

PERANCANGAN BACKUP ROUTER DENGAN METODE HSRP (HOT STANDBY ROUTER PROTOCOL)

Muhammad Irfan Fadhilah¹; Hendra Supendar²; Sulistianto SW³

Teknik Informatika^{1,3} Teknologi Informasi²

Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri, Jakarta^{1,3}

Universitas Bina Sarana Informatika, Jakarta²

E-mail : muhammad151187@nusamandiri.ac.id¹, hendrasupendari@gmail.com²

sulistianto.sow@nusamandiri.ac.id³

ABSTRAK

Sebuah perusahaan yang mempunyai banyak kantor cabang membutuhkan jaringan komputer yang stabil pada kantor pusat dan cabang, karenanya diperlukan sebuah system pencegahan dengan melakukan backup pada router jika terjadi kerusakan pada router utama, *HOT STANDBY ROUTER PROTOCOL* (HSRP) adalah sebuah protokol standar CISCO yang dapat membuat sebuah router yang secara otomatis akan mengambil alih aliran data jika router utama mati atau failed. HSRP disetting dengan dua buah router yang mempunyai status router yaitu aktif dan standby, jika router aktif terjadi failed maka router standby akan otomatis berubah menjadi aktif dan akan mengambil alih aliran data hanya dalam hitungan detik, karena nya aktifitas perusahaan tidak akan terhambat bahkan pegawai pun mungkin tidak menyadari adanya pergantian jalur router dan para pegawai IT pun dapat melakukan troubleshooting ke router yang *failed* atau *router down* tanpa mengganggu aktifitas perusahaan

Kata Kunci: Backup Router, HSRP, Secondary Router, Cisco

. ABSTRACT

A company that has many branch offices requires a stable computer network at the head office and branches, so we need a prevention system by backing up the router in case of damage to the main router, HOT STANDBY ROUTER PROTOCOL (HSRP) is a standard CISCO protocol that can make a router that will automatically take over the data flow if the main router fails or fails. HSRP is set up with two routers that have a router status that is active and standby, if an active router fails, then the standby router will automatically change to active and will take over the data flow in just seconds, because of its activities the company will not be hampered even employees might not aware of the router path changes and IT employees can also troubleshoot a failed router or router down without disrupting company activities

Keywords: Backup Router, HSRP, Secondary Router, Cisco

1. PENDAHULUAN

Kecepatan informasi dan penerimaan data yang cepat dan akurat sangat diandalkan dalam sebuah perusahaan publik. Terutama dengan banyaknya pelanggan dan Kantor Cabang yang melayaninya. Penerapan jaringan komputer dan terhubung dengan internet dengan memanfaatkan Router sebagai penghubung antar jaringan komputer satu sama lain sangat dibutuhkan. Dalam pelaksanaannya terkadang terjadi beberapa masalah, diantaranya Router yang terkadang mati di saat jam kerja dan Aktifitas perusahaan menjadi terhambat karena pihak IT harus melakukan *troubleshooting* dan menjalankan *router* kembali.

Menurut (Purwanto & Risnanto, 2018)“ Salah satu cara untuk mencapai *network uptime* hingga mendekati 100% adalah menggunakan HSRP. HSRP menyediakan redundansi untuk Jaringan IP, memastikan bahwa lalu lintas data dari user dapat dipulihkan secara cepat dan transparan dari kegagalan hop pertama (*Gateway*) pada perangkat jaringan komputer”

Sedangkan menurut (P. Kaur, Kaur, & Kaur, 2017)“*Hot Standby Router Protocol (HSRP)*, yang dirancang untuk mendukung kegagalan non-gangguan lalu lintas IP dalam keadaan tertentu. Secara khusus, protokol melindungi terhadap kegagalan hop berikutnya ketika host sumber tidak dapat mempelajari alamat IP hop berikutnya secara dinamis”

Menurut (I. Kaur & Bajaj, 2013)“Ini dapat berguna untuk *router* cabang ganda masing-masing dengan tautan serial tunggal kembali ke ujung kepala. Jika tautan serial *router* primer turun, Anda ingin *router* cadangan mengambil alih fungsi utama dan dengan demikian mempertahankan konektivitas ke ujung kepala”

Menurut (Cisco Corporate Author, 2015)Untuk meminimalkan lalu lintas jaringan, hanya *router* aktif dan siaga yang mengirim pesan HSRP secara berkala setelah protokol menyelesaikan proses pemilihan. Jika *router* aktif gagal, *standby router* mengambil alih sebagai *router* aktif. Jika *standby router* menjadi *router* aktif, *router* lain dipilih sebagai *standby router*

2. LANDASAN TEORI

A. Tinjauan Jurnal

Mengutip kata-kata dari website serbatekno.com:

”HSRP adalah sebuah protocol redundancy standar cisco yang menetapkan sebuah router yang secara otomatis mengambil alih jika router yang lain gagal”

Sedangkan dari jurnal infotronik volume 3 no.1 juni 2018 menurut (Purwanto & Risnanto, 2018:37) menyimpulkan :

Salah satu cara untuk meningkatkan waktu *uptime* hingga mendekati 100 persen, HSRP dapat

digunakan pada jaringan komputer dengan *availability* yang tinggi dengan menyediakan redundansi IP *address network* pada hop pertama *routing* untuk *host* dan jaringan komputer yang telah dikonfigurasi menggunakan sebuah IP *Address default gateway*.

