ISSN : 1410 – 7104

Implementasi *First Hop Redundancy Protocol* (FHRP) Pada Jaringan Data Untuk Meningkatkan Availibility Pada Pelanggan

Implementation of First Hop Redundancy Protocol (FHRP) on Data Networks to Increase Customer Availibility

Djoko Suprijatmono[1] dan Andre Siswadi[2]
E-mail : [1]djokojte@istn.ac.id, [2] andresiswadi8@gmail.com

Abstrak--- *FHRP merupakan suatu protokol yang berguna untuk jaringan agar selalu dalam kondisi on dengan cara menyediakan jalur (link) redundancy pada dua atau lebih perangkat physically yang di konfigurasi menjadi satu perangkat virtual, salah satu perangkat akan menjadi jalur active (utama) dan yang lain standby atau jalur cadangan (backup link) apabila jalur utama down, contoh dua perangkat menjadi satu interface virtual jadi pada dua perangkat tersebut akan sepakat hanya ada satu gateway pada dua link (jalur) dan pada link tersebut ada yang active dan backup. Tujuan pada penulisan ini adalah bagaimana mengimplementasikan protocol FHRP pada jaringan data, untuk mengatasi single point of failure dari switch layer 3. Hal ini dibutuhkan karena untuk meminimimalisir downtime yang terjadi di pelanggan sesuai Standard Level Agreement (SLA) yang telah disetujui dengan availability 99.8% perbulan yang jika dikalkulasikan adalah maksimal downtime perbulannya adalah 1jam 30menit per lokasi.*

Kata Kunci--- *FHRP, Redundancy, Downtime*

Abstract--- *FHRP is a protocol that is useful for the network so that it is always on condition by providing a redundancy link on two or more physically configured devices into one virtual device, one of the devices will be the active (main) and the other standby or backup path (backup link) when the main line is down, the example of two devices becomes one virtual interface so the two devices will agree there is only one gateway on the two links (path) and the link is active and backup. The purpose of writing this is how to implement the FHRP protocol on the data network, to overcome single point of failure of the layer 3 switch. This is needed because to minimize the downtime that occurs at the customer according to the approved Standard Level Agreement (SLA) with 99.8% availability monthly which if calculated is the maximum monthly downtime is 1 hour 30 minutes per location.*

Keywords*--- FHRP, Redundancy, Downtime*

1. PENDAHULUAN

Kestabilan jaringan komputer sangat dibutuhkan oleh sebuah perusahaan yang melakukan transaksi antar cabang. Sebuah perusahaan yang bergerak di bidang asuransi dan memiliki beberapa kantor cabang di kota-kota besar di Indonesia tentunya sangat membutuhkan jaringan komputer yang stabil antar kantor cabang. *Downtime* jaringan komputer pada perusahaan yang disebabkan masalah pada *Switch Cisco* utama dan perangkat ISP yang sering terjadi, bahkan dalam tiap minggu selalu ada kasus *downtime*.

Untuk menunjang jaringan komputer yang stabil antar kantor cabang, hal-hal yang dapat menyebabkan terjadinya *link down* harus diminimalisir seminimal mungkin dan lamanya *link down* juga harus diminimalisir. Banyak metode yang digunakan dan salah satu metode yang akan digunakan untuk meminimalisir penyebab dan lamanya *link down* adalah *First Hop Redundancy Protocol* (FHRP).

First Hop Redundancy Protocol (FHRP) adalah sebuah protokol yang menyediakan jaringan yang tinggi ketersediaan (high availability) dan menyediakan *hardware* hampir seketika *fail-over* tanpa *intervensi* administrator. Ini menghasilkan sebuah *hot standby router* group, termasuk *router*-utama yang meminjamkan jasa untuk setiap paket yang ditransfer ke alamat *router*-siaga. Jika *router* utama gagal, maka akan digantikan oleh *router*-siaga.

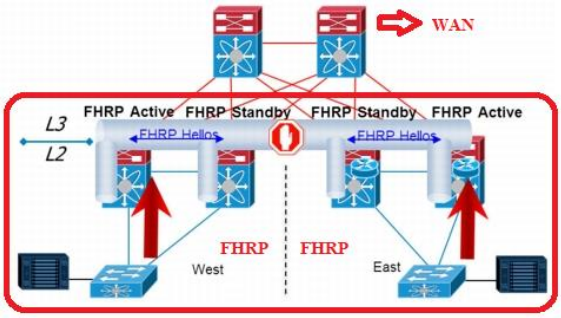
Semua *router* yang berpartisipasi dalam FHRP diasumsikan berjalan sesuai IP *protocol routing* dan memiliki set konsisten rute. Pembahasan protokol yang sesuai dan apakah routing yang konsisten dalam situasi tertentu adalah di luar lingkup spesifikasi ini. Ketersediaan jaringan komputer sangat diperlukan sehingga dibutuhkan sistem *First Hop Redundancy Protocol* (FHRP).

2. METODA

2.1. First Hop Redundancy Protocol (FHRP)

FHRP merupakan suatu *protocol* yang berguna untuk *network* agar selalu dalam kondisi ON dengan cara menyediakan jalur (Link) Redudancy pada dua atau lebih perangkat Phisiccally yang di konfigurasi menjadi satu perangkat *virtual*, salah satu perangkat akan menjadi jalur *active* (utama) dan yang lain

Standby atau jalur cadangan (Backup Link) apabila jalur utama *Down*, misal: dua perangkat menjadi satu *interface virtual* jadi pada dua perangkat tersebut akan sepakat hanya ada satu *gateway* pada dua *Link* (jalur) dan pada *Link* tersebut ada yang *active* dan *Backup*. Yang masuk pada Protocol FHRP ini adalah HSRP, VRRP, GLBP jadi semua berhubungan, berikut ini contoh gambarnya:



Gambar 1. Konfigurasi FHRP

Gambar 1 menjelaskan proses detail pada konfigurasi Protocol FHRP adalah sebagai berikut:

1. *Forwarding/Active Router* mengirim *Hello packet* ke *Standby Router* tiap beberapa detik2.
2. Secara *Default Router* yang menyala duluan akan menjadi *Forwarding Router3*. Apabila *Active Router* lagi *Down* dan tidak mengirim *Hello* paket ke *Standby Router* maka otomatis *Standby Router Active* dan menjadi *forwarding Router*.
3. Secara *Default* apabila *Active Router* UP lagi maka dia akan menjadi *Standby Router* dan posisinya sudah di ambil alih, (kecuali nilai Priority masih tertinggi maka dia akan jadi *Active Router* lagi).

