Optimasi Jaringan Komputer Menggunakan Protokol Open *Shortest Path First (OSPF) Berbasis Cisco Router* di Laboratorium Elektro Universitas Pakuan

Oleh :

Agustini Rodiah Machdi

Abstrak

Open Shortest Path First (OSPF) merupakan salah satu jenis dynamic routing protokol yang bekerja secara link-state, mengingat kerja router yang terus menerus dikarenakan kebutuhan akan pertukaran data secara real time, maka pemeliharaan, manajemen routing dan pembagian beban pada redudant router perlu dilakukan, sehingga digunakanlah protokol OSPF ini untuk mengoptimasi jaringan komputer berbasis Cisco Router di Laboratorium Teknik Elektro Universitas Pakuan dengan alat bantu software Cisco Packet Tracer versi 6.0.1.

Pada ujicoba transfer file konfigurasi router dengan protokol TFTP, OSPF dan EIGRP sama-sama mampu untuk melakukan upload dan download. Saat diuji fitur fault tolerant diketahui bahwa OSPF mempunyai kemampuan untuk mengantisipasi kegagalan yang terjadi pada jaringan dengan cara mencari rute alternatif pada saat jalur terpendek tidak memungkinkan untuk dilewati, jadi protokol OSPF sangat layak dijadikan routing protocol untuk backbbone.

Kata kunci : *Router, Protokol, Jaringan Komputer, OSPF, Bit rate, Backbone, Packet Tracer.*

1. PENDAHULUAN

Router merupakan sebuah alat yang berfungsi menghubungkan jaringan berbeda agar bisa melakukan komunikasi antar *device* di dalam jaringan tersebut. Router bekerja dengan cara menentukan jalur yang akan dipilih untuk mengirim paket-paket data dari sumber ke tujuan.

Proses pencarian dan penentuan jalur inilah yang disebut routing sedangkan sekumpulan aturan yang berkerja untuk menentukan dan menjalankan proses routing disebut *routing protokol.*

Open Shortest Path First (OSPF) merupakan salah satu jenis dynamic routing protokol yang bekerja secara link-state, dapat digunakan untuk jaringan dengan skala menengah hingga besar serta memiliki kemampuan administrasi jaringan yang baik karena mampu membagi jaringan besar menjadi beberapa area yang lebih kecil sehingga lebih terstruktur. Sifatnya yang *open standard* membuatnya mampu dikembangkan, diperbaiki, dan digunakan tanpa adanya keterikatan pada satu *vendor* tertentu. Hal inilah yang menjadi ketertarikan untuk lebih mengoptimalkan penggunaan OSPF pada jaringan di Laboratorium Elektro.

1.1 Latar Belakang

Mengingat kerja router yang terus menerus dikarenakan kebutuhan akan pertukaran data secara *real time*, maka pemeliharaan dan pembagian beban pada redudant router perlu dilakukan. Ada tiga metode pembagian beban yaitu *Virtual Router Redudancy Protocol (VRRP), Hot Standby Routing Protocol (HSRP) dan Gateway Load Balancing Protocol (GLBP)*. Diantara ketiga jenis metode pembagian beban pada redudant router tersebut, hanya VRRP yang bersifat open standard. HSRP maupun GLBP merupakan teknologi yang hanya bisa digunakanpada router Cisco seri tertentu. Ketiganya memiliki perbedaan dalam hal pemanfaatan sumber daya dan cara kerja. Sama seperti *routing protokol*, metode pembagian beban pada router ini memiliki kelebihan dan kekurangannya masing-masing, tergantung dari bandwidth, ketersediaan alat, jumlah data loss, serta dukungan pada saat koneksi terputus.

1.2. Maksud dan Tujuan

Tujuan dari penelitian ini adalah untuk mengoptimasi jaringan komputer menggunakan protokol routing OSPF berbasis *Cisco Router* di Laboratorium Teknik Elektro Universitas Pakuan.

1.3. Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut :

1) Penggunaan routing management dengan menggunakan routing protokol OSPF berbasis Cisco Router.
2) Konfigurasi dan uji kerja dilakukan dengan menggunakan simulator Packet Tracer versi 6.0.1, tidak diaplikasikan secara langsung pada jaringan internal Laboratorium Elektro Universitas Pakuan;

1.4. Metode Penelitian

Metode penelitian yang digunakan terdiri 4 komponen pendukung, setiap komponen tersebut akan dijabarkan berikut ini.

1.4.1. Tempat dan Waktu Penelitian

Tempat penelitian di Laboratorium Teknik Elektro Universitas Pakuan Bogor, waktu penelitian dilaksanakan pada tenggang waktu antara bulan September 2012 sampai Juni 2013

1.4.2. Bahan dan Peralatan

Bahan dan Alat yang digunakan dalam penelitian ini adalah alat tulis menulis, laptop, printer, switch layer 3, cisco router, serta jaringan internet. Untuk *Software* digunakan *Cisco Packet Tracer Version* 6.0.1.

1.4.3. Prosedur Penelitian

Prosedur penelitian terdiri dari 4 tahap *Network Development Life Cycle* (NDLC). Adapun tahapan- tahapan tersebut adalah :

1) Analisa, observasi dan survey, yaitu mengamati secara langsung mengenai sistem yang sedang dijalankan, peralatan pendukung serta permasalahan yang dihadapi selama berjalannya sistem yang sedang digunakan,
2) Studi pustaka dan membaca dokumentasi, yaitu mencari dan mengumpulkan bahan-bahan yang berkaitan dengan routing protocol dan router redudancy berupa cara kerja, peralatan pendukung, serta konfigurasinya. Dan mencari informasi mengenai jaringan dari dokumentasi yang pernah dibuat.
3) Desain jaringan, yaitu membuat rancangan jaringan yang bertujuan memperbaiki struktur topologi yang sudah sering digunakan sebelumnya, dan pemilihan teknologi yang akan diterapkan.
4) Simulasi dan prototyping setelah menganalisa dan mendapatkan desain jaringan berikut teknologi routing protocol yang akan digunakan, hal selanjutnya adalah membuat prototype dari jaringan yang baru. Prototype tersebut dibuat menggunakan software simulator Cisco Packet Tracer versi 6.0.1. Hasil pengujian performa jaringan yang diperoleh akan dibandingkan dengan jaringan yang sedang digunakan untuk mengetahui sampai sejauh mana optimasi yang dapat dilakukan.

1.4.4. Evaluasi Data

Evaluasi data ini dilakukan terhadap simulasi sistem jaringan yang baru berdasarkan kriteria yang telah disusun, sehingga dapat mengetahui sejauh mana tujuan awal telah dicapai.

2. TEORI LANDASAN

Jaringan komputer merupakan gabungan antara teknologi komputer dan teknologi telekomunikasi. Gabungan teknologi ini melahirkan pengolahan data yang dapat didistribusikan, mencakup pemakaian database, software aplikasi dan peralatan hardware secara bersamaan, sehingga pengguna komputer yang sebelumnya hanya berdiri sendiri, kini telah diganti dengan sekumpulan komputer yang terpisah – pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya, sistem seperti ini disebut jaringan komputer *(computer network)*.

