

PERANGKAT LUNAK SEMI HOT STANDBY ROUTER PROTOCOL PADA PC ROUTER BERBASIS LINUX

Nur Aini Rakhmawati, Febriliyan Samopa, Royyana Muslim I

Jurusan Teknik Informatika,

Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember

Kampus ITS, Jl. Raya ITS, Sukolilo – Surabaya 60111, Telp. + 62 31 5939214, Fax. + 62 31 5913804

Email : khaulah@inf.its-sby.edu, roy@its-sby.edu, iyan@its-sby.edu

ABSTRAK

Router memegang peranan penting dalam sebuah jaringan. Jika router mengalami suatu masalah dapat berakibat terhambatnya lalu lintas data dalam suatu jaringan. Untuk mengatasi masalah sebuah router, Cisco mengembangkan suatu sistem Hot Standby Router Protocol (HSRP). Namun HSRP ini belum dimiliki oleh router komputer. Padahal harga komputer lebih murah daripada router hardware.

Semi HSRP merupakan suatu metode yang diimplementasikan pada router komputer dengan keterbatasan yang dimiliki oleh sebuah komputer dimana sebuah router komputer tidak dapat mengirimkan pesan resign yang mengizinkan router lain untuk menggantikannya ketika router komputer ini mengalami kegagalan.

Dalam semi HSRP dibentuk suatu kelompok router yang memiliki subnet yang sama pada masing-masing interfacenya. Pada masing-masing router dijalankan aplikasi yang berfungsi untuk mengatur jalannya mekanisme HSRP. Aplikasi ini memungkinkan router-router tersebut dapat berhubungan untuk mengetahui apakah ada masalah yang terjadi pada router utama yang berfungsi untuk meneruskan data klien dengan menggunakan alamat virtual IP dan MAC. Dalam berhubungan router-router tersebut menggunakan komunikasi broadcast. Ketika router utama mengalami kegagalan maka akan terjadi pemilihan router berdasarkan prioritas yang dimiliki oleh masing-masing router. Router dengan prioritas tertinggi akan menjadi router utama baru. Router yang terpilih tersebut melakukan penambahan IP yang digunakan sebagai virtual IP yang dikenali klien dan mengubah alamat MAC yang sama dengan router utama sebelumnya.

HSRP pada router hardware dapat diimplementasikan dengan semi HSRP pada router komputer. Sebagaimana halnya HSRP Cisco perpindahan router dapat dilakukan secara otomatis dengan perpindahan alamat IP dan MAC. Perpindahan router ini tidak dipengaruhi besarnya lalu lintas jaringan dan jumlah router yang terdapat dalam satu kelompok

Kata kunci: Router, HSRP, MAC, IP

1. LATAR BELAKANG

Router merupakan salah satu bagian yang penting dalam sebuah jaringan komputer dimana router dapat menghubungkan dua atau lebih jaringan yang memiliki subnet berbeda dengan topologi yang sama. Namun karena beberapa hal router tidak dapat menjalankan fungsinya dengan sebagaimana mestinya, misalnya: kabel terlepas, kabel rusak, dan mati. Kejadian ini dapat menghambat lalu lintas data dalam subnet jaringan yang berbeda dan dari subnet tersebut ke luar LAN untuk beberapa waktu sampai router tersebut dapat segera diperbaiki.

Untuk mengatasi masalah tersebut, Cisco sebagai salah satu perusahaan yang memproduksi router membuat suatu sistem yang disebut *Hot Standby Router Protocol* (HSRP). HSRP merupakan suatu sistem dimana terdapat kelompok router yang bergabung dengan satu pemimpin router dan yang lain sebagai router pengganti atau dapat kita sebut

sebagai router *standby*. Jika pemimpin router ini mengalami kerusakan maka salah satu dari router *standby* otomatis menggantikannya.

Beberapa router dalam bentuk perangkat keras bermerek seperti Cisco, Intel, Proteon, Bay Network, 3Com beberapa diantaranya telah menerapkan HSRP. Namun harga router tersebut yang relatif tinggi sehingga tidak terjangkau oleh perusahaan kecil.

Pada saat ini telah tersedia router yang dibuat dari sebuah komputer dengan sistem operasi Linux. Router dengan sistem operasi linux ini dapat dibuat dengan komputer yang memiliki spesifikasi hardware cukup rendah. Namun router tersebut belum memiliki kemampuan HSRP. Oleh karena itu Penelitian ini membuat aplikasi yang menerapkan HSRP pada router komputer dengan sistem operasi linux.

