

27

**PENERAPAN PROTOKOL HSRP (*HOT STANDBY ROUTER PROTOCOL*)
FAILOVER DALAM JARINGAN LOKAL PADA DIREKTORAT POLITIK
DALAM NEGERI KEMENTERIAN DALAM NEGERI**

Rian Septian Anwar, Anggi Setiawan

Fakultas Teknik Dan Informatika, Universitas Bina Sarana Informatika

(Naskah diterima: 1 Juni 2022, disetujui: 28 Juli 2022)

Abstract

At the Directorate of Domestic Politics of the Ministry of Home Affairs, the application of a LAN (Local Area Network) network system is the right choice because it is in accordance with the conditions that exist in the field. In its application, the network system is important in order to facilitate employees so that the work runs well and smoothly. The purpose of this study is to implement a redundant protocol HSRP (Hot Standby Router Protocol) to mitigate constraints on local networks in the Directorate of Domestic Politics of the Ministry of Home Affairs. The research method was carried out based on existing network observations, interviews, and looking at references through literature studies. This research was conducted by adding a router as a backup router if the main router has a problem or deficiency failure using the HSRP (Hot Standby Router Protocol) method. In the testing phase, using the ping command, and tracert with the HSRP failover scenario that has been implemented. With the implementation of the HSRP redundancy protocol, it is hoped that the obstacles can be overcome properly and become an evaluation material for the network.

Keywords: LAN Network (Local Area Network), Redundancy Protocol, HSRP (Hot Standby Router Protocol).

Abstrak

Pada Direktorat Politik Dalam Negeri Kementerian Dalam Negeri, penerapan sistem jaringan LAN (*Local Area Network*) menjadi pilihan yang tepat karena sesuai dengan kondisi yang ada pada lapangan. Pada penerapannya sistem jaringan tersebut penting guna memfasilitasi para pegawai agar pekerjaan berjalan dengan baik dan lancar. Tujuan penelitian ini adalah untuk mengimplementasikan sebuah protokol redundansi HSRP (*Hot Standby Router Protocol*) guna mitigasi kendala pada jaringan lokal yang ada di Direktorat Politik Dalam Negeri Kementerian Dalam Negeri. Metode penelitian dilakukan berdasarkan observasi jaringan yang ada, wawancara, serta melihat referensi melalui studi pustaka. Penelitian ini dilakukan dengan menambah sebuah router sebagai router backup jika router utama terjadi kendala atau *defice failure* dengan metode HSRP (*Hot Standby Router Protocol*). Pada tahap pengujian menggunakan command ping, dan tracert dengan skenario failover HSRP yang sudah diimplementasikan. Dengan penerapan protokol redundansi HSRP diharapkan kendala dapat diatasi dengan baik dan menjadi bahan evaluasi pada jaringan tersebut.

Kata kunci: Jaringan LAN (*Local Area Network*), Protokol Redudansi, HSRP (*Hot Standby Router Protocol*).

I. PENDAHULUAN

Dizaman dengan kemajuan teknologi yang cukup pesat ini, perkembangan teknologi komputer dan jaringan mengalami kemajuan yang sejalan dan menghubungkan pengguna di seluruh dunia kedalam sebuah sistem jaringan *international network* atau bisa disebut internet. Sistem jaringan lokal atau dapat disebut LAN (*Local Area Network*) saat ini sudah menjadi sebuah sistem jaringan yang wajib diimplementasikan oleh perusahaan maupun perkantoran seperti halnya pada Direktorat Politik Dalam Negeri Kementerian Dalam Negeri yang menerapkan sistem jaringan LAN (*Local Area Network*).

Dalam penerapannya, jaringan lokal pada Direktorat Politik Dalam Negeri Kementerian Dalam Negeri ini kadang tidak berjalan dengan mulus, ada beberapa kelemahan yang terjadi bukan karena sistemnya yang buruk melainkan belum diterapkannya sebuah protokol yang mengatur masalah seperti *device failure* yang mengakibatkan terganggunya lalu lintas data pada sistem jaringan lokal tersebut.

Direktorat Politik Dalam Negeri sebagaimana dimaksud dalam Permendagri 13 Ta-

hun 2021, mempunyai tugas melaksanakan sebagian tugas Direktorat Jenderal Politik dan Pemerintahan Umum di bidang politik dalam negeri.