2.1. Klasifikasi Jaringan Komputer

Jenis jaringan komputer terdapat dua klasifikasi yang sangat penting yaitu teknologi transmisi dan jarak. Secara garis besar, terdapat dua jenis teknologi transmisi yaitu jaringan broadcast dan jaringan point to point. Jaringan broadcast memiliki saluran komunikasi tunggal yang dipakai bersama-sama oleh semua mesin yang ada pada jaringan. Berdasarkan dari jaraknya pertama adalah dataflow machine, komputer-komputer yang sangat paralel yang memiliki beberapa unit fungsi yang semuanya bekerja untuk program yang sama. Kemudian multicomputer, sistem yang berkomunikasi dengan cara mengirim pesan-pesannya melalui bus pendek dan sangat cepat. Setelah kelas multicomputer adalah jaringan sejati, komputer-komputer yang bekomunikasi dengan cara bertukar data/pesan melalui kabel yang lebih panjang. Jaringan seperti ini dapat dibagi menjadi local area network (LAN), metropolitan area network (MAN), dan *wide area network* (WAN).

Akhirnya, koneksi antara dua jaringan atau lebih disebut *internetwork*. Internet merupakan salah satu contoh yang terkenal dari suatu *internetwork*.

2.2. Komponen Jaringan Komputer

Jaringan terdiri dari beberapa komponen dasar yang meliputi komponen *hardware* dan *software*. Penggunaan komponen sendiri akan sangat tergantung dengan topologi jaringan yang di gunakan, tidak semua komponen akan di pasang pada sebuah tipologi.

2.3. Tipologi Jaringan Komputer

Topologi adalah bentuk koneksi fisik untuk menghubungkan sebuah node pada setiap jaringan. Pada sistem LAN terdapat tiga tipologi utama yang paling sering digunakan yaitu tipologi *bus, ring dan star.*

Topologi jaringan ini kemudian berkembang menjadi tipologi *tree, mesh, dan topologi wireless.*

2.4. Model OSI layer dan Protocol (TCP/IP)

Model referensi OSI terdiri atas lapisan berjumlah 7 buah (layer) yaitu :

1) *Physical*
2) *Data Link*
3) *Network*
4) *Transport*
5) *Session*
6) *Presentation*
7) *Application*

Sedangkan Protokol TCP/IP hanya memiliki empat layer, yaitu:

1) *Network Interface layer atau Physical layer*
2) *Internetworking layer atau internet layer*
3) *Host-to-host layer atau Transport layer*
4) *Aplication Layer*

2.5. IP address Public dan IP Address Private

IP address yang digunakan untuk keperluan LAN/intrenet disebut sebagai IP address private (tabel 1). Sedangkan IP address yang digunakan untuk keperluan internet disebut IP address public. Secara umum, IP address dapat dibagi menjadi 5 kelas, Kelas A, B, C, D, E. Namun dalam praktiknya hanya kelas A, B, dan C yang dipakai untuk keperluan umum. Ketiga kelas IP address ini disebut *IP address unicast.*

IP address kelas D dan E digunakan untuk keperluan khusus. IP address kelas D disebut juga *IP address multicast*. Sedangkan IP address kelas E digunakan untuk keperluan riset.

IP address (kelas A, B, dan C) dapat dipisahkan menjadi 2 bagian, yakni bagian network (bit-bit networks/networks bit) dan bagian host (bit-bit host/host bits). Network bit berperan sebagai pembeda antar-network atau identifikasi (ID) network. Sedangkan host bit berperan sebagai identifikasi (ID) host. Semua host yang terhubung pada network yang sama, pasti akan memiliki network bit yang sama juga.
Dengan servis yang menerjemahkan IP address private ke IP address public, host pada sebuah jaringan IP address private (contoh LAN) bisa mengakses ke jaringan internet. Servis ini disebut *Network Address Translation* (NAT). Diimplementasikan pada jaringan yang bisa mengakses internet.

2.6. Protokol OSPF

OSPF dikembangkan menggunakan algoritma Dijkstra's Shortest Path First (SPF). Protokol Link State (LS) dapat mengetahui kondisi network secara lebih akurat. Masing-masing router memiliki gambaran jelas tentang topologi network, termasuk juga info bandwith dari network lainnya. Beberapa hal yang menjadi karakteristik LS yaitu :

- Dapat merespon dengan cepat terhadap perubahan *network*.
- Mengirim update ketika terjadi perubahan pada *network*.
- Mengirim update secara periodic pada interval tertentu, yang disebut dengan *link state refresh*.

Untuk mengurangi perhitungan SPF, maka protokol OSPF perlu mempartisi network menjadi beberapa area. Berikut ini ada beberapa area yang terkait dengan network OSPF :

1) Backbone area, yaitu area 0 dan terhubung dengan setiap area
2) Regular area, yaitu nonbackbone area, database-nya berisi daftar *rute network internal* dan *network eksternal*.
3) Stub area, yaitu area yang database-nya hanya berisi *rute network* internal dan sebuah rute default.
4) Totally Stuby Area, yaitu merupakan area khusus yang diperuntukan bagi perangkat Cisco. Database-nya berisi rute untuk areanya sendiri dan sebuah rute default.
5) NSSA (Not-So-Stuby Area), yaitu area yang database-nya berisi rute internal dan sebuah optional rute default. Rute-rute didistribusikan ulang dari sebuah proses routing yang terkoneksi.
6) Totally NSSA, yaitu area yang sama dengan NSSA hanya saja didesain untuk perangkat Cisco.

3. PERANCANGAN JARINGAN

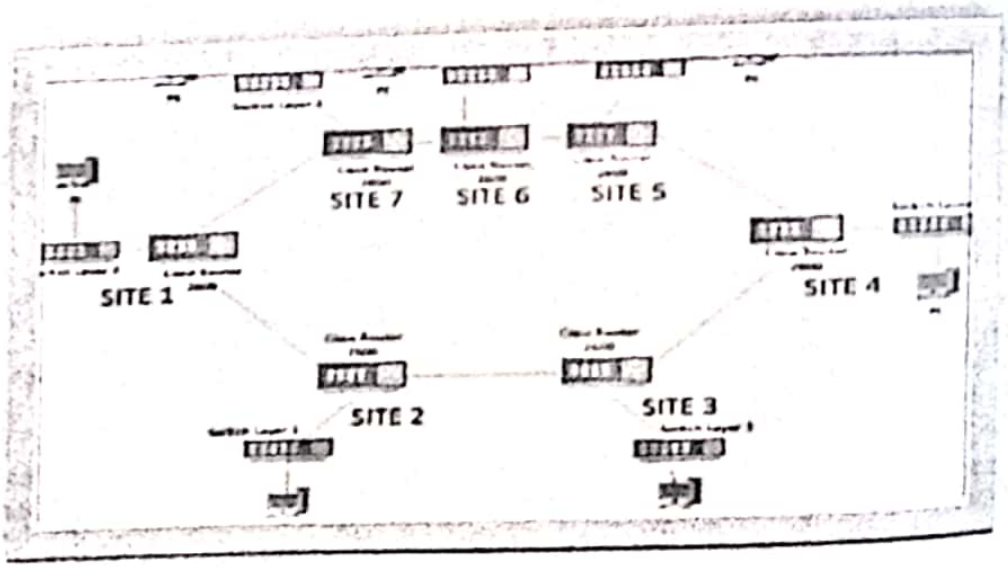
Langkah – langkah yang untuk mendesain jaringan yang akan mendukung protokol OSPF dan EIGRP adalah sebagai berikut :