Dan dalam jurnal cisco dengan ID :9234 (Cisco Corporate Author, 2015) menerangkan cara kerja HSRP yaitu :

Menggunakan HSRP, satu set router bekerja bersamaan untuk menyajikan ilusi satu router virtual ke host di LAN. Set ini dikenal sebagai grup HSRP atau grup *standby*. Router tunggal yang dipilih dari grup bertanggung jawab untuk meneruskan paket yang dikirim oleh host ke router virtual. Router ini dikenal sebagai router aktif. Router lain dipilih sebagai router Standby. Dalam hal router Aktif gagal, *Standby* mengasumsikan tugas penerusan paket router Aktif. Meskipun sejumlah router sewenang-wenang dapat menjalankan HSRP, hanya router aktif yang mengirimkan paket yang dikirim ke router virtual.

Dan dalam jurnal cisco yang sama (Cisco Corporate Author, 2015) juga menerangkan mengenai beberapa fitur dari HSRP yaitu :

1. Preemption

Fitur preemption HSRP memungkinkan router dengan prioritas tertinggi untuk segera menjadi router aktif. Prioritas ditentukan pertama oleh nilai prioritas yang Anda konfigurasi, dan kemudian oleh alamat IP. Dalam setiap kasus, nilai yang lebih tinggi adalah prioritas yang lebih besar. Ketika router dengan prioritas lebih tinggi mendahului router dengan prioritas lebih rendah, ia akan mengirim pesan kudeta. Ketika router aktif dengan prioritas lebih rendah menerima pesan kudeta atau pesan hello dari router aktif prioritas lebih tinggi, router itu berubah ke status bicara dan mengirim pesan untuk berhenti.

2. Preemption Delay

Fitur preempt delay memungkinkan preemption ditunda untuk periode waktu yang dapat dikonfigurasi, memungkinkan router untuk mengisi tabel peruteannya sebelum menjadi router yang aktif. Sebelum Cisco IOS Software merilis 12.0 (9), penundaan dimulai ketika router memuat ulang. Dalam Cisco IOS release 12.0 (9) penundaan dimulai ketika preemption pertama kali dicoba.

3. Interface Tracking

Interface tracking memungkinkan Anda untuk menentukan antarmuka lain pada router untuk memantau proses HSRP untuk mengubah prioritas HSRP untuk grup tertentu. Jika protokol garis antarmuka yang ditentukan turun, prioritas HSRP router ini berkurang,

sehingga router HSRP lain dengan prioritas lebih tinggi dapat menjadi aktif (jika preemption diaktifkan)

4. Redundansi IP

HSRP memberikan redundansi stateless untuk routing IP. HSRP dengan sendirinya terbatas untuk mempertahankan negaranya sendiri. Ini mengasumsikan bahwa setiap router membangun dan memelihara tabel routing sendiri secara terpisah dari router lain. Fitur redundansi IP menyediakan mekanisme yang memungkinkan HSRP untuk menyediakan layanan untuk aplikasi klien sehingga mereka dapat mengimplementasikan failover statefull. Redundansi IP tidak menyediakan mekanisme untuk aplikasi rekan untuk bertukar informasi keadaan. Ini diserahkan kepada aplikasi itu sendiri, dan sangat penting jika aplikasi tersebut ingin menyediakan failover statefull.

Dalam jurnal konferensi nasional sistem informasi 2018, (Firmansyah, Wahyudi, & Purnama, 2018) menguraikan perbandingan kinerja HSRP dengan Virtual Router Redundancy Protokol (VRRP) :

Adapun hasil pengukuran dari parameter packet loss terhadap jaringan VRRP jika terjadi permasalahan pada router master dan berpindah akses ke router 6 backup lebih unggul dibandingkan dengan jaringan HSRP yaitu VRRP 0,8% sedangkan HSRP 2%. Namun, perpindahan router backup to master jaringan HSRP lebih unggul dibandingkan dengan jaringan VRRP yaitu VRRP 1,2% sedangkan HSRP 0,7%. Sedangkan untuk analisis fail over master to backup pada jaringan VRRP dan HSRP memiliki nilai delay yang sama sebesar 03Ms. Sedangkan fail over backup to master jaringan HSRP lebih unggul dibandingkan dengan jaringan VRRP yaitu HSRP sebesar 01Ms sedangkan VRRP 10Ms. Dari hasil data diatas dapat dilihat bahwa redundancy HSRP lebih unggul dibandingkan dengan redundancy VRRP

Kemudian dalam jurnal *Indian Journals of Science and Technology*, Vol 9(20) (Ravikumar et al., 2016) menerangkan bahwa terdapat dua jenis router yang akan digunakan dalam fitur ini :

1) Router aktif

Router aktif adalah yang meneruskan paket IP ke router virtual. Ini berbagi alamat IP dan Medium Access Control (MAC) yang sama dengan *standby router*

2) *Standby Router*

Standby Router bertindak sebagai cadangan ke router aktif. Jika router aktif terganggu karena yang direncanakan adalah alasan yang tidak direncanakan, standby router akan menyediakan redundansi gateway sehingga memberikan ketahanan pada jaringan

Tinjauan di atas penulis jadikan acuan dalam merancang HSRP pada PT.PLN DISJAYA. Jadi jika

suatu saat router utama mengalami down, maka router utama yang merupakan *active router* akan mengirim pesan ke *standby router*, dan *standby router* akan berganti status menjadi *active router* dan akan meneruskan jalur data pada *active router* yang baru.

B. Konsep Dasar Jaringan

1. Jaringan Komputer

Menurut (Gitakarma & Ariawan, 2014) menjelaskan bahwa :

Jaringan adalah sebuah kemampuan dari dua buah komputer atau lebih untuk dapat saling mengetahui keberadaan satu dengan yang lainnya sehingga dapat melakukan pertukaran data. Dalam era internet, yang dimaksudkan dengan pertukaran data antara dua buah komputer bisa menjadi hal yang sangat luas, sebagai contoh: perjalanan sebuah e-mail dari satu server ke server yang lain, sebuah web browser yang men-download halaman HTML, sebuah PC men-download film dari HTTP server, peer-to-peer MP3 sharing, dan masih banyak lagi.

