Implementasi Dan Analisis *Hot Standby Router Protocol* (HSRP) Untuk Redundansi *Gateway* Pada Jaringan PT. XYZ Tbk

Implementation And Analysis Of Hot Standby Router Protocol (HSRP) For Gateway Redundancy In Networks At XYZ Tbk

Taufik Rahman[1)] , Kautsar Imam Hidayat[2)]

[1),2)] Program Studi Teknik Informatika, Fakultas Teknik, Universitas Bina Sarana Informatika
[1),2)]Jl. Kramat Raya No.98, RT.2/RW.9, Kwitang, Kec. Senen, Kota Jakarta Pusat, DK Jakarta 10450
Email : taufik@bsi.ac.id[1)], kautsar.i.hidayat@gmail.com[2)]
***Corresponding author. Phone :** +62 877 766 11636*

Abstrak

Penelitian ini membahas implementasi Hot Standby Router Protocol (HSRP) sebagai mekanisme redundansi gateway pada jaringan Cisco di Perusahaan XYZ Tbk untuk mengatasi risiko single point of failure. Integrasi HSRP dengan EIGRP, DHCP, VLAN, dan ACL diterapkan untuk meningkatkan efisiensi routing, otomatisasi pengalamatan IP, serta keamanan jaringan secara menyeluruh. Metode penelitian meliputi observasi, wawancara, studi pustaka, serta simulasi menggunakan PnetLab. Hasil pengujian pada jaringan eksisting menunjukkan terjadinya kegagalan konektivitas ketika gateway utama tidak berfungsi akibat tidak tersedianya jalur cadangan. Pada jaringan usulan, simulasi failover memperlihatkan perpindahan jalur dari router aktif ke router standby tanpa Request Time Out (RTO), meskipun terdapat jeda transisi dengan waktu mencapai 6,443 ms. Temuan tersebut menunjukkan bahwa implementasi HSRP mampu mempertahankan ketersediaan layanan jaringan dengan lebih stabil. Selain itu, penerapan EIGRP memperbaiki proses pertukaran rute, DHCP menyederhanakan manajemen IP, sementara VLAN dan ACL meningkatkan segmentasi dan keamanan trafik jaringan. Secara keseluruhan, rancangan jaringan usulan memberikan peningkatan keandalan dan performa dibandingkan jaringan eksisting.

***Kata kunci:** HSRP, Failover, Redundansi, EIGRP, Jaringan, Redundansi*

Abstract

This study examines the implementation of the Hot Standby Router Protocol (HSRP) as a gateway redundancy mechanism within the Cisco-based network of Perusahaan XYZ Tbk to mitigate the risk of a single point of failure. The integration of HSRP with EIGRP, DHCP, VLAN, and ACL is applied to enhance routing efficiency, automate IP addressing, and strengthen overall network security. The research methodology includes observation, interviews, literature review, and network simulation using PnetLab. Initial testing on the existing network reveals connection failures when the primary gateway becomes unavailable due to the absence of a backup path. In contrast, testing on the proposed network shows that the failover mechanism successfully shifts traffic from the active router to the standby router without generating a Request Time Out (RTO), although a brief transition delay of up to 6.443 ms occurs. These findings indicate that HSRP effectively maintains network availability and service continuity. Furthermore, the application of EIGRP improves route exchange, DHCP simplifies IP management, and VLAN along with ACL enhances traffic segmentation and network security. Overall, the proposed design provides higher reliability and performance than the existing network.

***Keywords**: HSRP, Failover, Redundancy, EIGRP, Network.*

1. PENDAHULUAN

Dalam era digital sekarang yang semakin maju, kebutuhan akan ketersediaan jaringan yang stabil dan andal menjadi sangat fatal, terutama bagi perusahaan yang bergerak di bidang teknologi informasi seperti Perusahaan XYZ Tbk. Gangguan jaringan sekecil apa pun dapat menyebabkan terganggunya operasional perusahaan, menurunnya produktivitas, hingga berpotensi menimbulkan kerugian finansial dan reputasi. Salah satu titik kritis dalam jaringan adalah *gateway*, yang berperan sebagai penghubung antara jaringan lokal (LAN) dengan jaringan eksternal. Ketika *gateway* mengalami gangguan atau kegagalan, seluruh akses keluar jaringan akan terputus. Solusi atas permasalahan ini adalah penerapan redundansi yang mampu menjamin ketersediaan jaringan meski terjadi kerusakan pada salah satu *gateway*. Salah satu solusi yang

dapat diimplementasikan adalah menggunakan protokol *Hot Standby Router Protocol* (HSRP) dari Cisco.

Pada beberapa penelitian sebelumnya, HSRP telah terbukti efektif meningkatkan ketersediaan jaringan dan mengurangi risiko *single point of failure*. [1] menunjukkan bahwa implementasi HSRP bersama Inter-VLAN dan VLSM mampu meningkatkan stabilitas jaringan sekolah dengan perbaikan signifikan pada proses *routing*. Sitanggang et al. [2] juga menemukan bahwa kombinasi HSRP dan VRRP memberikan redundansi gateway yang lebih baik pada lingkungan virtual. Selain itu, [3] menguji performa HSRP pada layanan video *streaming* dan memperoleh hasil bahwa protokol ini mampu menjaga kontinuitas layanan tanpa jeda signifikan. Temuan-temuan ini menegaskan bahwa penerapan HSRP relevan untuk meningkatkan keandalan jaringan perusahaan seperti Perusahaan XYZ. Penelitian penerapan *interface* virtual dan HSRP mampu meningkatkan efisiensi, keandalan, serta keamanan jaringan komputer secara signifikan [1]. Penerapan HSRP di PT.XYZ berhasil meningkatkan kinerja jaringan dengan ISP *backup* akan menggantikan fungsi ISP *main* ketika *down* [4]. Berdasarkan kondisi jaringan eksisting yang masih menggunakan satu *gateway* tanpa mekanisme *failover*, permasalahan utama yang muncul adalah tingginya risiko *single point of failure* yang menyebabkan terhentinya seluruh konektivitas ketika *gateway* mengalami gangguan. Kondisi tersebut menimbulkan *downtime* operasional dan berdampak pada ketersediaan layanan. Oleh karena itu, penelitian berfokus pada penerapan HSRP dalam menyediakan redundansi gateway, sejauh mana efektivitasnya dalam meningkatkan ketersediaan jaringan, serta mengukur kinerja jaringan selama proses failover pada lingkungan simulasi.

Penelitian bertujuan untuk menerapkan protokol HSRP sebagai solusi redundansi *gateway* pada jaringan Cisco serta menganalisis efektivitasnya dalam menjaga ketersediaan layanan jaringan. Selain itu, penelitian ini bertujuan mengevaluasi performa jaringan setelah implementasi HSRP, khususnya terkait waktu *failover* dan stabilitas konektivitas, serta mengidentifikasi tantangan teknis yang muncul selama proses konfigurasi untuk menghasilkan rekomendasi peningkatan infrastruktur jaringan.

2. DASAR TEORI

2.1. Jaringan Komputer

Jaringan komputer adalah himpunan "Interkoneksi" antara 2 komputer *autonomous* atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*) [3]. Untuk mencapai tujuan yang sama maka setiap bagian dalam suatu jaringan akan meminta dan memberikan layanan [4]. Berdasarkan Jarak Jangkauan Jaringan komputer secara geografis memiliki 3 macam, antara lain yaitu: *Local Area Network* (LAN), *Metropolitan Area Network* (MAN), *Wide Area Network* (WAN) [5].

2.2. Topologi Jaringan

Topologi jaringan adalah hubungan fisik antara setiap anggota (*links, node)* dan sebagainya, dari sebuah jaringan komputer [6]. *Gateway* adalah salah satu perangkat keras jaringan komputer yang terdapat situasi dimana dua atau lebih jaringan komputer dengan arsitektur yang berbeda akan digabungkan menjadi satu kesatuan sebagai jaringan yang utuh [7].

2.3. Konsep *High Availability*

High Availability merupakan suatu konsep yang mengacu pada kemampuan sebuah sistem untuk terus beroperasi tanpa mengalami gangguan atau *downtime* selama periode waktu yang sudah ditentukan[8]. Penyebab *Downtime* Jaringan disebabkan oleh FO (*Fiber Optic) cut* akibat Pembangunan jalan atau infrastukrur lainnya dan *over bandwidth* [9]. Strategi dan Teknik Implementasi *High Availability* diantaranya redundansi perangkat keras: Menggandakan komponen perangkat keras kritikal seperti *router*, *switch*, *firewall*, dan *power supply* juga redundansi jalur komunikasi [10]. Protokol Redundansi [11]. Konsep *Failover* dan *Failback Failover* adalah Teknik untuk membagi beban trafik di jaringan yang terlalu besar dan memindahkan secara otomatis apabila pada jaringan tersebut mengalami kendala dalam koneksi [12]. *Failback adalah* proses kembalinya komponen yang sebelumnya mengalami kegagalan. Terdapat dua model dari *failover,* yaitu *failover active-active* dan *failover active standby* [13].

