

ROUTING PROTOKOL EIGRP DAN OSPF PADA JARINGAN PT. INDONESIA COMNETS PLUS JAKARTA

Khifli Mulyadi
Teknik Informatika, STMIK Nusa Mandiri Jakarta
Jl. Kaliabang Raya No. 8 Bekasi
Email : khiflimulyadi@gmail.com

ABSTRACT

In a business, the customer is a very important factor for a service company such as PT Indonesia Comnets Plus engaged in VoIP providers. The increasing number of customers using VoIP services then it needs a routing system that can facilitate customer additions and to facilitate in analyzing the problem. The purpose of this thesis is to create a routing that can facilitate network administrators in handling problems that occur. The method used in the manufacture of the author of this thesis by comparing between using Dynamic Routing Enhanced Interior Gateway Routing Protocol and Open Shortest Path First. After comparing two routing results obtained EIGRP is best to apply in PT. Indonesia Comnets Plus in particular by the Division Unit Bisnis Multimedia because there is no need reconvergence time for performed by EIGRP when a change in route.

Keyword : Routing, static, dynamic, EIGRP, OSPF.

ABSTRAK

Dalam sebuah bisnis, pelanggan merupakan faktor yang sangat penting bagi sebuah perusahaan jasa seperti PT Indonesia Comnets Plus yang bergerak dibidang penyelenggara VoIP. Semakin banyaknya pelanggan yang menggunakan jasa voip maka dibutuhkan sebuah system *routing* yang dapat memudahkan penambahan pelanggan dan dapat mempermudah dalam menganalisa masalah. Tujuan penelitian ini adalah membuat suatu *routing* yang dapat mempermudah *network administrator* dalam penanganan –penanganan masalah yang terjadi. Metode yang digunakan adalah *Routing Dynamic Enhanced Interior Gateway Routing Protocol* dan *Open Shortest Path First*. Setelah membandingkan kedua *routing* tersebut didapatkan hasil EIGRP yang terbaik untuk diterapkan di PT.Indonesia Comnets Plus khususnya oleh Divisi Unit Bisnis Multimedia dikarenakan tidak perlunya waktu konvergensi ulang yang dilakukan oleh EIGRP ketika terjadi perubahan *route*.

Kata Kunci : *Routing, static, dynamic, EIGRP, OSPF.*

1. Pendahuluan

PT Indonesia Comnets Plus (ICON+) adalah anak perusahaan PT PLN (Persero), yang bergerak dibidang infrastruktur jaringan atau *networking* dengan menggunakan media transmisi *fiber optic*, yang memanfaatkan tiang listrik PLN yang ada diseluruh Indonesia sehingga jaringan PT Indonesia Comnets Plus (ICON+) memiliki jaringan yang sangat luas. Semakin luasnya jaringan PT Indonesia Comnets Plus

(ICON+) khususnya di Divisi Unit Bisnis Multimedia maka dibutuhkan sebuah *routing* yang memiliki fitur *backup route*, dimana jika terjadi perubahan pada jaringan tidak harus melakukan kalkulasi ulang untuk menentukan *route* terbaik karena dapat langsung menggunakan *backup route* tersebut.

Untuk meningkatkan kualitas pelayanan dan kecepatan dalam segi transmisi data, maka penggunaan *routing*

dynamic sangat membantu dalam mengatasi masalah – masalah yang tidak diinginkan, seperti putus *core* maupun kerusakan dari sisi *maintenance*, dan dapat memudahkan dalam *maintenance*. Untuk jaringan berskala kecil algoritma *routing* yang lebih sesuai adalah *routing* secara *static* karena lebih menghemat *bandwith* sedangkan jaringan dengan skala besar tepat menggunakan *dynamic routing*.(Edi, 2006:48)

Dari latar belakang yang telah penulis jabarkan maka perlu dibuat sebuah perencanaan jaringan yang menggunakan *Routing Dynamic*, Oleh karena itu dalam penelitian ini dilakukan implementasi *routing* protokol EIGRP dan OSPF pada jaringan PT. Indonesia Comnets Plus Jakarta yang selanjutnya dilakukan analisa terhadap kedua *routing* tersebut.

2. Bahan dan Metode Penelitian

2.1. Spesifikasi *Hardware* dan *Software*

Pada penelitian ini Div. Unit Bisnis Multimedia menggunakan *Router* Cisco 2911 dengan spesifikasi:

1. 3 integrated 10/100/1000 Ethernet ports (RJ-45 only)
2. 1 service module slot
3. 4 enhanced high-speed WAN interface card slots
4. 2 onboard digital signal processor (DSP) slots
5. 1 Internal Service Module slot for application services
6. Fully integrated power distribution to modules supporting 802.3af Power over Ethernet (PoE) and Cisco Enhanced PoE.

Sedangkan spesifikasi *software router* yang dipakai adalah sebagai berikut:

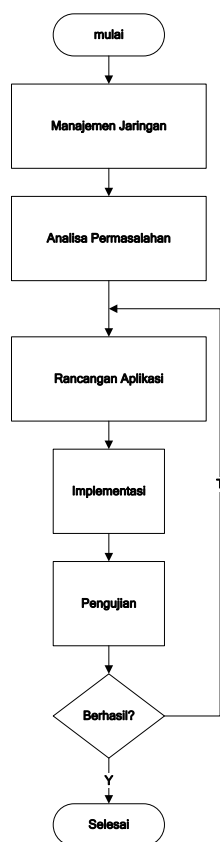
1. Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.0(1)M3, RELEASE SOFTWARE (fc2) Router uptime is 9 weeks, 5 days, 2 hours, 0 minutes System returned to ROM by reload at 04:04:09 UTC Fri Oct 12 2012 System image file is "flash0:c2900-universalk9-mz.SPA.150-1.M3.bin"
2. Last reload type: Normal Reload, Last reload reason: Reload Command, Cisco CISCO2911/K9 (revision 1.0) with 487424K/36864K bytes of memory. Processor board ID FHK1436F2U8,3 Gigabit Ethernet interfaces, DRAM configuration is 64 bits wide with parity enabled. 255K bytes of non-volatile configuration memory.
3. 254464K bytes of ATA System CompactFlash 0 (Read/Write).