Menurut (Supendar & Handrianto, 2017) menjelaskan bahwa “Jaringan komputer merupakan sekelompok komputer yang menggunakan protocol komunikasi untuk dapat saling berkomunikasi dan berbagi data atau informasi”

Menurut (Usman, Permana, & Wibisono, 2018) “Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung dalam satu kesatuan”.

2. Jenis jaringan komputer

Berdasarkan jangkauan luas daerahnya, jaringan komputer dapat dikelompokkan menjadi PAN, LAN, MAN, WAN.

a. Personal Area Network (PAN)

PAN menurut (Wongkar, Sinsuw, & Xaverius, 2015) :

PAN adalah singkatan dari *Personal Area Network*. Jenis jaringan komputer PAN adalah hubungan antara dua atau lebih sistem komputer yang berjarak tidak terlalu jauh. Biasanya Jenis jaringan yang satu ini hanya berjarak 4 sampai 6 meter saja. Jenis jaringan ini sangat sering kita gunakan.



Gambar 1. Personal Area Network

Sumber : (E-journal Tek. Elektro dan Komput., 2015)

b. Local Area Network (LAN)

Menurut (Usman, Permana, & Wibisono, 2018) LAN adalah :

Local Area Network (LAN), merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer, LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan *workstation* dalam kantor suatu perusahaan atau pabrik-pabrik untuk memakai bersama sumber daya (*resource*, misalnya printer) dan saling bertukar informasi.



Gambar 2. Local Area Network

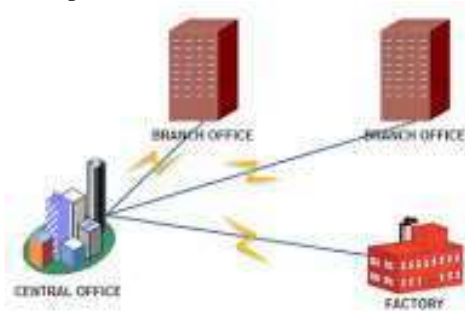
Sumber : (E-journal Tek. Elektro dan Komput., 2015)

c. Metropolitan Area Network (MAN)

MAN Menurut (Usman, Permana, & Wibisono, 2018) adalah:

Metropolitan Area Network (MAN), pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN.

MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum.



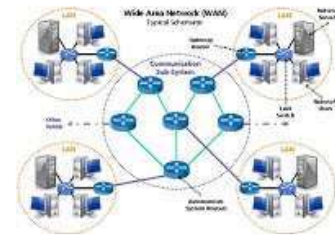
Gambar 3. Metropolitan Area Network

Sumber (E-journal Tek. Elektro dan Komput., 2015)

d. Wide Area Network (WAN)

WAN Menurut (Usman, Permana, & Wibisono, 2018) adalah:

Wide Area Network (WAN), jangkauannya mencakup daerah geografis yang luas, seringkali mencakup sebuah negara bahkan benua. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan program-program (aplikasi) pemakai.

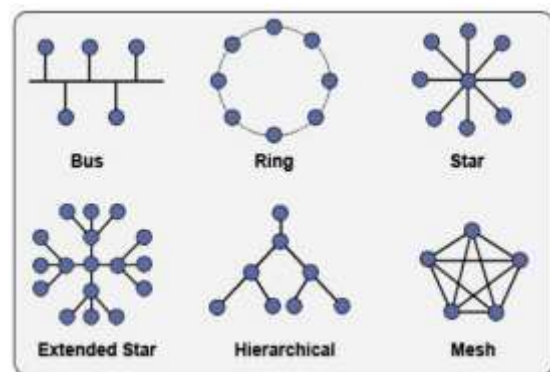


Gambar 4. Wide Area Network

Sumber : (E-journal Tek. Elektro dan Komput., 2015)

3. Topologi Jaringan

Menurut Tanenbuan, Andrew S dalam (Muhammad & Hasan, 2016) Topologi jaringan komputer secara umum terbagi dalam 6 bentuk sebagai berikut:



Gambar 5. Topologi Jaringan

Sumber : (J. Elektron. Sist. Inf. dan Komput., 2016)

Untuk tempat penelitian Topologi yang digunakan adalah sebagai berikut:

Topologi Star, adalah topologi jaringan yang menggunakan concentrator (hub/switch) untuk mengatur paket data. Topologi ini memiliki kontrol terpusat. Semua link harus melewati pusat yang menyalurkan data ke semua simpul (client). Simpul pusat disebut stasiun primer (server), simpul lain disebut stasiun sekunder (client server). Setelah hubungan dimulai oleh server, setiap client server dapat menggunakan jaringan tanpa menunggu perintah server. Topologi ini adalah paling fleksibel. Pemasangan/perubahan stasiun sangat mudah dan tidak mengganggu bagian jaringan lain. Juga memiliki kemudahan dalam pengelolaan jaringan. Kerugiannya antara lain adalah boros kabel, dan hub/switch menjadi suatu elemen yang kritis.

4. Manajemen Jaringan

a. IP Address

Menurut Syafrizal dalam (Siti Nur Khasanah, 2016) IP Address merupakan pengenalan yang digunakan untuk memberi alamat pada tiap-tiap komputer dalam jaringan. Format IP address adalah

bilangan 32 bit yang tiap 8 bit-nya dipisahkan oleh tanda titik”

Dari hal tersebut diketahui bahwa IP Address adalah alamat pada tiap komputer dengan format 32bit yang dibagi menjadi 4 oktet, 1 oktet terdiri dari 8bit bilangan biner. Sebagai contoh:

10101100.00010000.00011001.00000001

Ketika dikonversi ke bentuk desimal akan menjadi : 172.16.25.1

b. Pengalokasian IP Address

Menurut Syafrizal dalam (Siti Nur Khasanah, 2016) menjelaskan:

IP Address sebenarnya terdiri dari dua bagian, yaitu : Network ID dan Host ID. Network ID menentukan alamat dari suatu jaringan komputer dan Host Id menentukan alamat dari suatu komputer (host) dalam suatu jaringan komputer.