Maksud dan tujuan penelitian ini adalah Mengembangkan sistem jaringan yang ada dengan menerapkan konsep protokol *hsrp failover* pada jaringan lokal pada Direktorat Politik Dalam Negeri Kementerian Dalam Negeri.

Serta manfaat yang ditimbulkan setelah penelitian ini dibuat adalah

1. Menjadi bahan pertimbangan evaluasi pada sistem jaringan lokal Direktorat Politik Dalam Negeri Kementerian Dalam Negeri.
2. Memberikan sebuah gambaran hasil yang bisa membantu atau mempermudah pada operasional sistem jaringan pada Direktorat Politik Dalam Negeri Kementerian Dalam Negeri.

II. KAJIAN TEORI

Terdapat teori – teori dasar mengenai jaringan komputer, dasar pengertian, dan lain – lain. Berikut ini merupakan beberapa pengetahuan dasar mengenai sistem jaringan komputer.

1. Pengertian Jaringan Komputer

Jaringan komputer adalah kumpulan sumber daya komputer yang terhubung. Sumber daya ini termasuk tetapi tidak terbatas ke komputer dari semua jenis, perangkat jaringan, perangkat seperti printer dan menara cakram optik, MODEM (MODEM singkatan dari *MODulation DEModulation*), kabel yang digunakan untuk sumber daya ini terhubung. Sebagian besar komputer yang terhubung ke jaringan adalah personal komputer dan laptop, tetapi ada juga server, komputer *mainframe*, dan *superkomputer*. Baru-baru ini, perangkat seluler seperti ponsel pintar dan tablet telah menjadi bagian dari jaringan komputer. (Fox, R., & Hao, 2018)

2. Topologi

Topologi yang digunakan adalah jenis topologi tree. Topologi ini, juga dikenal sebagai topologi *multi-level*, biasanya digunakan untuk menghubungkan sistem pusat dan hierarkis. (Astuti, 2020). Berikut adalah ciri – ciri dari topologi tree:

- a. Setiap node dalam arsitektur ini terhubung satu sama lain di tingkat hierarki, ke setiap node tetangga di tingkat yang lebih rendah.
- b. Topologi pohon menggabungkan beberapa topologi bintang dengan

menghubungkan beberapa komponen ke node pusat.

- c. Setiap node sekunder memiliki koneksi langsung ke node induk, dan semua node sekunder di bawah yurisdiksinya memiliki koneksi langsung ke node tersier

3. Metode protokol HSRP

Hot Standby Routing Protocol (HSRP) menyediakan *failover* transparan dari perangkat hop pertama, yang biasanya bertindak sebagai *gateway* ke *host*. HSRP menyediakan redundansi perutean untuk host IP pada jaringan Ethernet yang dikonfigurasi dengan alamat IP *gateway default*. Diperlukan minimal dua perangkat untuk mengaktifkan HSRP; satu perangkat bertindak sebagai perangkat aktif dan mengurus penerusan paket, dan yang lain bertindak sebagai siaga, siap untuk mengambil alih peran perangkat aktif jika terjadi kegagalan. (Jain et al., 2018)

IP virtual dikonfigurasi pada segmen jaringan dari setiap antarmuka yang mendukung HSRP yang termasuk dalam grup HSRP yang sama. HSRP memilih salah satu antarmuka yang bertindak sebagai router HSRP aktif. Alamat MAC virtual diberikan grup umum dengan IP virtual. Router aktif

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. Jika tiga atau lebih perangkat merupakan bagian dari grup HSRP, perangkat HSRP siaga baru akan dipilih. Operator mengontrol perangkat yang bertindak sebagai perangkat HSRP aktif dengan mengatur prioritas antarmuka (default adalah 100). Semakin tinggi prioritas, semakin banyak perangkat yang akan bertindak sebagai perangkat HSRP aktif.

