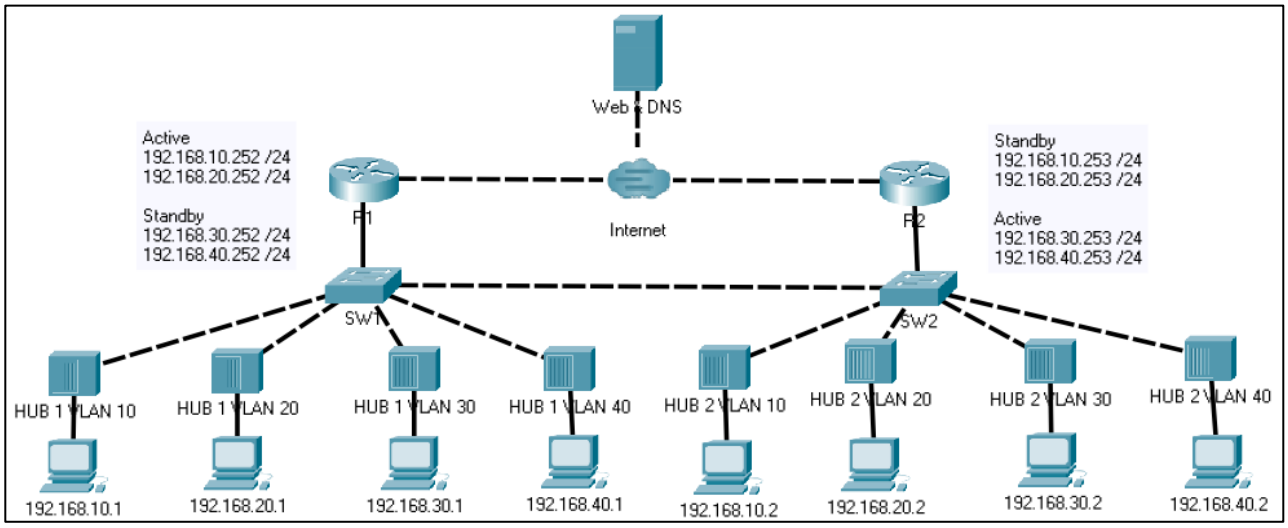
Preempt untuk setiap *group* diaktifkan dan dilakukan *tracking* terhadap jalur menuju internet dengan konfigurasi pada Tabel 4. Konfigurasi *Tracking Group* berikut ini:

TABEL IV
KONFIGURASI 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 digunakan untuk pengalihan jalur bila jalur dari *switch* menuju *router* baik, akan tetapi dari Internet atau ISP (*Internet Service Provider*) yang mengalami masalah.

p-ISSN : 2443-2210
e-ISSN : 2443-2229



Gambar 2. Topologi Jaringan

B. Desain Topologi

Berdasarkan topologi jaringan pada Gambar 2. Topologi Jaringan, dilakukan pengaturan *ip address* setiap *interface layer 3* yang terhubung dengan perangkat lainnya. Pengaturan *ip address* pada perangkat R1 dapat dilihat pada Tabel 5. Konfigurasi *IP Address* R1 di bawah ini:

TABEL V
KONFIGURASI *IP ADDRESS* R1

Port	***Link* Tujuan**	***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

Pada R2 konfigurasi *ip address* pada setiap *port interface* dan *sub-interface* terlihat pada Tabel 6. Konfigurasi *IP Address* R2 berikut:

TABEL VI
KONFIGURASI *IP ADDRESS* R2

Port	***Link* Tujuan**	***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

Sedangkan pada *router* internet, konfigurasi *ip address* yang dilakukan terlihat sebagai berikut:

TABEL VII
KONFIGURASI *IP ADDRESS* INTERNET

Port	***Link* Tujuan**	***IP Address***
G0/0	Web & DNS	10.0.0.1 /8
G1/0	R1	20.0.0.1 /8
G2/0	R2	30.0.0.1 /8

Ketiga *router* menggunakan RIP (R*outing Information Protocol*) sebagai routing dinamis di antara semua alamat jaringan yang terhubung dengan *router*. Pada *router* R1 dan R2 setiap jalur yang terhubung dengan *switch* (SW1 dan SW2) merupakan jalur dengan mode *trunk* untuk mengirimkan data ke setiap VLAN yang digunakan.

C. Implementasi

Penerapan dari rencana dan desain dimulai dari pembuatan VLAN pada SW1.

```
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
```

Gambar 3. Penerapan VLAN pada SW1

Kemudian VLAN yang sama juga diterapkan pada SW2, terlihat pada gambar 4. Penerapan VLAN pada 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)#
```

Gambar 4. Penerapan VLAN pada SW2

Penerapan VLAN pada SW1 dan SW2 mengikuti konfigurasi pada Tabel 1. Desain VLAN pada bagian perencanaan. Setelah VLAN berhasil dibuat, selanjutnya dilakukan konfigurasi tipe *port* yang digunakan untuk setiap jalur yang keluar. Dimulai dari SW1 yang dapat dilihat pada Gambar 5. Konfigurasi Tipe *Port* SW1 berikut ini:

```
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
```

Gambar 5. Penerapan Tipe Port pada SW1

Konfigurasi yang sama juga dilakukan pada SW2, terlihat pada Gambar 6. Penerapan Tipe *Port* pada SW2 berikut:

