PERANCANGAN DAN SIMULASI JARINGAN *FAST ETHERNET* DENGAN MENGGUNAKAN *ROUTING PROTOCOL* OSPF DAN EIGRP

SKRIPSI

OLEH:

AGUNG ADI PURWANTO

04 04 03 0032

DEPARTEMEN TEKNIK ELEKTRO

FAKULTAS TEKNIK UNIVERSITAS INDONESIA

GENAP 2007/2008

PERANCANGAN DAN SIMULASI JARINGAN *FAST ETHERNET* DENGAN MENGGUNAKAN ROUTING PROTOCOL OSPF DAN EIGRP

OLEH:

AGUNG ADI PURWANTO

04 04 03 0032

SKRIPSI INI DIAJUKAN UNTUK MELENGKAPI SEBAGIAN PERSYARATAN MENJADI SARJANA TEKNIK

DEPARTEMEN TEKNIK ELEKTRO

FAKULTAS TEKNIK UNIVERSITAS INDONESIA

GENAP 2007/2008

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

PERANCANGAN DAN SIMULASI JARINGAN *FAST ETHERNET* DENGAN MENGGUNAKAN *ROUTING PROTOCOL* OSPF DAN EIGRP

yang dibuat untuk melengkapi sebagian persyaratan menjadi Sarjana Teknik pada pendidikan Sarjana S1 Departemen Teknik Elektro Fakultas Teknik Universitas Indonesia, sejauh yang saya ketahui bukan merupakan tiruan atau duplikasi dari skripsi yang telah dipublikasikan dan atau pernah dipakai untuk mendapatkan gelar kesarjanaan di lingkungan Universitas Indonesia maupun di Perguruan Tinggi atau Instansi manapun, kecuali bagian yang sumber informasinya telah dicantumkan sebagaimana mestinya.

Depok, 24 Juni 2008

Agung Adi Purwanto

NPM 0404030032

LEMBAR PENGESAHAN

Skripsi dengan judul:

PERANCANGAN DAN SIMULASI JARINGAN *FAST ETHERNET* DENGAN MENGGUNAKAN *ROUTING PROTOCOL* OSPF DAN EIGRP

Dibuat untuk melengkapi sebagian persyaratan menjadi Sarjana Teknik pada program studi Teknik Elektro Departemen Teknik Elektro Fakultas Teknik Universitas Indonesia dan telah disidangkan pada 3 Juli 2008.

Depok, 24 Juni 2008

Dosen Pembimbing

Prof. Dr. Ir. Dadang Gunawan

NIK. 131 475 421

UCAPAN TERIMA KASIH

Puji syukur hanya kepada ALLAH SWT, Yang Maha Kasih, sehingga skripsi ini dapat diselesaikan dengan baik. Penulis juga mengucapkan terima kasih kepada :

Prof. Dr. Ir. Dadang Gunawan.

Selaku dosen pembimbing yang telah bersedia meluangkan waktu untuk memberikan pengarahan, diskusi dan bimbingan serta persetujuan sehingga seminar ini dapat selesai dengan baik.

Selain itu penulis juga mengucapkan terima kasih kepada:

1. Kedua orang tua serta adik saya yang telah memberikan doa dan dukungan moril maupun materi sehingga tugas ini dapat diselesaikan dengan baik.
2. Ibu Titi Riana Hasibuan dari divisi Humas serta Bapak Ari Rahmat Indra Cahyadi dan Bapak Sri Hadi Agustama dari divisi *Network Planning* and *Management* PT. Indonesia Comnets Plus yang telah memberikan arahan dan bantuan teknis yang sangat berarti dalam pengerjaan skripsi ini.
3. Rekan-rekan seperjuangan, Rizki Mayandi Hasibuan dan Agung Ismoyo. atas dukungan dan kebersamaan selama ini.
4. Rekan-rekan elektro khususnya angkatan 2004 atas semangat yang diberikan kepada penulis.