2.2. Graphic Network Simulator (GNS3)

GNS3 adalah simulator alat-alat jaringan Cisco yang sering digunakan sebagai media pembelajaran dan pelatihan dan juga dalam bidang penelitian simulasi jaringan komputer. Program ini dibuat oleh Cisco Systems dan disediakan gratis untuk fakultas, siswa dan alumni yang telah berpartisipasi di *Cisco Networking Academy*. Tujuan utama GNS3 adalah untuk menyediakan alat bagi siswa dan pengajar agar dapat memahami prinsip jaringan komputer dan juga membangun *skill* di bidang alat-alat jaringan Cisco.

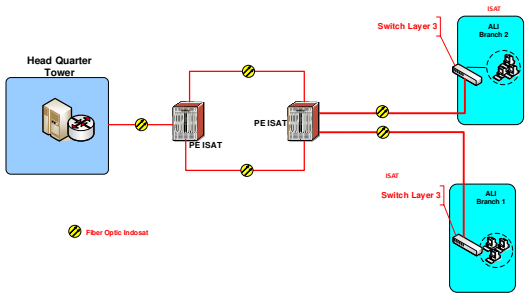
GNS3 terbaru yaitu versi 5.3.3. Dalam versi ini dapat mensimulasikan *Application layer protocols*, *Routing* dasar RIP, OSPF, and EIGRP, sampai tingkat yang dibutuhkan pada kurikulum CCNA yang berlaku, sehingga bila dilihat sekilas software ini bertujuan untuk kelas CCNA. Target GNS3 yaitu menyediakan simulasi jaringan yang real, namun ter dapat beberapa batasan berupa penghilangan beberapa perintah yang digunakan pada alat aslinya yaitu pengurangan command pada Cisco IOS. Dan juga GNS3 tidak bisa digunakan untuk memodelkan jaringan produktif/aktif. Dengan keluarnya versi 5.3, beberapa fitur ditambahkan, termasuk fitur BGP. BGP memang bukan termasuk kurikulum CCNA, akan tetapi termasuk kurikulum CCNP.

GNS3 biasanya digunakan siswa *Cisco Networking Academy* melalui sertifikasi *Cisco Certified Network Associate* (CCNA). Dikarenakan batasan pada beberapa fiturnya, *software* ini digunakan hanya sebagai alat bantu belajar, bukan sebagai pengganti *Cisco routers* dan *switches*.

GNS3 merupakan salah satu aplikasi keluaran Cisco sebagai simulator untuk merangkai dan sekaligus mengkonfigurasi suatu jaringan (network). Sama halnya dengan simulator–simulator jaringan lainnya seperti GNS3, Dynamips, Dynagen maupun simulator lain yang khusus digunakan pada Simulasi jaringan.

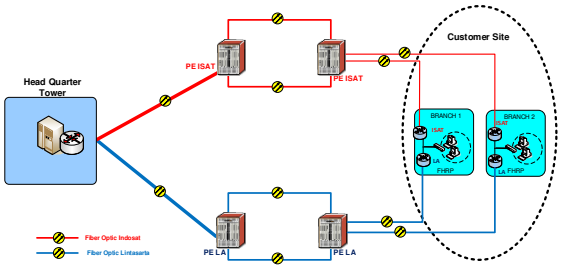
3. PERANCANGAN DAN IMPLEMENTASI JARINGAN

Dalam jurnal penelitian dilakukan pada jaringan existing yang berlokasi di Menara Jamsostek dengan topology jaringan existing yang ditunjukan pada Gambar 2 berikut:



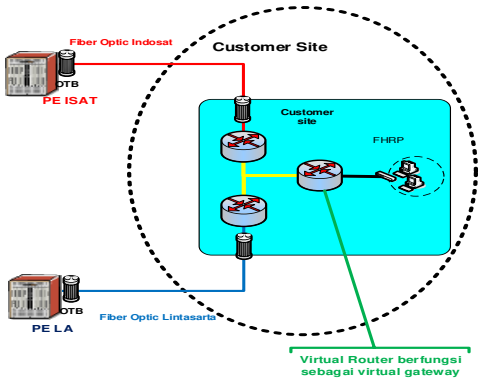
Gambar 2. Topology existing pada AXA General Insurance Indonesia

Setelah dilakukan analisa ditemukan adanya satu buah *layer 3 switch* sebagai *gateway* yang tentunya masih bersifat *single point of failure*. Masalah *availability* ini merupakan fokus perusahaan dalam pengembangan jaringan kali ini untuk menunjang *business* perusahaan yang sedang menuju era digital. Maka dari itu akhirnya disarankan agar merubah *network existing* dengan teknologi FHRP dengan rencana sebagai berikut pada gambar 3.



Gambar 3. Rencana jaringan baru

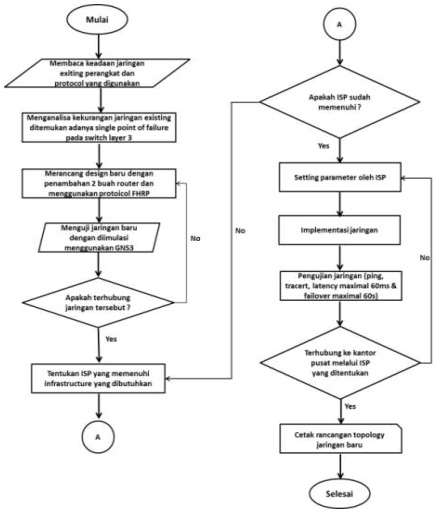
Pada gambar 3 masih belum terlihat dimana lokasi *virtual router* yang akan diimplementasikan. *Router* ini nantinya akan digunakan sebagai *default gateway* sebagai *primary router* ketika jaringan sudah diimplementasikan. Selanjutnya pada gambar 4 adalah lokasi dimana *router virtual* yang telah diimplementasikan:



Gambar 4. *Router Virtual* Baru

3.1. Topology Perencanaan Jaringan

Dalam merancang jaringan diperlukan tahapan-tahapan untuk membantu dalam proses perancangan. Gambar 5 merupakan gambar *flowchart* dari perancangan jaringan pada jurnal ini. Proses perancangan jaringan dari memulai proses setelah itu masuk proses selanjutnya yaitu melakukan perhitungan parameter-parameter pada rancangan jaringan. Kemudian setelah mendapatkan hasil perhitungan parameter jaringan, selanjutnya memasuki proses setting atau pengaturan hasil parameter ke dalam simulasi. Setelah semua hasil parameter di masukkan ke dalam simulasi, dilakukan proses sampai mendapatkan hasilnya.