2.2. Metode Penelitian

Penelitian ini terbagi menjadi 5 tahapan seperti dalam gambar 1.

2.2.1 Analisa Manajemen Jaringan

Pada tahap ini dilakukan analisa yang meliputi analisa sistem jaringan yang ada di divisi Unit Bisnis Multimedia PT. Indonesia Comnets Plus yang meliputi topologi yang digunakan, arsitektur jaringan, skema jaringan, dan keamanan untuk jaringan, rancangan, implementasi dan pengujian. Tahapan penelitian yang dilakukan dalam penelitian ini seperti dalam Gambar 1.



Gambar 1. Tahapan penelitian

2.2.2 Analisa Permasalahan

Permasalahan yang sering dihadapi oleh tim NOC adalah tidak adanya jalur alternatif yang menjadi pilihan dikala terjadi gangguan kabel.

2.2.3 Rancangan Aplikasi

Pada tahap ini dimulai dengan membuat design simulasi pada Cisco Packet Tracer, mengkonfigurasi ip pada setiap router dan mengkonfigurasi routing EIGRP dan OSPF, dilakukan pengujian, jika pengujian berhasil maka rancangan berhasil, jika tidak maka kembali mendesign topologi jaringan baru..

2.2.4 Implementasi

Pada tahapan ini implementasi dilakukan penerjemahan hasil perumusan bentuk algoritma yang dapat dimengerti oleh komputer.

2.2.5 Pengujian

Tahap ini dilakukan menggunakan simulasi *Traffic Generator* pada server. Pengujian dilakukan dengan mengirimkan paket antara server ke komputer-komputer klien menggunakan aplikasi ping dan FTP dan dengan interval periodik tertentu sebagai simulasi penerapan *traffic load*. Dari simulasi tersebut dilakukan pencatatan waktu yang dibutuhkan dalam pengiriman paket. Dari hasil tersebut dapat mencapai analisa untuk mencapai kesimpulan.

3. Hasil dan Pembahasan

3.1. Topologi Jaringan

Topologi yang digunakan dalam penelitian ini yakni dengan menggunakan metode *routing dynamic* dan menambahkan *link backup* yang bisa dijadikan jalur alternative apabila terjadi hal-hal yang tidak terduga dilapangan. Dengan ditambahkan jalur pada *router_PLN_1* ke arah *router_PLN_4* dan jalur *router_PLN_2* ke arah *router_PLN_5* maka akan ada banyak jalur alternative yang bisa dipilih oleh router untuk menanggulangi apabila terjadi putus kabel. Pada topologi jaringan seperti ini Administrator hanya menambahkan routing untuk IP – IP yang terhubung langsung kepada router.

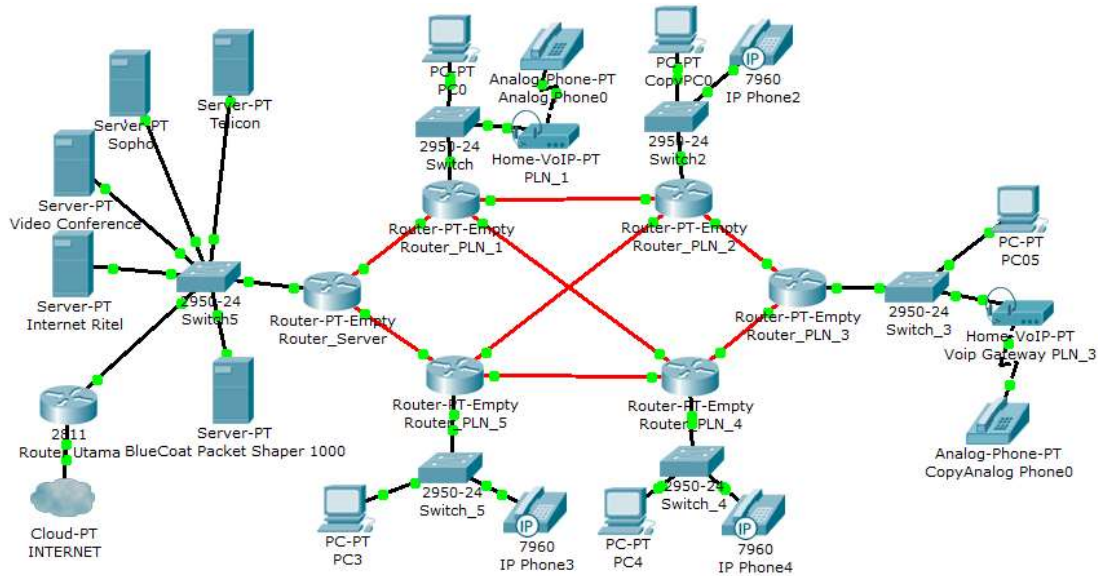
3.2. Skema Jaringan

Pada penelitian ini dilakukan simulasi jaringan dengan *software simulator* dari cisco yaitu Cisco Packet Tracer 5.3.2 (Gambar 2).

Adapun konfigurasi yang akan diterapkan pada setiap router baik

router server maupun router pelanggan dapat dilihat di tabel 1 untuk konfigurasi EIGRP

dan tabel 2 untuk konfigurasi OSPF.