Agung Adi Purwanto
NPM 04 04 03 0032
Departemen Teknik Elektro

Dosen Pembimbing
Prof. Dr. Ir. Dadang Gunawan

PERANCANGAN DAN SIMULASI JARINGAN FAST ETHERNET DENGAN MENGGUNAKAN *ROUTING PROTOCOL* OSPF DAN EIGRP

ABSTRAK

Perusahaan yang memiliki unit – unit usaha di lokasi tertentu tentunya ingin agar unit - unit usaha tersebut tersambung satu sama lain dalam satu jaringan dan dapat berbagi informasi penting untuk menunjang kelangsungan bisnis perushaan tersebut. Namun aspek privasi dari tiap unit – unit usaha tersebut tentunya tidak boleh dikesampingkan sehingga aktifiitas penggunaan jaringan oleh suau unit usaha tidak mengganggun unit usaha lain. Salah satu solusi yang bisa digunakan adalah penggunaan VPN. Dimana sumber daya jaringan dapat dipakai bersama namun aspek privasi antar unit usaha tidak dikesampingkan.

Salah satu alternatif pengimplementasian VPN adalah dengan L3VPN. Sesuai dengan namanya, *backbone* untuk menunjang L3VPN ini adalah divais yang beroperasi pada *layer*-3 yaitu *router*. Sehingga untuk mempesiapkan jaringan yang dapat digunakan untuk mengimplementasikan L3VPN perlu disiapkan sebuah jaringan *backbone* yang tersusun dari *router* – *router* yang walaupun tidak tersambung fisik tetapi harus tersambung secara logika. Ketersambungan secara logika ini dapat diakomodasi oleh *routing protocol*.

Dengan studi kasus dimana PT. Indonesia Comnets Plus bermaksud untuk membuat jaringan antar unit usaha PLN di Kota Palembang. Maka akan dilakukan perancangan jaringan yang dapat mendukung pengimplementasian L3VPN dengan memakai *routing protocol* OSPF yang akan dikonfigurasi menggunakan IOS *command* pada *router*.

Kata kunci : router, konfigurasi, OSPF, EIGRP

Agung Adi Purwanto
NPM 04 04 03 0032
Electrical Engineering Departement

Dosen Pembimbing
Prof. Dr. Ir. Dadang Gunawan

DESIGN AND SIMULATION OF FAST ETHERNET NETWORK USING OSPF AND EIGRP ROUTING PROTOCOL

ABSTRACT

Enterprise that has several branch unit within area surely wants so that its branch units can connect to each other within one network and share important information in order to support its business operations. Under that constraint, privacy among each branch units may not be neglected so the activity of network using won't bother other unit branch's activity. One solutin can be used is to implement VPN, on which network resources can be shared among unit branch and privacy aspect is still considerated.

One of the alternative for implementing VPN is to implement L3VPN. Backbone *network* used for supporting L3VPN is using layer-3 devices, which is router. So, in order to prepare a ntework to ready for L3VPN implementation it needs a backbone network which consist of routers, which are although not physically connected but logically connected. This logical connection between routers can be achieved using routing protocol.

With a case study on which PT. Indonesia Comnets Plus want to build network among PLN unit branch at Palembang, a network planning will be carried, under constraint that the network to be designed has to be able to support L3VPN implementation using OSPF dan EIGRP routing protocol configures using IOS command.

keyword: router, configuration, OSPF, EIGRP

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

ABR	Area Border Router
AS	Autonomous System
BGP	Border Gateway Protocol
CE	Customer Edge
DR	Designated Router
DUAL	Diffusing Update Algorithm
EIGRP	Enhanced Interior Gateway Routing Protocol
GH	Gardu Hubung
GI	Gardu Induk
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGRP	Interior Gateway Routing Protocol
IOS	Internet Operating System
IP	Internet Protocol
L3VPN	Layer 3 Vitual Private Network
LAN	Local Area Network
LDP	Label Distribution Protocol
LSA	Link State Advertisement
MAC	Medium Access Control
MPLS	Multiprotocol Label Switching
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
PDIOO	Planning Design Implementation Operation Optimisization
PDM	Protocol Dependent Modules
PE	Provider Edge
QoS	Quality of Service
RFC	Request for Comments

RIP	Routing Infromation Protocol
RIPv2	Routing Infromation Protocol version 2
RJ-45	Registered Jack 45
RSVP	Request Reservation Protocol
RTP	Reliable Transfer Protocol
STP	Shielded Twisted Pair
TFTP	Trivial File Transfer Protocol
UTP	Unshielded Twisted Pair
VPN	Virtual Private Network

BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Perkembangan teknologi jaringan komputer menunjukkan peningkatan yang sangat pesat seiring dengan semakin meningkatnya kebutuhan akan ketersambungan lokasi – lokasi yang terpisah secara jarak namun ingin tetap berbagi informasi dan menikmati layanan yang sama. Kebutuhan akan ketersambungan antar lokasi ini dirasakan benar pada level perusahaan, Sebuah perusahaan yang memiliki sejumlah unit usaha tentunya ingin agar setiap unit usahanya tersebut terhubung satu sama lain agar dapat bertukar informasi dan memiliki akses yang setara ke internet.

Untuk memenuhi hal ini maka harus dilihat dari dua sudut pandang, yaitu sudut pandang unit usaha dan sudut pandang kantor pusat [1]. Dari sudut pandang unit usaha, tentunya tujuan yang ingin dicapai adalah kesamaan *QoS* dan dan jaminan privasi yang terdapat pada *private network*, hal ini meliputi kemampuan setiap unit usaha untuk menentukan alamat jaringannya masing – masing, kemampuan untuk menambah jumlah *host*-nya, dan mengatur alokasi *bandwidth* sesuai dengan yang diberikan. Selain hal tersebut diusahakan konfigurasi *routing* yang digunakan pun tidak rumit. Sedangkan dari sisi penyedia jaringan atau dalam hal ini kantor pusat tujuan yang ingin dicapai adalah membangun jaringan seefisien mungkin dimana jaringan yang dibangun harus dapat dipakai bersama namun tetap mengutamakan aspek privasi antar unit-unit usaha dengan menggunakan satu jaringan yang bertindak sebagai *backbone*. Pengalokasian alamat IP yang tepat juga harus dilakukan untuk menghemat sumber daya berupa alamat IP. Selain itu unit – unit usaha tersebut juga diberi kebebasan untuk menambah jumlah *host* sesuai dengan alokasi jumlah maksimum *host* yang diberikan.

Dengan kondisi seperti ini maka solusi yang dapat dilakukan adalah mengimplementasikan VPN [1]. Alasannya adalah, pertama karena VPN dapat menyediakan konektivitas antar lokasi yang terpisah secara geografis. Kedua, karena privasi dalam operasi jaringannya, misalnya pengalamatan dan *routing*.

Ketiga, sifat privasi tersebut dapat dicapai walaupun unit – unit usaha tersebut menggunakan jaringan *backbone* yang sama.

Solusi berupa penggunaan VPN ini mempunyai beberapa alternatif, namun pengimplementasian, salah satu diantaranya adalah L3VPN. Pengimplementasian dengan L3VPN menggunakan *backbone* yang terdiri dari serangkaian *router – router*, dimana *router* merupakan divais yang beroperasi pada *Layer*-3 *(network layer)*. Untuk mengimplementasikan L3VPN pertama – tama *router – router* yang membentuk *backbone* harus dikonfigurasi sedemikian rupa sehingga tersambung satu sama lain dan dapat mengenali *router – router* lain yang ada pada jaringan *backbone* tersebut. *Router – router* ini dikonfigurasi dengan menggunakan perintah perintah berupa *IOS command* agar bekerja sesuai *routing protocol* tertentu. Terdapat beberapa *routing protocol*, diantaranya RIP, RIPv2, IGRP, EIGRP, dan OSPF. Namun pada skripsi ini pembahasan akan dibatasi hanya pada OSPF dan EIGRP karena dua *routing protocol* ini paling populer dan paling banyak digunakan dewasa ini [5].

1.2 PERUMUSAN MASALAH

Akan dilakukan perancangan jaringan dengan kasus di PT. Indonesia Comnetss Plus (ICON +) yang akan membangun jaringan untuk menghubungkan unit –unit usaha PLN yang lokasinya berada di kota Palembang. Jaringan yang akan dibangun akan menggunakan koneksi Fast Ethernet dan harus dapat menghubungkan setiap host antar kantor cabang, selain itu *host* juga harus dapat mengakses internet.