2.4. Hot Standby Router Protocol

HSRP adalah metode yang diterapkan pada perangkat jaringan *Cisco* dengan konsep menciptakan satu Alamat *IP virtual gateway* yang digunakan oleh dua perangkat, sehingga keduanya dapat berfungsi secara bersamaan [2]. Cara Kerja HSRP, dengan menerapkan HSRP gangguan dan downtime dalam jaringan dapat diminimalkan secara signifikan, mendekati Tingkat ketersediaan hampir 100%. *Router Active* dan *Router Standby*. Dalam sebuah grup HSRP, terdapat dua peran utama *router* yaitu *Router Active* yang merupakan perangkat utama dalam pengiriman paket dalam lalu lintas jaringan, dan *Router Standby* sebagai *router backup* apabila *router active* tidak berfungsi. Sehingga mampu mengantisipasi bila terjadinya *Request Time out (RTO)* atau terputusnya jaringan serta meningkatkan kualitas jaringan komputer [3]. Pada HSRP menggunakan dua jenis alamat yaitu alamat IP virtual dan alamat MAC virtual. Alamat IP virtual yang dikonfigurasi pada segmen jaringan dari setiap antarmuka yang mendukung HSRP yang termasuk dalam grup HSRP yang sama. HSRP memiliki salah satu antarmuka yang bertindak sebagai *router* HSRP *Active.* Alamat MAC Virtual diberikan grup umum dengan IP virtual. *Router active* menerima dan meneruskan paket yang ditujukan untuk Alamat MAC virtual grup. Jika perangkat HSRP aktif gagal, perangkat HSRP siaga mengontrol IP virtual dan Alamat MAC grup [14]. Proses Pemilihan *Router Active*. Dimana paket data akan melalui *router active* sebagai jalur utama untuk menuju *router* utama, jika terjadi gagal pengiriman paket data maka secara otomatis paket data akan menuju jalur alternatif yang berada pada *router backup* [15]. Pesan Hello HSRP: mengirimkan pesan hello secara periodik untuk memastikan bahwa router lainnya masih aktif. Jika *router* aktif mati atau terputus dari jaringan, *router standby* dengan prioritas tertinggi akan segera mengambil alih peran aktif untuk mempertahnakan kontinuitas layanan [16]. Mekanisme *Preemption* memungkinkan *router* dengan prioritas tertinggi untuk segera menjadi *router active*. Prioritas ditentukan oleh nilai prioritas yang anda konfigurasi, dan kemudian oleh Alamat IP. Prioritas HSRP: Konfigurasi HSRP pada kedua dengan memberikan prioritas tertinggi pada router utama dapat membantu dalam optimalisasi sisi client.

3. METODOLOGI PENELITIAN

3.1 Model Pengembangan Jaringan

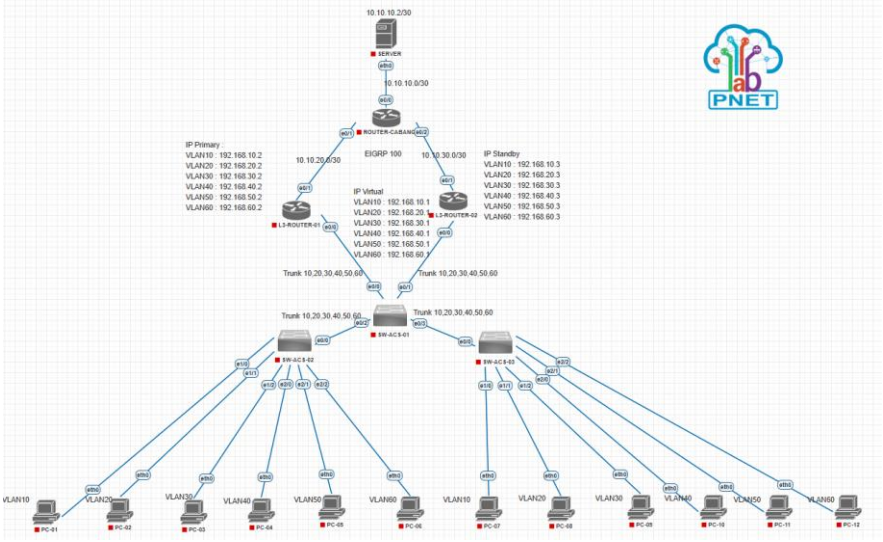
Implementasi dari tahapan metodologi dilakukan sebagai berikut:

1. Analisis kebutuhan jaringan → dilakukan dengan meninjau topologi eksisting yang hanya menggunakan satu *gateway* tanpa mekanisme *failover*.
2. Perancangan topologi redundansi → tahap ini menghasilkan rancangan dua *router* yang terhubung ke satu *switch* sebagai jalur utama dan cadangan, dengan penetapan IP virtual untuk HSRP.
3. Implementasi konfigurasi HSRP → seluruh *subinterface* VLAN pada kedua *router* dikonfigurasi HSRP dengan penentuan prioritas berbeda agar *router* master dan *standby* dapat berfungsi otomatis.
4. Pengujian *failover* → *router* master dimatikan untuk mengamati waktu perpindahan layanan dan memastikan *router standby* mengambil alih IP virtual.
5. Analisis dan evaluasi → hasil *latency*, *packet loss*, dan *failover* time dianalisis untuk mengukur peningkatan kinerja setelah implementasi.

3.2. Jaringan Usulan

Protokol HSRP pada perangkat router Cisco. Mencakup perubahan topologi, penyesuaian infrastruktur teknologi informasi, serta penerapan keamanan jaringan yang lebih optimal. Menggunakan topologi star (bintang) yang dimodifikasi dengan penerapan redundansi *gateway* menggunakan protokol HSRP pada perangkat router Cisco. Dirancang menggunakan simulator PnetLab, dengan tujuan untuk merepresentasikan implementasi HSRP dalam membentuk sistem *gateway* yang redundan. Simulasi ini menampilkan infrastruktur jaringan dengan dua *router* utama, satu *switch* layer 2, serta beberapa perangkat *end-user* seperti PC atau laptop. Gambar 1 menunjukkan skema jaringan usulan dengan penerapan HSRP menggunakan dua router yang dikonfigurasi sebagai *active* dan *standby*. Kedua *router* terhubung ke *switch* layer 2 dan menyediakan IP virtual yang digunakan sebagai *default gateway* oleh seluruh perangkat klien.

Skema ini menggambarkan arsitektur redundansi yang memungkinkan proses *failover* berjalan otomatis ketika *router* utama mengalami gangguan.



Sumber: Hasil Penelitian

Gambar 1. Skema Jaringan Usulan

A. Komponen Utama
   1. *Router* 1 *(Active Router)*
      a) *IP Interface*: 192.168.10.2, 192.168.20.2, 192.168.30.2, 192.168.40.2, 192.168.50.2, 192.168.60.2.
      b) Prioritas: 110
      c) Fungsi: Menangani trafik utama dan menjadi *gateway* aktif untuk semua klien
   2. *Router* 2 *(Standby Router)*
      a) *IP Interface*: 192.168.10.3, 192.168.20.3, 192.168.30.3, 192.168.40.3, 192.168.50.3, 192.168.60.3.
      b) Prioritas: 100
      c) Fungsi: Menjadi cadangan yang akan aktif jika *Router* 1 gagal
   3. IP Virtual Gateway
      a) Alamat: 192.168.10.1, 192.168.20.1, 192.168.30.1, 192.168.40.1, 192.168.50.1, 192.168.60.1.
      b) Dikonsumsi sebagai *default gateway* oleh seluruh perangkat klien di jaringan
   4. *Switch Layer 2*
      Menghubungkan kedua *router* dan perangkat klien dalam banyak segmen jaringan.
   5. *Client Devices* (*PC1, PC2*, dst.)
      a) Terhubung ke *switch*
      b) Menggunakan IP *default gateway*: 192.168.10.1, 192.168.20.1, 192.168.30.1, 192.168.40.1, 192.168.50.1, 192.168.60.1.

B. Proses Failover
   1. Bila *Router* 1 (aktif) mengalami gangguan, maka *Router* 2 akan otomatis mengambil alih sebagai *router* aktif dengan tetap mempertahankan IP *virtual gateway*.
   2. Klien tidak perlu mengubah konfigurasi gateway karena transisi terjadi secara otomatis tanpa mengganggu layanan jaringan.