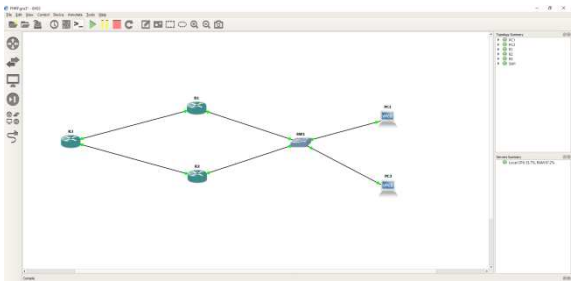


Gambar 5. Perencanaan Topology Jaringan

3.2. Perancangan Jaringan

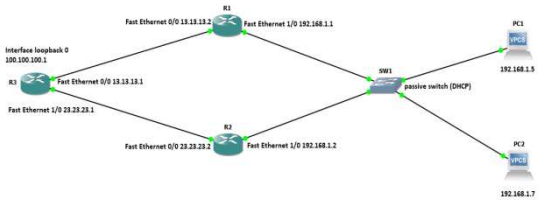
3.2.1. Simulasi Topology Jaringan

Sebelum dilakukan implementasi ke *real network*, simulasi ini dimaksudkan untuk melihat kinerja awal dari *network* yang akan dibangun. *Tools/software* yang digunakan untuk simulasi ini adalah GNS3. Topologi jaringan komputer pada simulasi ini sesuai dengan desain topologi jaringan komputer pada gambar 6.~~4.5~~



Gambar 6. Simulasi Topology di GNS3

Pada gambar 6 hubungan antar *router* dilakukan dengan menggunakan kabel RJ-45 yang akan menghubungkan *interface Fast Ethernet* dengan yang dapat mendukung bandwidth sampai dengan 100 Mbps. Pemilihan *interface Fast Ethernet* karena kebutuhan akan jaringan *backbone* yang berkecepatan tinggi dan setidaknya mendukung *bandwidth* tertinggi yang berada pada kantor pusat. Koneksi yang dilakukan pada antar *router* dilakukan dengan kabel *crossover* yang diwakili garis hitam putus-putus dan koneksi antara *router* ke *switch* dan *switch* ke PC dilakukan memakai kabel RJ-45 dengan konfigurasi *straight-through* yang diwakili garis hitam lurus. Bulatan berwarna merah tersebut menunjukkan bahwa *interface Fast Ethernet* pada *router* masih dalam keadaan *shutdown* dan belum aktif.



Gambar 7. Pengalokasian IP di GNS3

Gambar 7 adalah pengalokasian alamat IP untuk *interface* pada GNS3. Dalam hal ini *interface* berupa *router* harus dialokasikan IP dengan perencanaan yang baik, agar dapat menghubungkan router satu dengan lainnya. Untuk pengalokasian IP dalam *interface* ini harus dibuat seefisien mungkin sebagai penggunaan sumber daya berupa alamat IP.

Alokasi IP dipilih berdasarkan karakteristik dari *router* dimana pada pada koneksi pada *interface* suatu *router* ke *router* lain harus berada pada subnet yang sama. Sebagai contoh, port FastEthernet0/0 dari Router3 dengan alamat IP 13.13.13.1 dihubung

kan dengan FastEthernet1/0 dari Router1 dengan alamat IP 13.13.13.2, dimana kedua alamat ini ber ada pada satu subnet.

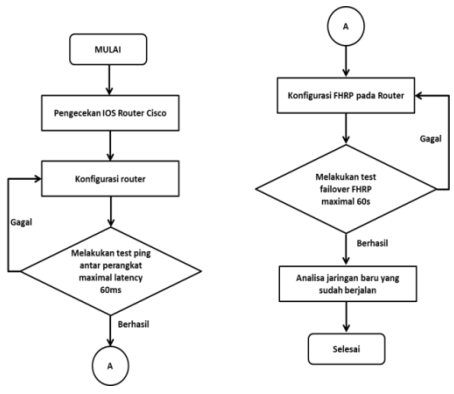
Pengalokasian IP berikutnya dilakukan untuk host yang berada pada masing–masing lokasi. Tabel 1 menunjukkan alokasi alamat IP pada masing–masing lokasi kantor cabang. Pengalamatan IP addresses di masing–masing lokasi disesuaikan dengan jumlah host yang ada. Hal ini dilakukan untuk mengefisiensikan penggunaan sumber daya berupa alamat IP jika nantinya akan ada user / pengguna baru.

Tabel 1. Distribusi alamat IP untuk *Interface – Interface Router*

Nama router	Fast Ethernet 0/0	Fast Ethenet 1/0	Static Route
Router3	13.13.13.1/30	23.23.23.1/30	ip route 100.100.100.0 255.255.255.0 13.13.13.1 ip route 192.168.1.0 255.255.255.0 13.13.13.1
Router1	13.13.13.2/30	192.168.1.1/30	ip route 100.100.100.0 255.255.255.0 23.23.23.1
Router2	23.23.23.2/30	192.168.1.2/30	ip route 192.168.1.0 255.255.255.0 23.23.23.2
User	192.168.1.0/24		

3.2.2. Konfigurasi Protocol FHRP Pada GNS3

Langkah awal implementasi melakukan konfigurasi dasar *router* seperti pemberian IP *address* dan routing, kemudian dilakukan pengetesan ping, jika *test* ping masih belum berhasil, cek kembali konfigurasi dasar setelah itu *test ping* kembali. Selanjutnya adalah melakukan konfigurasi FHRP. Ketika konfigurasi sudah berhasil, kemudian dilakukan pengetesan *ping*, jika setelah dilakukan konfigurasi FHRP ternyata *test ping* gagal, lakukan kembali pengecekan konfigurasi FHRP pada router setelah itu lakukan *test ping* ulang dan dilanjut dengan pengunggahan data dari FTP *server*. Ketika sedang proses pengunggahan dilakukan *test failover* atau mematikan *router* yang sedang beroperasi, dan dilakukan pengukuran dan pengambilan data.



Gambar 8. *Flowchart Implementasi* FHRP

Dari data yang sudah diperoleh dilakukan analisa untuk menentukan berapa nilai performansi jaringan komputer yang dapat ditingkatkan dengan fitur FHRP dan dapat dilihat pada flowchard pada gambar 8.