2. METODOLOGI

Penelitian ini dilakukan dengan mengikuti metodologi sebagai berikut:

Studi literatur

Pada tahap ini dipelajari prinsip penerapan HSRP pada Cisco, cara-cara mengembangkan perangkat lunak pada sistem operasi Linux terutama pemrograman *socket* dan kernel serta pengetahuan lain yang berhubungan jaringan komputer. Pembelajaran ini didapat baik dari buku-buku literatur, paper, manual Linux maupun beberapa artikel di internet.

Pada tahap ini juga akan dipelajari metodologi dan algoritma yang akan digunakan dalam pembuatan perangkat lunak sehingga membantu pada tahap perancangan dan pembuatan perangkat lunak.

Perancangan hardware dan instalasi sistem operasi Linux

Untuk membuat sebuah jaringan komputer dibutuhkan beberapa komputer yang saling terhubung dalam satu jaringan. Sehingga perlu dipersiapkan minimal 4 buah komputer dengan kelengkapan hardware agar dapat terhubung dengan jaringan. Pada tahap ini juga dilakukan instalasi komputer tersebut dengan sistem operasi Linux dimana ada komputer yang dipersiapkan khusus sebagai router dan ada pula yang dipersiapkan sebagai klien.

Perancangan Algoritma

Untuk membuat suatu sistem HSRP dibuat sebuah algoritma. Algoritma ini meniru prinsip kerja HSRP pada Cisco.

Pembuatan Perangkat Lunak

Pada tahap ini, dilakukan implementasi perangkat lunak berdasarkan rancangan yang telah dibuat pada tahap sebelumnya.

Uji Coba dan Evaluasi

Pada tahap ini aplikasi yang telah dibuat diuji dengan *parameter* sebagai berikut :

- Kemampuan router aktif dalam mengirimkan pesan ke router *standby*
- Kemampuan router *standby* menggantikan router aktif.

Penyusunan Buku Penelitian

Pada tahap terakhir ini disusun buku sebagai dokumentasi dari pelaksanaan penelitian. Dokumentasi ini juga dibuat sehingga bagi orang lain yang ingin mengembangkan sistem tersebut bisa mempelajari dari dokumentasi tersebut.

3. IP

Untuk membantu mencapai komputer tujuan, setiap komputer dalam jaringan TCP/IP harus diberikan minimal sebuah alamat IP. Alamat tersebut terdiri atas 32 bit biner yang bersifat unik dan berlaku

secara umum yang mendefinisikan host atau router di internet. 32 bit biner tersebut terbagi menjadi empat bagian yang mempunyai nilai dari 0-255 yang sering ditulis dalam bentuk [xxx.xxx.xxx.xxx]. Alamat ini mendefinisikan dua bagian yaitu net ID dan host ID. Net ID mendefinisikan sebuah jaringan dan host ID mendefinisikan sebuah host pada jaringan tersebut. Ada lima kelas yang berbeda pada alamat IP yaitu kelas A, B, C, D dan E. Kelas ini didesain untuk mencukupi kebutuhan akan jenis organisasi yang berbeda.

	Dari	Tujuan
Kelas A	0.0.0.0	127.255.255.255
Kelas B	128.0.0.0	191.255.255.255
Kelas C	192.0.0.0	223.255.255.255
Kelas D	224.0.0.0	239.255.255.255
Kelas E	240.0.0.0	255.255.255.255

Gambar 1. Kelas IP

4. MAC

Alamat *Media Control Access* (MAC) biasanya disebut sebagai alamat hardware merupakan alamat fisik untuk piranti yang terhubung ke jaringan. Alamat MAC adalah bagian dari lapisan *data link* yang berfungsi untuk mendeteksi *error*, membagi data menjadi banyak *frame*, menambahkan *header* pada *frame* dan memastikan bahwa data telah diterima dengan baik. Alamat ini diberikan kepada semua peralatan yang digunakan pada jaringan seperti *Net Interface Card* (NIC), *Interface Router*, *Switch* dan *Hub*.