1.3 TUJUAN

Tujuan dari penelitian ini adalah untuk membangun jaringan yang mendukung pengimplementasian L3VPN dengan cara mengimplementasikan *routing protocol* OSPF dan EIGRP pada jaringan yang akan dibangun. Serta menganalisis unjuk kerja jaringan berdasarkan *routing protocol* yang digunakan.

1.4 PEMBATASAN MASALAH

Pembahasan dalam penelitian ini dibatasi hanya pada perancangan jaringan dan pengujian jaringan untuk mengamati unjuk kerja *routing protocol* OSPF dan EIGRP.

1.5 METODOLOGI PENELITIAN

Penelitian dilakukan dengan melakukan studi literatur, kemudian melakukan implementasi dengan membangun sebuah jaringan untuk menguji unjuk kerja *routing protokol* OSPF dan EIGRP dengan menggunakan *software* simulasi Packet Tracer v4.11, lalu melakukan evaluasi terhadap hasil unjuk kerja dari jaringan yang telah dibangun.

1.6 SISTEMATIKA PENULISAN

Sistematika penulisan laporan tugas akhir ini meliputi :

Bab I Pendahuluan

Berisikan tentang latar belakang, perumusan masalah, tujuan, pembatasan masalah, metodologi penelitian, dan sistematika penulisan.

Bab II Perancangan Jaringan dan *Routing Protocol*

Membahas mengenai teori perancangan jaringan secara umum, dasar *routing protocol*, dan teknologi OSPF dan EIGRP yang akan digunakan untuk membangun jaringan.

Bab III Perancangan dan Pengimplementasian Jaringan

Bab ini membahas tentang perancangan jaringan mulai dari topologi yang dipilih, pengalokasian alamat IP, pemilihan divais yang akan digunakan, dan pengkonfigurasian protokol OSPF dan EIGRP.

BAB IV Ujicoba dan Analisis

Bab ini membahas mengenai hasil pengujian dan evaluasi unjuk kerja dari jaringan yang dibangun dengan pengujian berupa *ping*, *tracert*, kemampuan akses internet, dan kemampuan *fault tolerant*.

BAB II
PERANCANGAN JARINGAN DAN *ROUTING PROTOCOL*

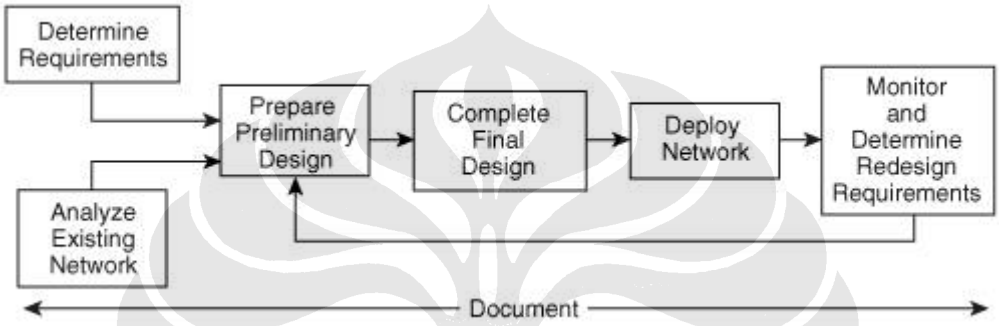
2.1 PENGENALAN PERANCANGAN JARINGAN

Perancangan jaringan membutuhkan perencanaan yang matang dan terstruktur. Agar alur perencanaan dapat berlangsung dengan sistematis maka diperlukan suatu prosedur yang baku, untuk mengakomodasi hal ini maka prosedur perencanaan yang telah dikembangkan Cisco, Inc dapat dijadikan acuan [2]. Prosedur perencanaan jaringan yang telah dikembangkan oleh Cisco, Inc ini diwakili dengan terminologi *Plan-Design-Implement-Operate-Optimize* (PDIOO). PDIOO ini akan menjadi siklus hidup dalam pembangunan jaringan dan digunakan untuk menjelaskan beragam fsae yang dilewati sebuah jaringan. Berikut ini adalah penjelasan tentang apa yang dilakukan pada tiap fase tersebut.