III. METODE PENELITIAN

1. Metode Pegumpulan Data

- Observasi, pengamatan secara langsung mengenai kegiatan, sistem jaringan, dan pemecahan masalah yang ditemui. Hasil dari observasi tadi dicatat langsung oleh penulis dan ditelaah agar dapat diketahui akar permasalahan yang terdapat saat kegiatan observasi.
- Wawancara, Melakukan wawancara dengan beberapa narasumber untuk mendapatkan data tentang sistem jaringan komputer yang ada pada Direktorat Politik Dalam Negeri Kementerian Dalam Negeri
- Studi Pustaka, Dengan metode studi pustaka penulis mendapatkan beberapa

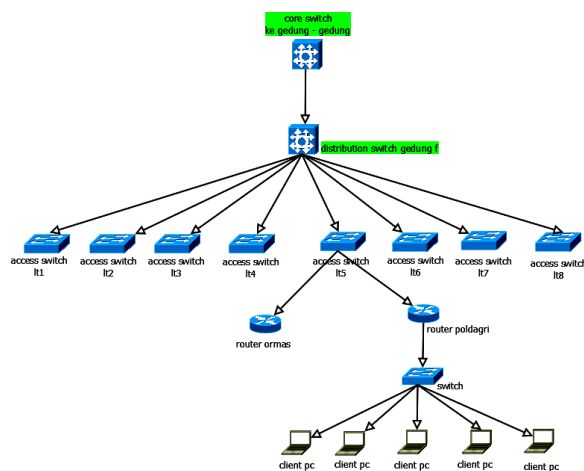
referensi dari penelitian – penelitian terkait dengan penelitian yang sedang penulis kerjakan.

IV. HASIL PENELITIAN

1. Manajemen Jaringan

Pada topologi yang digunakan dalam sistem jaringan yang ada di Direktorat Politik Dalam Negeri adalah topologi tree. Pada sistem jaringan yang terdapat pada Direktorat Politik Dalam Negeri Kementerian Dalam Negeri menggunakan model jaringan *client-server* terdapat 3 buah server yang berperan sebagai penyedia layanan koneksi, 3 *layer* tersebut mencakup *core switch*, *distribution switch*, dan *access switch*.

Berikut adalah gambaran dari skema jaringan yang ada pada Direktorat Politik Dalam Negeri:



Gambar 1: Skema Jaringan Direktorat POLDAGRI

- a. *Core Switch* yang terdapat dalam sistem jaringan ini mempunyai peran sebagai *backbone* atau tulang punggung jaringan. Bertanggung jawab dalam mengatasi lalu lintas atau *traffic* dalam jaringan juga sebagai penghubung antara sebuah *network switch* dengan beberapa *network switch* yang lain untuk membentuk sebuah sistem jaringan yang saling terhubung secara utuh atau disebut juga *Integrated Network*.
- b. *Distribution Switch* pada sistem jaringan berikut berfungsi sebagai jalur penghubung antara sebuah *Core Switch* dengan perangkat *Access Switch*.
- c. *Access Switch* yang terdapat di setiap lantai mempunyai fungsi sebagai penghubung antara *network* dengan sebuah perangkat komputer ataupun end user agar bisa menggunakan fasilitas koneksi internet.
- d. Kemudian ada sebuah router access point yang terdapat di tiap ruangan pada lantai 5 yang berperan sebagai pemancar sinyal untuk akses jaringan wireless.
- e. Switch pada sistem jaringan ini jenisnya adalah Cisco switch C2960X-24TS-L yang berfungsi menghubungkan perangkat komputer maupun *user client* lainnya dengan server sehingga dapat terbentuk sebuah jaringan lokal atau LAN.

- f. Perangkat komputer *client/user* pada Direktorat Politik Dalam Negeri, Ditjen Politik dan Pemerintahan Umum, Kementerian Dalam Negeri berfungsi sebagai *end user* atau *client* yang digunakan tiap pegawai Perangkat komputer *client/user* pada Direktorat Politik Dalam Negeri, Ditjen Politik dan Pemerintahan Umum, Kementerian Dalam Negeri berfungsi sebagai end user atau client yang digunakan tiap pegawai.

4. Spesifikasi IP Address

Spesifikasi alamat ip yang digunakan pada Direktorat Politik Dalam Negeri, Ditjen Politik dan Pemerintahan Umum, Kementerian Dalam Negeri adalah alamat ip kelas B dengan range 172.0.0.0, karena jumlah *client / user* yang akan terhubung pada sistem jaringan ini jumlahnya bisa mencapai ribuan maka pemilihan alamat ip kelas B merupakan pilihan yang tepat. Selain itu penggunaan alamat ip kelas B ini bisa meningkatkan kestabilan jaringan client/user dalam mengakses internet dan juga pemrosesan data oleh user dalam jaringan tersebut. Berikut merupakan tabel pembagian spesifikasi alamat ip pada jaringan lokal di Direktorat Politik Dalam Negeri, Ditjen Politik dan Pemerintahan Umum, Kementerian Dalam Negeri.