4. PENGUJIAN DAN PEMBAHASAN

1. Konfigurasi *Router Master*

Router Master adalah jalur utama yang disediakan oleh jaringan komputer di Perusahaan XYZ, jadi dalam keadaan normal, maka seluruh *traffic* jaringan akan berada pada *router* master ini. Konfigurasi yang kita lakukan pada *router* master ini antara lain pemberian IP Address pada

interface ethernet 0/1 yang terhubung kepada *Router* cabang dengan ip address 10.10.10.2 subnet mask 255.255.255.252.

Konfig *Interface Ethernet 0/0* berikut:

```
Building configuration...
Current configuration: 69 bytes
!
interface Ethernet0/0
description #To_Switch#
no ip address
end
```

Konfigurasi HSRP pada router master ditampilkan pada Gambar 2, yang menunjukkan status HSRP, prioritas, dan konfigurasi DHCP yang digunakan untuk mendistribusikan IP otomatis ke klien.

Setelah dihidupkan *interface ethernet 0/0,* maka selanjutnya adalah pemberian IP *Address* pada *sub interface vlan* yang akan terhubung ke *switch* utama dan akan terhubung ke jaringan komputer dibawahnya (*client)*. *IP address* pada *interface* pada *interface ethernet* 0/*0.10,* 0/*0.20, 0/0.30,* 0/*0.40, 0/0.50, 0/0.60* seperti pada Tabel IV.1 yaitu IP Virtual GW 192.168.10.1, 192.168.20.1, 192.168.30.1, 192.168.40.1, 192.168.50.1, 192.168.60.1 sedangkan untuk IP Master 192.168.10.2, 192.168.20.2, 192.168.30.2, 192.168.40.2, 192.168.50.2, 192.168.60.2

```
L3-ROUTER-01#show run | sec 0.0.
interface Ethernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.2 255.255.255.0
 standby 10 ip 192.168.10.1
 standby 10 priority 110
 standby 10 preempt
interface Ethernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.2 255.255.255.0
 standby 20 ip 192.168.20.1
 standby 20 priority 110
 standby 20 preempt
interface Ethernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.2 255.255.255.0
 standby 30 ip 192.168.30.1
 standby 30 priority 110
 standby 30 preempt
interface Ethernet0/0.40
 encapsulation dot1Q 40
 ip address 192.168.40.2 255.255.255.0
 standby 40 ip 192.168.40.1
 standby 40 priority 110
 standby 40 preempt
interface Ethernet0/0.50
 encapsulation dot1Q 50
 ip address 192.168.50.2 255.255.255.0
 standby 50 ip 192.168.50.1
 standby 50 priority 110
 standby 50 preempt
interface Ethernet0/0.60
 encapsulation dot1Q 60
 ip address 192.168.60.2 255.255.255.0
 standby 60 ip 192.168.60.1
 standby 60 priority 110
 standby 60 preempt
```

```
L3-ROUTER-01#show run | Sec dhcp
ip dhcp excluded-address 192.168.10.1 192.168.10.3
ip dhcp excluded-address 192.168.20.1 192.168.20.3
ip dhcp excluded-address 192.168.30.1 192.168.30.3
ip dhcp excluded-address 192.168.40.1 192.168.40.3
ip dhcp excluded-address 192.168.50.1 192.168.50.3
ip dhcp excluded-address 192.168.60.1 192.168.60.3
ip dhcp pool VLAN10
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
   dns-server 8.8.8.8
ip dhcp pool VLAN20
   network 192.168.20.0 255.255.255.0
   default-router 192.168.20.1
   dns-server 8.8.8.8
ip dhcp pool VLAN30
   network 192.168.30.0 255.255.255.0
   default-router 192.168.30.1
   dns-server 8.8.8.8
ip dhcp pool VLAN40
   network 192.168.40.0 255.255.255.0
   default-router 192.168.40.1
   dns-server 8.8.8.8
ip dhcp pool VLAN50
   network 192.168.50.0 255.255.255.0
   default-router 192.168.50.1
   dns-server 8.8.8.8
ip dhcp pool VLAN60
   network 192.168.60.0 255.255.255.0
   default-router 192.168.60.1
   dns-server 8.8.8.8
L3-ROUTER-01#
```

Gambar 2. *Show IP HSRP Router Master dan DHCP Router Master*

Pada Gambar 2 ditampilkan hasil perintah *show standby* dan *show running-config* yang menunjukkan konfigurasi HSRP serta DHCP pada router master. Informasi ini memperlihatkan bahwa router telah menjalankan peran sebagai gateway aktif dan menyediakan distribusi IP otomatis kepada klien.

Pada *router master* juga terdapat *config DHCP* (*Dynamic Host Configuration Protocol*). *DHCP* ini digunakan untuk seluruh Endpoint/Device *client* yang terhubung ke jaringan Perusahaan XYZ. Pada *Router* utama IP DHCP akan di *range* dari 192.168.10.4 – 192.168.10.254, 192.168.20.4 – 192.168.20.254, 192.168.30.4 – 192.168.30.254, 192.168.40.4 – 192.168.40.254,192.168.50.4 – 192.168.50.254, 192.168.60.4 – 192.168.60.254. *Router master* sudah dilakukan konfigurasi seperti pemberian IP *Address, config* HSRP, pemberian DHCP *server* dan juga *config routing* dinamis menggunakan EIGRP, selanjutnya adalah pengecekan pada *router master* untuk memastikan semua konfigurasi sudah tersimpan.

```
L3-ROUTER-01#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES NVRAM  up                    up
Ethernet0/0.10         192.168.10.2    YES NVRAM  up                    up
Ethernet0/0.20         192.168.20.2    YES NVRAM  up                    up
Ethernet0/0.30         192.168.30.2    YES NVRAM  up                    up
Ethernet0/0.40         192.168.40.2    YES NVRAM  up                    up
Ethernet0/0.50         192.168.50.2    YES NVRAM  up                    up
Ethernet0/0.60         192.168.60.2    YES NVRAM  up                    up
Ethernet0/1            10.10.20.2      YES NVRAM  up                    up
Ethernet0/2            unassigned      YES NVRAM  administratively down down
Ethernet0/3            unassigned      YES NVRAM  administratively down down
L3-ROUTER-01#
```

Gambar 3. *Show IP Interface Brief*

Gambar 3 menampilkan output *show ip interface brief* yang menunjukkan status seluruh subinterface pada router master. Subinterface VLAN pada Ethernet0/0 dikonfigurasi sesuai tabel alamat IP dan berfungsi sebagai jalur komunikasi utama menuju klien.

informasi dari IP Address di masing masing sub *Interface* pada router master, Dimana pada interface ethernet 0/0 tidak menggunakan IP untuk sub interface semua vlan menggunakan IP sesuai dengan Tabel 1.

2. Konfigurasi *Router Standby*

Konfigurasi pada *router standby* sama dengan konfigurasi pada *router master.* Untuk konfigurasi pertama adalah pemberian IP *Address* pada *router standby* yaitu pada *interface Ethernet 0/1* yang terhubung dengan *router* cabang akan diberikan IP *Address* 10.10.20.1/30 .

```
L3-ROUTER-02#show run | sec 0.0
interface Ethernet0/0
 no ip address
interface Ethernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.3 255.255.255.0
 standby 10 ip 192.168.10.1
 standby 10 preempt
interface Ethernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.3 255.255.255.0
 standby 20 ip 192.168.20.1
 standby 20 preempt
interface Ethernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.3 255.255.255.0
 standby 30 ip 192.168.30.1
 standby 30 preempt
interface Ethernet0/0.40
 encapsulation dot1Q 40
 ip address 192.168.40.3 255.255.255.0
 standby 40 ip 192.168.40.1
 standby 40 preempt
interface Ethernet0/0.50
 encapsulation dot1Q 50
 ip address 192.168.50.3 255.255.255.0
 standby 50 ip 192.168.50.1
 standby 50 preempt
interface Ethernet0/0.60
 encapsulation dot1Q 60
 ip address 192.168.60.3 255.255.255.0
 standby 60 ip 192.168.60.1
 standby 60 preempt
```

```
L3-ROUTER-02#show run | sec eigrp
router eigrp 100
 network 10.10.10.0 0.0.0.3
 network 10.10.20.0 0.0.0.3
 network 10.10.30.0 0.0.0.3
 network 192.168.10.0
 network 192.168.20.0
 network 192.168.30.0
 network 192.168.40.0
 network 192.168.50.0
 network 192.168.60.0
 no auto-summary
L3-ROUTER-02#
```