```
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
```

Gambar 6. Penerapan Tipe Port pada SW2

Selanjutnya setiap perangkat *layer 3* diberikan *ip address*. Dimulai dengan pemberian *ip address* pada *interface* dan *sub-interface* pada R1. Khusus *sub-interface*, sebelum diberikan *ip address* akan diaktifkan terlebih dahulu *encapsulation Dot1Q* dengan nomor VLAN yang sesuai. Proses pemberian *ip address* dapat dilihat pada Gambar 7. Konfigurasi *IP Address* R1 berikut ini:

```
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
```

Gambar 7. Konfigurasi IP Address R1

Pada router R2 dilakukan konfigurasi sesuai dengan Tabel 7. Konfigurasi *IP Address* R2. Proses Konfigurasi dapat dilihat pada Gambar 8. Konfigurasi *IP Address* R2 berikut ini:

```
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)#
```

Gambar 8. Konfigurasi IP Address R2

Router terakhir yang dikonfigurasi adalah *router* yang berperan sebagai internet. Skema konfigurasi yang dilakukan sesuai dengan Tabel 8. Konfigurasi *IP Address* Internet. Proses konfigurasi dapat dilihat pada Gambar 9. Konfigurasi IP Address Internet berikut ini:

```
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
```

Gambar 9. Konfigurasi IP Address Internet

Setelah semua *interface* dan *sub-interface* memiliki *ip address*, maka selanjutnya adalah mengaktifkan *routing*. *Routing* yang digunakan adalah *Routing Information Protocol* (RIP) versi 2. Langkah ini dimulai dari R1 dimana proses penerapannya dapat dilihat pada Gambar 10. RIP pada R1 berikut ini:

```
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)#
```

Gambar 10. RIP pada R1

RIP merupakan salah satu *routing* dinamis, dimana kita harus mendaftarkan setiap alamat jaringan yang terhubung langsung dengan *router*. Hal yang sama juga dilakukan pada *router* R2.

p-ISSN : 2443-2210
e-ISSN : 2443-2229

```
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
```

Gambar 11. RIP pada R2

Penerapan RIP pada *router* yang terakhir dilakukan pada *router* Internet yang dapat dilihat pada Gambar 12. RIP pada 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
```

Gambar 12. RIP pada Internet

Setelah RIP terpasang pada ketiga *router* dan semua *router* sudah saling berbagi *routing table*. Maka selanjutnya membuat *group load balancing* sesuai Tabel 4. *Group Load Balancing* HSRP, mengaktifkan *tracking* sesuai Tabel 5. Konfigurasi *Tracking Group*, memberi nilai *priority* 105 untuk *router active* dan nilai *priority* 100 untuk *router standby* serta mengaktifkan *preempt* untuk setiap *group* pada R1 dan R2. Dimana penerapan pada R1 dapat dilihat pada Gambar 13. HSRP pada R1 di bawah ini:

```
R1>ENABLE
R1#CONFIGURE TERMINAL
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#INTERFACE G0/0.10
R1(config-subif)#STANDBY 10 IP 192.168.10.254
R1(config-subif)#STANDBY 10 PRIORITY 105
R1(config-subif)#STANDBY 10 PREEMPT
R1(config-subif)#STANDBY 10 TRACK G1/0
R1(config-subif)#INTERFACE G0/0.20
R1(config-subif)#STANDBY 20 IP 192.168.20.254
R1(config-subif)#STANDBY 20 PRIORITY 105
R1(config-subif)#STANDBY 20 PREEMPT
R1(config-subif)#STANDBY 20 TRACK G1/0
R1(config-subif)#INTERFACE G0/0.30
R1(config-subif)#STANDBY 30 IP 192.168.30.254
R1(config-subif)#STANDBY 30 PRIORITY 100
R1(config-subif)#STANDBY 30 PREEMPT
R1(config-subif)#STANDBY 30 TRACK G1/0
R1(config-subif)#INTERFACE G0/0.40
R1(config-subif)#STANDBY 40 IP 192.168.40.254
R1(config-subif)#STANDBY 40 PRIORITY 100
R1(config-subif)#STANDBY 40 PREEMPT
R1(config-subif)#STANDBY 40 TRACK G1/0
```

Gambar 13. HSRP pada R1

Berikut ini adalah hasil validasi terhadap konfigurasi yang dilakukan pada R1:

```
R1>ENABLE
R1#SHOW STANDBY
GigabitEthernet0/0.10 - Group 10
State is Active
11 state changes, last state change 05:15:07
Virtual IP address is 192.168.10.254
Active virtual MAC address is 0000.0C07.AC0A
Local virtual MAC address is 0000.0C07.AC0A (v1
default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.292 secs
Preemption enabled
Active router is local
Standby router is 192.168.10.253
Priority 105 (configured 105)
Track interface GigabitEthernet1/0 state Up decrement 10
Group name is hsrp-Gig-10 (default)
GigabitEthernet0/0.20 - Group 20
State is Active
9 state changes, last state change 05:14:46
Virtual IP address is 192.168.20.254
Active virtual MAC address is 0000.0C07.AC14
Local virtual MAC address is 0000.0C07.AC14 (v1
default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.747 secs
Preemption enabled
Active router is local
Standby router is 192.168.20.253
Priority 105 (configured 105)
Track interface GigabitEthernet1/0 state Up decrement 10
Group name is hsrp-Gig-20 (default)
GigabitEthernet0/0.30 - Group 30
State is Standby
35 state changes, last state change 05:22:29
Virtual IP address is 192.168.30.254
Active virtual MAC address is 0000.0C07.AC1E
Local virtual MAC address is 0000.0C07.AC1E (v1
default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.101 secs
Preemption enabled
Active router is 192.168.30.253, priority 105 (expires in 7
sec)
MAC address is 0000.0C07.AC1E
Standby router is local
Priority 100 (default 100)
Track interface GigabitEthernet1/0 state Up decrement 10
Group name is hsrp-Gig-30 (default)
GigabitEthernet0/0.40 - Group 30
State is Active
8 state changes, last state change 05:10:20
Virtual IP address is 192.168.30.254
Active virtual MAC address is 0000.0C07.AC1E
Local virtual MAC address is 0000.0C07.AC1E (v1
default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.754 secs
Preemption enabled
Active router is local
Standby router is unknown
Priority 100 (default 100)
Group name is hsrp-Gig-30 (default)
```

```
GigabitEthernet0/0.40 - Group 40
State is Standby
18 state changes, last state change 05:22:30
Virtual IP address is 192.168.40.254
Active virtual MAC address is 0000.0C07.AC28
Local virtual MAC address is 0000.0C07.AC28 (v1
default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.524 secs
Preemption enabled
Active router is 192.168.40.253
Standby router is local
Priority 100 (default 100)
Track interface GigabitEthernet1/0 state Up decrement 10
Group name is hsrp-Gig-40 (default)
```