Setelah dilakukan konfigurasi FHRP kedua *router* berada dalam status awal. Kedua *router* akan saling mengecek IP virtual dan group, apakah kedua *router* memiliki IP virtual dan group yang sama. Jika kedua *router* memiliki IP virtual dan group yang berbeda maka masing-masing *router* akan dalam status *active* tetapi tidak saling mem-*backup* dan hanya router yang memili IP virtual sebagai *gateway host* yang dapat meneruskan paket data. Sebaliknya jika kedua *router* memiliki IP virtual dan group yang sama, akan lanjut ke langkah berikutnya yaitu *router* akan saling mengecek *priority*, dan *router* yang memiliki *priority* tertinggi akan menjadi *active router* dan lainnya menjadi *standby router*. Ketika sudah ditentukan *active* dan *standby router* untuk pertama kalinya, kedua *router* akan terus saling mengirim *hello messages* untuk saling mengetahui status dari kedua *router*. Ketika *standby router* tidak menerima *hello messages* yang bisa dikarenakan matinya *router*, putusnya link, dan penyebab lainnya sehingga terjadi gangguan pada *router* maka *standby router* akan berubah stastusnya dari *standby* menjadi init. Ketika menerima status *router* tidak berubah, tetap dalam status *standby*. Tidak diterimanya *hello messages* pada *standby router* dan menyebabkan perubahan status pada *standby router* tidak akan mengganggu proses komunikasi data karena data diteruskan melalui *active router*. Ketika *active router* tidak menerima *hello messages* yang bisa dikarenakan matinya *router*, putusnya *link*, dan penyebab lainnya sehingga terjadi gangguan pada *router* maka status *active router* akan berubah menjadi init dan *standby router* berubah statusnya menjadi *active router* dan mengambil alih kerja *active router* sebelumnya. Ketika *router* yang berada pada kondisi init kembali menerima *hello messages* maka status *router* akan berubah menjadi *standby router* dan kembali mengirimkan *hello messages*.

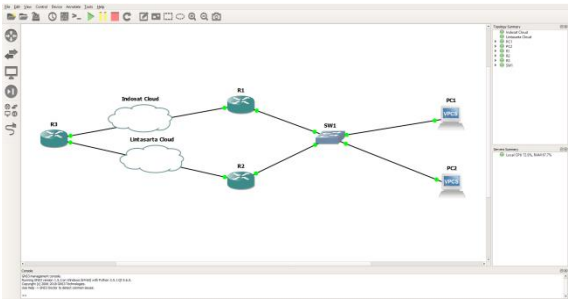
Konfigurasi akan dilakukan dengan menggunakan IOS *command* pada *router-router* yang menjadi *backbone*. IOS command sendiri merupakan bahasa pemrograman yang digunakan untuk mengkonfigurasi *device-device* jaringan.

Pada langkah selanjutnya adalah mengkonfigurasi router yang berada di kantor pusat agar dapat terhubung dengan router yang berada di kantor cabang, untuk detail konfigurasi pada router3 (router kantor pusat) adalah sebagai berikut :

Setelah *router primary* (R1) selesai di konfigurasi, selanjutnya lakukan hal yang sama pada *router secondary* (R2) dengan konfigurasi yang sama tetapi dibedakan dalam pengalamatan IP *address*nya sesuai yang telah dibagi pada tabel 1.

Setelah melewati proses–proses berupa pengaktifan *interface*, pengalokasian IP dan pengkonfigurasian *routing protocol* berupa FHRP, maka jaringan yang semula belum aktif seperti ditunjuk-

kan pada gambar 7 akan menjadi aktif. Pada jaringan yang telah aktif ini, bulatan–bulatan merah yang semula berada pada jalur penghubung *router, switch*, dan *host* akan berubah menjadi bulatan–bulatan hijau yang menandakan *interface* telah aktif dan konektivitasnya dengan *interface* pada *device* lain telah terbangun, seperti ditunjukkan pada gambar 9. Jaringan yang sudah aktif ini akan diuji-coba untuk melihat unjuk kerja jaringan yang meng-gunakan routing protocol FHRP dengan pengujian berupa *ping*, *traceroute*, kemampuan akses NMS dan kemampuan *fault tolerant*.



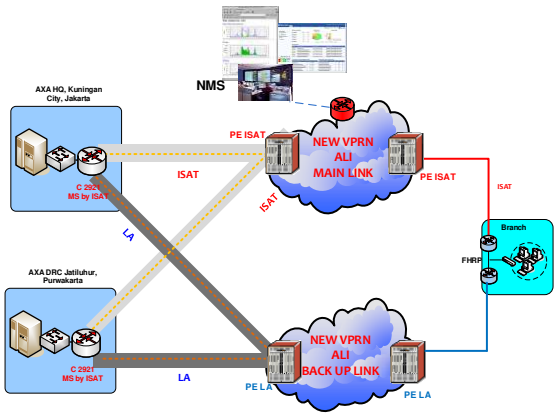
Gambar 9. Jaringan siap uji coba

4. IMPLEMENTASI JARINGAN

Untuk membuat jaringan infrastruktur FHRP, maka dibutuhkan peralatan seperti yang tertera di bawah ini :

1. Komputer untuk kebutuhan pengguna layanan jaringan
2. Router untuk jaringan backbone
3. Switch untuk sambungan antara pengguna dan Router

Adapun gambar dari jaringan fisik untuk jaringan ini dapat dilihat pada gambar 10.



Gambar 10. Jaringan Fisik FHRP

Gambar 10 di atas menunjukkan jaringan fisik yang dibangun berdasarkan jaringan logika yang ditunjukkan oleh Gambar 9 jaringan mempunyai *topology ring* yang artinya *router* tersebut dihubung kan satu sama lain tanpa harus berhubungan secara *full mesh*. Walaupun secara logika komputer pada masing- masing tempat secara logika berhubungan secara *full mesh*.

Alokasi IP pada router dapat dilihat dari tabel 2. di bawah ini :

Tabel 2. Alokasi IP pada kantor cabang

Nama *router*	*GigabitEthernet0/0*	*GigabitEthernet0/1*	*IP Route*
Router Indosat	10.48.166.170	10.48.104.51	ip route 10.48.105.0 255.255.255.0 10.48.104.1
Router Lintasarta	10.48.166.174	10.48.104.52	ip route 10.48.105.0 255.255.255.0 10.48.104.1
Router Kantor Pusat	10.48.7.45		ip route vrf AXA-ALI 0.0.0.0 0.0.0.0 GigabitEthernet0/0/2.162 10.48.7.33 track 33 ip route vrf AXA-ALI 10.46.0.0 255.255.0.0 GigabitEthernet0/0/2.162 10.48.7.33 track 33 ip route vrf AXA-ALI 10.48.0.0 255.255.0.0 GigabitEthernet0/0/2.162 10.48.7.33 track 33

Masing-masing pengguna menggunakan *gateway* yang sama dengan IP pada *port Gigabit Ethernet router* terdekat dengan pengguna itu sendiri. Pem-berian IP *gateway* ini bertujuan untuk mengetahui alamat dari *port* selanjutnya yang akan dituju.