- Fase *Plan*
  Kebutuhan jaringan diidentifikasi secara rinci dan peninjauan ulang jaringan yang sudah ada.
- Fase *Design*
  Jaringan dirancang berdasarkan kebutuhan awal dan data dari *existing network* yang sudah diidentifikasi pada fase *Plan*. Desain lalu diperbaiki bila perlu dengan masukan dari klien.
- Fase *Implement*
  Jaringan dibangun sesuai desain yang telah disetujui klien.
- Fase *Operate*
  Jaringan dioperasikan dan dipantau unjuk kerjanya. Fase ini merupakan pengujian terakhir untuk fase desain.
- Fase *Optimize*
  Permasalahan yang terjadi dianalisa dan diperbaiki, baik sebelum terjadi permasalahan, apabila ditemukan masalah, atau sesudah masalah terjadi. Desain ulang dapat dilakukan apabila terlalu banyak masalah ditemukan.

Secara garis besar, prinsip pembangunan jaringan dengan metodologi PDIOO dapat pada diagram yang ditunjukkan pada Gambar 2.1. Dari diagram

tersebut dapat dilihat bahwa untuk mempersiapkan suatu desain awal diperlukan informasi mengenai kebutuhan jaringan. Informasi ini harus dapat mengidentifikasi kebutuhan jaringan dari sisi teknis dan bisnis sekaligus faktor – faktor yang dapat membatasi desain jaringan tersebut. Dan dari diagram tersebut dapat dilihat juga, bahwa jaringan yang sudah ada juga harus dijadikan bahan pertimbangan. Dalam kasus ini harus diidentifikasi juga, sebuah desain jaringan yang dapat terintegrasi dengan jaringan yang sudah mapan tersebut untuk menjamin kontinuitas layanan dan efisiensi dari segi biaya.



Gambar 2.1. Diagram prinsip pembangunan jaringan [2]

Kebutuhan jaringan dari sisi teknis dapat meliputi hal –hal sebagai berikut [2]:

- Aplikasi yang akan dijalankan pada jaringan
- Kebutuhan akan sambungan internet
- Protokol yang akan digunakan pada jarigan, misalnya *Routing Protocol*.
- Spesifikasi kabel yang digunakan untuk interkoneksi elemen jaringan.
- Kebutuhan akan redundansi
- Spesifkasi kebutuhan *bandwidth* untuk tiap layanan dan jaminan ketersediaan *bandwidth* tersebut.
- Harus dapat mendukung peralatan yang sudah ada.
- Bagaimana keamanan pada jaringan akan diterapkan.

Setelah mengidentifikasi kebutuhan – kebutuhan jaringan yang akan dibangun, maka langkah selanjutnya dari tahapan desain ini adalah mempersiapkan desain awal. Terdapat dua pendekatan *(approach)* yang dapat dilakukan dalam melakukan desain jaringan, yaitu top-*down approach* dan

bottom-up approach. Berikut ini adalah penjelasan untuk kedua pendekatan tersebut [2]:

- *Top – down approach*
  Aplikasi yang akan berjalan pada jaringan ditentukan terlebih dahulu lalu dispesifikasikan komponen – komponen jaringan, misalnya kabel, topologi jaringan, divais jaringan, dan protokol yang dapat mendukung aplikasi teraebut.
- *Bottom – up approach*
  Langkah yang pertama dilakukan adalah memilih komponen – komponen jaringan lalu dengan spesfikasi jaringan ini dicobe untuk disesuaikan dengan aplikasi yang diinginkan.

Setelah tahapan – tahapan desain diselesaikan maka jaringan siap diuji coba, tahapan ini ditunjukkan pada blok "*deploy network*". Jaringan yang sudah diimplementasikan ini selanjutnya akan dipantau unjuk kerjanya untuk menjamin QoS pada jaringan tersebut, atau apabila bila ada masalah yang berlangsung terus menerus dapat menjadi bahan rujukan untuk desain ulang. Setiap kegiatan yang dilakukan pada setiaf fase harus didokumentasikan.

2.2 *ROUTER* DAN *SWITCH*

Pada sub-bab ini akan dijelaskan tentang karakteristik dan cara kerja dari r*outer* dan *switch*, serta pengkabelan untuk memberikan koneksi antara *router*, *switch*, dan *host*.