Setelah load balancing HSRP pada R1 telah selesai dilakukan dan divalidasi, maka dilanjutkan dengan mengkonfigurasi R2 agar kerja sama antar router dapat dibentuk. Proses konfigurasi pada R2 terlihat pada Gambar 14. HSRP pada R2 di bawah ini:

```
R2>ENABLE
R2#CONFIGURE TERMINAL
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#INTERFACE G0/0.10
R2(config-subif)#STANDBY 10 IP 192.168.10.254
R2(config-subif)#STANDBY 10 PRIORITY 100
R2(config-subif)#STANDBY 10 PREEMPT
R2(config-subif)#STANDBY 10 TRACK G2/0
R2(config-subif)#INTERFACE G0/0.20
R2(config-subif)#STANDBY 20 IP 192.168.20.254
R2(config-subif)#STANDBY 20 PRIORITY 100
R2(config-subif)#STANDBY 20 PREEMPT
R2(config-subif)#STANDBY 20 TRACK G2/0
R2(config-subif)#INTERFACE G0/0.30
R2(config-subif)#STANDBY 30 IP 192.168.30.254
R2(config-subif)#STANDBY 30 PRIORITY 105
R2(config-subif)#STANDBY 30 PREEMPT
R2(config-subif)#STANDBY 30 TRACK G2/0
R2(config-subif)#INTERFACE G0/0.40
R2(config-subif)#STANDBY 40 IP 192.168.40.254
R2(config-subif)#STANDBY 40 PRIORITY 105
R2(config-subif)#STANDBY 40 PREEMPT
R2(config-subif)#STANDBY 40 TRACK G2/0
```

Gambar 14. HSRP pada R2

Hasil validasi HSRP terhadap konfigurasi yang dilakukan pada R2:

```
R2>ENABLE
R2#SHOW STANDBY
GigabitEthernet0/0.10 - Group 10
  State is Standby
    12 state changes, last state change 05:21:46
  Virtual IP address is 192.168.10.254
  Active virtual MAC address is 0000.0C07.AC0A
    Local virtual MAC address is 0000.0C07.AC0A (v1
default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.895 secs
  Preemption enabled
  Active router is 192.168.10.252
  Standby router is local
  Priority 100 (default 100)
    Track interface GigabitEthernet2/0 state Up decrement
10
  Group name is hsrp-Gig-10 (default)
GigabitEthernet0/0.20 - Group 20
  State is Standby
    12 state changes, last state change 05:21:44
  Virtual IP address is 192.168.20.254
  Active virtual MAC address is 0000.0C07.AC14
    Local virtual MAC address is 0000.0C07.AC14 (v1
default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.142 secs
  Preemption enabled
  Active router is 192.168.20.252
  Standby router is local
  Priority 100 (default 100)
    Track interface GigabitEthernet2/0 state Up decrement
10
  Group name is hsrp-Gig-20 (default)
GigabitEthernet0/0.30 - Group 30
  State is Active
    15 state changes, last state change 05:21:45
  Virtual IP address is 192.168.30.254
  Active virtual MAC address is 0000.0C07.AC1E
    Local virtual MAC address is 0000.0C07.AC1E (v1
default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.376 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.30.252, priority 100 (expires
in 7 sec)
  Priority 105 (configured 105)
    Track interface GigabitEthernet2/0 state Up decrement
10
  Group name is hsrp-Gig-30 (default)
GigabitEthernet0/0.40 - Group 40
  State is Active
    12 state changes, last state change 05:21:54
  Virtual IP address is 192.168.40.254
  Active virtual MAC address is 0000.0C07.AC28
    Local virtual MAC address is 0000.0C07.AC28 (v1
default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.369 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.40.252, priority 100 (expires
in 6 sec)
  Priority 105 (configured 105)
    Track interface GigabitEthernet2/0 state Up decrement
10
  Group name is hsrp-Gig-40 (default)
```

Sampai dengan tahap ini dilakukan pemeriksaan terhadap semua konfigurasi yang telah dilakukan dengan memastikan seluruh konfigurasi VLAN sudah sesuai rancangan, dan seluruh PC telah diberikan *ip address*, *subnet mask* dan *gateway* yang sesuai. Apabila semua telah sesuai maka proses implementasi HSRP telah selesai dilakukan. Tahap selanjutnya adalah menentukan skenario pengujian sebagai acuan dalam mengambil data yang diperlukan.