4.1. Pengujian Analisa Jaringan FHRP

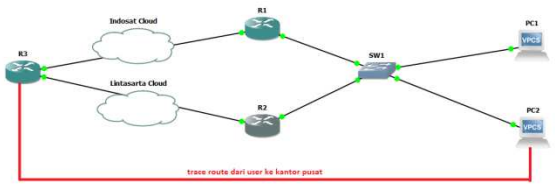
4.1.1. Ujicoba Menggunakan GNS3

Ujicoba unjuk kerja jaringan dilakukan pada jaringan *FastEthernet* yang sudah dibangun dengan GNS3 yang menggunakan *routing protocol* FHRP. Ujicoba unjuk kerja akan dilakukan dengan meng-gunakan skenario–skenario yang didukung oleh GNS3 sebagai berikut :

- Tracert
- Ping
- Fault tolerant

4.1.2 Uji Coba *Tracert*

Perintah *tracert* digunakan untuk mencari jalur yang akan dilalui paket data. *Tracert* menggunakan protokol ICMP (Internet Control Messaging Protocol), ICMP sendiri merupakan protocol yang digunakan jaringan berbasis IP untuk manajemen dan *messaging* antar *device-device* penyusun jaringan. Cara kerja *tracert* adalah dengan mengirim kan ICMP *messages* yang disebut IP *datagrams* dengan parameter waktu yang disebut *timeout*. Nilai dari *timeout* ini akan terus meningkat seiring dengan jumlah *hop* yang dilakukan. Apabila yang dibutuh-kan untuk mencapai alamat yang dituju ini melebihi *timeout*, maka alamat tersebut akan dinyatakan tak dapat dicapai (unreachable). Jaringan yang akan diujicoba dengan perintah *tracert* sama seperti pada gambar 11 namun dimodifikasi dengan ditambahkan *host* berupa PC1. Parameter yang ingin diamati dari pengujian *tracert* ini adalah jumlah *hop* dan *interface* yang dilewati untuk mencapai alamat *interface* yang berada pada *host* tujuan.



Gambar 11. Jaringan untuk ujicoba dengan tracert

Pada pengujian ini perintah *tracert* diketikkan pada *command prompt* dari sebuah *host*, dengan format sebagai berikut:

tracert [alamat IP tujuan]

Contoh tampilan hasil eksekusi perintah tracert yang diketikkan pada command prompt dari host PC1 ditunjukkan pada gambar 12, dimana diperlukan satu kali hop bagi primary router untuk menemukan alamat IP 100.100.100.1.

```
R3#ping 100.100.100.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.100.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R3#traceroute 100.100.100.1

Type escape sequence to abort.
Tracing the route to 100.100.100.1

  1 100.100.100.1 0 msec 0 msec 0 msec
R3#
```

Gambar 12. Tampilan hasil eksekusi perintah tracert

Untuk melihat perbandingan pencarian jalur tempat lewat dengan perintah *tracert* pada protokol FHRP, maka diambil sampel satu *host* yang akan melakukan *tracert* dan *host* tersebut adalah PC1. Host PC1 akan melakukan *tracert* ke *router* yang berada di AXA Tower. Jumlah *hop* dan *interface* yang dilalui oleh PC1 untuk mencapai host tujuan akan ditunjukkan pada gambar 13 berikut:

```
PC1> ping 100.100.100.1
84 bytes from 100.100.100.1 icmp_seq=1 ttl=254 time=46.490 ms
84 bytes from 100.100.100.1 icmp_seq=2 ttl=254 time=46.871 ms
84 bytes from 100.100.100.1 icmp_seq=3 ttl=254 time=46.880 ms
84 bytes from 100.100.100.1 icmp_seq=4 ttl=254 time=46.878 ms
84 bytes from 100.100.100.1 icmp_seq=5 ttl=254 time=46.837 ms

PC1> trace 100.100.100.1
trace to 100.100.100.1, 8 hops max, press Ctrl+C to stop
 1   192.168.1.1   15.978 ms  15.551 ms  15.301 ms
 2   *13.13.13.1   46.878 ms (ICMP type:3, code:3, Destination port unreachable)

PC1>
```

Gambar 13. Tampilan trace route ke AXA Tower

4.1.2 Ujicoba Dengan Ping

Ping merupakan kependekan dari *Packet Internet Groper*. Perintah *ping* digunakan untuk memeriksa ketersambungan sebuah *interface* pada suatu jaringan dengan cara mengirimkan paket data ICMP *echo request* kepada *interface* tersebut lalu menunggu balasan paket data yang disebut ICMP *echo response*. Apabila ICMP *echo response* diterima oleh *interface* pengirim perintah *ping*, maka *interface* yang dikirimi *ping* telah tersambung. Perintah *ping* akan menghasilkan parameter berupa *round trip* dan *packet loss*. *Round trip* merupakan lama perjalanan paket data ICMP *echo request* dari *interface* pengirim sampai *interface* tujuan yang diukur dalam millidetik, sementara *packet loss* merupakan persentase hilangnya paket data (packet loss), nilai *packet loss* 0% menandakan *interface* pengirim dan *interface* tujuan telah tersambung dengan baik. Pengujian *ping* dilakukan sebagai kelanjutan dari pengujian *tracert*, dimana pada pengujian tersebut hanya difokuskan untuk mengetahui jalur yang diambil untuk mencapai PC tujuan, dengan perintah *ping* jalur yang telah ditentukan maka konektivitas *interface* PC tujuan dapat diverifikasi. Pengujian *ping* dilakukan dengan cara mengetikkan perintah *ping* pada *command prompt* dari *host* dengan format sebagai berikut:

ping [alamat IP tujuan]

Contoh hasil eksekusi perintah *ping* yang diketikkan pada *command prompt* dari *host* PC1 ditunjukkan pada gambar 15. Pada Gambar 15 dapat dilihat bahwa PC1 melakukan *ping* kealamat IP 100.100.100.1 dengan paket data sepanjang 32 bytes sebanyak 5 kali dan dari 5 kali pengiriman data, persentase hilangnya paket data (packet loss) adalah sebesar 0%. Lamanya *round trip* adalah 46.598 ms, seperti ditunjukkan pada gambar 14.

```
PC1> ping 100.100.100.1
84 bytes from 100.100.100.1 icmp_seq=1 ttl=254 time=46.912 ms
84 bytes from 100.100.100.1 icmp_seq=2 ttl=254 time=37.997 ms
84 bytes from 100.100.100.1 icmp_seq=3 ttl=254 time=46.878 ms
84 bytes from 100.100.100.1 icmp_seq=4 ttl=254 time=46.887 ms
84 bytes from 100.100.100.1 icmp_seq=5 ttl=254 time=31.249 ms
```

Gambar 14. Hasil *test ping* ke AXA *Tower*

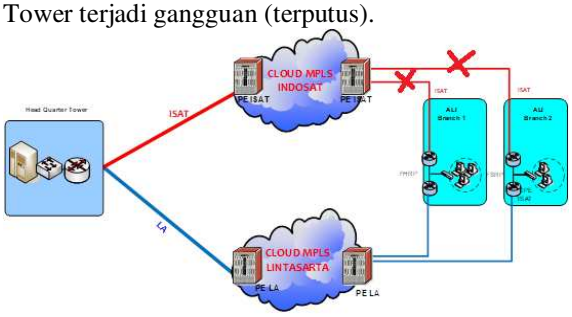
Konektivitas yang baik dinyatakan dengan persentase *packet loss* sebesar 0%, yang berarti paket data ICMP *request* yang dikirim oleh sebuah *host* semuanya diterima oleh *host* tujuan. Uji konektivitas ini akan dilakukan untuk semua *host* yang ada sehingga dapat benar–benar dipastikan bahwa jaringan yang dibangun dapat menghubung kan semua host.