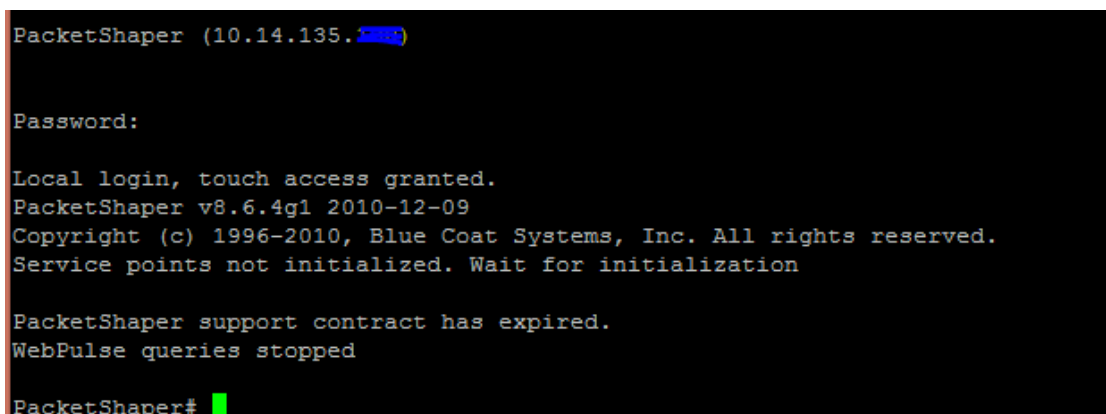


Gambar 2. Skema Jaringan Pada divisi Unit Bisnis Multimedia

3.3. Keamanan Jaringan

Keamanan jaringan yang digunakan oleh PT.Indonesia Comnets Plus khususnya pada Divisi Unit Bisnis Multimedia menggunakan *software firewall* bawaan Windows, Antivirus dan perangkat *Firewall* menggunakan *BlueCoat Packet Shaper 1000* (gambar 3) untuk *filter IP access* dan *Filter bandwidth*. untuk keamanan dari sisi

perangkat jaringan seperti *Router* dan *Switch* menggunakan *system Access List* (gambar 4) yang mana hanya IP-IP yang terdaftar yang diizinkan untuk bisa mengakses ke dalam jaringan, serta menggunakan *password* untuk perangkat-perangkat jaringan, seperti: *Router* dan *switch*.



Gambar 3. Security Bluecoat Packetshaper 1000

Tabel 1. Konfigurasi EIGRP

<i>Router_Server</i>	<pre>Router_Server>enable Router_Server#configure terminal Router_Server(config)#routerEIGRP 99 Router_Server(config-router)# network 10.14.116.0 0.0.0.63 Router_Server(config-router)# network 10.14.122.128 0.0.0.63 Router_Server(config-router)# network 10.14.135.128 0.0.0.63 Router_Server(config-router)# network 192.168.1.0 0.0.0.3 Router_Server(config-router)# network 192.168.1.4 0.0.0.3 Router_Server(config-router)# no auto-summary</pre>
<i>Router_PLN_1</i>	<pre>Router_PLN_1>enable Router_PLN_1#configure terminal Router_PLN_1(config)#routerEIGRP 99 Router_PLN_1(config-router)# network 172.27.14.0 0.0.0.255 Router_PLN_1(config-router)# network 192.168.1.0 0.0.0.3 Router_PLN_1(config-router)# network 192.168.1.8 0.0.0.3 Router_PLN_1(config-router)# network 192.168.1.24 0.0.0.3 Router_PLN_1(config-router)# no auto-summary</pre>
<i>Router_PLN_2</i>	<pre>Router_PLN_2>enable Router_PLN_2#configure terminal Router_PLN_2(config)#routerEIGRP 99 Router_PLN_2(config-router)# network 172.27.15.0 0.0.0.255 Router_PLN_2(config-router)# network 192.168.1.8 0.0.0.3 Router_PLN_2(config-router)# network 192.168.1.12 0.0.0.3 Router_PLN_2(config-router)# network 192.168.1.28 0.0.0.3 Router_PLN_2(config-router)# no auto-summary</pre>
<i>Router_PLN_3</i>	<pre>Router_PLN_3>enable Router_PLN_3#configure terminal Router_PLN_3(config)#routerEIGRP 99 Router_PLN_3(config-router)# network 172.27.16.0 0.0.0.255 Router_PLN_3(config-router)# network 192.168.1.12 0.0.0.3 Router_PLN_3(config-router)# network 192.168.1.16 0.0.0.3 Router_PLN_3(config-router)# no auto-summary</pre>
<i>Router_PLN_4</i>	<pre>Router_PLN_4>ena Router_PLN_4# configure terminal Router_PLN_4(config)#routerEIGRP 99 Router_PLN_4(config-router)# network 172.27.17.0 0.0.0.255 Router_PLN_4(config-router)# network 192.168.1.16 0.0.0.3 Router_PLN_4(config-router)# network 192.168.1.20 0.0.0.3 Router_PLN_4(config-router)# network 192.168.1.24 0.0.0.3 Router_PLN_4(config-router)# no auto-summary Router_PLN_4(config-router)#</pre>
<i>Router_PLN_5</i>	<pre>Router_PLN_5>enable Router_PLN_5# configure terminal Router_PLN_5(config)#routerEIGRP 99 Router_PLN_5(config-router)# network 172.27.18.0 0.0.0.255 Router_PLN_5(config-router)# network 192.168.1.4 0.0.0.3 Router_PLN_5(config-router)# network 192.168.1.20 0.0.0.3 Router_PLN_5(config-router)# network 192.168.1.28 0.0.0.3 Router_PLN_5(config-router)# no auto-summary</pre>

```
ip access-list extended akses-nat
permit ip 10.14.135.128 0.0.0.63 any
permit ip 10.14.135.192 0.0.0.15 any
permit ip 172.43.21.0 0.0.0.3 any
permit ip 10.14.135.0 0.0.0.63 any
permit ip 10.14.1.0 0.0.0.255 any
permit ip 10.14.140.0 0.0.0.255 any
permit ip 10.14.117.0 0.0.0.255 any
deny ip any any
```