D. Pengujian

Pengujian yang dilakukan ada tiga jenis, yang pertama digunakan untuk mengamati jalur pengiriman paket *load balancing*, pengujian kedua digunakan untuk mengamati kecepatan *redundancy link* mengatasi permasalahan pada jalur utama dan pengujian ketiga digunakan untuk mengamati kecepatan *redundancy link* kembali ke jalur utama apabila jalur utama sudah kembali terhubung.

Tipe pengujian pertama dilakukan dengan mengamati jalur pengiriman paket dengan melakukan *traceroute* dari seluruh *PC Client* yang berjumlah 8 buah menuju *PC Web Server* yang sekaligus menjadi *DNS Server*. Skenario pengujian *traceroute* dapat dilihat pada Tabel 8. Skenario Pengujian *Traceroute* berikut:

TABEL VIII
SKENARIO PENGUJIAN *TRACEROUTE*

VLAN	IP Asal	IP Tujuan
10	192.168.10.1	10.0.0.2
	192.168.10.2	
20	192.168.20.1	10.0.0.2
	192.168.20.2	
30	192.168.30.1	10.0.0.2
	192.168.30.2	
40	192.168.40.1	10.0.0.2
	192.168.40.2	

Skenario ini akan dilakukan berulang pada tiga kondisi berikut:

1. Normal
2. Jalur dari R1 ke Internet terputus
3. Jalur dari R2 ke Internet terputus

Selain *traceroute* akan dilakukan pula pengamatan pada mode simulasi *Cisco Packet Tracer* untuk melihat jalur pengiriman paket data yang digunakan.

Tipe pengujian kedua dilakukan dengan mengamati selisih waktu pada *debug log router* R1 & R2 pada saat terjadi pemutusan koneksi jalur utama dan perubahan *state* dari *standby* menjadi *active* pada jalur *backup* setiap *group*.

Pada tipe pengujian ketiga mirip seperti tipe pengujian kedua, namun yang diamati adalah selisih waktu antara jalur utama yang tadinya terputus menjadi tersambung kembali dengan perubahan *state* jalur utama dari *standby* menjadi *active* kembali.

III. HASIL DAN PEMBAHASAN

Proses pengujian pertama dapat dilihat pada Gambar 15. Contoh *Traceroute* di bawah ini:

```
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.
```

Gambar 15. Contoh Traceroute

Pada gambar terlihat proses *traceroute* dari PC dengan *ip address* 192.168.10.1 yang merupakan VLAN 10 dan *Group* HSRP 10 melewati jalur 192.168.10.252 pada *interface* R1 yang merupakan jalur utamanya. Data yang didapat pada saat pengujian berdasarkan skenario pengujian terlihat pada Tabel 9. Data *Traceroute* berikut ini:

TABEL IX
DATA *TRACEROUTE*

VLAN	IP Asal	IP Tujuan	*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	R2
	192.168.30.2		R2
40	192.168.40.1	10.0.0.2	R2
	192.168.40.2		R2

Dari tabel ini dapat dilihat *load* balancing secara manual sudah berhasil membagi VLAN 10 dan 20 melewati R1 sebagai jalur utamanya dan R2 sebagai jalur cadangan. Sedangkan VLAN 30 dan 40 melewati R2 yang merupakan jalur utamanya dengan R1 sebagai jalur cadangan.

Proses pengujian kedua dapat dilihat pada Gambar 16. Contoh Pemutusan Jalur Utama di bawah ini:

```
R1>ENABLE
R1#CONFIGURE TERMINAL
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#INTERFACE G1/0
R1(config-if)#SHUTDOWN

R1(config-if)#
*Mar 01, 00:36:12.3636: %LINK-5-CHANGED: Interface
GigabitEthernet1/0, changed state to administratively down
*Mar 01, 00:36:12.3636: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet1/0, changed state to down
```

Gambar 16. Contoh Pemutusan Jalur Utama

Data waktu pada saat jalur utama terputus ini akan menjadi acuan dalam selisih perhitungan ketika terjadi perubahan jalur cadangan dari *standby* menjadi *active* seperti terlihat pada Gambar 17. Contoh *Standby* Jadi *Active*

```
R2>
*Mar 01, 00:36:12.3636:  %HSRP-6-STATECHANGE: GigabitEthernet0/0.20
Grp 20 state Standby -> Active
*Mar 01, 00:36:14.3636:  %HSRP-6-STATECHANGE: GigabitEthernet0/0.10
Grp 10 state Standby -> Active
```

Gambar 17. Contoh Standby Jadi Active

Pada gambar 17 terlihat jalur cadangan *Group* 10 berubah menjadi *active* terlihat pada *timestamp* 00:36:14.3636 (hh:mm:ss.ms) sedangkan jalur utama terputus pada gambar 16 pada waktu 00:36:12.3636 (hh:mm:ss.ms), dari selisih waktu ini berarti HSRP mulai mengaktifkan jalur cadangan untuk *Group* 10 selama 3 detik setelah jalur utama terputus. Sedangkan pada *Group* 20 jalur cadangan *active* pada *timestamp* 00:36:12.3636 (hh:mm:ss.ms) sehingga selisih waktu yang diperlukan *Group* 20 pada contoh kejadian ini adalah 0 detik, atau jalur cadangan langsung *active* pada saat jalur utama terputus. Langkah ini dilakukan berulang sebanyak 5 kali untuk masing-masing interface pada jalur utama setiap *group*.

Jalur utama *Group* HSRP 10 merupakan *router interface* G1/0 dan G0/0 pada *router* R1. Interface G1/0 merupakan *interface* yang terhubung dengan Internet, sedangkan *interface* G1/0 merupakan *interface* yang memiliki 4 *sub-interface* untuk setiap VLAN 10, 20, 30 dan 40.