2.2.1 Router

Router merupakan divais pada *network layer* yang berfungsi meneruskan data dengan dengan cara memeriksa *network adress*-nya dan memutuskan apakah suatu data pada sebuah LAN harus tetap di LAN itu atau diteruskan ke jaringan lain. *Router* dapat melakukan koneksi sejumlah jaringan, dalam hal ini bertindak sebagai *gateway* dari sebuah LAN, sehingga membentuk jaringan besar yang terdiri dari sejumlah LAN. Divais ini juga dapat memberikan pilihan jalur terbaik untuk transmisi paket data pada jaringan dengan algoritma *routing* tertentu. Pada praktisnya r*outer* mempunyai banyak modul yang dapat dipasang pada bagian

belakang *router* sesuai dengan *interface* yang diinginkan seperti *Ethernet, Fast Ethernet, Gigabit Ethernet,* dan kabel serial. Konfigurasit *router* dilakukan dengan menggunakan IOS *command* [6].

2.2.2 Switch

Switch merupakan divais pada *data link layer* yang memungkinkan sejumlah segmen fisik LAN untuk dihubungkan satu sama lain membentuk satu jaringan yang lebih besar. *Switch* meneruskan *(forwarding)* data berdasarkan *database* yang dibuat berdasarkan MAC *address*. MAC *address* sendiri merupakan identitas suatu divais yang terdiri dari 48 bits dimana 24 bit pertama diberikan oleh IEEE *Standard Association* sebagai OUI dan 24 bit sisanya diberikan ke vendor untuk memperoleh alamat yang bersifat unik untuk setiap *network interface* yang mereka buat.

Proses penerusan data pada *switch* dimulai dengan memeriksa alamat *source* dari paket yang datang, bila alamat yang diperiksa tidak terdapat dalam *database* maka tidak ada dalam *forwarding database* maka alamat tersebut akan dimasukkan dalam *database* beserta *port* dimana data tersebut datang . Proses selanjutnya adalah memeriksa alamat *destination*, apabila alamat *destination* tersebut tidak terdapat pada *forwarding database* maka paket tersebut akan dikirimkan ke seluruh *port* kecuali *port* tempat paket data tersebut datang. Bila alamat destination tersebut ada pada *database* maka paket data akan diteruskan melewati *port* tersebut asal *port* tersebut berbeda dengan *port* tempat paket data tersebut datang. Pada *switch*, sebuah paket data harus diterima secara lengkap dulu baru dapat diteruskan, hal ini menyebabkan adanya *latency* yang tergantung dari besarnya paket data [6].

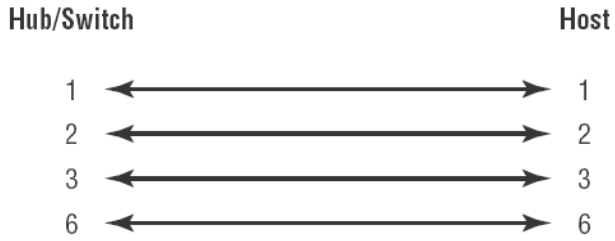
2.2.3 Pengkabelan

Pada r*outer* dan *switch* yang menggunakan interface berupa *Ethernet*, digunakan kabel RJ-45 yang dapat berupa UTP atau STP. Kabel RJ-45 ini mendukung transfer data berkecepatan tinggi sehingga dapat digunakan untuk menghubungkan interface *Fast Ethernet.* Terdapat dua macam konfigurasi pengkabelan dengan fungsi yang berbeda, yaitu kabel *straight-through* dan kabel *crossover* [5].