Oleh karena itu, dalam pembuatan IP Address harus diketahui terlebih dahulu tujuan jaringan yang ingin di buat sehingga dapat membuat konfigurasi yang lebih efisien .

Menurut (Syafrizal, 2005) Dalam IP Address, ada dua cara pembagian IP, yaitu *classfull* dan *classless addressing* :

1) Classfull

Classfull merupakan metode pembagian IP address berdasarkan kelas, dimana IP address (yang berjumlah sekitar 4 milyar) dibagi kedalam lima kelas yakni:

Kelas A

Format :

Onnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

Bit pertama : 0

Panjang NetID : 8 bit

Panjang HostID : 24 bit

Byte pertama : 0-127

Jumlah : 126 Kelas A (0 dan 127 dicadangkan)

Range IP : 1.xxx.xxx.xxx sampai 126.xxx.xxx.xxx

Jumlah IP : 16.777.214 IP Address disetiap Kelas A

Dekripsi : Diberikan untuk jaringan dengan jumlah host yang besar

Kelas B

Format :

10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh

Bit pertama : 10

Panjang NetID : 16 bit

Panjang HostID : 16 bit

Byte pertama : 128-191

Jumlah : 16.384 Kelas B

Range IP : 128.0.xxx.xxx sampai 191.255.xxx.xxx

Jumlah IP : 65.532 IP Address pada setiap Kelas B

Deskripsi : Dialokasikan untuk jaringan besar dan sedang

Kelas C

Format :

110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh

Bit pertama : 110

Panjang NetID : 24 bit

Panjang HostID : 8 bit

Byte pertama : 192-223

Jumlah : 2.097.152 Kelas C

Range IP : 192.xxx.xxx.xxx s/d 223.255.255.xxx

Jumlah IP : 254 IP Address pada setiap Kelas C

Deskripsi : Digunakan untuk jaringan berukuran kecil

2) Classless Addressing

Metode **classless addressing** (pengalamatan tanpa kelas) saat ini mulai banyak diterapkan, yakni dengan pengalokasian IP Address dalam notasi Classless Inter Domain Routing (**CIDR**). Istilah lain yang digunakan untuk menyebut bagian IP address yang menunjuk suatu jaringan secara lebih spesifik, disebut juga dengan **Network Prefix**.

Dalam penggunaan, IP Address dibedakan menjadi dua yaitu IP Address Public yang langsung terhubung ke jaringan internet, dan IP Address Private yaitu IP yang digunakan dan dipakai oleh user dalam LAN. Berikut adalah range dari IP Private:

1. Kelas A: 10.0.0.0 s/d 10.255.255.255

2. Kelas B: 172.16.0.0 s/d 172.31.255.255

3. Kelas C: 192.168.0.0 s/d 192.168.255.255

4. Konsep Penunjang Usulan

a. Definisi HSRP

Menurut (Cisco Corporate Author, 2015) menyimpulkan bahwa:

Untuk meminimalkan lalu lintas jaringan, hanya *router* aktif dan *standby* yang mengirim pesan HSRP secara berkala setelah protokol menyelesaikan proses pemilihan. Jika *router* aktif gagal, *standby router* mengambil alih sebagai *router* aktif. Jika *standby router* menjadi *router* aktif, *router* lain dipilih sebagai *standby router*

Jadi dalam menjalankan fitur HSRP ini, akan digunakan dua buah router yang akan menjadi *gateway* dimana salah satu router akan diubah menjadi router aktif yang menjadi *gateway* utama dan juga akan diberikan 'Prioritas' sebagai jalur utama dalam jaringan lokal dan router lain akan menjadi *standby* atau *backup* router. Hal ini adalah langkah pencegahan jika suatu saat router utama yang menjadi *gateway*

utama mengalami kerusakan atau putus jalur, maka router *standby* akan merubah status menjadi router aktif dan jalur data akan segera bisa di-*backup* oleh router *standby* tersebut

b. Cara Kerja Fitur HSRP

(Kaur, Kaur, & Kaur, 2017) menjelaskan cara kerja HSRP yaitu:

Untuk memungkinkan dua gateway yang terhubung dikonfigurasi untuk memberikan redundansi maka masalah ini dapat diselesaikan oleh HSRP. Ini memberikan alamat MAC dan IP virtual yang dibagi antara dua perangkat ini; perangkat aktif yang bertanggung jawab untuk penanganan lalu lintas ke alamat IP virtual, sedangkan tanggung jawab perangkat *standby* adalah memantau perangkat aktif untuk tanda-tanda kegagalan. Router *standby* akan mengambil alih tugas menangani lalu lintas yang dikirim ke alamat IP virtual dengan menerima lalu lintas ke alamat IP dan dengan mengambil alih alamat MAC virtual dengan menggunakan Address Resolution Protocol (ARP) ketika router aktif akan gagal. Host yang dikonfigurasi pada subnet menggunakan alamat IP virtual sebagai alamat IP gateway mereka, dan peralihan tidak memerlukan konfigurasi tambahan pada perangkat host jika ada kegagalan di antara perangkat HSRP.