Pengujian dilakukan dengan memutuskan salah satu dari kedua *interface* ini secara bergantian masing-masing sebanyak 5 kali.

Data yang diperoleh dapat dilihat pada Tabel 10. Data *Failover Group* HSRP 10 berikut ini:

TABEL X
DATA *FAILOVER GROUP* HSRP 10

INTERFACE	**WAKTU *FAILOVER* (s)**
G1/0	1.00
	2.00
	0.00
	2.00
	2.00
G0/0	8.01
	9.00
	9.01
	7.00
	8.00

Kolom *interface* pada tabel merupakan *interface* yang dimatikan sebagai simulasi jalur utama terputus. Sedangkan waktu *failover* merupakan waktu yang diperlukan jalur cadangan (*standby*) untuk berubah menjadi jalur pengiriman data (*active*).

Terlihat bahwa *failover* lebih cepat dilakukan apabila jalur putus adalah jalur *interface* G1/0 yang terhubung dengan internet dengan rata-rata waktu sebesar 1.40 detik.

Sedangkan apabila jalur yang putus adalah jalur lokal yang memiliki *sub-interface* yang mewakili 4 Group HSRP dengan rata-rata waktu 8.20 detik.

Pengujian yang sama dilakukan terhadap *Group* HSRP 20. Data pengujian terlihat pada Tabel 11. Data *Failover Group* HSRP 20 di bawah ini:

TABEL XI
DATA *FAILOVER GROUP* HSRP 20

INTERFACE	**WAKTU *FAILOVER* (s)**
G1/0	1.00
	0.98
	0.00
	1.00
	1.00
G0/0	6.06
	8.00
	8.01
	9.13
	7.00

Data yang didapat tidak jauh beda dengan data pengujian *group* HSRP 10, dimana pada pengujian *group* HSRP 20 waktu *failover* memerlukan waktu lebih lama apabila interface yang mati adalah *interface* yang memiliki 4 *sub-interface* dengan waktu rata-rata *failover* sebesar 7.64 detik, sedangkan apabila yang mati adalah *interface* yang terhubung dengan internet (G0/0) waktu rata-rata *failover* yang didapat sebesar 0.80 detik.

Selanjutnya pengujian *failover* untuk *group* HSRP 30 dan 40 dilakukan pada router R2 dengan *interface* G2/0 sebagai *interface* yang terhubung dengan internet dan *interface* G0/0 sebagai *interface* yang memiliki 4 *group* HSRP.

Data pengujian *failover group* HSRP 30 yang didapat dapat dilihat pada Tabel 12. Data *Failover Group* HSRP 30 berikut ini:

TABEL XII
DATA FAILOVER GROUP HSRP 30

INTERFACE	**WAKTU FAILOVER (s)**
G2/0	0.00
	2.24
	3.26
	3.00
	1.00
G0/0	7.00
	8.33
	5.65
	7.00
	10.00

Pada pengujian Group HSRP 30 kecepatan rata-rata jalur cadangan aktif apabila yang terputus adalah interface yang terhubung dengan internet adalah 3.05 detik sedangkan apabila yang terputus adalah interface pada jalur lokal, waktu rata-rata yang diperlukan adalah 8.32 detik.

Pengujian *failover* yang terakhir pada *group* HSRP 40 terdapat pada Tabel 13. Data *Failover Group* HSRP 40:

TABEL XII
DATA FAILOVER GROUP HSRP 40

INTERFACE	**WAKTU *FAILOVER* (s)**
G2/0	0.18
	2.24
	2.00
	2.00

INTERFACE	**WAKTU *FAILOVER* (s)**
	0.30
G0/0	7.00
	8.00
	7.00
	7.00
	7.96

Hasil rata-rata waktu yang diperlukan untuk mengaktifkan jalur cadangan adalah 1.35 detik apabila *interface* yang terhubung internet putus, sedangkan apabila *interface* pada jalur lokal yang terputus memerlukan waktu rata-rata sebesar 7.39 detik.

Dari keempat pengujian pada Group HSRP setiap kali jalur lokal dengan 4 *sub-interface* yang terputus memakan waktu rata-rata 7.71 detik, sedangkan apabila *interface* yang mati adalah *interface* yang terhubung dengan internet, waktu yang diperlukan memiliki rata-rata 1.36 detik.

Selama keempat pengujian jalur dengan 4 *sub-interface* selalu memakan waktu lebih lama dibandingkan dengan jalur yang memiliki satu *interface*.

Setelah pengujian *failover* untuk masing-masing *group* HSRP, pengujian selanjutnya adalah mengaktifkan kembali jalur terputus dan mengamati waktu yang diperlukan router untuk kembali mengirim paket menggunakan jalur utama dari masing-masing *group*.

Data pengujian *group* HSRP 10 dapat dilihat pada Tabel 14. Data *Recovery Group* HSRP 10 di bawah ini:

TABEL XIV
DATA RECOVERY GROUP HSRP 10

INTERFACE	**WAKTU *FAILOVER* (s)**
G2/0	2.00
	0.00
	0.00
	2.00
	1.00
G0/0	8.01
	8.90
	7.00
	8.00
	8.00

Berdasarkan data pengujian didapati bahwa untuk kembali menggunakan jalur utama dimana perubahan status jalur utama dari *standby* menjadi *active* apabila *interface* yang terhubung internet mati kemudian hidup kembali memiliki rata-rata waktu 1.00 detik, bahkan pada beberapa pengujian jalur langsung menjadi aktif tanpa ada waktu tunggu. Sedangkan apabila *interface* lokal dengan 4 *sub-interface* yang mewakili 4 *group* HSRP yang mati dan hidup kembali waktu rata-rata yang diperlukan adalah 7.98 detik.