Berikut adalah tabel dari spesifikasi IP Address yang ada pada Direktorat Politik Dalam Negeri Kementerian Dalam Negeri:

Tabel 1: Spesifikasi IP Address

No	User Name	IP Address	Subnet Mask
1	Server	172.24.154.xxx	255.255.255.0
2	Core Switch	172.24.155.xxx	255.255.255.0
3	Distribution Switch	172.24.156.xxx	255.255.255.0
4	Access Switch Lt 1 – 8 Gedung F	172.24.156.2 – 172.24.156.10	255.255.255.0
5	PC client ruang TU Poldagri	172.24.157.2 – 172.24.157.9	255.255.255.0
6	PC client ruang Subdit Poldagri	172.24.158.2 – 172.24.158.30	255.255.255.0

Penjelasan penggunaan alamat IP pada Direktorat Politik Dalam Negeri Kementerian Dalam Negeri adalah 172.24.156.6 dengan netmask /24 yang berarti subnetmask dari alamat IP tersebut adalah 255.255.255.0. Dilihat dari kelas alamat IP tersebut bisa dipastikan kelas B dengan subnetmask defaultnya adalah 255.255.0.0, karena subnetmask yang digunakan 255.255.255.0 jadi IP address yang digunakan telah mengalami *subnetting* yang ditujukan untuk mengetahui Net ID dan Host ID pada alamat IP tersebut:

Tabel 2: Pembagian Net.ID dan Host.ID

IP Address			
172	24	156	2
Subnet			
255	255	255	0
Subnet dalam Bit			
11111111	11111111	11111111	00000000

5. Identifikasi Masalah dan Pemecahan

Kendala yang sering terjadi pada konektivitas jaringan pada lantai 5 Direktorat Politik Dalam Negeri antara lain adalah sebagai berikut:

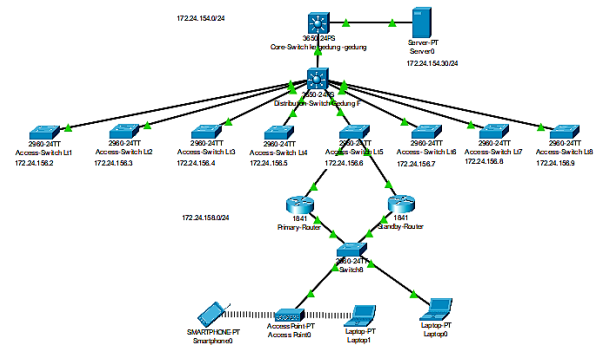
1. Permasalahan pada perangkat keras (*Hardware*)
 - a. Permasalahan mengenai aksesibilitas kedalam koneksi jaringan wifi terkadang tidak bisa langsung terkoneksi kedalam jaringan.
 - b. Permasalahan mengenai router utama yang seringkali mendapati kendala
2. Permasalahan pada perangkat lunak (*Software*)
 - a. Adanya *delay* yang cukup lama saat proses autentifikasi *user*.
 - b. *Software* penunjang kerja *client/user* masih menggunakan versi lama (belum *up to date*).

Setelah mengetahui beberapa fakta Mengenai permasalahan yang ada pada sistem jaringan pada Direktorat Politik Dalam Negeri, Ditjen Politik dan Pemerintahan Umum, Kementerian Dalam Negeri, penulis memberikan beberapa solusi untuk pemecahan masalah tersebut, diantaranya:

1. Pemecahan masalah perangkat keras (*Hardware*)
 - a. Mengenai aksesibilitas pada jaringan wifi yang kadang menemui kendala, penulis mengusulkan untuk *update* driver wifi atau mengupgrade komponen *wifi card* yang ada pada perangkat *client/user*.
 - b. Untuk mengatasi kendala pada router utama, maka penulis mengusulkan untuk memberikan router backup disertakan protokol HSRP (*Hot Standby Router Protocol*).
2. Pemecahan masalah perangkat lunak (*Software*)
 - a. Melakukan pembersihan *cache* pada pc atau *defragment disk* untuk mengembalikan performa sistem operasi yang lambat.
 - b. *Update* secara berkala software penunjang kerja pada perangkat *client/user* menghindari *delay* atau lambatnya aplikasi saat pertama kali dibuka.