Gambar 4. Security Access List Pada Router Utama

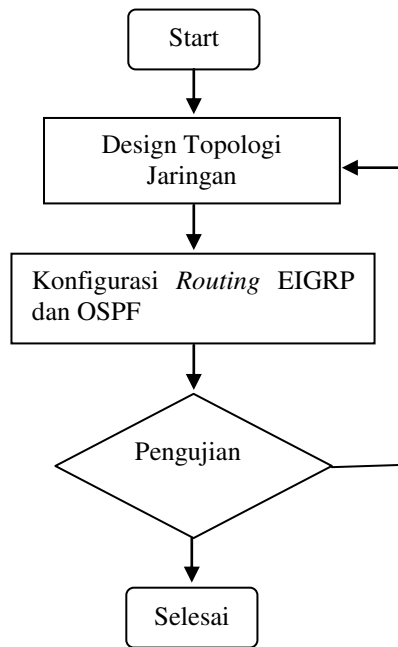
Tabel 2. Konfigurasi OSPF

<i>Router_Server</i>	<pre> Router_Server>enable Router_Server#configure terminal Router_Server(config)#routerOSPF 1 Router_Server(config-router)# router-id 1.1.1.1 Router_Server(config-router)# network 10.14.116.0 0.0.0.63 area 1 Router_Server(config-router)# network 10.14.122.128 0.0.0.63 area 1 Router_Server(config-router)# network 10.14.135.128 0.0.0.63 area 1 Router_Server(config-router)# network 192.168.1.0 0.0.0.3 area 0 Router_Server(config-router)# network 192.168.1.4 0.0.0.3 area 0 </pre>
<i>Router_PLN_1</i>	<pre> Router_PLN_1>enable Router_PLN_1#configure terminal Router_PLN_1(config)#routerOSPF 1 Router_PLN_1(config-router)# router-id 2.2.2.2 Router_PLN_1(config-router)# network 172.27.14.0 0.0.0.255 area 2 Router_PLN_1(config-router)# network 192.168.1.0 0.0.0.3 area 0 Router_PLN_1(config-router)# network 192.168.1.8 0.0.0.3 area 0 Router_PLN_1(config-router)# network 192.168.1.24 0.0.0.3 area 0 </pre>
<i>Router_PLN_2</i>	<pre> Router_PLN_2>enable Router_PLN_2#configure terminal Router_PLN_2(config)#routerOSPF 1 Router_PLN_2(config-router)# router-id 3.3.3.3 Router_PLN_2(config-router)# network 172.27.15.0 0.0.0.255 area 3 Router_PLN_2(config-router)# network 192.168.1.8 0.0.0.3 area 0 Router_PLN_2(config-router)# network 192.168.1.12 0.0.0.3 area 0 Router_PLN_2(config-router)# network 192.168.1.28 0.0.0.3 area 0 </pre>
<i>Router_PLN_3</i>	<pre> Router_PLN_3>enable Router_PLN_3#configure terminal Router_PLN_3(config)#routerOSPF 1 Router_PLN_3(config-router)# router-id 4.4.4.4 Router_PLN_3(config-router)# network 172.27.16.0 0.0.0.255 area 4 Router_PLN_3(config-router)# network 192.168.1.12 0.0.0.3 area 0 Router_PLN_3(config-router)# network 192.168.1.16 0.0.0.3 area 0 </pre>
<i>Router_PLN_4</i>	<pre> Router_PLN_4>ena Router_PLN_4# configure terminal Router_PLN_4(config)#routerOSPF 1 Router_PLN_4(config-router)# router-id 5.5.5.5 Router_PLN_4(config-router)# network 172.27.17.0 0.0.0.255 area 5 Router_PLN_4(config-router)# network 192.168.1.16 0.0.0.3 area 0 Router_PLN_4(config-router)# network 192.168.1.20 0.0.0.3 area 0 Router_PLN_4(config-router)# network 192.168.1.24 0.0.0.3 area 0 </pre>
<i>Router_PLN_5</i>	<pre> Router_PLN_5>enable Router_PLN_5# configure terminal Router_PLN_5(config)#routerOSPF 1 Router_PLN_5(config-router)# router-id 7.7.7.7 Router_PLN_5(config-router)# network 172.27.18.0 0.0.0.255 area 6 Router_PLN_5(config-router)# network 192.168.1.4 0.0.0.3 area 0 Router_PLN_5(config-router)# network 192.168.1.20 0.0.0.3 area 0 Router_PLN_5(config-router)# network 192.168.1.28 0.0.0.3 area 0 </pre>

3.4. Rancangan Aplikasi

Rancangan aplikasi yang akan dibuat oleh penulis yaitu memulai dengan membuat design simulasi pada Cisco Packet tracert, mengkonfigurasi ip pada setiap *router* dan mengkonfigurasi *routing* EIGRP dan OSPF,

dilakukan pengujian, jika pengujian berhasil maka rancangan berhasil, jika tidak maka kembali mendesign topologi jaringan baru. *Flowchart* rancangan aplikasi seperti pada gambar 5.



Gambar 5. Flowchart Rancangan Aplikasi

3.5. Pengujian Jaringan

Pengujian dilakukan menggunakan simulasi *Traffic Generator* pada *server*. Pengujian dilakukan dengan mengirimkan paket antara *server* ke komputer-komputer klien menggunakan aplikasi ping dan FTP dan dengan interval periodik tertentu sebagai simulasi penerapan *traffic load*. Dari simulasi tersebut dilakukan pencatatan waktu yang dibutuhkan dalam pengiriman paket. Dari hasil tersebut dapat mencapai analisa untuk mencapai kesimpulan.