1) Mendesain jaringan logika
2) Mengimplementasikan dengan software, dengan software yang digunakan pada penelitian ini adalah *Cisco Packet Tracer versi* 6.0.1

3.1. Mendesain Jaringan Logika

Jaringan logika jaringan hanya memfokuskan pada konektivitas secaralogika dan tidak memperhitungkan hal-hal yang menunjang konektivitas secarafisik, misalnya panjang kabel yang digunakan. Jaringan logika dibuat untukmemberikan gambaran tentang seperti apa jaringan yang akan dibangun nantinya.

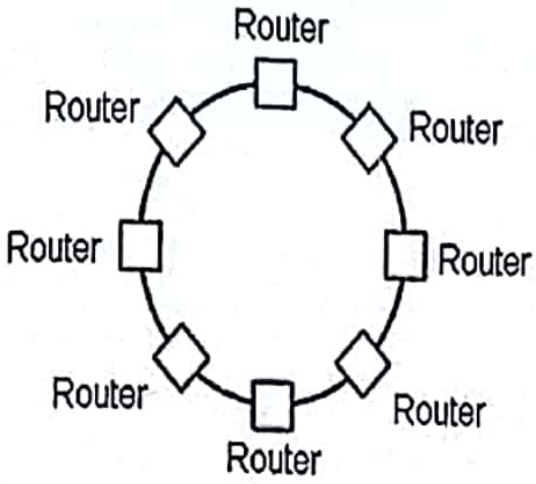
Dalam penelitian ini akan dihubungkan 7 site, dimana masing-masing site mempunyai satu router backbone sebagai *gateway* jaringan *site* itu sendiri.



Gambar 3.1. Desain Jaringan Logika

Gambar 3.1 memperlihatkan desain jaringan logika yang menghubungkan titik-titik (site-site) dengan menggunakan router-router yang disusun dengan tipologi ring.

Pada tahapan desain ini yang dipentingkan adalah pengaplikasian topologi yang telah dipilih beserta *divais-divais* yang ingin digunakan.



Gambar 3.2 Topologi Ring

Pengaplikasian topologi ring dapat dilihat dari koneksi antar router-router yang ditempatkan di lokasi-lokasi router yang berbentuk looptertutup seperti yang terlihat pada gambar 3.2.

Router-router yang tersusun dengan topologi ring tersebut akan bertindak sebagai backbone. Penempatan switch sebagai divais perantara antarahost dengan router dimaksudkan sebagai pembagi koneksi, dalam hal ini *koneksiFast Ethernet* yang *interface-nya* terdapat pada router. Dengan susunan seperti ini, *router* pada satu titik site bertindak sebagai *gateway.*

3.2. Pembangunan Jaringan

Langkah-langkah awal pengimplementasian dengan menggunakan *software* adalah sebagai berikut :

1) Memilih *divais* yang mendukung protokol yang akan dipakai dan menentukan penghubung antar divais
2) Mengalokasikan IP untuk port-port divais pada jaringan dan host-host.

Setelah langkah-langkah awal dilakukan maka jaringan siap dikonfigurasi

3.2.1. Pemilihan Divais

Untuk membuat jaringan yang dapat mendukung penggunaan routing protocolOSPF dan EIGRP dan dapat diujicoba, digunakan divais-divais berikut :

1) Komputer (PC)
   Komputer ini berfungsi untuk mewakili host-host pada site-site yang akan mengakses jaringan.

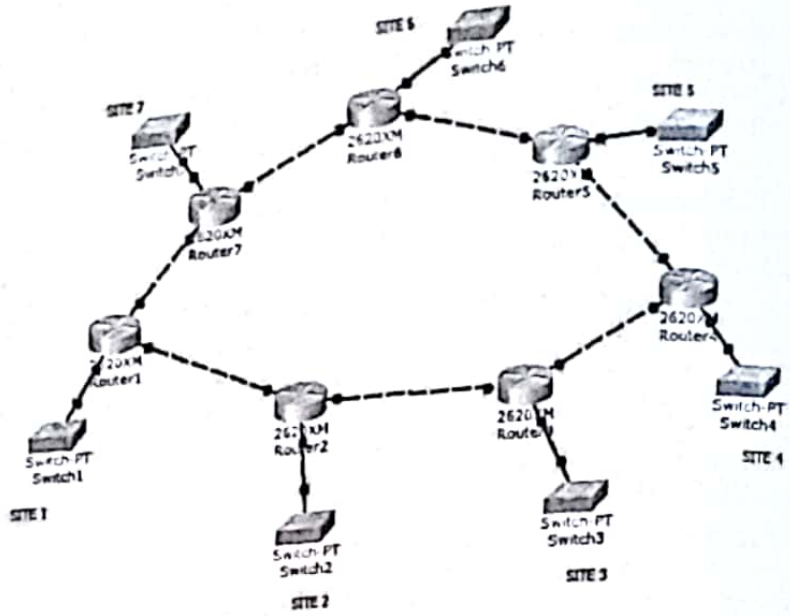
2) Switch
   Berfungsi sebagai divais untuk membagi koneksi dari backbone ke host-host, hal ini dilakukan untuk efisiensi. Switch yang digunakan adalah *Allied Telesys AT-8326GS*

3) Router
   Untuk membuat jaringan backbone OSPF dan EIGRP, router yang dipilihadalah router Cisco tipe 2600 Series dengan modul *Fast Ethernet.*

   Pemilihan modul FastEthernet ini dilakukan untuk mengakomodasi keperluan akan backbone yangingin dibangun dengan koneksi *Fast Ethernet.*

4) Pengkabelan
   Digunakan kabel RJ-45 dengan konfigurasi *straight-through* dan crossover untuk menghubungkan *interface Fast Ethernet* .

Setelah pemilihan divais-divais penyusun jaringan dilakukan, maka desain jaringan logika seperti yang ditunjukkan pada Gambar 3.1akandirealisasikan dengan menngunakan software simulasi Packet Tracer v6.0.1. Gambar 3.3 memperlihatkan jaringan yang dibangun dengan menggunakan *Packet Tracer v6.*0.1 dengan menggunakan divais – divais yang sudah dipilih.