6. Rancangan Usulan

Usulan skema yang diajukan oleh penulis untuk Direktorat Politik Dalam Negeri Kementerian Dalam Negeri adalah sebagai berikut:

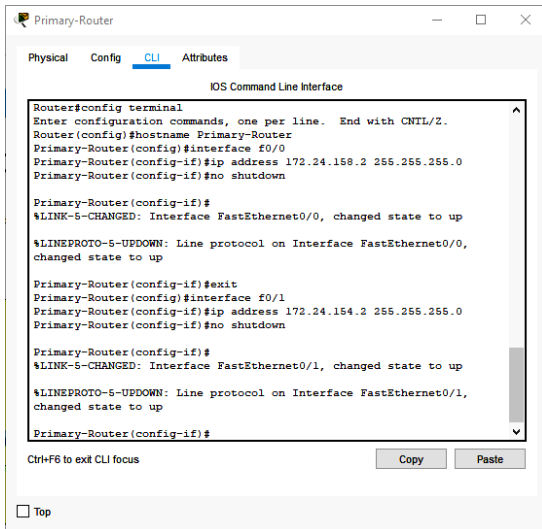


Gambar 2: Rancangan Usulan

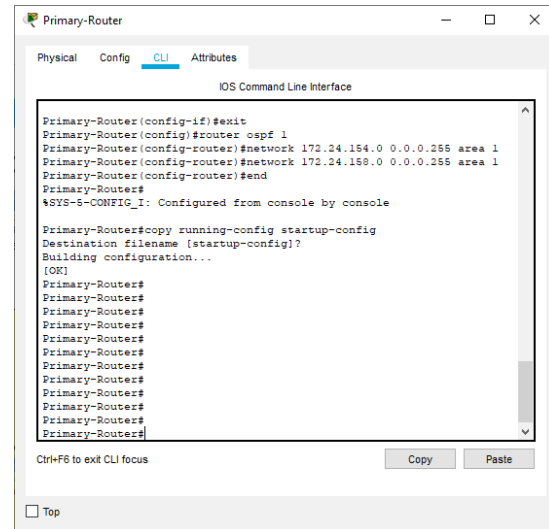
Berdasarkan skema usulan diatas, dapat disimpulkan bahwa pada bagian *access switch* lantai 5 terhubung oleh 2 router. Salah satu dari router tersebut merupakan *router standby* atau *backup router* jika router utama terjadi kendala atau *device failure*. Penulis juga mengusulkan untuk diberikan protokol redundansi tambahan yaitu HSRP (*Hot Standby Router Protocol*). Kemudian ditambahkan juga hub switch pada sisi *end user* untuk pengoptimalan dalam sisi *client*.

7. Konfigurasi HSRP

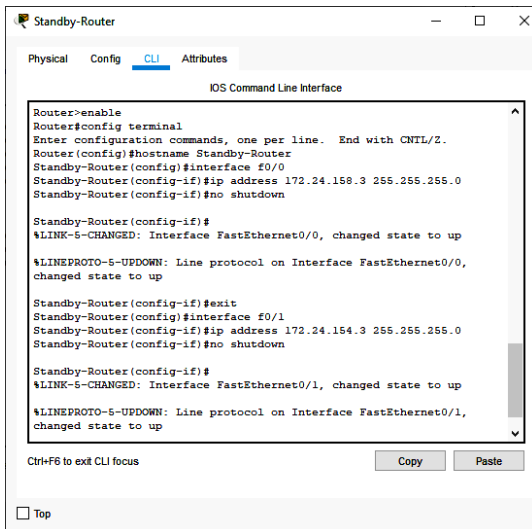
Langkah pertama dalam konfigurasi HSRP adalah memberi alamat ip pada tiap port interface yang ada pada router utama dan router standby.