Gambar 4. *Show IP Address Ethernet 0/0 Router Standby dan EIGRP Router Standby*

Pada gambar 4 terdapat informasi mengenai perintah pemberian *IP Address* untuk *interface ethernet* 0/0 pada *router standby*. IP *Address* yang diberikan adalah 192.168.10.3/24, 192.168.20.3/24, 192.168.30.3/24, 192.168.40.3/24, 192.168.50.3/24, 192.168.60.3/24. dan *interface ethernet 0/0* ini untuk menghubungkan jaringan ke *client.* Setelah semua *interface router standby* sudah di *config* dengan IP *Address*, maka selanjutnya adalah config untuk *HSRP* nya yang berada di *nterface ethernet 0/0*, HSRP di *config* di *interface sub interface ethernet 0/0* karena *sub interface ethernet 0/0* ini yang akan terhubung pada client. Konfigurasi dari *routing dynamic router standby,* pada *router* standby terdapat *config* EIGRP dengan *Antonomous System* (AS) *number* 100 dengan *router master,* AS ini digunakan sebagai pengelompokan bagi *router* untuk saling berbagi informasi *routing*. Pada *Router Standby*, *network* yang di routing adalah 10.10.30.0 pada *interface ethernet 0/1* yang terhubung ke *router* cabang dan *network* 10.10.10.0, 10.10.20.0, 192.168.10.0, 192.168.20.0, 192.168.30.0, 192.168.40.0, 192.168.50.0, 192.168.60.0 adalah *network* yang terhubung ke *client.* Setelah melakukan konfigurasi EIGRP, selanjutnya *router standby* juga harus dilakukan *config* untuk DHCP agar jika *router master* mengalami gangguan, maka *router standby* sudah menyiapkan *IP Address* secara otomatis untuk melemparkan IP DHCP secara otomatis ke *client*.

Router standby sudah dilakukan konfigurasi pemberian *IP Address, config HSRP, DHCP server* dan juga *config routing dinamis* menggunakan EIGRP seperti pada *router master,* selanjutnya adalah pengecekan pada *router standby* untuk memastikan semua konfigurasi sudah tersimpan pada *router.* Terdapat informasi *matriks neighbors* dari EIGRP *router standby*, pada matriks tersebut terlihat ada dua (2) *network neighbors* dari *network router standby, neighbors* tersebut adalah network 10.10.30.1 yaitu koneksi dari *router* cabang dan 192.168.x.2 adalah koneksi dari *router master, neighbor* ini berfungsi sebagai jalur *traffic* yang akan dipilih oleh EIGRP sebagai jalur terbaik, untuk menampilkan *matriks neighbors* dapat dilakukan dengan memasukkan *command show ip eigrp neighbors.*

```
L3-ROUTER-02#show run | sec dhcp
ip dhcp excluded-address 192.168.10.1 192.168.10.3
ip dhcp excluded-address 192.168.20.1 192.168.20.3
ip dhcp excluded-address 192.168.30.1 192.168.30.3
ip dhcp excluded-address 192.168.40.1 192.168.40.3
ip dhcp excluded-address 192.168.50.1 192.168.50.3
ip dhcp excluded-address 192.168.60.1 192.168.60.3
ip dhcp pool VLAN10
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
   dns-server 8.8.8.8
ip dhcp pool VLAN20
   network 192.168.20.0 255.255.255.0
   default-router 192.168.20.1
   dns-server 8.8.8.8
ip dhcp pool VLAN30
   network 192.168.30.0 255.255.255.0
   default-router 192.168.30.1
   dns-server 8.8.8.8
ip dhcp pool VLAN40
   network 192.168.40.0 255.255.255.0
   default-router 192.168.40.1
   dns-server 8.8.8.8
ip dhcp pool VLAN50
   network 192.168.50.0 255.255.255.0
   default-router 192.168.50.1
   dns-server 8.8.8.8
ip dhcp pool VLAN60
   network 192.168.60.0 255.255.255.0
   default-router 192.168.60.1
   dns-server 8.8.8.8
L3-ROUTER-02#
```

```
L3-ROUTER-02#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
6   192.168.30.2            Et0/0.30          13 00:10:08    8   200  0  38
5   192.168.20.2            Et0/0.20          13 00:10:09    8   200  0  35
4   192.168.60.2            Et0/0.60          14 00:10:09   10   200  0  32
3   192.168.40.2            Et0/0.40          14 00:10:09    9   200  0  43
2   192.168.50.2            Et0/0.50          14 00:10:09    2   200  0  41
1   192.168.10.2            Et0/0.10          11 00:10:09   13   200  0  27
0   10.10.30.1              Et0/1             13 00:10:42   10   200  0  12
L3-ROUTER-02#
```

Gambar 5. *Show DHCP Router Standby* dan *EIGRP Neighbor Router Standby*

Pada Gambar 5 diperlihatkan konfigurasi DHCP pada *router standby* yang berfungsi sebagai backup server. Selain itu, daftar neighbor EIGRP memastikan bahwa proses pertukaran routing antara *router master*, *router standby*, dan router cabang berjalan sebagaimana mestinya. HSRP berfungsi sebagai redundansi gateway pada segmen LAN, sedangkan EIGRP digunakan untuk pertukaran informasi routing antar-router pada jalur antar-jaringan. HSRP tidak dapat menentukan rute terbaik menuju jaringan lain, sehingga tetap diperlukan protokol routing dinamis seperti EIGRP agar router dapat memilih jalur optimal menuju network 10.10.x.x dan antar-segmen yang tidak berada dalam satu broadcast domain. Dengan demikian, HSRP dan EIGRP bekerja pada lapisan yang berbeda dan saling melengkapi.

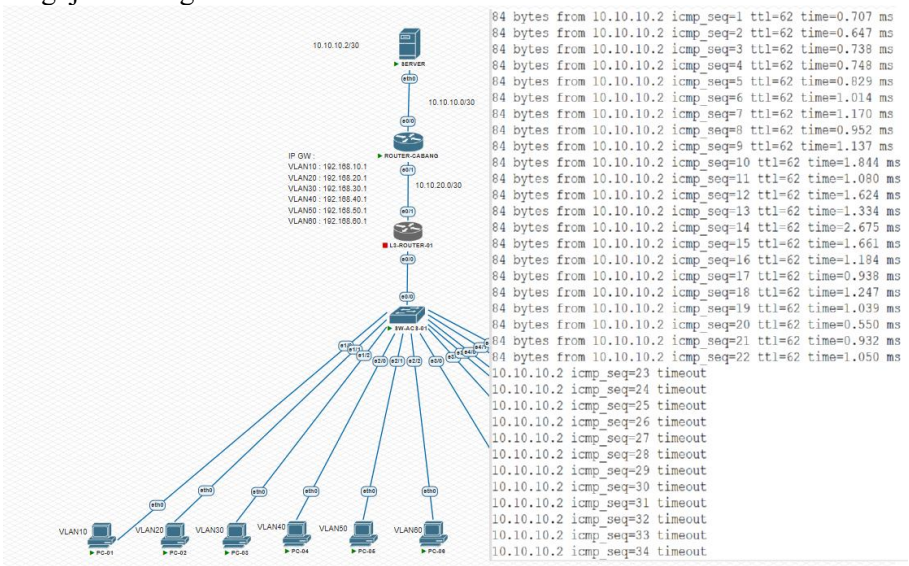
4.1. Pengujian Jaringan

Pengujian jaringan dilakukan untuk mengevaluasi kinerja jaringan sebelum dan sesudah implementasi HSRP, VLAN, dan DHCP. Pengujian dilakukan menggunakan tools seperti: *Ping* dan *Traceroute* (untuk uji *konektivitas* dan jalur data)

Perbandingan juga dilakukan terhadap perangkat keras jaringan seperti:

1. *Router*: *Router* standar (tanpa *HSRP*) vs *Router* dengan konfigurasi *HSRP*
2. *Client PC*: Perangkat tanpa *DHCP* vs perangkat dengan pengalamatan otomatis