Gambar 3.3 Desain Jaringan Menggunakan Packet Tracer

Gambar 3.3 menunjukan hubungan antar router dilakukan dengan menggunakan kabel RJ-45 yang akan menghubungkan *interface Fast Ethernet* dengan yang dapat mendukung *bandwidth sampai dengan 100 Mbps [5].* Koneksi yang dilakukan pada antar routerdilakukan dengan kabel crossover yang diwakili garis hitam putus - putus dan koneksi antara router ke switch dan switch ke PC dilakukan memakai kabel RJ-45dengan konfigurasi straight-through yang diwakili garis hitam lurus [5]. Gambar 3.3 dapat dilihat, pada *router-router backbone*, misal router di Site 1.

3.2.2. Pengalokasian IP

Pengalokasian alamat IP untuk interface sebuah router harus direncanakandengan baik agar dapat menghubungkan router dan tetap efisien dalampenggunaan sumber daya berupa alamat IP. Tabel 3.3 memperlihatkan distribusialamat IP untuk interface-interface yang ada pada router.

Alokasi IP dipilih berdasarkan karakteristik dari router dimana pada padakoneksi pada interface suatu router ke router lain harus berada pada subnet yangsama [5]. Sebagai contoh, port Fast Ethernet 1/0 dari Router1 dengan alamat IP10.100.101.1 dihubungkan dengan Fast Ethernet 1/0 dari Router2 dengan alamatIP 10.100.101.2, dimana kedua alamat ini berada pada satu subnet .

Pengalokasian IP berikutnya dilakukan untuk host yang berada pada masing-masing lokasi. Tabel 3.4 menunjukkan alokasi alamat IP pada masing-masing site. Pengalamatan IP di masing-masing lokasi disesuaikan dengan jumlah host yang ada. Hal ini dilakukan untuk mengefisiensikan penggunaan sumber daya berupa alamat IP.

Tabel 3.1 Distribusi alamat IP untuk interface
–
interface router

Nama router	Fast Ethernet 1/0	Fast Ethernet1/1	Fast Ethernet 0/0
Router1	10.100.101.1/29	10.100.101.50/29	192.168.101.1/29
Router2	10.100.101.2/29	10.100.101.9/29	192.168.101.9/29
Router3	10.100.101.17/29	10.100.101.10/29	192.168.101.17/29
Router4	0.100.101.18/29	10.100.101.25/29	192.168.101.49/29
Router5	10.100.101.33/29	10.100.101.26/29	192.168.101.65/28
Router6	10.100.101.34/29	10.100.101.41/29	192.168.101.129/26
Router7	10.100.101.49/29	10.100.101.42/29	192.168.101.225/29

3.2.3. Konfigurasi dengan Protokol OSPF dan EIGRP

Konfigurasi akan dilakukan dengan menggunakan IOS command pada router-router yang menjadi backbone. IOS command sendiri merupakan bahasa

pemrogaman yang digunakan untuk mengkonfigurasi divais-divaisjaringan.

3.2.4. Konfigurasi dengan protokol OSPF

Berikut ini adalah konfigurasi OSPF sekaligus pengalokasian alamat IPuntuk interface - interface yang dilakukan untuk router-router yang menyusun backbone. Perintah – perintah konfigurasi ini diketikkan pada CLI dari router.
Contoh command line interface (CLI) konfigurasi pada Router1 :

```
Router1>ena Router1#conf t
Router1(config)#inter fa1/0
Router1(config-if)#ip        add        10.100.101.1
255.255.255.248
Router1(config-if)#no shut
Router1(config-if)#inter fa1/1
Router1(config-if)#ip        add        10.100.101.50
255.255.255.248
Router1(config-if)#no shut
Router1(config-if)#inter fa0/0
Router1(config-if)#ip        add        192.168.101.1
255.255.255.248
Router1(config-if)#no shut
Router1(config-if)#router ospf 1
Router1(config-router)#netw  10.100.101.0  0.0.0.7
area 0
Router1(config-router)#netw  10.100.101.48  0.0.0.7
area 0
Router1(config-router)#netw  192.168.101.1  0.0.0.7
area 0
Router1(config-router)#^Z
```

3.2.5. Konfigurasi dengan protokol EIGRP

Konfigurasi EIGRP lebih mudah dari pada OSPF karena hanya subnet untuk network – network tidak perlu dispesifikasikan satu persatu. Berikut ini adalah konfigurasi di dua lokasi, yaitu di site 1 dan site 2. Hanya diberikan konfigurasi pada dua site ini karena konfigurasi pada router site-site yang lain akan sama dengan konfigurasi kedua router site ini

1. Konfigurasi router site 1

```
Router1>ena
Router1#conf t
Router1(config-router)# router eigrp 1
Router1(config-router)#                netw
192.168.101.0
Router1(config-router)# netw 10.0.0.0
Router1(config-if)#no auto-summary
Router1(config-router)#^Z
```

2. Konfigurasi router site 2

```
Router2>ena
Router2#conf t
Router2(config-router)# router eigrp 1
Router2(config-router)#                netw
192.168.101.0
Router2(config-router)# netw 10.0.0.0
Router2(config-if)#no auto-summary
Router2(config-router)#^Z
```

4. SKENARIO PEMGUJIAM

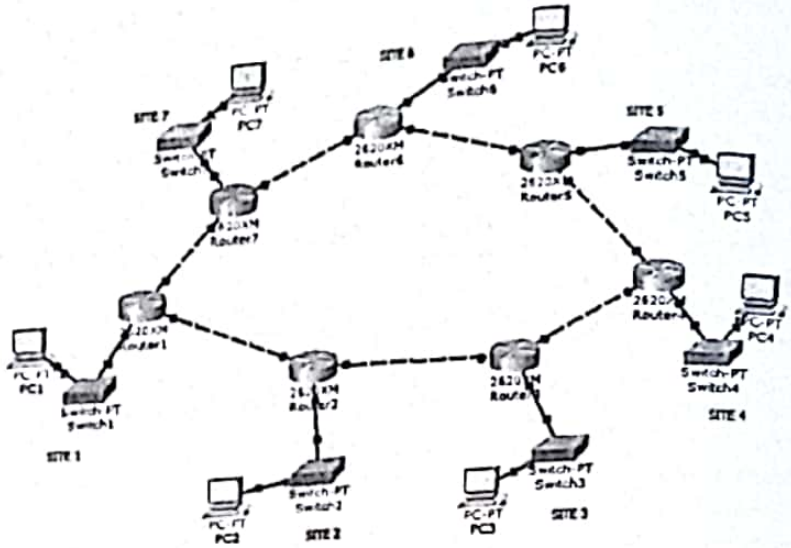
Ujicoba unjuk kerja jaringan dilakukan pada jaringan Fast Ethernet yangsudah dibangun dengan Packet Tracer v.6.0.1 yang menggunakan routing protocolOSPF dan EIGRP. Ujicoba unjuk kerja akan dilakukan dengan menggunakan skenario-skenario yang didukung oleh Packet Tracer v6.0.1 sebagai berikut :

- Tracert
- Ping
- Akses internet
- Fault tolerant

4.1. Ujicoba Tracert

Perintah tracert digunakan untuk mencari jalur yang akan dilalui paketdata. Tracert menggunakan protokol ICMP (Internet Control Messaging Protocol), ICMP sendiri merupakan protokol yang digunakan jaringan berbasis IP untuk manajemen dan messaging antar divais-divais penyusun jaringan. Carakerja tracert adalah dengan mengirimkan ICMP messages yang disebut IPdatagrams dengan parameter waktu yang disebut timeout. Nilai dari timeout ini akan terus meningkat seiring dengan jumlah hop yang dilakukan. Apabila yang dibutuhkan untuk mencapai alamat yang dituju ini melebihi timeout, maka alamat tersebut akan dinyatakan tak dapat dicapai (unreachable) [5].