Sebuah alamat MAC mempunyai nilai unik yang bersesuaian dengan *network adapter*. Alamat MAC mempunyai 12 digit angka hexadesimal (panjangnya 48 bit) dimana biasanya ditulis dengan format di bawah ini:

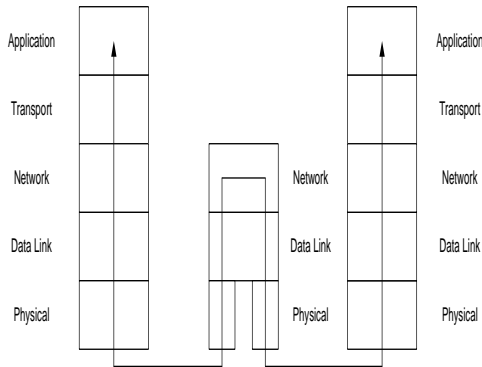
MM:MM:MM:SS:SS:SS

Enam digit pertama melambangkan nomor seri dari pabrik yang membuat. ID ini merupakan standar internet. Sedangkan enam digit kedua melambangkan nomor seri.

5. ROUTER

Route yang berarti jalur adalah sebuah bagian yang tak dapat dipisahkan untuk kita berhubungan dengan network lain bahkan dengan internet. Setiap *host* didalam jaringan akan membutuhkan routing untuk berhubungan. Sebagai contoh sederhana sebagai analogi adalah bila anda akan berjalan keluar dari rumah A dengan tujuan rumah B anda harus melewati sebuah pintu keluar (routing default rumah A) kemudian berjalan misalkan melewati jalan AB (routing network A-B) hingga anda akan menemukan rumah B dan bertemu dengan si B. Demikian pula halnya dalam sebuah jaringan komputer untuk

menuju Internet. Perangkat yang melakukan routing dan berfungsi sebagai jalan menuju network lainnya di sebut Router. Router bekerja pada lapisan *data link* dan lapisan *physical*.



Gambar 2. Wilayah Kerja Router

6. HSRP

HSRP ini pada mulanya dikenalkan oleh Cisco sebagai salah satu perusahaan pembuat router berbentuk perangkat keras. Berdasarkan RFC2281, protokol HSRP menyediakan mekanisme untuk menentukan router aktif dan router *standby*. Berdasarkan nilai prioritas dari masing-masing router. Untuk melakukan mekanisme ini, semua router dalam satu kelompok tersebut saling mengirimkan pesan. Untuk mengurangi lalu lintas jaringan, hanya router aktif dan *standby* yang mengirim secara periodik pesan HSRP sekali setelah protokol menyelesaikan proses pemilihan.

HSRP menyediakan mekanisme yang dibuat untuk mendukung *non-disruptive failover* dari lalu lintas IP pada suatu keadaan. Hal yang utama adalah protokol melindungi dari kemungkinan kegagalan dari *hop* pertama router ketika komputer pengirim tidak mengenali alamat IP dari *hop* pertama router secara dinamis. Hal ini dilakukan ketika router aktif gagal, router *standby* dapat mengambil alih tanpa interupsi pada koneksi *host*. Selain itu, router *standby* juga mengambil alih pengiriman paket dari router aktif.

Pada LAN *multiple hot grup standby* mungkin *coexist* (hidup pada waktu yang sama) dan *overlap*. Tiap *standby* group memulai satu virtual router. Tiap grup *standby* dialokasikan satu alamat MAC, mirip seperti alamat IP. Alamat IP seharusnya menjadi *primary* subnet dalam penggunaannya pada LAN, tetapi harus berbeda dari alamat yang dialokasikan sebagai alamat *interface* untuk semua router dan *host* pada LAN, termasuk virtual alamat IP untuk grup HSRP yang lain.

Jika beberapa grup menggunakan satu LAN, pemisahan dapat dilakukan dengan cara mendistribusi *host* menjadi *standby* group yang berbeda. Pada kasus *multiple group*, tiap grup

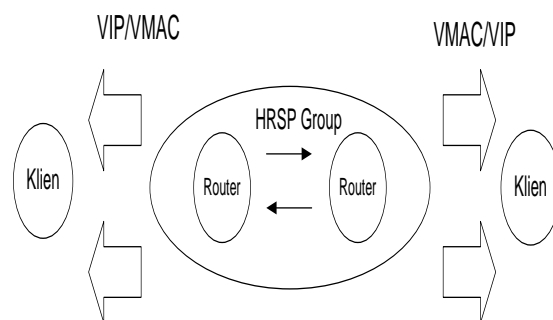
beroperasi *independent* terhadap yang lain. Individual router dapat berpartisipasi dalam *multiple* grup. Pada kasus ini, router mengatur state berbeda dan waktu untuk tiap grup.