3.5.1. Pengujian Jaringan Awal

Pada pengujian jaringan awal penulis akan mengujikan topologi jaringan yang sedang berjalan menggunakan *routing static* dengan aplikasi sebagai berikut:

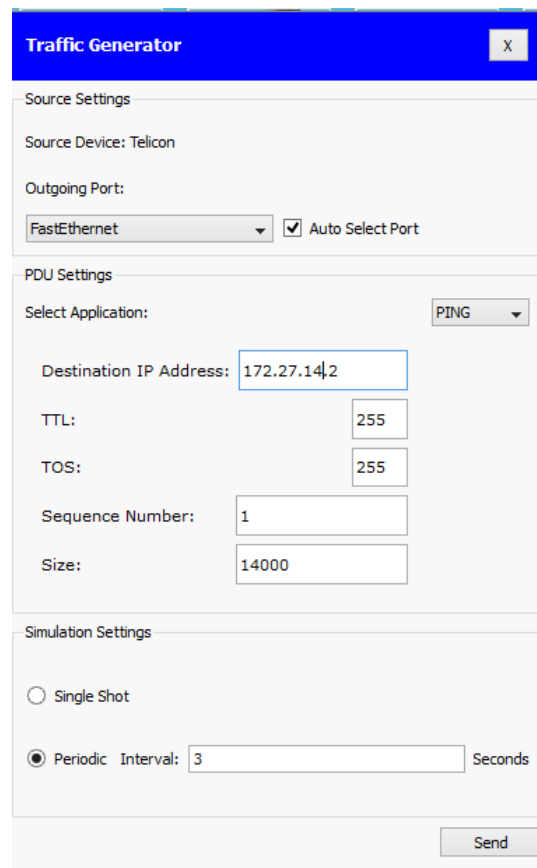
A. Aplikasi Ping

Diisikan nilai TTL (*time to live*) yaitu 255, nilai TOS (*Time of Services*) yaitu 255, *sequence number* 1 dan *size* 14000 bit, TTL merupakan lama waktu paket saat mengirim hingga sampai lagi. *Setting* ini berlaku untuk

semua komputer yang diujikan. Untuk *Source* dan *Destination IP Address* dapat dilihat di tabel 3 dan hasil pengujian menggunakan aplikasi ping dapat dilihat di tabel 4.

Tabel 3. IP Komputer Asal dan Tujuan Pengiriman Paket

Source IP Address	Destination IP Address
10.14.116.4	172.27.14.2
10.14.116.4	172.27.15.2
10.14.116.4	172.27.16.2
10.14.116.4	172.27.17.2
10.14.116.4	172.27.18.2



Gambar 6. Traffic Generator

Tabel 4. hasil Pengujian Aplikasi Ping

Source IP Address	Destination IP Address	Time
10.14.116.4	172.27.14.2	0.032
10.14.116.4	172.27.15.2	0.032
10.14.116.4	172.27.16.2	0.032
10.14.116.4	172.27.17.2	0.032
10.14.116.4	172.27.18.2	0.032
Rata-Rata		0.032

B. Aplikasi FTP

Diisikan nilai TTL(*time to live*) yaitu 255, nilai TOS (*Time of Services*) yaitu 255, *source port* 80, *destination port* 21 dan *size* 10000 bit, TTL merupakan lama waktu paket saat mengirim hingga sampai lagi. Setting ini berlaku untuk semua komputer yang diujikan. Hasil pengujian menggunakan Aplikasi FTP dapat dilihat di tabel 5.

Tabel 5. Hasil Pengujian Aplikasi FTP

Source IP Address	Destinatio n IP Address	Time
10.14.116.4	172.27.14.2	0.014
10.14.116.4	172.27.15.2	0.014
10.14.116.4	172.27.16.2	0.014
10.14.116.4	172.27.17.2	0.014
10.14.116.4	172.27.18.2	0.014
Rata – Rata		0.014

Untuk pengujian *RoutingStatic* ketika *Link* diputus antara *Router_PLN_3* dan *Router_PLN_4* masih menggunakan Aplikasi Ping dan FTP sebagai berikut:

A. Aplikasi Ping

Diisikan nilai TTL(*time to live*) yaitu 255, nilai TOS (*Time of Services*) yaitu 255, *sequence number* 1 dan *size* 14000 bit, TTL

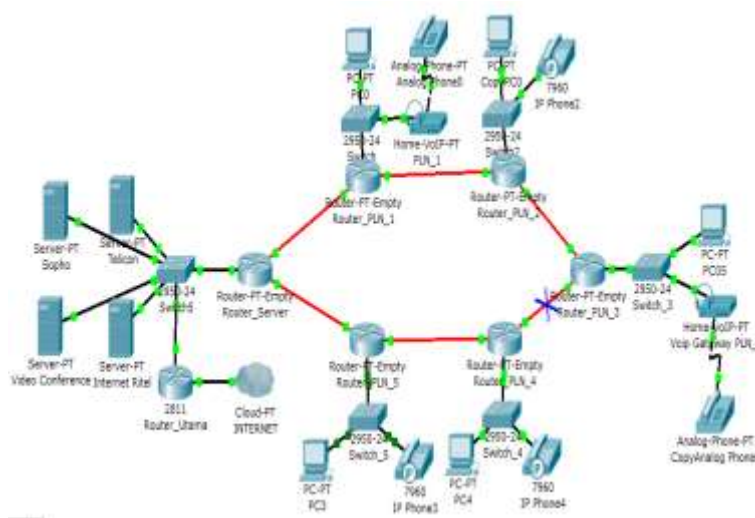
merupakan lama waktu paket saat mengirim hingga sampai lagi. *Setting* ini berlaku untuk semua komputer yang diujikan. Untuk hasil pengujian *Routing Static* menggunakan aplikasi Ping ketika *Link* di putus bisa dilihat di tabel 6.

Tabel 6. hasil Pengujian Aplikasi Ping ketika *link* diputus

Source IP Address	Destination IP Address	Time
10.14.116.4	172.27.14.2	RTO
10.14.116.4	172.27.15.2	RTO
10.14.116.4	172.27.16.2	RTO
10.14.116.4	172.27.17.2	RTO
10.14.116.4	172.27.18.2	RTO
Rata-Rata		RTO

B. Aplikasi FTP

Diisikan nilai TTL(*time to live*) yaitu 255, nilai TOS (*Time of Services*) yaitu 255, *source port* 80, *destination port* 21 dan *size* 10000 bit, TTL merupakan lama waktu paket saat mengirim hingga sampai lagi. Setting ini berlaku untuk semua komputer yang diujikan. Untuk hasil pengujian *Routing Static* menggunakan aplikasi FTP ketika *Link* di putus bisa dilihat di tabel 7.