Dalam mengkonfigurasi fitur ini, kedua router akan diberikan IP *Virtual* yang berguna sebagai media komunikasi antar kedua router tersebut dengan mengirimkan paket *hello*, jika suatu saat terjadi kegagalan pada router utama, maka router *standby* akan berubah status menjadi aktif dan akan menangani lalu lintas dan mengambil alih alur jaringan tanpa harus mengatur kembali host (*user*) dalam jaringan tersebut

Menurut T. Li dalam Imperial Journal of Interdisciplinary Research (IJIR) Vol-3, Issue-1, 2017 (Kaur et al., 2017) terdapat 5 status *router* dalam HSRP, yaitu :

1. *Initial*: - Ini adalah keadaan awal router dan menunjukkan bahwa HSRP tidak berjalan. Keadaan ini dimasukkan melalui perubahan konfigurasi atau saat antarmuka pertama kali muncul.
2. *Learn*: - Alamat IP virtual belum ditentukan oleh router dan belum melihat pesan Hello yang diautentikasi dari router aktif. Dalam kondisi ini router masih menunggu untuk mendengar dari router aktif.
3. *Listen*: - Karena router mengetahui alamat IP virtual, tetapi bukan router aktif atau router siaga. Itu mendengarkan pesan Hello dari router lain.
4. *Speak*: - Halo pesan dikirim secara berkala oleh router dan secara aktif berpartisipasi dalam pemilihan router aktif atau siaga. Jika router

tidak memiliki alamat IP virtual, maka router tidak dapat masuk ke status *Speak*.

5. *Standby*: - Router berada dalam antrian kandidat untuk menjadi router aktif berikutnya dan secara berkala mengirimkan pesan Hello. Harus ada paling banyak satu router dalam grup dalam kondisi Siaga.

6. *Active*: - Router saat ini meneruskan paket yang dikirim ke alamat MAC virtual grup. Router secara berkala mengirimkan pesan Hello. Tidak termasuk kondisi sementara, HARUS ada paling banyak satu router dalam status Aktif dalam grup

c. Perangkat Jaringan

1) Router

Menurut (Muhammad & Hasan, 2016):

Router adalah perangkat yang melewatkan paket IP dari suatu jaringan ke jaringan yang lain menggunakan metode addressing dan protocol tertentu. Router-router yang terhubung dalam jaringan tergabung dalam suatu algoritma routing untuk menentukan jalur terbaik yang dilalui paket IP. Proses routing dilakukan secara hop by hop. IP tidak mengetahui seluruh jalur menuju tujuansetiap paket. IP hanya routing menyediakan IP address dari router berikutnya yang lebih dekat ke host tujuan

Router Bekerja pada lapisan ke-3 OSI (layer network)

Menurut Herlambang, M. Linto & Catur, Azis dalam (Muhammad & Hasan, 2016) tentang Fungsi *Router* :

- a. Membaca alamat logika/IP *address source* dan *destination* untuk menentukan *routing* dari suatu LAN ke LAN lainnya.
- b. Menyimpan *routing table* untuk menentukan rute terbaik antara LAN ke WAN.
- c. Perangkat *layer* ke-3 dalam *Open Systems Interconnection (OSI) Layer*.
- d. Dapat berupa "box" atau sebuah OS yang menjalankan sebuah *daemon routing*.
- e. *Interfaces Ethernet, Serial, ISDN BRI*.

2) Switch

Menurut (Ariawal, Dian, & Purbo, 2016):

Setiap *port* dalam *switch* memiliki *domain collision* sendiri-sendiri. *Switch* menciptakan *Virtual Private Network (VPN)* dari *port* pengirim dan *port* penerima sehingga jika 2 *host* sedang berkomunikasi, mereka tidak akan saling mengganggu. Jika satu *port* pada *switch* sedang sibuk, *port-port* lain tetap dapat berfungsi dengan baik. Istilahnya, *switch* itu *unicast* yang mempunyai jalur-jalur sendiri di setiap portnya. *Switch* mempunyai tabel CAM (*Content Addressable Memory*) yang digunakan untuk menyimpan data MAC Address dari *end device*

yang terpasang pada *port switch*. Dengan demikian, data yang ditransfer akan langsung menuju ke device tujuan.

3) NIC (*Network Interface Card*)

Menurut (Irawati, Yovita, & Wibowo, 2015): “NIC merupakan antarmuka yang menghubungkan antara PC dengan sebuah jaringan. Pertukaran data antar komputer dalam jaringan dapat terjadi melalui media NIC card. NIC juga berfungsi mengontrol aliran data antara komputer dan sistem kabel, serta menerjemahkannya ke dalam bit yang bisa dimengerti oleh komputer”.

4) Kabel Jaringan

(a). Twisted Pair

Menurut (Usman et al., 2018) Kabel *twisted pair* memiliki karakteristik sebagai berikut :

- (1). Paling murah dan paling banyak digunakan.
- (2). Panjang pilinan 5-15 cm, ketebalan 0,4–0,9 mm.

(b). Serat Optik

Menurut (Usman et al., 2018) mengenai karakteristik serat optik:

- (1). Medium yang tipis dan fleksibel, mampu merambatkan sinar optik.
- (2). Diameter inti 2-125 m
- (3). Karakteristik yang membedakan serat optik dari *twisted pair* dan kabel koaksial:
 - [a]. Kapasitas lebih besar
 - [b]. Ukuran lebih kecil dan lebih ringan
 - [c]. Redaman lebih rendah
 - [d]. Isolasi elektromagnetik
 - [e]. Jarak antar-repeater lebih jauh
- (4). Laju data ratusan Gbps untuk jarak puluhan km
- (5). *Long haul* 1500km dengan kapasitas 20.000-60.000 kanal suara
- (6). Metropolitan *trunking* (12km) dengan 100.000 kanal suara
- (7). Sentral *rurai* memiliki panjang sirkuit 40-160km dan <5000 kanal suara
- (8). LAN dikembangkan dengan kapasitas 100 Mbps hingga 10 Gbps

3.METODE PENELITIAN

1. Metode Pengumpulan Data

a. Observasi

Menggunakan metode Observasi sebagai sarana pengambilan data-data, dimana metode ini merupakan hasil peninjauan langsung dari objek yang telah diamati.

b. Wawancara

Metode Wawancara dengan menanyakan secara langsung kepada Petugas yang sedang bertugas

- (3). Laju data 64 kbps untuk PBX digital, 4 Mbps untuk aplikasi jarak jauh, 10 Mbps untuk LAN (jarak 1 km), 100 Mbps-1Gbps untuk jumlah terminal terbatas (jarak puluhan meter).