Dengan grup *standby*, router secara periodik memasang informasi state menggunakan berbagai macam pesan. Pesan ini termasuk dalam satu paket *Standby* protokol beroperasi pada atas UDP dan menggunakan port number 1985. Paket dikirim ke alamat *multicast* 224.0.0.2 dengan TTL 1. Router menggunakan alamat IP-nya sebagai alamat sumber untuk protokol paket, bukan alamat IP virtual. Hal ini penting sehingga HSRP router dan mengidentifikasi satu sama lain.

7. INSCO

Aplikasi yang bernama **InSCO** ini mengimplementasikan HSRP pada PC router. Aplikasi ini berjalan pada sekelompok router (berupa komputer) yang terdapat dalam satu subnet. Pada router-router tersebut dijalankan aplikasi yang sama. Tidak ada perbedaan aplikasi antara router aktif dan *standby*. Aplikasi sendiri yang akan mengatur mekanisme yang terjadi antara router aktif dan *standby*.

Mekanisme tersebut dapat terjadi karena router-router tersebut berhubungan secara *broadcast* pada port tertentu. Sehingga router *standby* dapat mengetahui jika sewaktu-waktu router aktif mati atau tidak dapat lagi menjalankan fungsinya. Router-router tersebut masing-masing memiliki alamat IP yang berbeda. Namun ketika menjadi aktif, router tersebut harus menggunakan alamat IP virtual yang telah ditetapkan karena alamat IP virtual ini digunakan oleh klien-klien sebagai alamat IP router mereka. Selain alamat IP virtual, router aktif akan menggunakan alamat MAC virtual. Sehingga klien tidak perlu mengetahui mekanisme yang terjadi kelompok router tersebut.



Gambar 3. Sistem HSRP

Untuk mengatasi kesalahan dalam pengiriman data, sistem ini dilengkapi dengan *Cyclic Redundancy Checking* (CRC). Dimana data yang akan dikirim diberi tambahan nilai CRC sehingga

ketika data telah diterima akan diperiksa dengan generator CRC.

Pada sistem ini tidak meimplementasikan HSRP seluruhnya karena keterbatasan dari sebuah router komputer, yaitu router aktif tidak dapat mengirimkan pesan resign yang bertujuan memberi tahu router lain agar segera menggantikannya. Oleh karena itu sistem ini dinamakan **semi hot standby router protocol**.

Transisi State Insc0

Tiap router dalam grup yang berpartisipasi pada protokol ini dapat digambarkan dalam *state machine* sederhana. Berikut ini *state-state* yang dilalui oleh router:

1. Initial
Merupakan state awal dan mekanisme belum berjalan. Pada saat ini router melakukan konfigurasi protokol HSRP-nya sendiri.
2. Listen
Router belum mengetahui apakah ada router lain yang telah aktif atau tidak. State ini terjadi pada saat aplikasi baru dijalankan.
3. Speak
Kondisi ini terjadi ketika router aktif mati. Setelah itu semua router standby melakukan pemilihan router aktif.
4. Standby
Pada saat ini router dapat menggantikan router aktif jika router aktif gagal dan mengirim pesan 'S' secara periodik pada router aktif.
5. Active
Pada saat ini router dalam kondisi aktif dan mengirim pesan 'A' jika ada router standby yang mengirimkan pesan 'S' atau 'R'.

State pada aplikasi ini hampir sama dengan HSRP Cisco, hanya *state learn* yang ditiadakan. *State learn* tidak berfungsi karena aplikasi ini akan berjalan jika semua parameter telah dikonfigurasi dan jika setelah aplikasi berjalan telah ada router lain yang aktif, maka nilai konfigurasi virtual IP dan virtual MAC diambil dari pesan router aktif.

Untuk menuju *state* satu ke *state* lain ada *event* yang terjadi pada router tersebut. Berikut ini *event-event* yang terjadi pada router:

- a. HSRP dikonfigurasi.
- b. Waktu registrasi habis dan tidak menerima pesan dari router lain.
- c. Waktu registrasi habis dan menerima pesan 'A'.
- d. Waktu registrasi habis dan menerima pesan 'R' dengan prioritas lebih tinggi.
- e. Waktu registrasi habis dan menerima pesan 'R' dengan prioritas tertinggi dan sama, namun menerima nilai IP lebih tinggi.
- f. Waktu registrasi habis dan menerima pesan 'R' dengan prioritas tertinggi, sama dan nilai IP tertinggi.

- g. Waktu standby habis dan tidak menerima pesan 'A'.
- h. Waktu standby habis dan menerima pesan 'A'.
- i. Menerima pesan 'S'.
- j. Program *error* atau dihentikan.