Gambar 7. Pengujian *routing static* ketika *link* terputus

Tabel 7. Hasil Pengujian Aplikasi FTP

Source IP Address	Destination IP Address	Time
10.14.116.4	172.27.14.2	RTO
10.14.116.4	172.27.15.2	RTO
10.14.116.4	172.27.16.2	RTO
10.14.116.4	172.27.17.2	RTO
10.14.116.4	172.27.18.2	RTO
Rata – Rata		RTO

Terputusnya jaringan diakibatkan karena ada salah satu jalur yang putus dan diperlukannya design *routing* ulang yang dilakukan manual oleh *Network Administrator*.

3.5.2. Pengujian Jaringan Akhir

Pengujian jaringan akhir menggunakan 2 metode *routing* dinamik yaitu menggunakan EIGRP dan OSPF sebagai pembandingan.

A. Pengujian menggunakan EIGRP

Pengujian dilakukan menggunakan simulasi *Traffic Generator* pada *server*. Pengujian dilakukan dengan mengirimkan paket antara *server* ke komputer – komputer klien menggunakan aplikasi ping dan FTP dan dengan interval periodik tertentu sebagai simulasi penerapan *traffic load*. Dari simulasi tersebut dilakukan pencatatan waktu yang dibutuhkan dalam pengiriman paket berikut adalah pengujian menggunakan aplikasi ping dan FTP:

1) Aplikasi Ping

Diisikan nilai TTL(*time to live*) yaitu 255, nilai TOS (*Time of Services*) yaitu 255, *sequence number* 1 dan *size* 14000 bit, TTL merupakan lama waktu paket saat mengirim hingga sampai lagi. Setting ini berlaku untuk semua komputer yang diujikan. Hasil waktu

yang tercatat menggunakan EIGRP dapat dilihat di tabel 8.

Tabel 8. Hasil Waktu Menggunakan EIGRP

Source IP Address	Destination IP Address	Time
10.14.116.4	172.27.14.2	0.028
10.14.116.4	172.27.15.2	0.030
10.14.116.4	172.27.16.2	0.032
10.14.116.4	172.27.17.2	0.030
10.14.116.4	172.27.18.2	0.028
Rata – Rata		0.0296

2) Aplikasi FTP

Diisikan nilai TTL(*time to live*) yaitu 255, nilai TOS (*Time of Services*) yaitu 255, *source port* 80, *destination port* 21 dan *size* 10000 bit, TTL merupakan lama waktu paket saat mengirim hingga sampai lagi. Setting ini berlaku untuk semua komputer yang diujikan. Hasil pengujian Aplikasi FTP menggunakan *Routing* EIGRP dapat dilihat di tabel 9.

Tabel 9. Hasil Waktu Menggunakan EIGRP

Source IP Address	Destination IP Address	Time
10.14.116.4	172.27.14.2	0.010
10.14.116.4	172.27.15.2	0.012
10.14.116.4	172.27.16.2	0.014
10.14.116.4	172.27.17.2	0.012
10.14.116.4	172.27.18.2	0.010
Rata – Rata		0.0116

Untuk pengujian *Routing* EIGRP ketika *Link* diputus antara *Router_Server* dan *Router_PLN_1*. Pengujian masih menggunakan Aplikasi Ping dan FTP sebagai berikut:

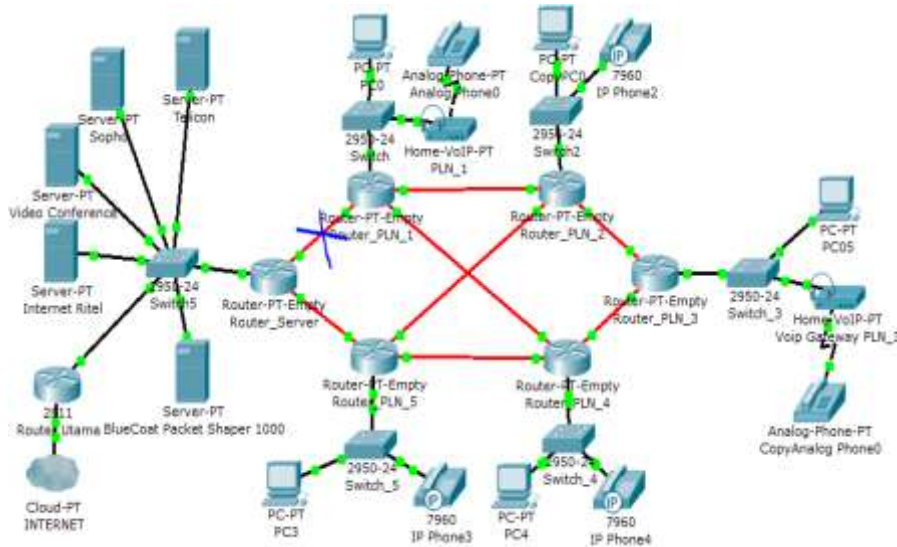
1) Aplikasi Ping

Diisikan nilai TTL(*time to live*) yaitu 255, nilai TOS (*Time of Services*) yaitu 255, *sequence number* 1 dan *size* 14000 bit, TTL merupakan lama waktu paket saat mengirim hingga sampai lagi. Setting ini berlaku untuk

semua komputer yang diujikan. Hasil pengujian menggunakan aplikasi Ping ketika *link* diputus bisa dilihat di tabel 10 dan gambar 9.