- (4). Jarak amplifier 5-6 km untuk sinyal analog, jarak repeater 2-3 km untuk transmisi digital
- (5). Redaman sangat sensitif terhadap kenaikan frekuensi

Menurut (Usman et al., 2018) Terdapat dua jenis *twisted pair* yang sering digunakan pada jaringan, yaitu UTP (*Unshielded Twisted Pair*) dan STP (*Shielded Twisted Pair*).

Unshielded = merupakan kawat telepon biasa, tipe 100-ohm banyak dijumpai di gedung perkantoran

Shielded = memiliki kinerja lebih baik pada laju data yang tinggi, *twisted pair* dilindungi oleh logam untuk mengurangi interferensi. Kabel STP memang lebih baik dari UTP, tetapi lebih mahal

guna mendapatkan informasi dan data, serta menambah wawasan keilmuan terkait yang belum diketahui.

c. Studi Pustaka

Digunakan oleh penulis untuk menambah informasi berupa teori atau hasil kajian dibidang ilmu yang sama dengan tujuan bertambahnya muatan informasi.

2. Analisa Penelitian

a. Analisa Kebutuhan

Berisi tentang semua kebutuhan yang akan dibutuhkan dalam merancang konsep suatu jaringan dengan sistem redundansi router menggunakan fitur HSRP yang difokuskan pada perangkat router.

b. Desain

Mendesain konsep jaringan dengan sistem redundansi router menggunakan fitur HSRP, seperti skema jaringan, topologi jaringan, simulasi jaringan dengan software Cisco Packet Tracer.

c. Testing

Pada tahap ini membuat simulasi jaringan dengan software Cisco Packet Tracer.

d. Implementasi

Jaringan yang telah disimulasikan akan diuji untuk dilihat kinerja dan dilakukan evaluasi.

4.HASIL DAN PEMBAHASAN

1. Jaringan Usulan

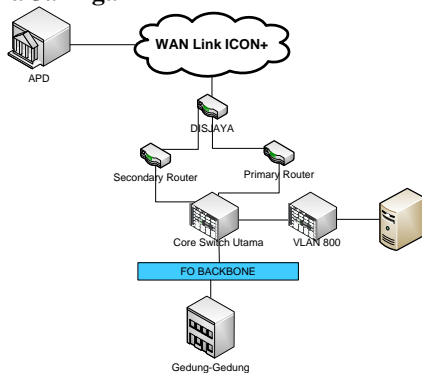
PT. PLN DISJAYA merupakan anak perusahaan dari PT. PLN yang bergerak di bidang penyediaan layanan listrik dan memiliki banyak kantor cabang di sekitar Jakarta, karena itu kestabilan jaringan komputer adalah hal utama yang dibutuhkan oleh perusahaan untuk menjalin komunikasi antar kantor cabang dan kantor pusat sehingga proses pekerjaan dapat terlaksana tanpa adanya kendala. Untuk

menunjang jaringan komputer yang lebih stabil, dibutuhkan sistem yang dapat meminimalisir hal-hal yang dapat memicu terjadinya *link down*, dan juga penanganan *link down* harus dipercepat agar proses pekerjaan dapat berjalan lebih lancar. Salah satu protocol yang dapat digunakan untuk meminimalisir hal tersebut adalah *Hot Standby Router Protocol* (HSRP). Dengan konsep tersebut diusulkan untuk menambahkan dua buah *router* sebagai jalan masuk jaringan internal, diharapkan hal tersebut dapat meminimalisir terjadinya *link down* di area internal dan jaringan dengan kantor cabang ataupun kantor pusat dapat lebih stabil

a. Topologi Jaringan

Topologi yang akan digunakan adalah topologi yang sudah berarda pada sistem PT. PLN DISJAYA yaitu topologi star, dan tidak membuat perubahan pada topologi internal, jadi hanya menambahkan 1 buah *router* tambahan kemudian mengkonfigurasi kedua *router* tersebut dengan HSRP. HSRP akan membuat sistem redudansi yang memanfaatkan *ip virtual* dan *mac address virtual* yang dikonfigurasi pada kedua *router* tersebut, sehingga apabila *router* utama terjadi *link down* maka *standby router* akan langsung berubah status ke *active* dan menangani jalur komunikasi jaringan.

b. Skema Jaringan



Gambar 6. Skema Jaringan Usulan

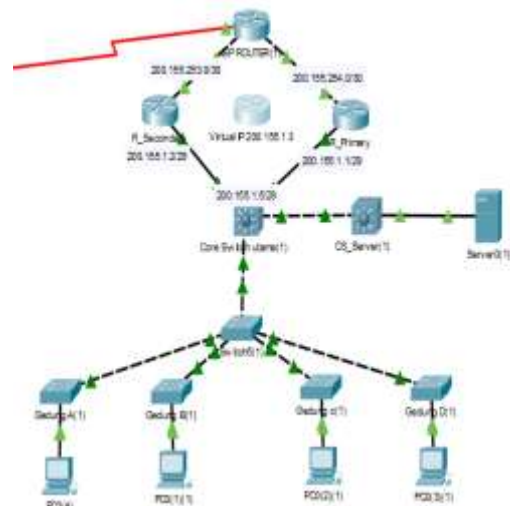
Sumber : Analisi Penelitian

Fitur HSRP memanfaatkan sebuah *virtual IP* yang dikonfigurasi pada kedua *router*. *Virtual IP* tersebut nantinya akan dijadikan sebagai jalur routing utama untuk koneksi menuju WAN. Skema jaringan yang menggambarkan akan menggunakan dua buah *router* Cisco dimana *primary router* akan dikonfigurasi sebagai *router* utama dengan status *active* dan *secondary router* akan dikonfigurasi dengan status *standby* yang akan berfungsi sebagai *router backup*. Kedua *router* akan memiliki IP dengan *network* yang sama begitupun untuk *ip virtual* yang akan ditambahkan pada kedua *router*. Hal ini dimaksudkan agar kedua *router* dapat terus saling bertukar *hello* messages untuk mengetahui status *router* utama. Dan jika terjadi *link down* pada *router* utama, maka *router standby* akan langsung berubah menjadi *active* dan akan menggantikan *router* utama