4.1.3 Ujicoba Kemampuan *Fault Tolerant*

Fault tolerant adalah kemampuan jaringan untuk mengatasi gangguan yang dialami saat jaringan tersebut beroperasi secara normal. Kemampuan ini diperlukan sebuah jaringan untuk tetap dapat melayani *user* sambil menunggu kerusakan yang terjadi diperbaiki. Uji coba *fault tolerant* akan dilaksanakan dengan skenario berikut ini. Pertama akan diambil data dari ujicoba *tracert* yang telah dilakukan lebih awal, gunanya untuk mengetahui jalur yang akan dilalui oleh paket data IP datagrams. Setelah itu diadakan ujicoba *tracert*

secara normal untuk memverifikasi jalur yang dipilih untuk sampai ke tujuan. Lalu diadakan uji *tracert* dimana pada saat pengujian sedang berjalan, kabel yang menghubungkan *router* yang akan menjadi jalur dihilangkan sebelumnya *hop*-nya mencapai *router* tersebut. Hal ini akan membuat routing *protocol* harus membuat *routing table* baru karena jalur yang tadinya ada menjadi tidak ada.

Skenario ini mensimulasikan kegagalan yang mungkin terjadi apabila kabel antar *router backbone* tanpa sengaja terputus atau tercabut dari *port Fast Ethernet*. Ilustrasi dari skenario ini dapat ditunjukkan pada Gambar 16, dimana kabel yang mengubungkan antara Router Primary ke AXA Tower terjadi gangguan (terputus).



Gambar 15. Ilustrasi kegagalan jaringan

Skenario kegagalan untuk jaringan dengan protokol FHRP yang akan disimulasikan adalah sebagai berikut :

1. Tracert dari PC user, lalu ditengah berjalannya proses tracert kabel antara Router Secondary dan Router AXA Tower dihilangkan.
2. Tracert dari PC user, lalu ditengah berjalannya proses tracert kabel antara Router Primary dan Router AXA Tower dihilangkan.

4.2. Perbandingan Kemampuan *Fault Tolerant* Pada FHRP

Dari dua skenario kegagalan yang telah didefinisikan, rute alternatif yang dipilih protokol FHRP ditunjukkan pada Gambar 16. Gambar di bawah ini adalah *trace route* dalam keadaan normal ketika belum terjadi gangguan.

```
PC1> trace 100.100.100.1
trace to 100.100.100.1, 8 hops max, press Ctrl+C to stop
 1   192.168.1.1   15.978 ms  15.551 ms  15.301 ms
 2   *13.13.13.1   46.878 ms (ICMP type:3, code:3, Destination port unreachable)

PC1>
PC1>
```

Gambar 16. Trace route dalam keadaan normal

Jika terjadi gangguan maka dari R-*Primary* akan muncul *notification* yang ditunjukan pada Gambar 1.7 yang menunjukan bahwa jalur telah berpindah dari *primary* ke *secondary router*.

```
R1#
*Aug 31 18:32:22.871: %FHRP-5-STATECHANGE: FastEthernet1/0 Grp 1 state Active -> Init
*Aug 31 18:32:23.499: %SYS-5-CONFIG_I: Configured from console by console
R1#
*Aug 31 18:32:24.859: %LINK-5-CHANGED: Interface FastEthernet1/0, changed state to administratively down
*Aug 31 18:32:25.859: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to down
R1#
R2#
*Aug 31 18:31:38.623: %FHRP-5-STATECHANGE: FastEthernet1/0 Grp 1 state Standby -> Active
R2#
```

Gambar 17. Perpindahan Jalur Ke *Secondary Link*

Sehubungan dengan adanya gangguan pada *Router Primary* pada Gambar 17 maka jalur akan otomatis berpindah ke router secondary. Kemudian akan ada *notification* pada *R-Secondary* sebagai berikut:

Setelah jalur berpindah secara otomatis ke *router secondary* lakukan *trace route* pada PC1. Lalu jalur berubah melewati *router secondary*:

```
PC1> trace 100.100.100.1
trace to 100.100.100.1, 8 hops max, press Ctrl+C to stop
 1   192.168.1.2   15.904 ms  15.628 ms  15.624 ms
 2   *23.23.23.1   46.903 ms (ICMP type:3, code:3, Destination port unreachable)

PC1>
```

Gambar 18. Trace Route Dalam Keadaan Fault / Ada Outage

Ketika terjadi perubahan terjadi secara *seamless* atau tidak ada *effect* yang dialami oleh *user* karena perpindahan *routing* yang sangat cepat.

```
PC1> ping 100.100.100.1 -t
84 bytes from 100.100.100.1 icmp_seq=1 ttl=254 time=46.879 ms
84 bytes from 100.100.100.1 icmp_seq=2 ttl=254 time=46.893 ms
84 bytes from 100.100.100.1 icmp_seq=3 ttl=254 time=25.265 ms
84 bytes from 100.100.100.1 icmp_seq=4 ttl=254 time=47.035 ms
84 bytes from 100.100.100.1 icmp_seq=5 ttl=254 time=46.500 ms
84 bytes from 100.100.100.1 icmp_seq=6 ttl=254 time=46.881 ms
84 bytes from 100.100.100.1 icmp_seq=7 ttl=254 time=46.875 ms
84 bytes from 100.100.100.1 icmp_seq=8 ttl=254 time=46.517 ms
84 bytes from 100.100.100.1 icmp_seq=9 ttl=254 time=46.824 ms
84 bytes from 100.100.100.1 icmp_seq=10 ttl=254 time=47.003 ms
84 bytes from 100.100.100.1 icmp_seq=11 ttl=254 time=46.523 ms
84 bytes from 100.100.100.1 icmp_seq=12 ttl=254 time=46.876 ms
84 bytes from 100.100.100.1 icmp_seq=13 ttl=254 time=46.889 ms
84 bytes from 100.100.100.1 icmp_seq=14 ttl=254 time=46.632 ms
84 bytes from 100.100.100.1 icmp_seq=15 ttl=254 time=46.609 ms
84 bytes from 100.100.100.1 icmp_seq=16 ttl=254 time=46.871 ms
84 bytes from 100.100.100.1 icmp_seq=17 ttl=254 time=46.914 ms
84 bytes from 100.100.100.1 icmp_seq=18 ttl=254 time=46.839 ms
84 bytes from 100.100.100.1 icmp_seq=19 ttl=254 time=46.483 ms
84 bytes from 100.100.100.1 icmp_seq=20 ttl=254 time=46.995 ms
84 bytes from 100.100.100.1 icmp_seq=21 ttl=254 time=46.875 ms
84 bytes from 100.100.100.1 icmp_seq=22 ttl=254 time=26.719 ms
```