Jaringan yang akandiujicoba dengan perintah tracert sama seperti yang terlihat pada Gambar 4.1 dimana pada desain tersebut sudah ditambahkan PC pada tiap site untuk dilakukan uji coba jaringan. Pada pengujian ini, host pada satu site akan menggunakan tracert untuk mencari jalur menuju host pada site lain.



Gambar 4.1 Desain Jaringan Siap Uji Coba

Tabel 4.1 menunjukkan alamat IP dan lokasi host. Parameter yangingin diamati dari pengujian tracert ini adalah jumlah hop dan interface yangdilewati untuk mencapai alamat interface yang berada pada host tujuan.

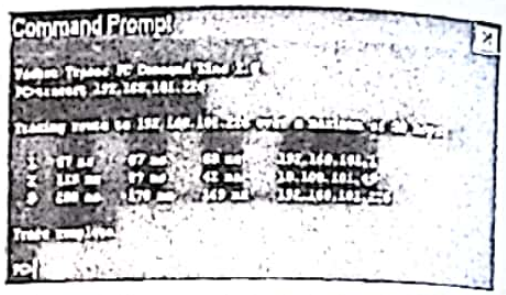
Tabel 4.1. Daftar alamat IP untuk host di masing-masing lokasi

No	Lokasi	Nama Host	Alamat IP
1	Site 1	PC1	192.168.101.2
2	Site 2	PC2	192.168.101.10
3	Site 3	PC3	192.168.101.18
4	Site 4	PC4	192.168.101.50
5	Site 5	PC5	192.168.101.66
6	Site 6	PC6	192.168.101.130
7	Site 7	PC7	192.168.101.226

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

tracert [alamat IP tujuan]

Contoh tampilan hasil eksekusi perintah tracert yang diketikkan pada commandprompt dari host PC1 ditunjukkan pada Gambar 4.2, dimana diperlukan tiga kalihop bagi PC1 untuk menemukan alamat IP 192.168.101.226.



Gambar 4.2. Tampilan hasil eksekusi perintah tracert

4.1.1. Perbandingan *tracert* pada OSPF dan EIGRP

Untuk melihat perbandingan pencarian jalur tempat lewat dengan perintahtracert pada protokol OSPF dan EIGRP, maka diambil sampel dua host yang akanmelakukan tracert. Dua host tersebut adalah PC1 dan PC4. Host PC1akanmelakukan tracert ke PC2, PC3, PC4, PC5, PC6, dan PC7. Sementara itu PC4akan melakukan traceorute ke PC5, PC6, PC7, PC1, PC2, dan PC3.

Jumlah hop dan interface yang dilalui oleh PC1 untuk mencapai host tujuan akanditunjukkan pada Tabel 4.2, Tabel 4.3, Tabel 4.4, Tabel 4.5, Tabel 4.6, dan Tabel4.7. Sementara jumlah hop dan interface yang dilewati PC4 untuk mencapai hosttujuan ditunjukkan pada Tabel 4.8, Tabel 4.9, Tabel 4.10, Tabel 4.11, Tabel 4.12,dan Tabel 4.13.

Tabel 4.2. Tracert dari PC1 ke PC2

OSPF		EIGRP	
hop	*Interface* yang dilewati	*hop*	*Interface* yang dilewati
1	192.168.101.1	1	192.168.101.1
2	10.100.101.2	2	10.100.101.2
3	192.168.101.10	3	192.168.101.10

Tabel 4.3. Tracert dari PC1 ke PC3

OSPF		EIGRP	
hop	*Interface* yang dilewati	*hop*	*Interface* yang dilewati
1	192.168.101.1	1	192.168.101.1
2	10.100.101.2	2	10.100.101.2
3	10.100.101.2	3	10.100.101.2
4	192.168.101.18	4	192.168.101.18

Tabel 4.4. Tracert dari PC1 ke PC4

OSPF		EIGRP	
hop	*Interface* yang dilewati	*hop*	*Interface* yang dilewati
1	192.168.101.1	1	192.168.101.1
2	10.100.101.2	2	10.100.101.2
3	10.100.101.10	3	10.100.101.10
4	10.100.101.18	4	10.100.101.18
5	192.168.101.50	5	192.168.101.50

Tabel 4.5. Tracert dari PC1 ke PC5

OSPF		EIGRP	
hop	*Interface* yang dilewati	*hop*	*Interface* yang dilewati
1	192.168.101.1	1	192.168.101.1
2	10.100.101.49	2	10.100.101.49
3	10.100.101.41	3	10.100.101.41
4	10.100.101.33	4	10.100.101.33
5	192.168.101.66	5	192.168.101.66

Tabel 4.6. Tracert dari PC1 ke PC6

OSPF		EIGRP	
hop	*Interface* yang dilewati	*hop*	*Interface* yang dilewati
1	192.168.101.1	1	192.168.101.1
2	10.100.101.49	2	10.100.101.49
3	10.100.101.41	3	10.100.101.41
4	192.168.101.130	4	192.168.101.130

Tabel 4.7. Tracert dari PC1 ke PC7

OSPF		EIGRP	
hop	*Interface* yang dilewati	*hop*	*Interface* yang dilewati
1	192.168.101.1	1	192.168.101.1
2	10.100.101.49	2	10.100.101.49
3	192.168.101.226	3	192.168.101.226

Tabel 4.8. Tracert dari PC4 ke PC5

OSPF		EIGRP	
hop	*Interface* yang dilewati	*hop*	*Interface* yang dilewati
1	192.168.101.49	1	192.168.101.49
2	10.100.101.26	2	10.100.101.26
3	192.168.101.66	3	192.168.101.66

Tabel 4.9. Tracert dari PC4 ke PC6

OSPF		EIGRP	
hop	*Interface* yang dilewati	*hop*	*Interface* yang dilewati
1	192.168.101.49	1	192.168.101.49
2	10.100.101.26	2	10.100.101.26
3	10.100.101.34	3	10.100.101.34
4	192.168.101.66	4	192.168.101.66

Tabel 4.10. Tracert dari PC4 ke PC7

OSPF		EIGRP	
hop	*Interface* yang dilewati	*hop*	*Interface* yang dilewati
1	192.168.101.49	1	192.168.101.49
2	10.100.101.26	2	10.100.101.26
3	10.100.101.34	3	10.100.101.34
4	10.100.101.42	4	10.100.101.42
5	192.168.101.226	5	192.168.101.226