Gambar 3: Konfigurasi IP pada router utama

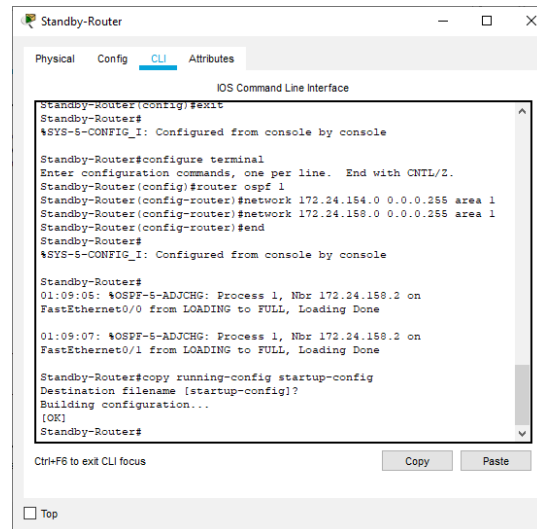


Gambar 5: Konfigurasi OSPF router utama



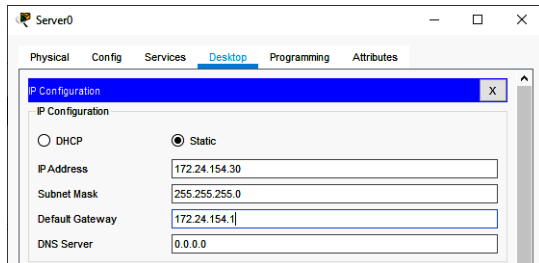
Gambar 4: Konfigurasi IP pada router standby

Konfigurasi routing OSPF pada tiap router.



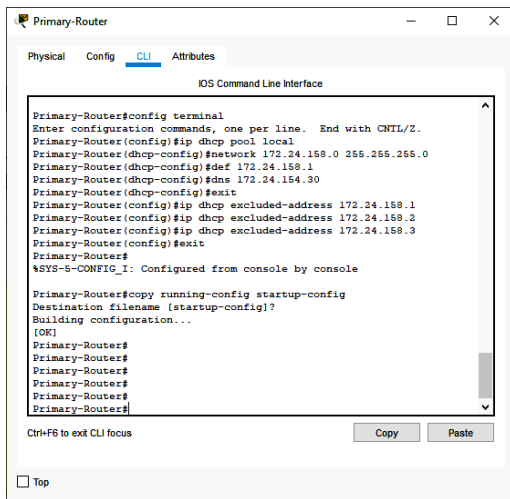
Gambar 6: Konfigurasi OSPF router standby