4.2.1. Pengujian Jaringan Awal




```
84 bytes from 10.10.10.2 icmp_seq=1 ttl=62 time=0.707 ms
84 bytes from 10.10.10.2 icmp_seq=2 ttl=62 time=0.647 ms
84 bytes from 10.10.10.2 icmp_seq=3 ttl=62 time=0.738 ms
84 bytes from 10.10.10.2 icmp_seq=4 ttl=62 time=0.748 ms
84 bytes from 10.10.10.2 icmp_seq=5 ttl=62 time=0.829 ms
84 bytes from 10.10.10.2 icmp_seq=6 ttl=62 time=1.014 ms
84 bytes from 10.10.10.2 icmp_seq=7 ttl=62 time=1.170 ms
84 bytes from 10.10.10.2 icmp_seq=8 ttl=62 time=0.952 ms
84 bytes from 10.10.10.2 icmp_seq=9 ttl=62 time=1.137 ms
84 bytes from 10.10.10.2 icmp_seq=10 ttl=62 time=1.844 ms
84 bytes from 10.10.10.2 icmp_seq=11 ttl=62 time=1.080 ms
84 bytes from 10.10.10.2 icmp_seq=12 ttl=62 time=1.624 ms
84 bytes from 10.10.10.2 icmp_seq=13 ttl=62 time=1.334 ms
84 bytes from 10.10.10.2 icmp_seq=14 ttl=62 time=2.675 ms
84 bytes from 10.10.10.2 icmp_seq=15 ttl=62 time=1.661 ms
84 bytes from 10.10.10.2 icmp_seq=16 ttl=62 time=1.184 ms
84 bytes from 10.10.10.2 icmp_seq=17 ttl=62 time=0.938 ms
84 bytes from 10.10.10.2 icmp_seq=18 ttl=62 time=1.247 ms
84 bytes from 10.10.10.2 icmp_seq=19 ttl=62 time=1.039 ms
84 bytes from 10.10.10.2 icmp_seq=20 ttl=62 time=0.550 ms
84 bytes from 10.10.10.2 icmp_seq=21 ttl=62 time=0.932 ms
84 bytes from 10.10.10.2 icmp_seq=22 ttl=62 time=1.050 ms
10.10.10.2 icmp_seq=23 timeout
10.10.10.2 icmp_seq=24 timeout
10.10.10.2 icmp_seq=25 timeout
10.10.10.2 icmp_seq=26 timeout
10.10.10.2 icmp_seq=27 timeout
10.10.10.2 icmp_seq=28 timeout
10.10.10.2 icmp_seq=29 timeout
10.10.10.2 icmp_seq=30 timeout
10.10.10.2 icmp_seq=31 timeout
10.10.10.2 icmp_seq=32 timeout
10.10.10.2 icmp_seq=33 timeout
10.10.10.2 icmp_seq=34 timeout
```

Gambar 6. Pengujian Koneksi Saat terjadi *Link Failure*

Pengujian awal dilakukan pada jaringan eksisting di Perusahaan XYZ Tbk untuk mengidentifikasi kelemahan dan masalah umum. Jaringan awal masih menggunakan *single*

gateway tanpa redundansi, tanpa segmentasi VLAN, dan pengaturan IP secara manual di setiap perangkat.

1. Pengujian Koneksi Jaringan Normal

Pengujian pertama adalah pengujian koneksi jaringan komputer, pada simulasi ini pengujian koneksi dengan cara melakukan perintah *PING* dari *device* ke IP *Address Server* yang ada pada cabang yaitu 10.10.10.2 pada saat jaringan normal atau tidak ada nya kegagalan pada *router.*

2. Pengujian Jaringan Berjalan Saat Terjadi *Error* pada *Router*

Pengujian selanjutnya adalah simulasi pada jaringan berjalan Perusahaan XYZ saat terjadinya *downtime* yang diakibatkan oleh terputus nya jalur komunikasi pada *router.* Gambar 6 menunjukkan kondisi pengujian ketika terjadi *link failure* pada router master. Dalam kondisi jaringan eksisting tanpa HSRP, paket ICMP dari PC menuju server tidak dapat mencapai tujuan karena tidak tersedia jalur cadangan. Hasil pengujian melakukan *ping* dari PC-01 ke IP *Address server* di cabang yaitu 10.10.10.2 dengan kondisi *link failure* pada *router.* Hasil menunjukan bahwa koneksi ke arah server terputus, hal ini terjadi karena tidak ada jalur Cadangan pada *router* jika *router* utama mengalami *downtime.*

3. Pengujian QoS (*Quality of Services*)

Dalam Pengujian QoS ini hanya menguji dua (2) QoS yaiu *latency* dan *packet loss* pada jaringan berjalan di Perusahaan XYZ melalui simulasi yang sudah disiapkan penulis menggunakan *software gns3.*

a) Latency

Latency adalah waktu yang diperlukan oleh paket data untuk mencapai *endpoint* tujuan dan Kembali lagi ke *endpoint* awal. Rumus dari perhitungan *latency* adalah : RTT= Waktu Paket Kembali (*in)*-Waktu Paket Keluar (*Out).*

```
VPCS> ping 10.10.10.2

84 bytes from 10.10.10.2 icmp_seq=1 ttl=62 time=1.700 ms
84 bytes from 10.10.10.2 icmp_seq=2 ttl=62 time=1.230 ms
84 bytes from 10.10.10.2 icmp_seq=3 ttl=62 time=1.521 ms
84 bytes from 10.10.10.2 icmp_seq=4 ttl=62 time=0.931 ms
84 bytes from 10.10.10.2 icmp_seq=5 ttl=62 time=2.098 ms

VPCS>
```

Gambar 7. Pengujian ke-1 *Latency*

Skenario redundansi *gateway* (*router* normal) digunakan untuk memastikan bahwa HSRP tidak menambah delay signifikan saat jalur utama aktif.

Pada Gambar 7 terlihat hasil pengujian latency pertama pada jaringan eksisting. Nilai RTT menunjukkan fluktuasi yang mengindikasikan ketidakstabilan jalur komunikasi tanpa adanya mekanisme redundansi.

Tabel 1. Pengujian *Latency*

Pengujian	*Ke-1 (MS)*	*Ke-2 (MS)*	*Ke-3 (MS)*	*Ke-4 (MS)*	*Ke-5 (MS)*	*Ke-6 (MS)*
Ping ke 1	*1.561 ms*	*1.593 ms*	*1.292 ms*	*0.801 ms*	*1.628 ms*	*1.241 ms*
Ping ke 2	*1.185 ms*	*1.628 ms*	*2.329 ms*	*1.628 ms*	*1.603 ms*	*1.526 ms*
Ping ke 3	*0.869 ms*	*1.420 ms*	*1.799 ms*	*1.099 ms*	*1.647 ms*	*1.744 ms*
Ping ke 4	*1.344 ms*	*1.714 ms*	*1.699 ms*	*0.800 ms*	*1.142 ms*	*1.138 ms*
Ping ke 5	*1.248 ms*	*1.274 ms*	*1.599 ms*	*1.363 ms*	*2.075 ms*	*1.619 ms*
Total	***1.241 ms***	***1.526 ms***	***1.744 ms***	***1.138 ms***	***1.619 ms***	***7.268 ms***

Dari Tabel 1 menyajikan hasil pengujian latency pada jaringan eksisting sebelum implementasi HSRP. Pengujian dilakukan sebanyak enam kali, dan hasilnya menunjukkan variasi waktu tanggap yang berkaitan dengan kestabilan jaringan.

b) Pengujian *Packet Loss*

Skenario *failover* (*router* master down) digunakan mengukur seberapa besar dampak perpindahan jalur terhadap pengalaman pengguna. *Latency* dapat meningkat pada saat transisi state, namun peningkatan ini harus tetap berada dalam ambang batas yang dapat diterima.

```
VPCS> ping 10.10.10.2 -c 10

84 bytes from 10.10.10.2 icmp_seq=1 ttl=62 time=1.898 ms
84 bytes from 10.10.10.2 icmp_seq=2 ttl=62 time=1.050 ms
84 bytes from 10.10.10.2 icmp_seq=3 ttl=62 time=0.929 ms
84 bytes from 10.10.10.2 icmp_seq=4 ttl=62 time=1.638 ms
84 bytes from 10.10.10.2 icmp_seq=5 ttl=62 time=0.924 ms
84 bytes from 10.10.10.2 icmp_seq=6 ttl=62 time=0.928 ms
84 bytes from 10.10.10.2 icmp_seq=7 ttl=62 time=1.328 ms
84 bytes from 10.10.10.2 icmp_seq=8 ttl=62 time=1.633 ms
84 bytes from 10.10.10.2 icmp_seq=9 ttl=62 time=0.921 ms
84 bytes from 10.10.10.2 icmp_seq=10 ttl=62 time=0.797 ms

VPCS>
```

Gambar 8. Uji *Packet Loss*

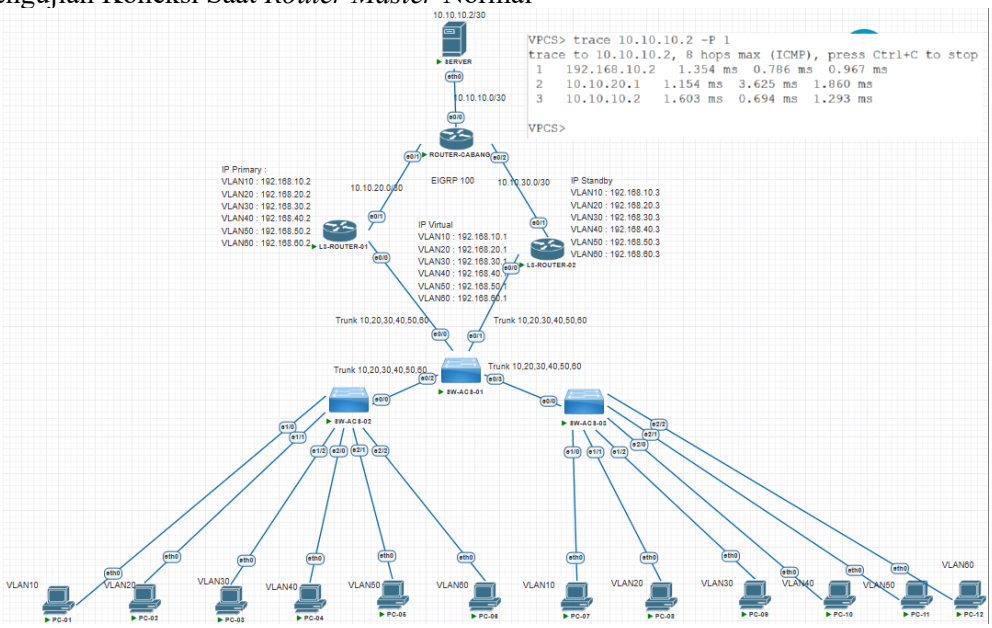
Gambar 8 menunjukkan hasil pengujian packet loss pada jaringan eksisting. Dari sepuluh paket yang dikirim, seluruhnya diterima sehingga packet loss bernilai 0%. Namun, kondisi ini tidak dapat dijadikan acuan penuh karena tidak diuji pada kondisi gagal jalur.