Ketika *event* berlangsung diperlukan *action* sebelum menuju ke state berikutnya. Action pada aplikasi ini tidak melakukan pengiriman pesan *Coup* dan *Resign* seperti HSRP Cisco. Hal tersebut dilakukan karena router yang sedang dalam kondisi aktif tidak perlu diubah menjadi standby yang akan berakibat pada ketidakstabilan lalu lintas jaringan. *Action* pada router yang menggunakan aplikasi ini adalah sebagai berikut:

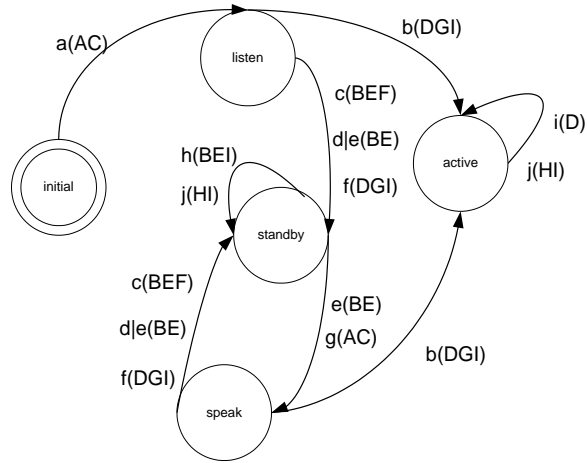
- A. Memulai waktu registrasi
Action ini muncul pada awal aplikasi setelah *state initial* dan ketika router aktif mati. *Action* dilakukan setelah mengirimkan pesan 'R'.
- B. Memulai waktu standby
Action ini dilakukan oleh router *standby* yang akan menunggu pesan dari router aktif.
- C. Mengirim pesan 'R'
Action ini muncul pada awal aplikasi setelah *state initial* untuk mengetahui apakah ada router aktif dan pemilihan antar router *standby*.
- D. Mengirim pesan 'A'
Action ini dilakukan oleh router aktif yang menerima pesan 'S' dari router *standby*.
- E. Mengirim pesan 'S'
Action ini dilakukan oleh router *standby* untuk mengetahui apakah router aktif masih hidup.
- F. Ubah nilai VIP dan VMAC sama dengan VIP dan VMAC router aktif.
Action ini dilakukan ketika router mendapat pesan 'A' dari router aktif.
- G. Mengubah nilai MAC menjadi VMAC dan menambahkan nilai VIP
Action ini dilakukan oleh router yang akan menjadi router aktif.
- H. Mengubah nilai VMAC menjadi MAC dan membuang nilai VIP
Action ini dilakukan oleh router yang akan menjadi router *standby*. Selain itu aplikasi ini dilakukan jika program mengalami *error* atau terhentikan.
- I. Mengembalikan *routing table*
Action ini dilakukan oleh router yang mengalami perubahan status dari *standby* ke aktif atau sebaliknya.

Hubungan antara *state*, *event* dan *action* dapat digambarkan pada tabel 3.1. Untuk setiap *event* dan *state* router harus melakukan serangkaian *action*. Notasi angka menunjukkan *state* berikutnya, huruf *lowercase* menunjukkan *event* dan huruf *uppercase* menunjukkan *action*. Untuk mengetahui keterangan

masing-masing notasi (angka dan huruf) lihat keterangan di atas. Tanda *slash (/)* memisahkan antara *action* dan *state* berikutnya.

Tabel 1. Transisi State

	1	2	3	4	5
	Initial	Listen	Speak	Standby	Active
Event					
a	AC/2				
b		DGI/5	DGI/5		
c		BEF/4	BEF/4		
d		BE/4	BE/4		
e		BE/4	BE/4	BE/3	
f		DGI/4	DGI/4		
g				AC/3	
h				BEI/4	
i					D
j				HI	HI

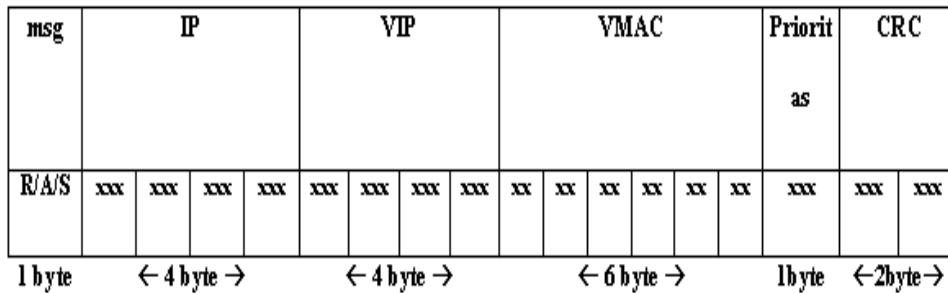


Gambar 4. State Machine Insc0

Untuk memperjelas tabel 1 tersebut, dapat digambarkan *state machine* pada Gambar 4. Yang terdapat dalam tanda kurung merupakan aksi yang harus dilakukan untuk menuju ke state berikutnya.