Kemudian setting ip address server dengan ip static

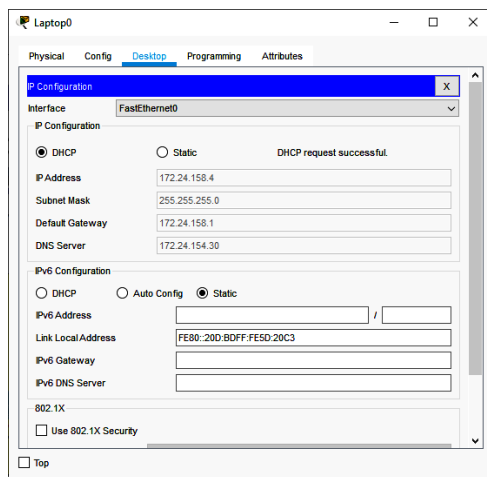


Gambar 7: Setting IP server

Konfigurasi router utama menjadi DHCP server untuk sektor client

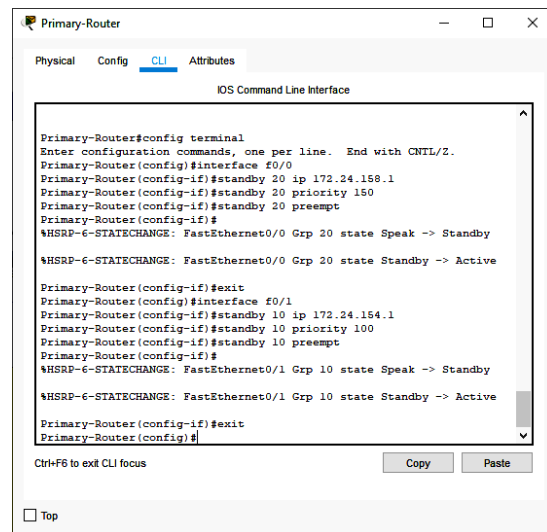


Gambar 8: Router utama sebagai DHCP server

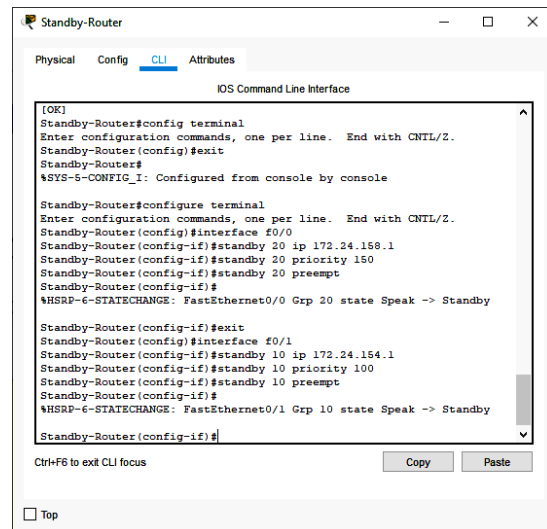


Gambar 9: Hasil Request IP melalui DHCP pada client

Kemudian konfigurasi HSRP pada kedua router yang ada, setting prioritas tertinggi pada router utama.



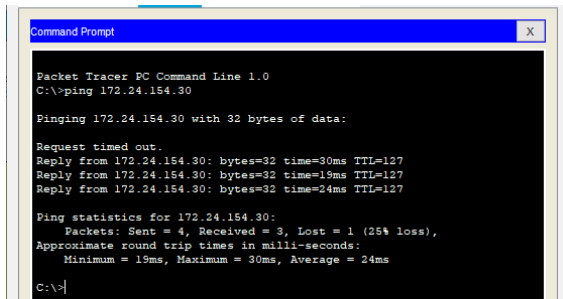
Gambar 10: Konfigurasi HSRP pada router utama



Gambar 11: Konfigurasi HSRP pada router standby

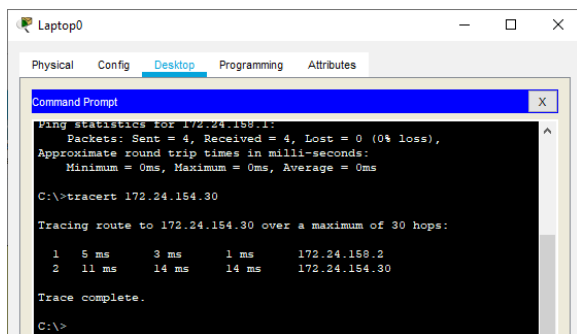
8. Pengujian Skema Usulan

Pada pengujian awal dilakukan dengan test ping terhadap server.



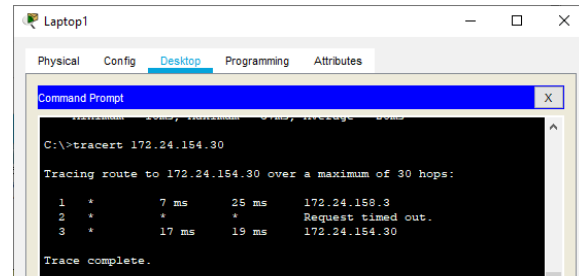
Gambar 12: Test ping terhadap ip server

Skenario pengetesan menggunakan command tracert sebelum dilakukan pemutusan jalur kearah router utama



Gambar 13: Pengujian Tracert sebelum jalur router utama diputus

Saat dilakukan pengujian dengan command tracert, rute yang diambil melalui jalur router utama dengan ip address 172.24.158.2



Gambar 14: Pengujian tracert sesudah jalur router utama diputus

Gambar 15 memperlihatkan bahwa skenario pemutusan jalur pada router utama yaitu dengan ip 172.24.158.2 berhasil dilakukan. Dengan diputusnya jalur tersebut, maka traffic akan berpindah secara otomatis menuju jalur router standby dengan alamat ip 172.24.158.3.