Tabel 10. Hasil Waktu EIGRP Menggunakan Aplikasi Ping Ketika *Link* Terputus

Source IP Address	Destination IP Address	Time
10.14.116.4	172.27.14.2	0.028
10.14.116.4	172.27.15.2	0.030
10.14.116.4	172.27.16.2	0.032
10.14.116.4	172.27.17.2	0.030
10.14.116.4	172.27.18.2	0.028
Rata – Rata		0.0296



Gambar 8. Pengujian *Routing* EIGRP Ketika *Link* Terputus

```

SERVER>ping 172.27.17.2

Pinging 172.27.17.2 with 32 bytes of data:

Reply from 172.27.17.2: bytes=32 time=27ms TTL=125
Reply from 172.27.17.2: bytes=32 time=21ms TTL=125
Reply from 172.27.17.2: bytes=32 time=16ms TTL=125
Reply from 172.27.17.2: bytes=32 time=29ms TTL=125

Ping statistics for 172.27.17.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 29ms, Average = 23ms
    
```

Gambar 9. Pengujian *Routing* EIGRP Ketika *Link* Terputus

2) Aplikasi FTP

Diisikan nilai TTL(*time to live*) yaitu 255, nilai TOS (*Time of Services*) yaitu 255, source port 80, destination port 21 dan size 10000 bit, TTL merupakan lama waktu paket saat mengirim hingga sampai lagi. *setting* ini berlaku untuk semua komputer yang diujikan. Hasil pengujian menggunakan aplikasi FTP ketika *link* terputus dapat lihat di tabel 11.

Tidak adanya jeda waktu dalam pengalihan rute atau tidak adanya RTO ketika *Link* terputus dikarenakan *routing* Table pada *Routing*EIGRP memiliki algoritma *Backup* route, sehingga ketika *link* terputus maka tidak diperlukannya penghitungan atau tanpa menunggu waktu konvergensi ulang yang dilakukan oleh *router*.

Tabel 11. Hasil Waktu EIGRP Menggunakan Aplikasi FTP Ketika *Link* Terputus

<i>Source IP Address</i>	<i>Destination IP Address</i>	<i>Time</i>
10.14.116.4	172.27.14.2	0.010
10.14.116.4	172.27.15.2	0.012
10.14.116.4	172.27.16.2	0.014
10.14.116.4	172.27.17.2	0.012
10.14.116.4	172.27.18.2	0.010
Rata – Rata		0.0116

B. Pengujian menggunakan OSPF

Pengujian dilakukan menggunakan simulasi *Traffic Generator* pada *server*. Pengujian dilakukan dengan mengirimkan paket antara *server* ke komputer – komputer klien menggunakan aplikasi ping dan FTP dan dengan interval periodik tertentu sebagai simulasi penerapan *traffic load*. Dari simulasi tersebut dilakukan pencatatan waktu yang dibutuhkan dalam pengiriman paket. Dari hasil tersebut dapat mencapai analisa untuk mencapai kesimpulan. Berikut adalah pengujian *routing* OSPF menggunakan aplikasi ping dan FTP :

1. Aplikasi Ping

Diisikan nilai TTL (*time to live*) yaitu 255, nilai TOS (*Time of Services*) yaitu 255, *sequence number* 1 dan *size* 14000 bit, TTL merupakan lama waktu paket saat mengirim hingga sampai lagi. Setting ini berlaku untuk semua komputer yang diujikan. Hasil pengujian menggunakan aplikasi pada OSPF dapat dilihat pada tabel 12.

2. Aplikasi FTP

Diisikan nilai TTL(*time to live*) yaitu 255, nilai TOS (*Time of Services*) yaitu 255, *source port* 80, *destination port* 21 dan *size* 10000 bit, TTL

merupakan lama waktu paket saat mengirim hingga sampai lagi. Setting ini berlaku untuk semua komputer yang diujikan. Hasil pengujian menggunakan Aplikasi FTP pada *routing* OSPF dapat dilihat pada tabel 13.

Tabel 12. Hasil Waktu Menggunakan Aplikasi Ping Pada OSPF

<i>Source IP Address</i>	<i>Destination IP Address</i>	<i>Time</i>
10.14.116.4	172.27.14.2	0.028
10.14.116.4	172.27.15.2	0.030
10.14.116.4	172.27.16.2	0.032
10.14.116.4	172.27.17.2	0.030
10.14.116.4	172.27.18.2	0.028
Rata – Rata		0.0296

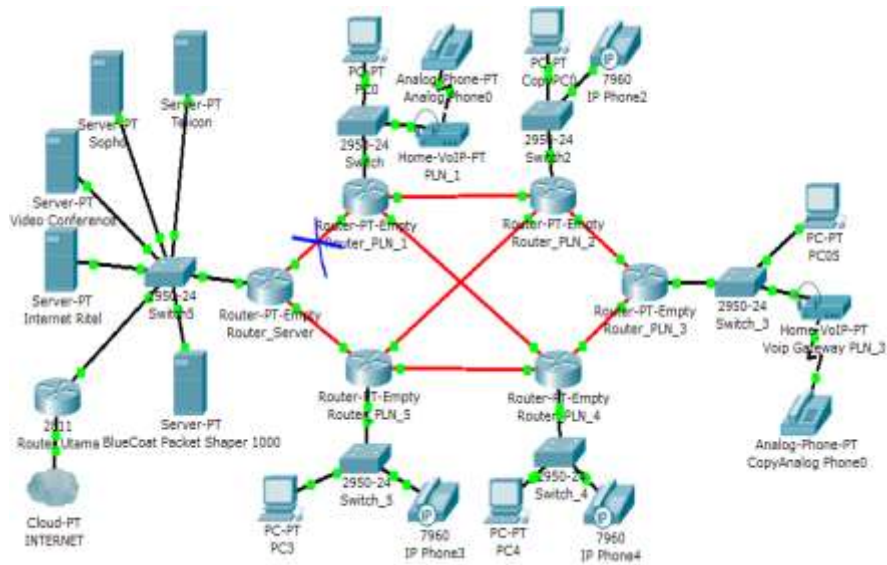
Tabel 13. Hasil Waktu Menggunakan OSPF

<i>Source IP Address</i>	<i>Destination IP Address</i>	<i>Time</i>
10.14.116.4	172.27.14.2	0.010
10.14.116.4	172.27.15.2	0.012
10.14.116.4	172.27.16.2	0.014
10.14.116.4	172.27.17.2	0.012
10.14.116.4	172.27.18.2	0.010
Rata - Rata		0.0116