Format Data Protokol Insc0

Dalam berhubungan router dalam kelompok HSRP menggunakan protocol INSCO. Struktur protocol INSCO disusun berdasarkan format seperti gambar 5.



Gambar 5. Kerangka Format Protocol INSCO

Keterangan :

- a. **msg**
Msg bertipe data char. Msg dapat bernilai 'R', 'S' dan 'A'. Msg bernilai 'R' berarti registrasi router
- b. **IP**
IP bertipe data string yang terdiri atas 4 karakter. Setiap karakter bernilai antara 0 sampai dengan 255. IP ini bernilai sesuai dengan alamat IP router pengirim.
- c. **VIP**
VIP bertipe data string yang terdiri atas 4 karakter. Setiap karakter bernilai antara 0 sampai dengan 255. VIP ini bernilai sesuai dengan alamat IP virtual kelompok HSRP.
- d. **VMAC**

- e. **prioritas**
Prioritas bertipe data char. Prioritas bernilai antara 0 sampai dengan 255. Nilai menunjukkan tingkat prioritas sebuah router dibandingkan dengan router lainnya pada saat terjadi pemilihan router. Semakin tinggi prioritas maka semakin besar peluang sebuah router untuk menggantikan router aktif jika mengalami kegagalan.
- f. **CRC**

CRC bertipe data string yang terdiri atas 2 karakter. CRC ini berfungsi sebagai pemeriksa kesalahan data yang diterima. Penghitungan CRC ini didapatkan dari seluruh data paket yang dikirimkan sebelum ditambahkan CRC.

8. UJI COBA

Skenario uji coba dilakukan dengan menjalankan aplikasi pada semua router. Kemudian semua klien disetting routing sesuai yang diinginkan. Antara klien sama-sama melakukan proses ping atau pengiriman data, sedangkan antara router melakukan proses ping terhadap IP virtual kelompok insco. Selain itu, dijalankan juga program **Ethereal** yang akan melakukan monitor setiap paket yang masuk pada host khusus pada jaringan sesungguhnya, sedangkan pada jaringan user mode linux hanya menggunakan waktu pada syslog. Ketika klien sedang berkomunikasi, router aktif dimatikan. Masing-masing skenario pada jaringan sebenarnya dilakukan dua kali uji coba, yaitu uji coba dengan mengirimkan file dan tanpa mengirimkan file.

Uji Coba 1

Semua router mempunyai default routing gateway ke 10.126.10.1 dan semua router salah satu kabel jaringannya terhubung dengan switch jaringan network address 10.126.10.0. Dimana switch tersebut berhubungan dengan Core Builder Fakultas Teknologi Informasi. Sedangkan kabel jaringan router yang lain terhubung dengan switch jaringan network 10.126.100.0. Agar klien untuk network 10.126.100.0 dapat berhubungan dengan jaringan luar pada Core Builder ditambahkan routing untuk 10.126.100.0 melewati alamat IP 10.126.10.170. Alamat IP 10.126.10.170 ini akan menjadi alamat

virtual IP kelompok router untuk network address 10.126.10.0, sedangkan alamat IP 10.126.100.1 menjadi alamat virtual IP untuk network address 10.126.100.0. Salah satu komputer menjadi klien pada network address 10.126.10.0 terhubung pada switch network address 10.126.10.0 dan diberikan nilai routing default gateway ke 10.126.10.1, sedangkan komputer klien pada network address 10.126.100.0 terhubung pada switch network address 10.126.100.0 dan diberikan nilai routing default gateway ke 10.126.100.1. Skenario ini ditunjukkan oleh gambar 6.

Uji Coba 2

Skenario dua sama dengan skenario pertama, namun pada skenario ini hanya dua buah router yang dijalankan, yaitu falcon dan hsrp. Skenario ini ditunjukkan oleh gambar 7.