Tabel 4.11 Tracert dari PC4 ke PC1

OSPF		EIGRP	
hop	Interface yang dilewati	hop	Interface yang dilewati
1	[illegible]	1	[illegible]
2	[illegible]	2	[illegible]
3	[illegible]	3	[illegible]
4	[illegible]	4	[illegible]
5	[illegible]	5	[illegible]

Tabel 4.12 Tracert dari PC4 ke PC2

OSPF		EIGRP	
hop	Interface yang dilewati	hop	Interface yang dilewati
1	[illegible]	1	[illegible]
2	[illegible]	2	[illegible]
3	[illegible]	3	[illegible]
4	[illegible]	4	[illegible]

Tabel 4.13 Tracert dari PC4 ke PC3

OSPF		EIGRP	
hop	Interface yang dilewati	hop	Interface yang dilewati
1	192.168.101.49	1	[illegible]
2	10.100.101.17	2	[illegible]
3	192.168.101.33	3	[illegible]

Dari hasil pengujian tracert yang dapat dilihat dari pada Tabel 4.2 sampai dengan Tabel 4.13 dapat dilihat bahwa baik OSPF maupun EIGRP memilih jalur interface yang sama dan mempunyai jumlah hop yang sama pula dalam mencapai suatu alamat tujuan.

Jalur yang diambil oleh protokol OSPF dan EIGRP merupakan jalur terpendek dalam mencapai tujuan, contohnya pada Tabel 4.11dapat dilihat bahwa saat PC4 bermaksa mencapai *PC1*, jumlah *hop* yang dilakukan adalah 5 kali.

Pada hop pertama, paket IP data gramz melewati interface 192.168.101.49 yang merupakan port Fast Ethernet Router4. Paket lalu bergerak melewati interface 10.100.101.17, 10.100.101.9, dan 10.100.101.1 yang masing-masing merupakan port Fast Ethernet Router3, Router2, dan Router1. Lalu pada hop kelima IP data gramz sampai ke alamat yang dituju.

Dengan merujuk pada Gambar 4.1, maka secara visual jalur terpendek yang antara PC4 dan PC1 adalah melewati *Router 3, Router 2, dan Router 1*. Hal ini sesuai dengan jalur yang digunakan protokol OSPF dan EIGRP untuk mencapai PC 1, sehingga untuk pengujian ini dapat disimpulkan bahwa OSPF dan EIGRP dapat diaplikasikan dijaringan karena dapat memilih jalur paling pendek untuk mencapai tujuan.

4.2. Uji Coba Dengan Ping

Ping merupakan kependekan dari Packet Internet Grouper. Perintah ping digunakan untuk memeriksa keterseambungan sebuah interface pada suatu jaringan dengan cara mengirimkan paket data ICMP echo request kepada interface tersebutlalu 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 terseambung.

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 interfacetujuan yang diukur dalam milli detik, sedangkan packet loss merupakan persentase hilangnya paket data (packet loss), nilai packet loss 0% menandakan interface pengirim dan interface tujuan telah terseambung dengan baik [3].

Pengujian yang dilakukan sebagai kelanjutan dari pengujian tracert, dimana pada pengujian tersebut hanya dilakukan untuk mengetahui jalur yang diambil untuk mencapai PC tujuan, dengan perintah ping jalur yang telah ditentukan maka koneksi/sinn 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]

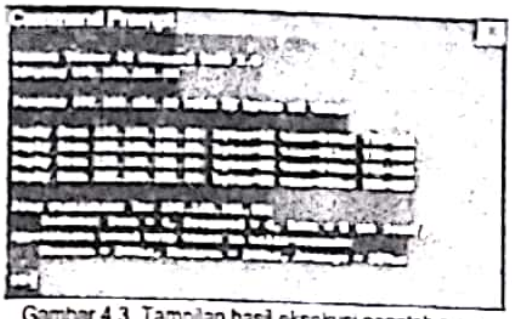
Contoh hasil *eksekusi* perintah ping yang diketikkan pada command prompt dari host PC2 ditunjukkan pada Gambar 4.3.

Pada Gambar 4.3 dapat dilihat bahwa PC1 melakukan ping kealamat IP 192.168.101.66

dengan paket data sepanjang 32 bytes sebanyak 4 kali. Dan dari 4 kali pengiriman data, persentase hilangnya paket data (packet loss) adalah sebesar 0%. Lamanya round trip rata-rata adalah 227 ms, seperti ditnjukkan pada Gambar 4.3 dengan panah berwarna putih.

Jaringan yang digunakan untuk pengujian ping ini sama dengan jaringan yang ditunjukkan pada Gambar 4.1, dan parameter yang akan diamati pada pengujian ini adalah *konektivitas*.

Konektivitas yang baik dinyatakan dengan persentase packet loss sebesar 0% , yang berarti paket data ICMP request yang dikirim olehsebuah 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 menghubungkan host yang berada pada masing-masing site.



Gambar 4.3. Tampilan hasil eksekusi perintah ping oleh PC2

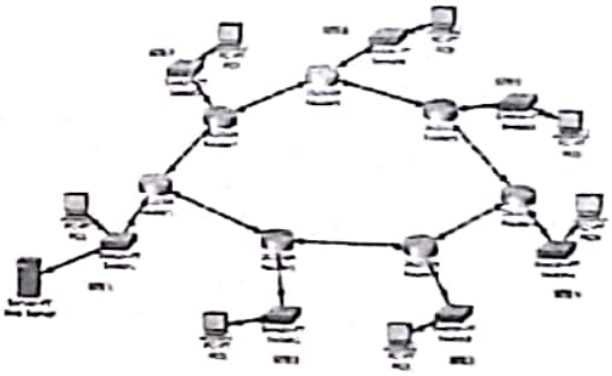
4.2.1. Hasil pengujian ping pada OSPF dan EIGRP

Hasil pengujian ping antara seluruh host yang berada di masing-masing site ditunjukkan pada Tabel 4.14. Hasil pengujian ini disajikan hanya dengan menggunakan satu tabel sebab dari pengujian yang dilakukan didapatkan hasil bahwa semua host pada telah tersambung satu sama lain sehingga dapat disimpulkan bahwa jaringan telah dikonfigurasi dengan benar sehingga syarat konektivitas antar host telah dapat dipenuhi. Pada Tabel 4.14 dapat dilihat bahwa ping antar host telah berhasil dan ditandai dengan "OK".

Tabel 4.14. Ping antar host dengan protokol OSPF dan EIGRP

4.3. Ujicoba Akses Internet

Ujicoba akses internet dilakukan dengan cara pengaksesan halaman web berbasis HTTP dan pengunaan protokol TFTP untuk melakukan upload dan download file. HTTP merupakan protokol pada application layer yang memungkinkan sebuah halaman web terdiri dari gabungan file-file teks dan gambar yang beragam sehingga menghasilkan sebuah halaman web yang dapat menampilkan informasi dengan penampilan yang menarik. TFTP merupakan protokol yang digunakan untuk melakukan upload dam download file ke sebuah server. Pada aplikasi untuk jaringan Fast Ethernet yang sedang diuji coba, TFTPakan menjadi protokol yang mengakomodasi penyimpanan konfigurasi router disebuah server yang ditempatkan di site 1. Parameter yang akan dibandingkan antara jaringan yang menggunakan protokol OSPF dan EIGRPadalah bit rate pada saat upload dan download konfigurasi router ke server.