2.2.4 Kabel *straight-through*

Kabel *straight-through* digunakan untuk menghubungkan :

- *Host* ke *switch*
- *Router* ke *switch*



Gambar 2.2. Konfigurasi kabel *straight-through*

2.2.5 Kabel *crossover*

Kabel crossover digunakan untuk menghubungkan :

- *Switch* ke *switch*
- *Host* ke *host*
- *Router* ke *host*

Gambar 2.3. Konfigurasi kabel *crossover*

2.3 *ROUTING*

2.3.1 Pengenalan *Routing*

Routing merupakan proses berpindahnya data melalui jaringan dengan melalui beberapa segmen jaringan menggunakan peralatan yang disebut *router*. *Router* sebagai pengatur rute akan memilihkan jalur data yang tepat sesuai dengan arah yang ingin dituju data. Pada aplikasinya, r*outer* akan mengolah informasi tentang arah jalur paket data menjadi skema yang disebut *routing table*. Tabel ini berisi informasi *interface/port* dari r*outer* pada jaringan yang digunakan untuk mengirim data melalui segmen jarigngan tertentu. Sebuah r*outer* tidak akan menjalankan paket yang tidak diketahui tujuannya. Terdapat dua macam *routing*, yaitu *static routing* dan *dynamic routing* [3].

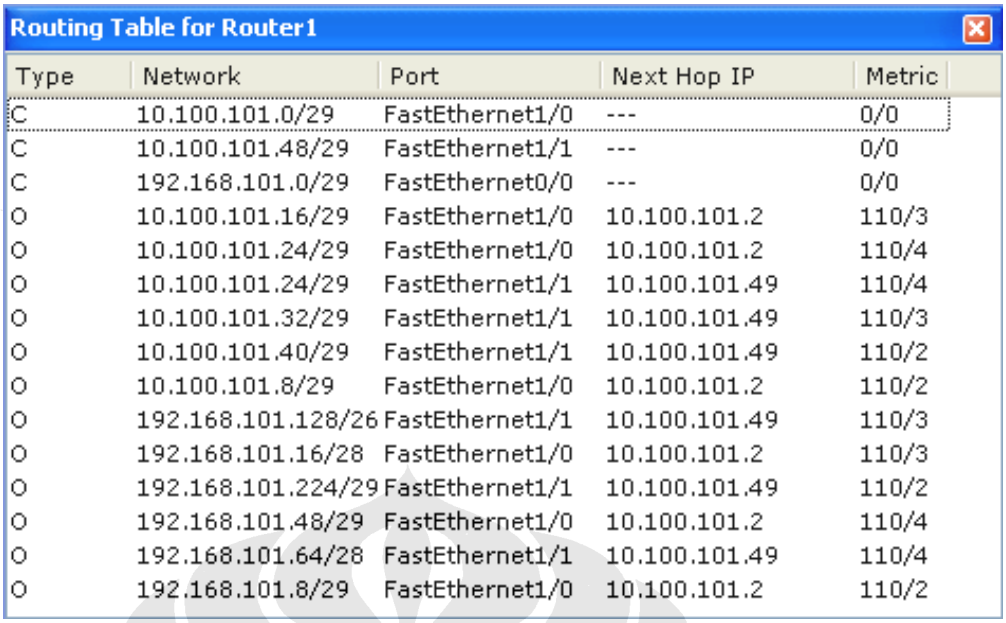
- *Static routing*

Pada *static routing* administrator jaringan akan melakukan *update* secara manual ke *routing table*-nya. Administrator akan memasukkan jaringan ke dalam *routing table* dan memilih *port* di mana r*outer* tersebut menempatkan data. Static *routing* memiliki kelebihan berupa tidak ada *bandwidth* yang digunakan di antara *router* dan selain itu dari terdapat keuntungan dari aspek keamanan karena proses *routing* benar – benar diawasi oleh administrator. Di sisi lain kerugiannya adalah keterbatasan kemampuan dari administrator sendiri karena semua proses *maintaining* dan penambahan jaringan harus dilakukan secara manual oleh administrator [3].

- *Dynamic routing*

Pada *dynamic routing* protokol – protokol digunakan untuk mencari jaringan dan memperbaharui *routing table* yang berisi jalur – jalur paket data. Contoh *routing table* dapat dilihat pada Gambar 2.4.

Penggunaan *dynamic routing* pada dasarnya lebih mudah dilakukan karena seorang administrator jaringan hanya harus sekali mengkonfigurasi *router* – r*outer* pada jaringan dengan suatu protokol dan selanjutnya r*outer – router* tersebut dapat menentukan sendiri jalur yang akan dipilih untuk mengirimkan paket data data. *Dynamic routing* bergantung pada algoritma dari masing protokol untuk memilih jalur yang terbaik dengan pertimbangan – pertimbangan seperti ketersediaan *bandwidth* pada jalur yang akan dilalui dan panjang waktu yang dibutuhkan untuk mengirimkan paket dari sumber ke tujuan. *Routing Protocol* yang umum digunakan antara lain RIP, IGRP, EIGRP, dan OSPF [3].