Pengujian yang sama dilakukan pada *group* berikutnya, yaitu *group* HSRP 20 memberikan hasil yang terlihat pada Tabel 15. Data *Recovery Group* HSRP 10 berikut:

TABEL XV
DATA RECOVERY GROUP HSRP 20

INTERFACE	**WAKTU *FAILOVER* (s)**
G2/0	2.00
	0.00
	2.00
	2.03
	1.00
G0/0	8.01
	10.90
	12.89
	8.00
	6.85

Rata-rata waktu yang diperlukan untuk *recovery* jalur utama apabila *interface* yang mati dan hidup kembali adalah *interface* yang terhubung dengan internet adalah 1.41 detik. Sedangkan apabila *interface* yang mati adalah *interface* lokal, waktu rata-rata didapat 9.33 detik.

Untuk pengujian *group* HSRP 30 dan 40, pengujian dilakukan terhadap pada *router* R2 dengan *interface* G2/0 sebagai *interface* yang terhubung internet dan *interface* G2/2 yang merupakan *interface* lokal dengan 4 *group* HSRP yang diwakili oleh 4 *sub-interface*. Data pengujian yang didapat untuk *group* HSRP 30 dapat dilihat pada Tabel 16. Data *Recovery Group* HSRP 30 berikut:

TABEL XIV
DATA RECOVERY GROUP HSRP 30

INTERFACE	**WAKTU *FAILOVER* (s)**
G2/0	3.00
	4.25
	0.00
	2.00
	1.00
G0/0	9.00
	8.66
	9.00
	5.97
	8.96

Waktu rata-rata yang didapat apabila *interface* G0/2 pada R2 yang mati kemudian hidup kembali adalah 2.05 detik, sedangkan apabila *interface* G0/0 yang mati lalu hidup kembali memakan waktu rata-rata 8.32 detik agar jalur pengiriman data kembali ke jalur utama.

Uji *recovery* terakhir pada *group* HSRP 40 dapat dilihat pada Tabel 17. Data *Recovery Group* HSRP 40 di bawah ini:

TABEL XVII
DATA RECOVERY GROUP HSRP 40

INTERFACE	**WAKTU *FAILOVER* (s)**
G2/0	2.00
	2.25
	3.00
	1.00
	1.00
G0/0	9.00

	7.00
	8.00
	1.97
	9.01

Hasil yang didapat apabila *interface* G2/0 yang mati dan hidup kembali memerlukan waktu rata-rata sebesar 1.85 detik agar pengiriman data kembali melalui jalur utama. Sedangkan apabila *interface* G0/0 yang mati dan hidup kembali, memerlukan waktu rata-rata 7.00 detik.

Keempat pengujian pada 4 *group* HSRP apabila *interface* fisik yang terhubung dengan internet yang mati dan hidup kembali memiliki waktu rata-rata *recovery* 1.58 detik. Sedangkan apabila jalur yang mati dan hidup kembali adalah jalur lokal yang menangani 4 *group* HSRP yang diwakili oleh 4 *sub-interface* yang berbeda memerlukan rata-rata waktu lebih lama sebesar 7.00 detik.

Baik dari pengujian *failover* dan *recovery* hal ini selalu sejalan, dimana apabila yang mengalami masalah adalah *interface* yang menangani keempat *group* akan selalu memakan waktu lebih lama untuk *failover* dan *recovery*. Sedangkan apabila jalur yang mengalami masalah adalah jalur *interface* fisik yang terhubung internet, *failover* dan *recovery* dapat lebih cepat dilakukan.

Dari semua pengujian, baik pengujian *failover* maupun pengujian *recovery* jarang didapati adanya *request time out* atau *packet missing* seperti pada Gambar 18. Pengujian *Request Time Out.*

```
C:\>PING -T 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time=14ms TTL=126
Reply from 10.0.0.2: bytes=32 time=16ms TTL=126
Reply from 10.0.0.2: bytes=32 time=19ms TTL=126
Reply from 10.0.0.2: bytes=32 time=11ms TTL=126
Reply from 10.0.0.2: bytes=32 time=13ms TTL=126
Reply from 10.0.0.2: bytes=32 time=13ms TTL=126
Reply from 10.0.0.2: bytes=32 time=14ms TTL=126
Request timed out.
Request timed out.
Reply from 10.0.0.2: bytes=32 time=13ms TTL=126
```

Gambar 18. Pengujian Request Time Out

Namun walaupun transisi *failover* maupun *recovery* terlihat tanpa *request time out*, setiap kali terjadi *failover* maupun *recovery*, waktu pengiriman paket terlihat terjadi peningkatan.

```
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time=1ms TTL=126
Reply from 10.0.0.2: bytes=32 time=11ms TTL=126
Reply from 10.0.0.2: bytes=32 time=12ms TTL=126
Reply from 10.0.0.2: bytes=32 time=12ms TTL=126
Reply from 10.0.0.2: bytes=32 time=12ms TTL=126
Reply from 10.0.0.2: bytes=32 time=13ms TTL=126
Reply from 10.0.0.2: bytes=32 time=12ms TTL=126
Reply from 10.0.0.2: bytes=32 time=15ms TTL=126
Reply from 10.0.0.2: bytes=32 time=15ms TTL=126
Reply from 10.0.0.2: bytes=32 time=12ms TTL=126
Reply from 10.0.0.2: bytes=32 time=13ms TTL=126
```