9. HASIL UJI COBA

Setelah uji coba 1, 2 dan 3 dilakukan, selanjutnya dilakukan proses penghitungan waktu *reply* dari klien ke klien, klien ke router maupun router ke router ketika terjadi perpindahan router dengan rumus :

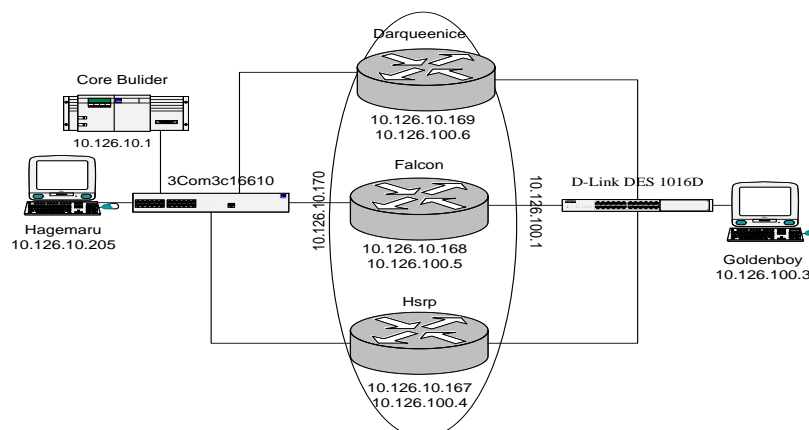
$$\Delta T = Trp - Trq$$

ΔT = Selisih waktu paket request pertama setelah reply dengan waktu paket reply setelah request terakhir ketika terjadi perpindahan router.

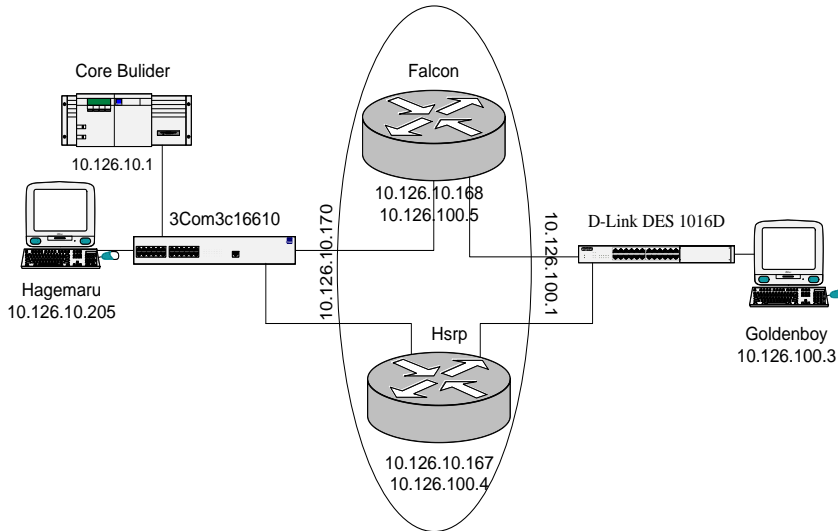
Trp = Waktu paket reply setelah request terakhir ketika terjadi perpindahan router.

Trq = Waktu paket request setelah reply pertama ketika terjadi perpindahan router.

Waktu tersebut didapatkan melalui program Ethereal.



Gambar 6. Skenario Uji Coba 1



Gambar 7. Skenario Uji Coba 2

No. -	Time	Source	Destination	Protocol	Info
2	2004-08-03 11:52:00.629841	10.126.10.205	10.126.100.1	ICMP	Echo (ping) request
3	2004-08-03 11:52:00.630320	10.126.100.1	10.126.10.205	ICMP	Echo (ping) reply
7	2004-08-03 11:52:01.629376	10.126.10.205	10.126.100.1	ICMP	Echo (ping) request
19	2004-08-03 11:52:07.128524	10.126.10.205	10.126.100.1	ICMP	Echo (ping) request
35	2004-08-03 11:52:12.629831	10.126.10.205	10.126.100.1	ICMP	Echo (ping) request
36	2004-08-03 11:52:12.630417	10.126.100.1	10.126.10.205	ICMP	Echo (ping) reply

Gambar 8. Hasil Ethereal 10.126.10.205 Ping 10.126.100.1 (1.1)

Sedangkan untuk jaringan UML, ketika aplikasi dijalankan pada router dilakukan monitoring dengan perintah `tail -f /var/log/syslog`. Pada syslog akan terlihat waktu kapan aplikasi mulai jalan, pemilihan router, aplikasi mati dan lainnya. Hasil uji coba ini berkaitan dengan selisih waktu ketika router aktif mati dengan router standby menjadi aktif. Gambar 8 adalah hasil salah satu uji coba pada uji coba 1.