V. KESIMPULAN

1. Pada uji jaringan awal, dilakukan pengiriman ping kepada *IP gateway* HSRP disektor *client* yaitu HSRP 20 dengan *gateway* 172.24.158.1. dan juga dilakukan pengujian ping kepada *IP gateway* HSRP disektor server yaitu HSRP 10 dengan *gateway* 172.24.154.1.
2. Pada dua pengujian tersebut bisa didapat bahwa ping bisa terkirim dengan baik serta mendapat *response* balik dari masing – masing *gateway* yang ada.
3. Kemudian dicoba pengujian ketiga dengan metode yang sama yaitu ping kepada

alamat IP server 172.24.154.30 dan bisa terkirim dengan baik.

4. Pada pengujian jaringan usulan, kedua router sudah menerapkan protokol redundansi HSRP tetapi pada pengujiannya diterapkan sebuah skenario bahwa router utama masih dapat berfungsi dengan baik, kemudian penulis mencoba melacak rute ke server 172.24.154.30 dengan perintah *tracert*.
5. Kemudian didapat fakta bahwa rute menuju alamat 172.24.154.30 melewati rute dengan alamat 172.24.158.2 yang melalui jalur router utama.
6. Lalu dilakukan skenario kedua dengan memutus kabel jalur yang melewati jalur router utama, kemudian dilakukan lagi pengujian rute dengan perintah *tracert* pada alamat 172.24.154.30
7. Hasil yang didapat adalah rute menuju alamat 172.24.154.30 berpindah jalur melalui alamat 172.24.158.3 yang ada pada *router standby*

DAFTAR PUSTAKA

Anas, M. A., Soepriyanto, Y., & Susilaningsih. (2018). PENGEMBANGAN MULTIMEDIA TUTORIAL TOPOLOGI JARINGAN UNTUK SMK KELAS X TEKNIK

KOMPUTER DAN JARINGAN Muchammad Azwar Anas, Yerry Soepriyanto, Susilaningsih. *Multimedia Tutorial*, 1(4), 307–314.

Astuti, I. K. (2020). *Jaringan Komputer*. <https://doi.org/10.31219/osf.io/p6ytf>

Comer, D. E. (2019). The Internet book: everything you need to know about computer networking and how the Internet works. In *Choice Reviews Online* (Vol. 36, Issue 02). <https://doi.org/10.5860/choice.36-1005>

Fadhilah. (2020). Perancangan Backup Router Dengan Metode Hsrp (Hot Standby Router Protocol). *Teknokris*, 23(1), 1–10.

Firmansyah, Wahyudi, M & Rachmat, P. (2018). Analisis Perbandingan Kinerja Jaringan CISCO Virtual Router Redundancy Protocol (VRRP) Dan CISCO Hot Standby Router Protocol (HSRP). *Teknik Komputer AMIK BSI Tegal*, 1(1), 764–769.

Fox, R., & Hao, W. (2018). Internet Infrastructure Networking, Web Services, and Cloud Computing. In *Journal of Chemical Information and Modeling* (Vol. 110, Issue 9).

Jain, V., Edgeworth, B., & Furr, R. (2018). *Troubleshooting Cisco Nexus Switches and NX-OS*.

Mair, Z. R. (2018). *Teori Dan Praktek Sistem Operasi*.

Maslan, A. (2020). *Jaringan Komputer dan Simulasi CISCO Packet Tracer*.

Deepublish Publisher.

Pamungkas, W. H., & Prayitno, E. (2018). Perancangan Jaringan Redundancy Link Menggunakan Konsep HSRP dan Etherchannel. *METIK Jurnal*, 2(1), 75–82.

Purwanto, W., & Risnanto, S. (2018). Implementasi Metode Hsrp Pada Bank Jawa Barat Dan Banten Kantor Wilayah I Dan Kcp Simpang Dago. *Infotronik : Jurnal Teknologi Informasi Dan*

Elektronika, 3(1), 35.
<https://doi.org/10.32897/infotronik.2018.3.1.88>

Puspitasari, A., Nasution, R., Studi, P., Informasi, S., Cengkareng, K., Barat, K. J., Studi, P., & Informatika, T. (2020). *IMPLEMENTASI HOT STANDBY ROUTER PROTOCOL (HSRP) PADA PT*. 55–60.

West, J., Andrews, J., & Dean, T. (2019). *Network+ Guide To Networks*.