Gambar 19. Peningkatan Delay

Peningkatan ini hanya bersifat sementara sebelum akhirnya menjadi normal kembali, seperti terlihat pada Gambar 20. Kondisi *Delay* Normal Kembali di bawah ini:

```
Reply from 10.0.0.2: bytes=32 time=13ms TTL=126
Reply from 10.0.0.2: bytes=32 time=13ms TTL=126
Reply from 10.0.0.2: bytes=32 time=19ms TTL=126
Reply from 10.0.0.2: bytes=32 time=13ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time=1ms TTL=126
```

Gambar 20. Kondisi Delay Normal Kembali

Cisco Packet Tracer yang digunakan tidak memiliki kemampuan analisis yang lebih mendalam dan tidak dapat digunakan bersama-sama dengan *tools* lain untuk menganalisis dan meng-*capture* data yang menggunakan *Transport Control Protocol* (TCP) dan *User Datagram Protocol* (UDP), sehingga analisis terhadap *delay*, *jitter*, *Packet Loss* dan *Throughput* tidak dapat dilakukan secara maksimal untuk merepresentasikan kondisi penggunaan perangkat fisik jaringan.

Satu-satunya *protocol* yang dapat digunakan sebagai analisis *Quality of Service (QoS)* pada *Packet Tracer* adalah menggunakan perintah *ping* yang menggunakan *Internet Control Message Protocol* (ICMP). Hal ini pun dirasa kurang untuk dapat merepresentasikan kondisi apabila menggunakan perangkat fisik jaringan, dikarenakan pada semua *software* simulasi jaringan kondisi seluruh perangkat akan dianggap selalu berada dalam kondisi ideal. Hal ini tentunya sangat jarang terjadi pada apabila jaringan dibuat dengan menggunakan perangkat fisik sungguhan.

Sehingga analisis yang dilakukan menggunakan perintah ping ini hanya dijadikan sebagai acuan dalam menganalisis *Quality of Service (QoS)* apabila konfigurasi yang sama dibangun menggunakan perangkat fisik sungguhan.

Analisis yang pertama dilakukan adalah analisis *delay* dengan menggunakan lamanya *round trip time* (RTT), yaitu waktu pengiriman paket sampai tujuan dan respon dari tujuan sampai kembali ke pengirim. Perhitungan yang dicari adalah waktu rata-rata *round trip time* dari banyaknya paket yang dikirim. Data waktu yang digunakan dapat dilihat pada Gambar 21. Sumber Data *Delay*.

```
C:\>ping 10.0.0.2 -n 100

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time=11ms TTL=126
Reply from 10.0.0.2: bytes=32 time=10ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
```

Gambar 21. Sumber Data Delay

p-ISSN : 2443-2210
e-ISSN : 2443-2229

Pengujian yang dilakukan adalah dengan mengirimkan paket *ping* sebanyak 100 kali dan memutuskan jalur utama sumber internet lalu menghidupkannya kembali, kemudian setelah kembali normal jalur yang dimatikan adalah jalur dalam jaringan lokal dan menghidupkannya kembali. Hal ini dilakukan sebanyak dua kali secara berurutan. Analisis dilakukan dengan menggunakan rumus:

$$\textit{Delay}\ \text{Rata-Rata} = \frac{\text{Total } \textit{Delay}}{\text{Total Paket diterima}}$$

Data yang memiliki nilai dibawah 1 *milisecond* (ms) dibulatkan menjadi 0 ms. Hasil rata-rata *delay* yang didapat dari 100 kali pengiriman ping *round trip time* adalah 1.16 ms.

Perhitungan *jitter* dilakukan menggunakan data yang sama dengan data perhitungan *delay* pada Gambar 21 Sumber Data *Delay*. Perhitungan *delay* dilakukan dengan mengambil data waktu *round trip time*, sedangkan pada perhitungan *jitter* yang diambil adalah selisih waktu *round trip time* pengiriman paket dari *round trip time* sebelumnya. *Jitter* yang merupakan fluktuasi nilai *delay* dalam suatu periode dihitung nilai rata-ratanya menggunakan rumus:

$$\textit{Jitter}\ \text{Rata-Rata} = \frac{\text{Total Variasi } \textit{Delay}}{\text{Total Paket}}$$

Hasil yang didapat adalah jitter yang dihasilkan memiliki waktu rata-rata sebesar 2.08 ms.

Analisis berikutnya yang dilakukan adalah analisis terhadap packet loss, dimana pada analisis ini yang dilihat adalah banyaknya paket yang sampai ke tujuan dan berhasil memberikan respon serta paket yang tidak sampai tujuan atau respon yang tidak mencapai komputer pengirim. Rumus yang digunakan adalah:

$$\textit{Packet Loss} = \frac{\text{Paket Dikirim- Paket Diterima}}{\text{Paket Dikirim}} \times 100\%$$

Jumlah paket yang tidak berhasil diterima dapat diketahui dari banyaknya paket ping dengan status request time out seperti terlihat pada gambar 22. Sumber Data Packet Loss.

```
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Request timed out.
Request timed out.
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
```

Gambar 22. Sumber Data Packet Loss

Dari hasil perhitungan didapat persentase jumlah *packet loss* sebesar 3% dan *request time out* ini terjadi hanya jika jalur yang putus adalah jalur dari sumber internet.