Gambar 19. Hasil Test Ping Ketika Terjadi Fault/Outage

4.3 Implementasi Pada *Internet Service Provider*

4.3.1 Ujicoba Menggunakan *Provider Indosat* dan *Lintasarta*

Ujicoba unjuk kerja jaringan dilakukan pada jaringan *Fast Ethernet* yang sudah dibangun dengan *provider Indosat* dan *provider* Lintasarta yang menggunakan *routing protocol* FHRP. Ujicoba unjuk kerja akan dilakukan dengan menggunakan skenario–skenario yang sebagai berikut :

- Redaman fiber optic
- Tracert
- Ping
- Latency
- Fault tolerant

4.3.2 Pencarian *Core Fiber Optic* Yang *Available*

Dikarenakan *bandwidth*nya yang besar, untuk link ini infrastrukturnya menggunakan *full link fiber optic* dalam pengaplikasiannya. Pengukuran *fiber optic* dilakukan antara ruang *server* pelanggan dan

node handhole terdekat yang dimiliki oleh PT Indosat dan PT Lintasarta yang dilaksanakan pada hari Selasa, 15 Agustus 2017. Pelaksana pengukuran adalah *team backbone* Indosat dan *backbone* Lintasarta. Pengukuran *fiber optic* didampingi oleh PIC dari sisi pelanggan. Pengukuran yang dilakukan pada *fiber optic* bertujuan untuk mencari *core available* sesuai *standard* yang akan dipakai untuk men*delivered link*. Berikut adalah hasil *survey* dan terminasi *fiber optic* yang dilakukan di sisi Indosat dan di ruang server pelanggan.

Gambar 20. OTB pada sisi pelanggan dan sisi provider

Setelah dilakukan instalasi *fiber optic* pada server BTS dan server pelanggan langkah selanjutnya adalah melakukan pencarian *core* yang *available* dan sesuai standard yang telah ditentukan. Pengukuran yang dilakukan menggunakan *optical power* meter untuk mencari *core* dengan redaman yang paling sesuai. Gambar 21 adalah contoh ketika *team* melakukan pengukuran dalam mencari *core* ter baik yang akan digunakan.

Gambar 21. Hasil pengukuran redaman *fiber optic* di kedua provider

Pencarian *core* telah selesai dilakukan untuk langkah selanjutnya adalah survey rack perangkat di sisi *provider* dan pelanggan. *Survey* ini diperlukan untuk penempatan perangkat *fiber optic* dan *router* setelah semua infrastruktur tersedia.

Gambar 22. Rack di sisi pelanggan dan di sisi provider

Langkah terakhir dari semua rangkaian kegiatan ini adalah installasi *router* di sisi pelanggan. *Router* yang sudah disiapkan untuk *link primary* dan *secondary* segera kita *install* dan uji *performance router* sebelum *router* digunakan. *Device router* dapat dilihat pada gambar 23.

Gambar 23. *Router* pelanggan dan *router provider*

Setelah semua fasilitas siap, *link via provider* Indosat dan *provider* Lintasarta siap digunakan dan diintegrasikan ke kantor pusat di AXA Tower.

4.3.3 Ujicoba *Tracert*

Pada pengujian *trace route* kali ini *trace route* dilakukan dari sisi *router provider* yang mengarah ke AXA Tower. Parameter yang ingin diamati dari pengujian *tracert* ini adalah jumlah hop dan *interface* yang dilewati untuk mencapai alamat *inter face* yang berada pada *host* tujuan ketika jaringan diimplementasikan. Berikut hasil *trace route* yang didapatkan pada kedua *provider* Indosat pada Gambar 24.

```
ID-JKT-ALI-JST-ISAT#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/1       10   130 P Active  local           10.48.104.52    10.48.104.254
ID-JKT-ALI-JST-ISAT#tra
ID-JKT-ALI-JST-ISAT#traceroute 10.48.7.45
Type escape sequence to abort.
Tracing the route to 10.48.7.45
VRF info: (vrf in name/id, vrf out name/id)
  1  *
    10.48.166.169 [AS 4761] 0 msec 0 msec
  2 10.48.6.2 [AS 4761] 0 msec 4 msec 0 msec
  3 10.48.6.1 [AS 4761] 4 msec 0 msec 4 msec
  4 10.48.7.45 [AS 4761] 0 msec *  0 msec
ID-JKT-ALI-JST-ISAT#
```

Gambar 24. Trace route pada provider Indosat

Lakukan hal yang sama pada *provider* Lintas-arta untuk mengetahui jumlah *hop* yang didapat

ISSN : 1410 – 7104

ketika melakukan *trace route* yang akan ditunjukan pada gambar 25.

```
ID-JKT-ALI-JST-LA#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/1       10   100 P Standby 10.48.104.51    local           10.48.104.254
ID-JKT-ALI-JST-LA#traceroute 10.48.7.45
Type escape sequence to abort.
Tracing the route to 10.48.7.45
VRF info: (vrf in name/id, vrf out name/id)
  1 10.48.104.51 0 msec 0 msec 0 msec
  2  *  *
    10.48.166.169 [AS 4761] 4 msec
  3 10.48.6.2 [AS 4761] 4 msec 0 msec 4 msec
  4 10.48.6.1 [AS 4761] 0 msec 4 msec 0 msec
  5 10.48.7.45 [AS 4761] 0 msec *  0 msec
ID-JKT-ALI-JST-LA#
```

Gambar 25. Trace route pada provider Lintasarta

Dikarenakan jumlah *hop* nya yang sedikit, maka *provider* Indosat dijadikan sebagai *primary link* dikarenakan jumlah *hop* nya yang lebih sedikit dengan asumsi *latency* yang semakin bagus juga. Gambar 26 menunjukan bahwa *provider* Indosat telah dipilih sebagai jalur *primary*.

```
ID-JKT-ALI-JST-ISAT#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/1       10   130 P Active  local           10.48.104.52    10.48.104.254
ID-JKT-ALI-JST-ISAT#
```