Router aktif adalah darqueenice sedangkan router standby adalah falcon dan hsrp. Klien yang digunakan adalah 10.126.10.205 dan 10.126.100.3. Gambar 11 merupakan hasil ethereal pada klien 10.126.10.205.

Berdasarkan gambar 11, router 10.126.100.1 kembali dapat terhubung setelah 11.001041 detik. Sedangkan gambar 12 merupakan salah satu contoh hasil uji coba pada jaringan UML.

Router tiga merupakan router aktif, sedangkan router satu, dua dan empat merupakan router standby. Berikut hasil pencatatan waktu syslog sebelum router tiga dimatikan. Berdasarkan gambar 12 router satu akan menerima pesan 'A' setelah 3 detik dari awal waktu standby. Hasilnya bisa dilihat di tabel 2.

Tabel 2 Hasil Uji Coba Reply Klien ke Klien

Uji Coba Dari 10.126.10.205	Tujuan(dalam detik)
	10.126.100.3
1 tanpa file	11.001283
1 dengan file	11.001044
2 tanpa file	12.001034
2 dengan file	10.970234
2 tanpa file	11.001047
2 dengan file	11.793236

10. EVALUASI

Berdasarkan tabel hasil uji 2 dan kecepatan *reply* antar klien ke klien, router ke klien maupun router ke router ketika terjadi perpindahan router untuk aplikasi Inscod tidak dipengaruhi oleh :

1. Lalu lintas jaringan

Uji coba satu dan dua berada pada jaringan dengan lalu lintas yang padat daripada uji coba tiga, namun kecepatan *reply* tidak ada perubahan yang signifikan. Selain itu pada uji satu, dua dan tiga ketika terjadi pengiriman file juga tidak mempengaruhi kecepatan *reply*.

2. Jumlah router dalam satu kelompok

Pada uji coba satu yang menggunakan tiga buah router kecepatan *reply* tidak jauh berbeda yang menggunakan dua buah router. Hal ini terjadi karena adanya pembatasan waktu dalam pemilihan router yang hanya berlangsung 3 (tiga) detik. Sehingga router yang mengalami waktu standby yang habis terakhir tidak dapat ikut dalam pemilihan router. Jika dalam 3 (tiga) detik telah ada router yang memiliki prioritas tertinggi secara otomatis router ini akan menjadi router aktif dan melakukan *broadcast* pesan 'A'.

11. KESIMPULAN

1. Komputer router dengan sistem operasi Linux dapat mengimplementasikan sistem semi HSRP sebagaimana halnya router perangkat keras.
2. Perpindahan router dapat dilakukan secara otomatis dengan memindahkan alamat virtual IP dan MAC router.
3. Besarnya lalu lintas jaringan tidak mempengaruhi waktu perpindahan router.
4. Jumlah router dalam satu kelompok Insc0 untuk jumlah router lebih dari dua tidak mempengaruhi waktu perpindahan router.

12. SARAN

1. Mengurangi proses yang dilakukan router aktif, sehingga router aktif dapat meneruskan paket klien dan memberikan

respon lebih cepat setiap pesan dari router standby.

2. Melakukan enkripsi protokol yang dikirimkan sehingga keamanan data dapat terjaga. Hal ini dilakukan karena aplikasi ini menggunakan komunikasi broadcast dimana seluruh komputer pada jaringan sapat menerima semua pesan yang dikirimkan oleh router aktif maupun standby.
3. Mengurangi jumlah data dalam protokol sehingga tidak membebani jaringan dengan cara kompresi data yang akan dikirim.
4. Pengembangan antarmuka pengguna sehingga memudahkan penggunaan terutama bagi user yang masih awam linux.

13. DAFTAR PUSTAKA

1. Behrouz A. Forouzan, "*TCP/IP Protocol Suite*", McGraw Hill, 2000.
2. http://daq.trium.ca/online/software/multinet/programmers_reference
3. <http://pont.net/>
4. <http://utenti.lycos.it/okarti/modules.php?name=News&file=article&sid=22>
5. <http://www.faqs.org/rfcs/rfc2281.html>
6. <http://www.ietf.org/html.charters/vrrp-charter.html>
7. <http://www.w3.org/TR/html4/>
8. Neil Matthew, Richard Stones, "*Professional Linux Programming*", Wrox Press, 2000.