Besarnya *throughput* atau kemampuan sebenarnya dari konfigurasi jaringan yang dibangun didapat dari jumlah total besarnya paket yang sukses dikirim dan direspon pada interval waktu pengiriman data tersebut. Interval waktu didapat dari lama waktu pengiriman data pertama dan terakhir, sehingga rumus yang digunakan adalah:

$$\textit{Throughput} = \frac{\text{jumlah } \textit{bit} \text{ diterima}}{\text{total waktu pengiriman}}$$

Karena sumber data ping masih dalam satuan *bytes* maka perlu diubah terlebih dahulu menjadi *bit* dengan dikalikan dengan 8 *bit* untuk setiap *byte*, dan total waktu masih dalam satuan *milisecond* (ms) sehingga perlu dibagi dengan 1000 terlebih dahulu baru dilakukan perhitungan menggunakan rumus yang ada.

```
C:\>ping 10.0.0.2 -n 100

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time=11ms TTL=126
Reply from 10.0.0.2: bytes=32 time=10ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
```

Gambar 23. Sumber Data Throughput

Hasil *througput* yang didapat adalah sebesar 220.689,7 *bit per second* (bps) atau sama dengan 220,6 *kilo bit per second* (kbps).

Hasil analisis ini merupakan hasil dari simulasi jaringan sehingga tidak menggambarkan kualitas jaringan apabila konfigurasi yang sama dibangun menggunakan perangkat jaringan fisik. Apabila konfigurasi yang sama dibangun menggunakan perangkat keras fisik, sebaiknya gunakan *tools* tambahan seperti wireshark yang dapat merekam data lalu lintas jaringan TCP dan UDP. Analisa hasil rekaman lalu lintas data yang didapat dari wireshark dilakukan analisa menggunakan cara dan rumus yang sama untuk mendapatkan nilai *Quality of Service* (Qos) seperti *delay*, *jitter*, *packet loss*, dan *throughput*.

IV. SIMPULAN

Berdasarkan keseluruhan hasil simulasi dan pengujian didapati bahwa *load balancing* pada *redundancy link* HSRP dapat dilakukan dengan membagi setiap VLAN yang digunakan ke dalam *group* HSRP yang diwakili oleh *sub-interface* sebanyak jumlah VLAN yang digunakan. Akan tetapi *failover* dan *recovery* akan memerlukan waktu lebih lama apabila yang mengalami permasalahan adalah bagian

interface yang memiliki *multigroup* atau banyak *sub-interface* dibanding dengan waktu *failover* dan *recovery* pada satu *interface* fisik yang mengarah ke jaringan di luar VLAN yang digunakan. Proses transisi ketika terjadi *failover* dan *recovery* sangat jarang mengalami *packet missing* atau *time out* namun terjadi penambahan *delay* pada proses pengiriman data selama beberapa saat, sebelum akhirnya berjalan normal kembali.

Sangat disarankan untuk melakukan konfigurasi jaringan yang sama menggunakan peralatan fisik dan *tool* seperti *wireshark* yang dapat digunakan untuk merekam data lalu lintas jaringan menggunakan TCP dan UDP sehingga mendapatkan hasil analisis QoS yang lebih akurat sesuai dengan kualitas dan kondisi hardware yang digunakan.

DAFTAR PUSTAKA

[1] P. Firmansyah, Wahyudi, M & Rachmat, "Analisis Perbandingan Kinerja Jaringan CISCO Virtual Router Redundancy Protocol (VRRP) Dan CISCO Hot Standby Router Protocol (HSRP)," *Tek. Komput. AMIK BSI Tegal*, vol. 1, no. 1, pp. 764–769, 2018.

[2] A. Akmaludin, A. Mt, S. U. Masruroh, and M. Sc, "Evaluasi Kinerja Hot Standby Router Protocol (HSRP) dan Gateway Load Balancing Protocol (GLBP) untuk Layanan Video Streaming," *CyberSecurity dan Forensik Digit.*, vol. 2, no. 1, pp. 43–51, 2019.

[3] Cisco, "First Hop Redundancy Protocols Configuration Guide, Cisco IOS XE Release 3S - HSRP MD5 Authentication [Cisco IOS XE 3S]," *Cisco*, no. 6387, 2018.

[4] P. Dubey, S. Sharma, and A. Sachdev, "Review of first hop redundancy protocol and their functionalities," *Int. J. Eng. Trends Technol.*, vol. 4, no. 5, pp. 1085–1088, 2013.

[5] Y. Haiyan, "Application of Vlan and HSRP Technology in the Dual Core Campus Network," *Proc. - 2018 Int. Conf. Smart Grid Electr. Autom. ICSGEA 2018*, pp. 332–333, 2018, doi: 10.1109/ICSGEA.2018.00088.

[6] A. K. Singh and A. Kothari, "HSRP (Hot Stand by Routing Protocol) reliability issues over the Internet service provider's network," *Orient. J. Comput. Sci. Technol.*, vol. 4, no. 2, 2011.

[7] U. Anwar, "Performance Analysis and Functionality Comparison of FHRP Protocols," *2019 IEEE 11th Int. Conf. Commun. Softw. Networks*, pp. 111–115, 2019, doi: 10.1109/ICCSN.2019.8905333.

[8] M. Mansour, "Performance Evaluation of First Hop Redundancy Protocols," *Procedia Comput. Sci.*, vol. 177, pp. 330–337, 2020, doi: 10.1016/j.procs.2020.10.044.

[9] Z. U. Rahman *et al.*, "Performance Evaluation of First HOP Redundancy Protocols (HSRP , VRRP & GLBP)," *J . Appl . Env. . Biol . Sci*, vol. 7, no. 3, pp. 268–278, 2017.

[10] V. Nirmala and A. Sridevi, "Packet Delivery and Numerous Redundancies in Ipv4 Network through GLBP," *J. Chem. Pharm. Sci.*, no. 8, pp. 146–148, 2016.

[11] Cisco, *Campus Network for High Availability Design Guide Cisco*. Cisco Systems, Inc, 2008.