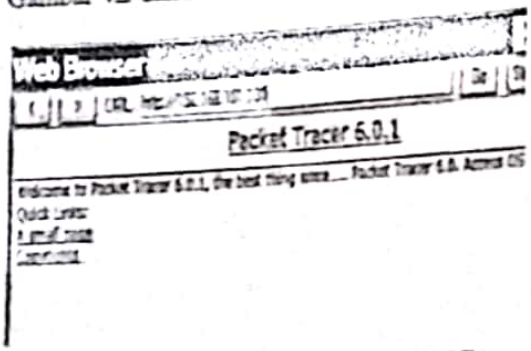


Gambar 4.4 Desain Jaringan Uji Coba Dengan Web Server

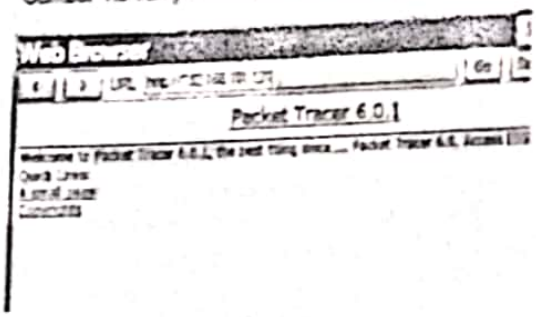
Jaringan yang digunakan untuk pengujian ini mirip dengan yang ditunjukkan pada Gambar 4.1, hanya saja pada ditambahkan *web server* yang ditempatkan di site 1 seperti ditunjukkan pada Gambar 4.4.

4.3.1. Perbandingan akses internet pada jaringan OSPF dan EIGRP

Halaman web diakses dengan cara mengetikkan alamat server pada fasilitas web browser yang ada pada PC. Web browser ini merupakan simulasi akses ke jaringan internet. Tampilan halaman web yang diakses oleh jaringan yang menggunakan protokol OSPF dan EIGRP ditunjukkan pada Gambar 4.5 danGambar 4.6.



Gambar 4.5 Tampilan halaman web (jaringan OSPF)



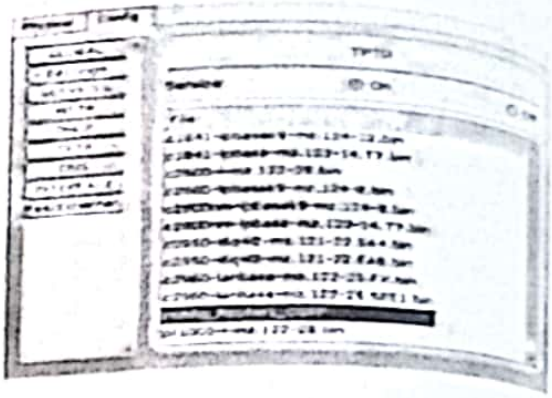
Gambar 4.6. Tampilan halaman web (jaringan EIGRP)

Pada pengujian ini, baik jaringan yang menggunakan routing protocol OSPF dan EIGRP, keduanya mampu mengakses halaman web berbasis HTTP, seperti ditunjukkan pada Gambar 4.5 dan Gambar 4.6.

4.3.2. Perbandingan transfer file pada Jaringan OSPF dan EIGRP

Pada ujicoba ini file yang akan ditransfer adalah konfigurasi dari router yang ditempatkan di masing-masing site, yaitu Router1, Router2, Router3,Router4, Router5, Router6, dan Router7.

Parameter yang akan diamati pada ujicoba ini adalah bit rate yang digunakan untuk upload dan download file konfigurasi tersebut. Misalnya file yang disimpan di web server adalah konfigurasi routing protocol OSPF pada Router1 yang diberi nama"config_Router1_OSPF". Maka setelah di-upload tampilan pada web server seperti ditunjukkan pada Gambar 4.7. Bagian yang di-highlight warna biru adalah file konfigurasi yang telah disimpan.



Gambar 4.7. Tampilan pada web server

Hasil pengujian *upload* dan *download* yang dilakukan oleh jaringan dengan *routing protocol* OSPF dan EIGRP (Tabel 4.15 dan Tabel 4.16.)

Tabel 4.15 *Bit rate upload* ke web server

	OSPF (bps)	EIGRP (bps)
Router1	2000	2000
Router2	1000	1000
Router3	1000	1000
Router4	2000	2000
Router5	3000	2000
Router6	4000	4000
Router7	3000	2000

Tabel 4.16 *Bit rate download* dari web server

	OSPF (bps)	EIGRP (bps)
Router1	4516	3916
Router2	5341	2799
Router3	2867	4338
Router4	4237	3423
Router5	6444	11402
Router6	8822	8118
Router7	6000	5609

Dengan informasi dari Tabel 4.15 dan Tabel 4.16 dapat dicari rata-rata bit ratedari jaringan yang memakai protokol OSPF dan EIGRP sebagai berikut :

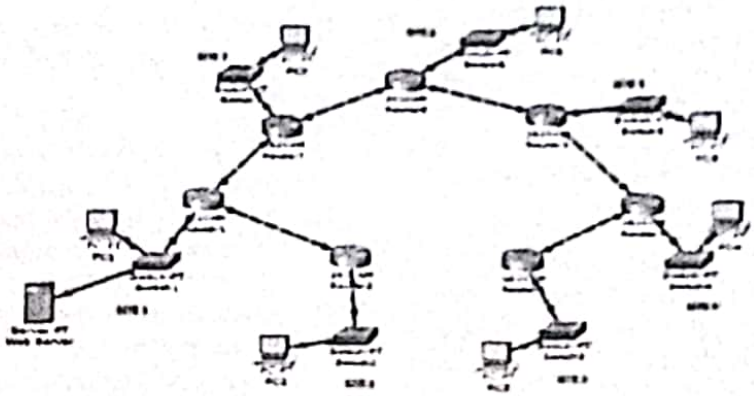
Jaringan dengan konfigurasi OSPF :
Rata-rata bit rate upload : 2285.7 bps
Rata-rata bit rate download : 5589.6 bps
Jaringan dengan konfigurasi EIGRP :
Rata-rata bit rate upload : 2285.7 bps
Rata-rata bit rate download : 5688.3 bps

Dari perhitungan yang telah dilakukan didapatkan hasil bahwa rata-rata bitrate upload adalah sama untuk jaringan yang menggunakan protokol OSPF danEIGRP. Sedangkan untuk rata – rata bit rate download, jaringan yang memakai protokol OSPF lebih cepat. Hal ini menunjukkan apabila semua router penyusun backbone dihapus konfigurasinya dan diminta untuk men-download konfigurasi dari server, maka jaringan yang memakai protokol OSPF akan lebih cepat terkonfigurasi.