c. Keamanan Jaringan

Keamanan jaringan yang berjalan pada PT. PLN DISJAYA menggunakan checkpoint sebagai firewall yang disetting dengan aplikasi GUI bernama smart console, kemudian terdapat beberapa proxy yang digunakan untuk mengatur traffic dalam jaringan LAN dan juga untuk me-monitor aktifitas jaringan LAN menuju internet, kemudian terdapat juga antivirus yang terpasang pada tiap server yang akan menyaring informasi dan juga virus yang masuk dari jaringan internet. Sedangkan untuk PC *client* menggunakan antivirus *Kaspersky* dan *smadav* untuk pencegahan masuknya virus-virus dari segi internal. Dari riset yang sudah dilakukan, tidak menemukan permasalahan apapun pada keamanan jaringan sehingga tidak akan melakukan perubahan apapun pada keamanan jaringannya.

d. Rancangan Aplikasi



Gambar 7. Rancangan Aplikasi

Sumber : Analisis Penelitian

Rancangan aplikasi yang diusulkan adalah membuat sebuah sistem *backup router* menggunakan fitur *Hot Standby Router Protocol* (HSRP). Kedua *router* yang dikonfigurasi menggunakan HSRP akan saling berkomunikasi satu sama lain melewati sebuah *ip virtual* dimana *ip virtual* tersebut akan dijadikan sebagai jalan masuk bagi *core switch* untuk mengakses jaringan luar. *Router* utama akan dijadikan sebagai *router active* dengan prioritas lebih tinggi sehingga jalur data akan melewati *router* tersebut, dan *router* kedua akan dijadikan sebagai *router standby* yang akan terus memantau dan mengirimkan pesan *hello* ke *router active* sehingga ketika *router active* mengalami *link down* maka *router standby* akan berubah status ke *active* dan akan mengalihkan jalur data sehingga client yang sedang mengakses *server* tidak akan merasakan dampak yang terlalu tinggi terhadap masalah tersebut.

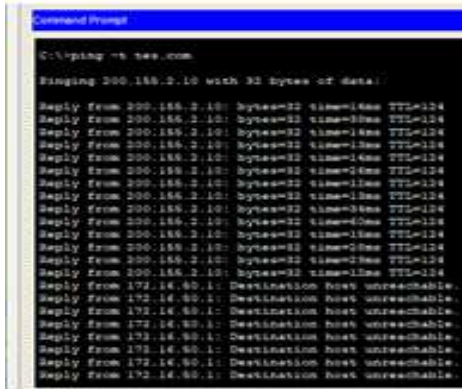
2 Pengujian Jaringan

Pengujian jaringan dilakukan dalam dua tahap, tahap awal dan akhir, tahap awal akan menggunakan kondisi pertama yang masih menggunakan jaringan

berjalan pada PT. PLN DISJAYA. Dan tahap akhir akan menggunakan rancangan yang akan diusulkan.

a. Pengujian Jaringan Awal

Pengujian jaringan awal menggunakan skema jaringan berjalan pada PT. PLN DISJAYA

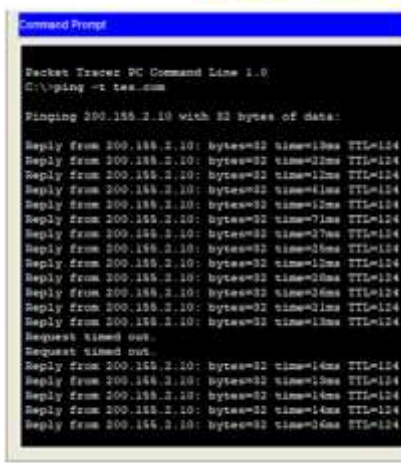
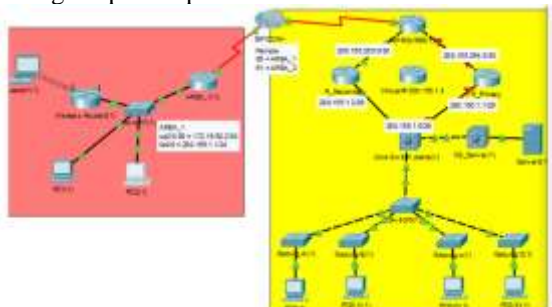


Gambar 8. Pengujian Jaringan Awal
Sumber: Analisis Penelitian

Pada jaringan kantor PLN DISJAYA hanya terdapat sebuah *router*, sehingga ketika *router* tersebut mengalami *link down* ataupun *router* mati, maka koneksi menuju server akan lumpuh total dan tidak bisa diakses dari jaringan diluar kantor PLN DISJAYA

b. Pengujian Jaringan Akhir

Pada pengujian akhir akan menggunakan topologi jaringan usulan yang sudah dirancang dengan skema jaringan usulan pada Gambar 6. dengan rancangan aplikasi pada Gambar 7.