4.2.2. Pengujian Jaringan Akhir

Pengujian ini dilakukan menggunakan metode dan tools yang sama seperti pada tahap awal agar dapat dibandingkan secara objektif, yaitu menggunakan *Ping***,** serta pengamatan manual terhadap fungsionalitas *DHCP*.

A. Tahap Pengujian

1. Pengujian Koneksi Saat *Router Master* Normal



Gambar 9. Uji *Trace Router Master*

Pada gambar 9 adalah hasil dari pengujian *trace* pada jaringan usulan, *packet* melewati *hop count* pertama yaitu 192.168.10.2 (*router master)*, lalu masuk ke *hop* selanjut nya yaitu *interface* pada *router cabang* dengan ip 10.10.20.1 dan akhirnya sampai pada *endpoint* penerima dengan IP 10.10.10.2.

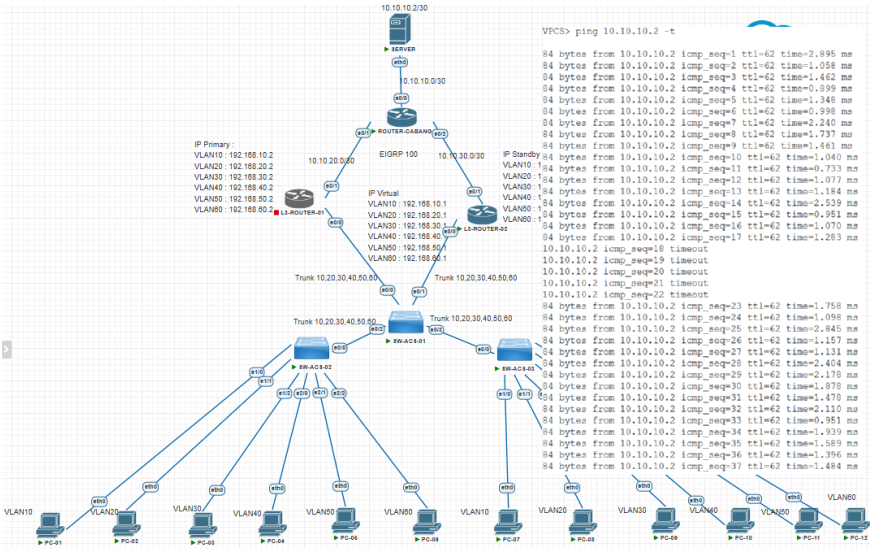
```
L3-ROUTER-01#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Et0/0.10    10   110 P Active  local           192.168.10.3    192.168.10.1
Et0/0.20    20   110 P Active  local           192.168.20.3    192.168.20.1
Et0/0.30    30   110 P Active  local           192.168.30.3    192.168.30.1
Et0/0.40    40   110 P Active  local           192.168.40.3    192.168.40.1
Et0/0.50    50   110 P Active  local           192.168.50.3    192.168.50.1
Et0/0.60    60   110 P Active  local           192.168.60.3    192.168.60.1
L3-ROUTER-01#
```

Gambar 10. Status HSRP *Router Master*

Gambar 10 menampilkan status HSRP pada router master dalam keadaan aktif. Informasi ini menunjukkan parameter prioritas, state active, serta virtual IP yang sedang digunakan oleh klien.

2. Pengujian Koneksi Saat *Router Master Down*

Pengujian koneksi jika *router master* mengalami gangguan *down* dan mengakibatkan jaringan komputer mengalami *downtime*. Skenario pengujian sama seperti saat *router master* normal, yaitu melakukan pengiriman *packet ping* ke IP *Address* 10.10.10.2, pada scenario ini jalur router master akan diputus.



Gambar 11. Uji Konektifitas HSRP

Terlihat pada gambar 11 *router standby* akan mengambil alih jalur pengiriman *packet data.* Pada saat *router master* terputus maka pada pengiriman *packet* akan terjadi *packet loss* sebelum jaringan komputer tersedia kembali.

```
L3-ROUTER-02#
*Nov 15 16:17:28.183: %HSRP-5-STATECHANGE: Ethernet0/0.20 Grp 20 state Standby -> Active
*Nov 15 16:17:28.623: %HSRP-5-STATECHANGE: Ethernet0/0.30 Grp 30 state Standby -> Active
*Nov 15 16:17:28.867: %HSRP-5-STATECHANGE: Ethernet0/0.60 Grp 60 state Standby -> Active
*Nov 15 16:17:28.915: %HSRP-5-STATECHANGE: Ethernet0/0.50 Grp 50 state Standby -> Active
*Nov 15 16:17:29.335: %HSRP-5-STATECHANGE: Ethernet0/0.10 Grp 10 state Standby -> Active
*Nov 15 16:17:30.187: %HSRP-5-STATECHANGE: Ethernet0/0.40 Grp 40 state Standby -> Active
L3-ROUTER-02#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Et0/0.10    10   100 P Active  local           unknown         192.168.10.1
Et0/0.20    20   100 P Active  local           unknown         192.168.20.1
Et0/0.30    30   100 P Active  local           unknown         192.168.30.1
Et0/0.40    40   100 P Active  local           unknown         192.168.40.1
Et0/0.50    50   100 P Active  local           unknown         192.168.50.1
Et0/0.60    60   100 P Active  local           unknown         192.168.60.1
L3-ROUTER-02#
```

Gambar 12. *Status Router Standby*

Pada gambar 12 status *router standby* Kembali menjadi *standby* yang sebelumnya berada pada posisi *active* pada jaringan komputer, hal ini disebabkan karena *router master* sudah kembali normal dan fitur *preempt pada konfigurasi* HSRP mengembalikan jalur utama ke *router master* secara otomatis.

3. Pengujian QoS (*Quality of Services)*

Menguji tiga (3) QoS yaitu *Latency, Packet loss* dan *failover* pada jaringan usulan di Perusahaan XYZ melalui simulasi menggunakan software PnetLab. Pada pengujian QoS ini menggunakan 2 skenario yaitu pada saat *router master* normal dan ketika *router master down*.

a) Pengujian *Latency*

Pengujian *latency* melakukan pengirim *packet ping* ke server IP 10.10.10.2 melalui PC *client,* mengirimkan *packet ping* sebanyak 5 kali untuk mendapatkan hasil yang relevan.

```
VPCS> ping 10.10.10.2

84 bytes from 10.10.10.2 icmp_seq=1 ttl=62 time=2.210 ms
84 bytes from 10.10.10.2 icmp_seq=2 ttl=62 time=1.265 ms
84 bytes from 10.10.10.2 icmp_seq=3 ttl=62 time=1.697 ms
84 bytes from 10.10.10.2 icmp_seq=4 ttl=62 time=1.569 ms
84 bytes from 10.10.10.2 icmp_seq=5 ttl=62 time=1.033 ms

VPCS>
```

Gambar 13. Pengujian ke-1 *Latency HSRP*

Pada Gambar 13 adalah hasil pengujian ke-1 dari *latency* jaringan usulan di Perusahaan XYZ. Simulasi pengujian dilakukan dengan *ping* ke Alamat IP 10.10.10.2 hasilnya adalah sebagai berikut:

Tabel 2. Pengujian ke-1 *Latency* HSRP

Pengujian	*Ke-1 (MS)*	*Ke-2 (MS)*	*Ke-3 (MS)*	*Ke-4(MS)*	*Ke-5(MS)*
Ping ke 1	*2.210 ms*	*3.404 ms*	*1.576 ms*	*2.393 ms*	*1.976 ms*
Ping ke 2	*1.265 ms*	*1.190 ms*	*1.672 ms*	*1.033 ms*	*1.570 ms*
Ping ke 3	*1.697 ms*	*2.313 ms*	*0.957 ms*	*0.849 ms*	*1.684 ms*
Ping ke 4	*1.569 ms*	*1.727 ms*	*0.964 ms*	*1.093 ms*	*2.506 ms*
Ping ke 5	*1.033 ms*	*1.188 ms*	*1.019 ms*	*1.079 ms*	*1.961 ms*
Total	***1.555 ms***	***1.964 ms***	***1.238 ms***	***1.289 ms***	***1.939 ms***

Pengujian *latency* sebanyak 5 kali pengujian sudah di lakukan melalui PC-01 yang disimulasikan PC-01 melakukan *ping* ke IP *address* 10.10.10.2 yaitu Alamat IP pada *server* di cabang, dari hasil pengujian sebanyak 5 kali ini didapatkan data sebagai berikut:

Tabel 3. Hasil Pengujian *Latency* HSRP

Pengujian	*Value Latency (ms)*
Ping ke 1	*1.555 ms*
Ping ke 2	*1.964 ms*
Ping ke 3	*1.238 ms*
Ping ke 4	*1.289 ms*
Ping ke 5	*1.939 ms*
Total	***7.985 ms***

Tabel 2 dan Tabel 3 menyajikan detail hasil pengukuran latency pada lima kali pengujian. Nilai rata-rata menunjukkan peningkatan stabilitas setelah implementasi HSRP.

Dari tabel 3 didapatkan nilai hasil pengujian *latency* sebanyak 5 kali pengujian *ping* ke IP 10.10.10.2, selanjutnya adalah mengetahui total rata rata dari value pengujian, rumus dari mencari nilai *latency* adalah : total nilai / total pengujian, didapatkan hasil 7.985/5 = **1.597 ms.** Perlu ditekankan, bahwa hasil ini tidak mencerminkan hasil *latency* di keadaan *real device*, hasil ini adalah simulasi menggunakan *PnetLab*.

b) Pengujian *Packet Loss*

Selanjutnya adalah pengujian *packet loss* pada jaringan usulan di Perusahaan XYZ, melakukan *ping* sebanyak 10 kali pada sampel satu (1) *client* di topologi usulan.

```
VPCS> ping 10.10.10.2 -c 10

84 bytes from 10.10.10.2 icmp_seq=1 ttl=62 time=2.692 ms
84 bytes from 10.10.10.2 icmp_seq=2 ttl=62 time=5.570 ms
84 bytes from 10.10.10.2 icmp_seq=3 ttl=62 time=2.729 ms
84 bytes from 10.10.10.2 icmp_seq=4 ttl=62 time=1.351 ms
84 bytes from 10.10.10.2 icmp_seq=5 ttl=62 time=3.222 ms
84 bytes from 10.10.10.2 icmp_seq=6 ttl=62 time=2.119 ms
84 bytes from 10.10.10.2 icmp_seq=7 ttl=62 time=2.209 ms
84 bytes from 10.10.10.2 icmp_seq=8 ttl=62 time=14.199 ms
84 bytes from 10.10.10.2 icmp_seq=9 ttl=62 time=1.149 ms
84 bytes from 10.10.10.2 icmp_seq=10 ttl=62 time=1.424 ms

VPCS>
```

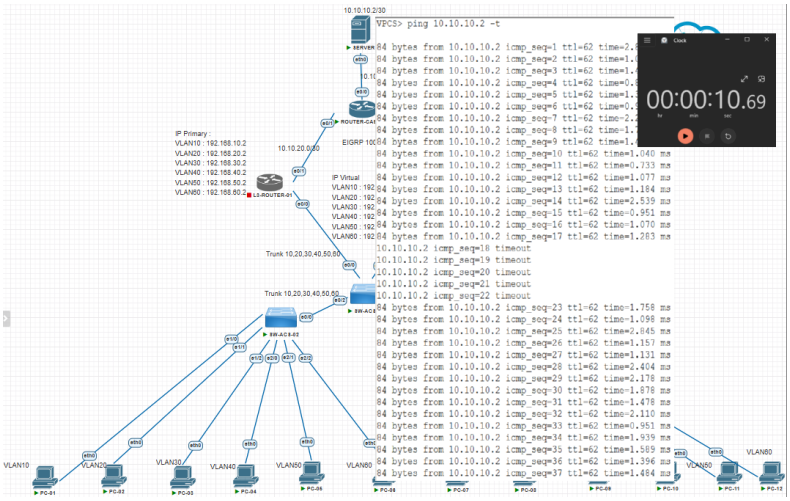
Gambar 14. Pengujian *Packet Loss* HSRP

Gambar 14 menunjukkan hasil pengujian *packet loss* pada jaringan usulan. Tidak ditemukan paket hilang sehingga jaringan dalam kondisi stabil.

Hasil pengujian didapatkan informasi semua *packet* terkirim tanpa adanya *packet loss* 0%. Pengujian ini dilakukan melalui simulasi menggunakan PnetLab, dan perlu pengujian secara *real device* untuk mendapatkan hasil yang lebih akurat.

c) Pengujian *Failover*

Pengujian QoS bagian *failover,* simulasi menggunakan PnetLab dan aplikasi *stopwatch* untuk mencatat waktu *failover*, dan untuk scenario pengujian penulis akan melakukan pengiriman *packet* secara terus menerus ke Alamat IP *address* 10.10.10.2 dari satu (1) *client* pada topologi usulan.



Gambar 15. Pengujian *Failover*

Pada gambar 15 terlihat simulasi pengujian *failover* pada jaringan usulan HSRP, pengiriman *packet ping* ke IP *Address* 10.10.10.2 dan pada saat pengiriman *packet ping* tersebut dengan mematikan *router master*, sehingga jalur pengiriman akan berpindah ke *router standby*. Terlihat terdapat RTO (*Request Time Out*), terjadi karena ada perpindahan jalur komunikasi dari *router* master ke *router standby* dengan metode HSRP. Waktu failover dari *router master* ke *router standby* selama 10 detik.

```
84 bytes from 10.10.10.2 icmp_seq=1 ttl=62 time=0.707 ms
84 bytes from 10.10.10.2 icmp_seq=2 ttl=62 time=0.647 ms
84 bytes from 10.10.10.2 icmp_seq=3 ttl=62 time=0.738 ms
84 bytes from 10.10.10.2 icmp_seq=4 ttl=62 time=0.748 ms
84 bytes from 10.10.10.2 icmp_seq=5 ttl=62 time=6.443 ms
84 bytes from 10.10.10.2 icmp_seq=6 ttl=62 time=1.014 ms
84 bytes from 10.10.10.2 icmp_seq=7 ttl=62 time=1.170 ms
84 bytes from 10.10.10.2 icmp_seq=8 ttl=62 time=0.952 ms
84 bytes from 10.10.10.2 icmp_seq=9 ttl=62 time=1.137 ms
84 bytes from 10.10.10.2 icmp_seq=10 ttl=62 time=1.844 ms
84 bytes from 10.10.10.2 icmp_seq=11 ttl=62 time=1.080 ms
84 bytes from 10.10.10.2 icmp_seq=12 ttl=62 time=1.624 ms
84 bytes from 10.10.10.2 icmp_seq=13 ttl=62 time=1.334 ms
84 bytes from 10.10.10.2 icmp_seq=14 ttl=62 time=2.675 ms
84 bytes from 10.10.10.2 icmp_seq=15 ttl=62 time=1.661 ms
84 bytes from 10.10.10.2 icmp_seq=16 ttl=62 time=6.443 ms
84 bytes from 10.10.10.2 icmp_seq=17 ttl=62 time=0.938 ms
84 bytes from 10.10.10.2 icmp_seq=18 ttl=62 time=1.247 ms
84 bytes from 10.10.10.2 icmp_seq=19 ttl=62 time=1.039 ms
84 bytes from 10.10.10.2 icmp_seq=20 ttl=62 time=0.550 ms
84 bytes from 10.10.10.2 icmp_seq=21 ttl=62 time=0.932 ms
84 bytes from 10.10.10.2 icmp_seq=22 ttl=62 time=1.050 ms
84 bytes from 10.10.10.2 icmp_seq=39 ttl=62 time=2.638 ms
84 bytes from 10.10.10.2 icmp_seq=40 ttl=62 time=0.965 ms
84 bytes from 10.10.10.2 icmp_seq=41 ttl=62 time=1.186 ms
84 bytes from 10.10.10.2 icmp_seq=42 ttl=62 time=1.365 ms
84 bytes from 10.10.10.2 icmp_seq=43 ttl=62 time=1.688 ms
84 bytes from 10.10.10.2 icmp_seq=44 ttl=62 time=1.734 ms
84 bytes from 10.10.10.2 icmp_seq=45 ttl=62 time=0.951 ms
84 bytes from 10.10.10.2 icmp_seq=23 ttl=62 time=1.758 ms
84 bytes from 10.10.10.2 icmp_seq=24 ttl=62 time=1.098 ms
84 bytes from 10.10.10.2 icmp_seq=25 ttl=62 time=2.845 ms
84 bytes from 10.10.10.2 icmp_seq=26 ttl=62 time=1.157 ms
84 bytes from 10.10.10.2 icmp_seq=27 ttl=62 time=1.131 ms
84 bytes from 10.10.10.2 icmp_seq=28 ttl=62 time=2.404 ms
84 bytes from 10.10.10.2 icmp_seq=29 ttl=62 time=2.178 ms
84 bytes from 10.10.10.2 icmp_seq=30 ttl=62 time=1.878 ms
84 bytes from 10.10.10.2 icmp_seq=31 ttl=62 time=1.478 ms
84 bytes from 10.10.10.2 icmp_seq=32 ttl=62 time=2.110 ms
```