4.4. Ujicoba Kemampuan Fault Tolerant

Fault tolerant adalah kemampuan jaringan untuk mengatasi gangguan yangdialami saat jaringan tersebut beroperasi secara normal. Kemampuan ini diperlukan sebuah jaringan untuk tetap dapat melayani user walaupun terjadi gangguan yang menyebabkan kerusakan yang terjadi diperbaiki.

Uji coba fault tolerant akan dilaksanakan dengan skenario berikut ini. Pertama-tama akan diambil data dari ujicoba tracert yang telah dilakukan lebih awal, gunanya untuk mengetahui jalur yang akan dilalui oleh paket data IP dari gratra. Setelah itu dilakukan ujicoba tracert secaranormal untuk memverifikasi jalur yang dipilih untuk sampai ke tujuan. Lalu dilakukan 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 semula ada menjadi tidak ada.Skenario ini mensimulasikan kegagalan yang mungkin terjadi apa bila kabel antar router backbone tanpa sengaja terputus atau tercabut dari port Fast Ethernet. Ilustrasi dari skenario ini dapat ditunjukkan pada Gambar 4.8, dimana kabel yang mengubungkan antara Router 2 dan Router 3 putus.



Gambar 4.8. Ilustrasi kegagalan jaringan

Skenario kegagalan untuk jaringan dengan protokol OSPF dan EIGRP yang akan disimulasikan adalah sebagai berikut :

Tracert dari PC1 ke PC4, lalu ditengah berjalannya proses tracert kabel antara Router 2 dan Router 3 dihilangkan. Tracert dari PC4 ke PC6, lalu ditengah berjalannya proses tracert kabel antara Router 4 dan Router 5 dihilangkan.

4.4.1. Perbandingan kemampuan fault tolerant pada OSPF dan EIGRP

Dari dua skenario kegagalan yang telah didefinisikan, rute alternatif yang dipilih

protokol OSPF dan EIGRP ditunjukkan pada Tabel 4.17 dan Tabel 4.18.

Tabel 4.17. Tracert dari PC1 ke PC4 dengan adanya fault

OSPF		EIGRP	
Hop	Jaringan yang dilewati	Hop	Jaringan yang dilewati
1	192.168.101.1	1	192.168.101.1
2	10.100.101.2	2	10.100.101.2
3	10.100.101.41	3	10.100.101.41
4	10.100.101.33	4	10.100.101.33
5	10.100.101.25	5	10.100.101.25
6	192.168.101.50	6	192.168.101.50

Tabel 4.18. Tracert dari PC4 ke PC6 dengan adanya fault

OSPF		EIGRP	
Hop	Jaringan yang dilewati	Hop	Jaringan yang dilewati
1	192.168.101.49	1	192.168.101.49
2	10.100.101.17	2	10.100.101.17
3	10.100.101.9	3	10.100.101.9
4	10.100.101.1	4	10.100.101.1
5	10.100.101.89	5	10.100.101.49
6	10.100.101.41	6	10.100.101.41
7	192.168.101.130	7	192.168.101.130

Jalur yang terdapat pada Tabel 4.17 dan 4.18 merupakan jalur alternatif yang dipilih oleh OSPF dan EIGRP karena jalur yang seharusnya dilewati mengalami kegagalan dan menjadi tidak dapat dilewati. OSPF dan EIGRP mampu memberikan alternative jalur saat terjadi kegagalan mendadak pada jaringan, sehingga kedua protokol ini layak diaplikasikan pada jaringan karena dapat memberikan kemampuan fault tolerant.

5. KESIMPULAN

Hasil pengujian dan analisis terhadap jaringan *Fast Ethernet* yang dibangun dengan software *Packet Tracer v6.0.1*, dapat disimpulkan sbb:

1) Syarat konektivitas jaringan telah dipenuhi, baik oleh jaringan yangmenggunakan routing protocol OSPF maupun EIGRP, dimana host-hostyang berada pada masing-masing site telah dapat tersambung satu sama lain. Dibuktikan dengan ujicoba ping yang berhasil untuk semua host.
2) Routing protocol OSPF dan EIGRP mampu menemukan jalur yang palingpendek untuk mencapai alamat tujuan yang diinginkan.
3) Host pada masing-masing site telah dapat mengakses internet, yangdisimulasikan dengan menggunakan dengan kemampuan mengakses *webserver*.
4) Pada ujicoba transfer file konfigurasi router dengan protokol TFTP, OSPF danEIGRP sama-sama mampu untuk melakukan upload dan download. EIGRPmemberikan hasil sedikit lebih baik dari pada OSPF dimana bit rate EIGRP mencapai5688.3bps sedangkan bitrate OSPF 5589.6 bps. Sedangkan untuk upload, didapatkab bit rate yang sama untuk OSPF dan EIGRP yaitu sebesar 2285.7 bps.
5) Dari pengujian fault tolerant diketahui bahwa OSPF dan EIGRP mempunyai kemampuan untuk mengantisipasi kegagalan yang terjadi pada jaringan dengan cara mencari rute alternatif pada saat jalur terpendek tidak memungkinkan untuk dilewati.
6) Dari pengujian-pengujian yang dilakukan baik OSPF dan EIGRP layak dijadikan routing protocol untuk backbbone.

6. DAFTAR PUSTAKA

[1] Ina Minei, Julian Lucek,"MPLS-Enabled Applications",John Willey & Sons, 2005.

[2] Diane Teare, Catherine Paquet,"Campus Network Design Fundamentals", Cisco Press, 2005.

[3] Edi S Mulyanta,"Pengenalan Protokol Jaringan Wireless Komputer", Andi Yogyakarta, 2005.

[4] Cisco Systems, Inc, "Internetworking Technologies Handbook, Forth Edition",Cisco Press, 2003.

[5] Todd Lammle,"Cisco Certified Network Associate Study Guide, Forth Edition", SYBEX Inc, 2004.

[6] Gilbert Held,"Ethernet Networks, Forth Edition", John Willey & Sons, 2003. Packet Tracer v6.0.1.

[7] Andrew S. Tannenbaum,"Computer Networks", Pearson Education, Inc, 2003. Jim Murray,"Physical vs Logical Topologies". Diakses dari http://www.giac.org/resources/whitepaper/network/32.php pada bulan Desember 2012.

[8] Harpreet Chadha,"Want high availability in Metro Ethernet

networks? Resiliency is key". Diakses dari http: //www.commsdesign.com/showArticle .jhtml?articleID=189400440 pada bulan Desember 2012.

[9] Iftekhar Hussain,"Fault Tolerant IP and MPLS Networks", Cisco Press, 2004.

[10] Jim Guichard, Ivan Pepelnjak,"MPLS and VPN Architectures",Cisco Press, 2000.

[11] Martin P. Clark, "Data Networks, IP and the Internet",John Willey & Sons, 2003.

RIWAYAT PENULIS

Agustini Rodiah Machdi S.T, M.T, Staf Pengajar Program Studi Elektro, Fakultas Teknik – Univeritas Pakuan Bogor.