Gambar 9. Pengujian Jaringan Akhir
Sumber: Analisis Penelitian

Pada topologi tersebut hanya menambahkan sebuah *router* tambahan yang diperuntukan sebagai *router backup* kemudian kedua *router* tersebut sudah dikonfigurasi HSRP dengan menambahkan sebuah IP Virtual yang digunakan oleh *core switch* utama sebagai jalan masuk untuk mengakses koneksi ISP agar dapat terkoneksi dengan jaringan luar.

Pengujian dilakukan dengan melakukan ping terus menerus dari PC2 pada jaringan AREA 1 atau cabang dari kantor menuju ke web server yang berada di wilayah PT. PLN DISJAYA. Kemudian melakukan pengujian HSRP dengan cara menonaktifkan *R_Primary* sebagai *router* utama. Dan hasil dari simulasi tersebut terlihat ketika *router* utama mati, komunikasi akan kembali berjalan hanya dalam waktu beberapa detik saja, dan dapat disimpulkan sampai tahap ini fitur HSRP sudah bekerja dengan baik dan menjaga *availability* jaringan komputer.

5.KESIMPULAN

Hasil dari analisis didapatkan bahwa : *Hot Standby Router Protocol* (HSRP) adalah suatu fitur dari cisco yang mampu menjaga *availability* jaringan komputer apabila terjadi gangguan pada perangkat *router* di PT. PLN DISJAYA, dalam hal ini perlu adanya maintenance terhadap sistem secara terjadwal dan ada reaksi yang cepat terhadap permasalahan yng mungkin terjadi pada kedua *router* tersebut. Konfigurasi HSRP menggunakan 2 buah *router* yang digunakan sebagai jalur menuju jaringan luar, dimana salah satu *router* akan berperan sebagai *active router* dan *router* satunya akan menjadi *standby* yang akan menggantikan *active router* ketika terjadi *link down*, oleh sebab itu diperlukan adanya uji *Quality of Services* (QOS) meliputi *delay*, *jitter* dan *packet loss* agar sistem HSRP dapat bekerja lebih optimal

DAFTAR PUSTAKA

[1] Ariawal, Dian, & Purbo, O. W. (2016). Simulasi Jaringan Komputer dengan Cisco Packet Tracer. Jakarta: Elex Media Komputindo.

[2] Cisco Corporate Author. (2015). *Hot Standby Router Protocol Features and Functionality - Cisco. Troubleshooting TechNotes.*

[3] Firmansyah, Wahyudi, M., & Purnama, R. A. (2018). Analisis Kinerja Protocol Redundancy Hot Standby Router Protocol (HSRP) dan Virtual Redundancy Protocol (VRRP). 11–28.

[4] Gitakarma, M. S., & Ariawan, K. U. (2014). Jaringan Komputer. Yogyakarta: Graha Ilmu.

- [5] Irawati, I. D., Yovita, L. V., & Wibowo, T. A. (2015). Jaringan Komputer dan Data Lanjut. Yogyakarta: Deepublish.
- [6] Kaur, I., & Bajaj, H. (2013). *Performance Evaluation of HSRP Protocol for Wireless Network for Fault Tolerance to Improve Quality of Service*. 3(5), 267–269.
- [7] Kaur, P., Kaur, H., & Kaur, J. (2017). *Hot Standby Routing Protocol (HSRP)*. 3(1), 2110–2112.
- [8] Muhammad, M., & Hasan, I. (2016). Analisa Dan Pengembangan Jaringan Wireless Berbasis Mikrotik Router Os V.5.20 Di Sekolah Dasar Negeri 24 Palu. *Jurnal Elektronik Sistem Informasi Dan Komputer*, 2(1), 10–19. Retrieved from stmik-binamulia.ac.id
- [9] Purwanto, W., & Risnanto, S. (2018). Implementasi metode hsrp pada bank jawa barat dan banten kantor wilayah i dan kcp simpang dago. *Jurnal Infotronik*, 3(1).
- [10] Ravikumar, C. V., Srikanth, Y. M., Sairam, P., Sundeep, M., Bagadi, K. P., & Annepu, V. (2016). *Performance analysis of HSRP in provisioning layer-3 gateway redundancy for corporate networks*. *Indian Journal of Science and Technology*, 9(20), 2–6. <https://doi.org/10.17485/ijst/2016/v9i20/89851>
- [11] Siti Nur Khasanah. (2016). KEAMANAN JARINGAN DENGAN PACKET FILTERING FIREWALL (STUDI KASUS: PT. SUKSES BERKAT MANDIRI JAKARTA). *JURNAL KHATULISTIWA INFORMATIKA*, IV(2), 11.
- [12] Supendar, H., & Handrianto, Y. (2017). Simple Queue Dalam Menyelesaikan Masalah Manajemen Bandwidth Pada Mikrotik Bridge. *Ict Journal*, 4(1), 21–30.
- [13] Syafrizal, M. (2005). Pengantar Jaringan Komputer. Penerbit Andi, p. 29. Retrieved from https://books.google.co.id/books?hl=en&lr=&id=UKNyejI7H0IC&oi=fnd&pg=PA1&dq=Syafrizal,+2005&ots=qGfQVme1_i&sig=KOvbYtCx2M5vzCvc3LsyelEvOvM&redir_esc=y#v=onepage&q=Syafrizal%2C2005&f=false
- [14] Usman, U. K., Permana, A. G., & Wibisono, G. (2018). Jaringan Telekomunikasi dan Teknologi Informasi. Bandung: Informatika Bandung.
- [15] Wongkar, S., Sinsuw, A., & Xaverius, N. (2015). Analisa Implementasi Jaringan Internet Dengan Menggabungkan Jaringan LAN Dan WLAN Di Desa Kawangkoan Bawah Wilayah Amurang II. *E-Journal Teknik Elektro Dan Komputer*, 4(6), 62–68.