Untuk pengujian *Routing* OSPF ketika *Link* diputus (gambar 10) antara *Router_Server* dan *Router_PLN_1*. Pengujian masih menggunakan aplikasi Ping dan FTP sebagai berikut:

1) Aplikasi Ping

Diisikan nilai TTL(*time to live*) yaitu 255, nilai TOS (*Time of Services*) yaitu 255, *sequence number* 1 dan *size* 14000 bit, TTL merupakan lama waktu paket saat mengirim hingga sampai lagi. Setting ini berlaku untuk semua komputer yang diujikan. Hasil pengujian aplikasi ping pada OSPF ketika *link* terputus dapat dilihat pada tabel 14 dan gambar 11.



Gambar 10. Pengujian *Routing* OSPF Ketika *Link* Terputus

```

SERVER>ping 172.27.17.2

Pinging 172.27.17.2 with 32 bytes of data:

Reply from 172.27.17.2: bytes=32 time=26ms TTL=125
Reply from 172.27.17.2: bytes=32 time=17ms TTL=125
Request timed out.
Reply from 10.14.116.1: Destination host unreachable.

Ping statistics for 172.27.17.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 26ms, Average = 25ms
    
```

Gambar 11. Pengujian *Routing* OSPF Ketika *Link* Terputus

Tabel 14. Hasil Waktu Aplikasi Ping Pada OSPF Ketika *Link* Terputus

Source IP Address	Destination IP Address	Time
10.14.116.4	172.27.14.2	0.028
10.14.116.4	172.27.15.2	0.030
10.14.116.4	172.27.16.2	0.032
10.14.116.4	172.27.17.2	0.030
10.14.116.4	172.27.18.2	0.028
Rata - Rata		0.0296

2) Aplikasi FTP

Diisikan nilai TTL(*time to live*) yaitu 255, nilai TOS (*Time of Services*) yaitu 255, source port 80, destination port 21 dan size 10000 bit, TTL merupakan lama waktu paket saat mengirim hingga sampai lagi. Setting ini berlaku untuk semua komputer yang diujikan. Hasil pengujian menggunakan

aplikasi FTP pada OSPF dapat dilihat pada tabel 15.

Tabel 15. Hasil Waktu OSPF Menggunakan FTP

Source IP Address	Destination IP Address	Time
10.14.116.4	172.27.14.2	0.010
10.14.116.4	172.27.15.2	0.012
10.14.116.4	172.27.16.2	0.014
10.14.116.4	172.27.17.2	0.012
10.14.116.4	172.27.18.2	0.010
Rata - Rata		0.0116

Terjadi jeda waktu dalam pengalihan rute atau adanya RTO ketika *Link* terputus dikarenakan *routing* tabel pada *Routing* OSPF tidak memiliki algoritma *Backup* route, sehingga ketika *link* terputus maka diperlukannya penghitungan ulang yang dilakukan oleh *router*.

4. Kesimpulan dan Saran

4.1. Kesimpulan

Kesimpulan dari penelitian ini adalah:

1. Sistem berjalan yang ada pada Indonesia Comnets Plus divisi Unit Bisnis Multimedia untuk *routing* jaringan masih menggunakan *Routing Static* dengan memasukkan secara manual setiap *network-network* yang terhubung,
2. *Static routing* harus mengetahui tiap-tiap *network* tujuan sedangkan *routing dynamic* tidak perlu mengetahui *network-network* yang lainnya karena *router* akan mengirim *hallo* paket pada *router – router* yang terhubung,
3. EIGRP tidak memerlukan waktu untuk konvergensi ulang pada saat terjadi perubahan *network*, memiliki *backup route* dan hanya didukung oleh *router – router cisco (cisco proprietary)*. Sedangkan OSPF, tidak memiliki *backup route* sehingga memerlukan waktu untuk mengkonvergensi ulang *routing* tabelnya dan didukung oleh semua *provider router*.

4.2. Saran

Saran untuk pengembangan penelitian yaitu:

1. Teknisi harus mempunyai data-data yang lengkap mengenai *IP Address* dan arah-arah *routing* setiap perangkat. Melakukan *reconfigure router*

sebaiknya dilakukan pada malam hari untuk menghindari hal-hal yang tidak diharapkan dan *backup* semua konfigurasi sebelum melakukan implementasi.

2. Keamanan jaringan menggunakan *bluecoat* harus di *reconfigure* ulang dikarenakan banyaknya link yang belum di filter.
3. Diperlukannya penelitian lebih lanjut untuk penggunaan EIGRP beberapa tahun kemudian ketika pengimplementasian EIGRP yang tidak terencana dikarenakan mudahnya pengkonfigurasi dalam penambahan jaringan baru.

Daftar Pustaka

- Pankaj Rakheja, Prabhjotkaur, Anjaligupta, Aditi Sharma. *Performance Analysis Of RIP, OSPF, IGRP And EIGRP Routing Protocol In Network*. ISSN :0975-8888 *Internasional Journal of Computer Application Volume 48- No 18, June 2012*.
- Pethe dan Burnase. *Technical Era Language Of The Networking – EIGRP*. ISSN :0975-5462 *NCICT Special Issue Feb 2011*.
- Edi, Doru. *Kajian Algoritma Routing Dalam Jaringan Komputer*. *Jurnal Informatika UKM*, Vol II, No 3 Juni 2006 : 47 – 55