Gambar 16. Uji *Failover Router Master Active*

Pada gambar 16 terlihat simulasi pengujian *failover* pada jaringan usulan HSRP, pengiriman *packet ping* ke IP *Address* 10.10.10.2 dan pada saat pengiriman *packet ping* tersebut penulis mengaktifkan Kembali jalur ke *router master,* sehingga jalur pengiriman akan berpindah *router standby* Kembali ke *router master.* Terlihat pada gambar 17 tidak terdapat RTO (Request Time Out), namun kita melihat Angka *Time* yang cukup besar sampai 6.443 ms hal ini terjadi karena perpindahan state dari standby ke *active* dan dari *Active* ke *standby* tidak menyebabkan downtime tapi akan ada waktu transisi perpindahan dari Jalur Router Standby ke *Router Active*.

5. KESIMPULAN

Penelitian implementasi HSRP (*Hot Standby Router Protocol*) terbukti meningkatkan keandalan jaringan dengan menyediakan redundansi gateway sehingga tetap berjalan meski router utama gagal. Pada simulasi failover menunjukkan perpindahan jalur dari router standby ke master tidak menimbulkan RTO (*Request Time Out*), hanya jeda transisi dengan *time* mencapai 6.443 ms. Hal ini membuktikan HSRP efektif menjaga ketersediaan jaringan tanpa downtime. Selain

itu, penerapan EIGRP membuat routing lebih efisien, DHCP mempermudah manajemen IP, serta VLAN dan ACL meningkatkan segmentasi dan keamanan jaringan. Dari hasil pengujian, HSRP merupakan protokol yang paling berpengaruh terhadap peningkatan ketersediaan jaringan karena menyediakan mekanisme failover otomatis. EIGRP tetap memiliki peran penting dalam optimalisasi jalur routing, namun peningkatan keandalan secara langsung terutama disebabkan oleh implementasi HSRP.

DAFTAR PUSTAKA

[1] T. Rahman and E. T. Pamungkas, "Optimalisasi Jaringan Komputer Di Smk Travina Prima Dengan Implementasi INTERVLAN, VLSM, DAN HSRP," *J. Inform. Univ. Muhammadiyah Tangerang P*, vol. 8, no. 4, pp. 2722–2713, 2024, doi: http://dx.doi.org/10.31000/jika.v8i4.12379.

[2] Z. Saharuna, "Performa Hot Standby Routing Protocol (HSRP) Pada Video streaming," vol. 18, no. 1, pp. 1–6, 2021, doi: https://doi.org/10.31963/elekterika.v5i1.2710.

[3] R. S. Anwar and A. Setiawan, "Penerapan Protokol HSRP (Hot Standby Router Protocol) Failover Dalam Jaringan Lokal Pada Direktorat Politik Dalam Negeri Kementerian Dalam Negeri," *J. AKRAB JUARA*, vol. 7, no. 3, pp. 63–74, 2022, doi: https://doi.org/10.58487/akrabjuara.v7i3.1867.

[4] A. K. Anam and T. Nurhastuti, "Perancangan Jaringan LAN Menggunakan Metode HSRP (Hot Standby Router Protocol)di PT.Citra Solusi Pratama," *J. Teknol. Inf.*, vol. 8, no. 2, pp. 106–117, 2022, doi: https://doi.org/10.52643/jti.v8i2.2725.

[5] A. Sustia and R. Albar, "Analisis dan Pemanfaatan Metode Variable Length Subnet Mask (VLSM) Guna Membangun Jaringan Lokal Area Network (LAN)," *J. Informatics Comput. Sci.*, vol. 10, no. 1, pp. 90–97, 2024, doi: https://doi.org/10.33143/jics.v10i1.3907.

[6] D. Apriani, D. Kartika, N. Harahap, and R. Riphaldi, "Pelatihan Simulasi Perancangan Topologi Jaringan Bus Menggunakan Cisco Packet Tracer," *JURIBMAS J. Has. Pengabdi. Masy.*, vol. 1, no. 1, pp. 16–22, 2022, doi: https://doi.org/10.62712/juribmas.v1i1.5.

[7] B. S. Fajrin, Priatno, and M. R. Effendi, "Penerapan Sistem Keamanan Jaringan Menggunakan Vpn Dengan Metode PPTP Pada PT Hinoka Sinergi Tanyo" *JSI (Jurnal Sist. Informasi) Univ. Suryadarma*, vol. 11, no. 2, pp. 185–196, 2024, doi: https://doi.org/10.35968/jsi.v11i2.1252.

[8] S. E. Prasetyo, G. Wijaya, N. Hasanah, and P. Syahfira, "Rancangan Jaringan Highly Available PT Pundi Mas Berjaya (PMB)," *TELCOMATICS*, vol. 8, no. 1, pp. 1–9, 2023, doi: http://dx.doi.org/10.37253/telcomatics.v8i1.7359.

[9] I. I. Muwajihan and D. Jatikusumo, "Perancangan Jaringan Ethernet Link Dengan Menggunakan Teknologi Link Aggregation Dan Auto," vol. 6, no. 2, pp. 128–137, 2021, doi: https://doi.org/10.31294/ijcit.v6i2.10866.

[10] A. Octavian and G. Purnama, "Perancangan Jaringan Redundancy Menggunakan Konsep Etherchannel Dan Hsrp Dengan Intervlan Routing Pada PLN UID Jakarta Raya," *JITET(Jurnal Inform. dan Tek. Elektro Ter.*, vol. 12, no. 2, pp. 1211–1220, 2024, doi: https://doi.org/10.23960/jitet.v12i2.4193.

[11] R. H. Saputra, A. Subardono, and D. Teknik, "Pengaruh Failover Pada Jaringan Software-Defined," *J. Internet Softw. Eng.*, vol. 1, no. 1, pp. 1–9, 2020, doi: https://doi.org/10.22146/jise.v1i1.761.

[12] R. A. N. B, Ruuhwan, and R. Hartono, "Merancang IP Failover & Replikasi Database Menggunakan Heartbeat Pada Komputer Server (Studi Kasus : SMK Pariwisata Tasikmalaya)," vol. 5, no. 2, pp. 51–59, 2023, doi: https://doi.org/10.36423/index.v5i2.1354.

[13] E. K. Silalahi, Y. C. Sitanggang, E. Suryaningsih, and D. Kiswanto, "Implementasi Dan Analisis Protokol Hsrp Dan Vrrp Dalam Meningkatkan Redundansi Gateway Pada Jaringan Virtual," *JITET (Jurnal Inform. dan Tek. Elektro Ter.*, vol. 13, no. 2, pp. 1431–1444, 2025, doi: https://doi.org/10.23960/jitet.v13i2.6474.

[14] S. Wahyudi and S. Destya, "Analisis Perbandingan Performa FHRP Pada Routing EIGRP Menggunakan IPV4 dan IPV6," *Indones. J. Comput. Sci.*, vol. 13, no. 4, pp. 6627–6640, 2024, doi: https://doi.org/10.33022/ijcs.v13i4.4297.

[15] T. E. Geraldi, M. I. Wahyuddin, and A. Aningsih, "Perancangan Backup Link Menggunakan Metode HSRP (Hot Standby Router Protocol) Dalam Penyediaan Layer -3 Redundansi," *J. Media Inform. Budidarma*, vol. 4, no. 1, pp. 201–207, 2020, doi: https://doi.org/10.30865/mib.v4i1.1873.

[16] V. R. Dewi and G. Purnama, "Perancangan Jaringan Sistem Failover Dengan Metode Hot Standby Routing Protocol (HSRP)," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 8, no. 1, pp. 339–345, 2024, doi: https://doi.org/10.36040/jati.v8i1.8523.