Gambar 26. Provider Lintasarta sebagai secondary link dengan state standby

4.3.4 Ujicoba Dengan Ping

Setelah semua *link* selesai diintegrasikan dan sudah ditentukan *router primary* dan *secondary*nya untuk langkah selanjutnya adalah melakukan *test ping* dari masing-masing *router* menuju *Router* AXA Tower. Berikut adalah hasil *test ping* yang di lakukan dari *router* pelanggan yang menuju ke arah AXA Tower menggunakan *provider* Indosat:

```
ID-JKT-ALI-JST-ISAT#ping 10.48.7.45 repeat 1000
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 10.48.7.45, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/2/12 ms
ID-JKT-ALI-JST-ISAT#
```

Gambar 27. Test ping menggunakan provider Indosat

Lakukan hal yang sama pada provider Lintas-arta juga sebagai bentuk uji kelayakan jaringan yang sudah diimplementasikan. Pada gambar 28 adalah *test ping* yang dilakukan pada jaringan mengguna kan *link provider* Lintasarta

```
ID-JKT-ALI-JST-LA#ping 10.48.7.45 repeat 1000
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 10.48.7.45, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/2/24 ms
ID-JKT-ALI-JST-LA#
```

Gambar 28. Test ping menggunakan provider Lintasarta

Jika dilihat dari *test ping* kedua *provider*, *latency* terbaik dimiliki oleh Indosat dengan *latency* 1/2/12ms berbanding dengan 1/2/24ms yang dimiliki oleh *provider* Lintasarta. Hal ini membuat pelanggan semakin yakin bahwa *primary link* diputuskan kepada *provider* Indosat.

4.3.5 Ujicoba Kemampuan *Fault Tolerant*

Untuk scenario ujicoba menggunakan *fault tolerant* tidak dapat digunakan karena *link* yang sudah *live* dan digunakan oleh pelanggan. Mengacu pada percobaan *fault tolerant* yang dilakukan pada GNS3 hasil dari *fault tolerant* dapat dipastikan sama karena *command* yang dimasukkan sama. Untuk hasil yang yang didapat pada simulasi GNS3 per-pindahan jalur antara *router primary* ke *secondary* adalah <1 detik. Hal ini sudah memenuhi SLA yang dijanjikan kepada pelanggan dengan *avaibility* 99.80% setiap bulannya atau setelah dikonversi dalam bentuk jam adalah 1 jam 38 menit maksimal *downtime* perbulannya. Sambil menunggu perbaikan *link* jika ada gangguan jaringan *user* masih bisa memakai jaringan karena masih ter-*backup* oleh 1 *router virtual* dan 1 *router secondary* dengan ada-nya fitur FHRP. Hasil perbandingan dari simulasi pada GNS3 dan implementasi dapat dilihat pada tabel 3.

Tabel 3. Perbandingan GNS3 dan Implementasi

	Standard Level Agreement	GNS3	Implementasi
Jumlah Hop	Tergantung infrastructure provider	R1 = 1Hop R2 = 1 Hop	R Primary :4 Hop R Secondary : 5 Hop
Latency	Max. 60ms	R1 = 44/55/80 ms R2 = 48/52/60 ms	R Primary : 1/2/12ms R Secondary : 1/2/24ms
Failover	Max. 60s	< 1 second	< 1 second

5. SIMPULAN

Dari pengujian dan analisis terhadap jaringan Fast Ethernet yang dibangun dengan software GNS3 dan diimplementasikan secara langsung pada branch AXA Jamsostek dapat dijelaskan sebagai berikut :

1) *Routing protocol* FHRP di design agar tidak ter jadi *single point of failure* yang ada di kantor cabang agar *business* tetap berjalan meskipun sempat ada *outage/downtime* pada salah satu *internet service provider*;

2) Dari pengujian *availability/fault tolerant* diketahui bahwa FHRP mempunyai kemampuan untuk mengantisipasi kegagalan yang terjadi pada jaringan *primary* dengan secara otomatis berpindah ke jaringan *secondary* tanpa *user* sadari (<1 second), di bawah *standard failover maximum* 60 *second*;
3) Terdapat perbedaan jumlah *hop* (simulasi 1 *hop* dan implementasi Indosat 4 *hop*, Lintasarta 5 *hop*) hal tersebut disebabkan oleh karena perbedaan infrastruktur di setiap *provider* disamping itu tingginya *latency* pada simulasi GNS3 tergantung pada jenis *device laptop*/komputer yang digunakan saat pengujian. GNS3 membutuhkan RAM yang besar yang ada pada *device* ketika digunakan. Pada sisi *latency* hasil yang didapatkan *provider* Indosat adalah 1/2/12ms lebih baik daripada *provider* Lintasarta yaitu 1/2/24ms. Dari hasil ujicoba kedua provider di atas hasil yang didapat sangat baik karena jauh di bawah *standard latency* yang ditentukan yaitu 60ms;
4) Jaringan membutuhkan *bandwidth* yang sama antara *link primary* dan *secondary* dikarenakan fungsinya agar dapat saling mem-*backup*;
5) Dengan hasil-hasil yang diperoleh telah dibuktikan bahwa *routing protocol* FHRP dapat memenuhi *avaibility* yang diharapkan oleh pelanggan.

DAFTAR PUSTAKA

[1] Ina Minei, Julian Lucek. (2005).”*MPLS-Enabled Applications*”, John Willey & Sons.
[2] Diane Teare, Catherine Paquet. (2005). “*Campus Network Design Fundamentals*”, Cisco Press.
[3] Edi S Mulyanta. (2005). ”*Pengenalan Protokol Jaringan Wireless Komputer*”, Andi Yogyakarta.
[4] Cisco Systems, Inc. (2003).”*Internetworking Technologies Handbook, Forth Edition*”, Cisco Press.
[5] Todd Lammle. (2004). ”*Cisco Certified Network Associate Study Guide, Forth Edition*”, SYBEX Inc.
[6] Gilbert Held. (2003). ”*Ethernet Networks, Forth Edition*”, John Willey & Sons.
[7] Packet Tracer v4.11
[8] Andrew S. Tannenbaum. (2003). ”*Computer Networks*”, Pearson Education, Inc.
[9] Jim Murray. ”*Physical vs Logical Topologies*”. Diakses dari www.giac.org/resources/ whitepaper/network/32.php, pada bulan Juni, 2008.
[10] Harpreet Chadha. ”*Want high availability in Metro Ethernet networks?Resiliency is key*”. Diakses dari http://www.commsdesign.com/ showArticle.jhtml?articleID=189400440 pada bulan Juni 2008.
[11] Iftekhar Hussain. (2004).”*Fault Tolerant IP and MPLS Networks*”, Cisco Press.
[12] Jim Guichard, Ivan Pepelnjak. (2000). ”*MPLS and VPN Architectures*”,Cisco Press.
[13] Martin P. Clark, “*Data Networks*. (2003), “*IP and the Internet*”, John Willey & Sons.