Routing Table for Router1

Type	Network	Port	Next Hop IP	Metric
C	10.100.101.0/29	FastEthernet1/0	---	0/0
C	10.100.101.48/29	FastEthernet1/1	---	0/0
C	192.168.101.0/29	FastEthernet0/0	---	0/0
O	10.100.101.16/29	FastEthernet1/0	10.100.101.2	110/3
O	10.100.101.24/29	FastEthernet1/0	10.100.101.2	110/4
O	10.100.101.24/29	FastEthernet1/1	10.100.101.49	110/4
O	10.100.101.32/29	FastEthernet1/1	10.100.101.49	110/3
O	10.100.101.40/29	FastEthernet1/1	10.100.101.49	110/2
O	10.100.101.8/29	FastEthernet1/0	10.100.101.2	110/2
O	192.168.101.128/26	FastEthernet1/1	10.100.101.49	110/3
O	192.168.101.16/28	FastEthernet1/0	10.100.101.2	110/3
O	192.168.101.224/29	FastEthernet1/1	10.100.101.49	110/2
O	192.168.101.48/29	FastEthernet1/0	10.100.101.2	110/4
O	192.168.101.64/28	FastEthernet1/1	10.100.101.49	110/4
O	192.168.101.8/29	FastEthernet1/0	10.100.101.2	110/2

Gambar 2.4. Contoh *routing table* [7]

2.4 DASAR *ROUTING PROTOCOL*

Terdapat sejumlah hal yang penting untuk dibahas untuk untuk memahami *dynamic routing*. Hal tersebut adalah *administrative distance*, tipe – tipe *routing protocol*, *routing loop*, dan komunikasi antar *router*.

2.4.1 *Administrative Distance*

Administrative distance(AD) digunakan untuk mengukur reliabilitas informasi *routing* dari yang diterima oleh sebuah *router* dari *router* tetangganya. Nilai *AD* berkisar pada bilangan bulat antara 0 sampai 255. Dimana 0 merupakan menunjukkan kemampuan penerusan data yang tertinggi dan 255 menunjukkan tidak ada data yang akan diteruskan melewati sebuah rute. *Routing Protocol* RIP, IGRP, EIGRP dan, OSPF masing – masing mempunyai nilai *AD* 120, 100, 90, dan 120 [5].

2.4.2 Tipe – tipe Routing Protocol

Terdapat tiga tipe *routing protocol* [5] :

- *Distance vector*

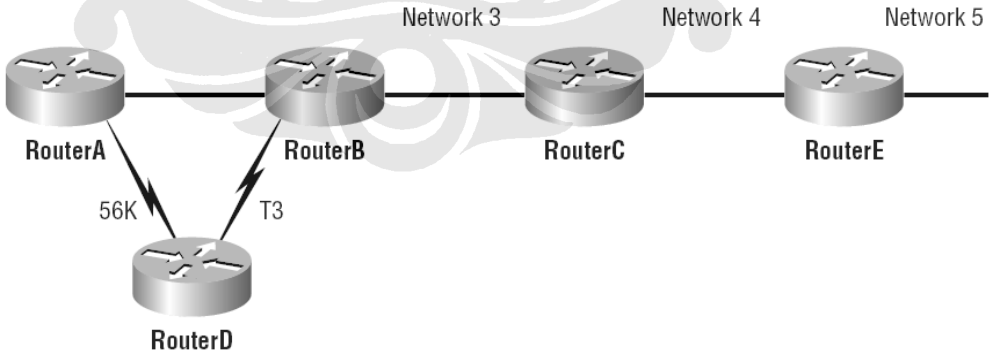
  Protokol yang bersifat *distance vector* akan mencari jalur terbaik ke sebuah jaringan lain yang terpisah dengan mempertimbangkan jaraknya. Setiap saat paket data melewati *router*, hal ini disebut *hop*. Jalur dengan jumlah *hop* paling sedikit akan dipakai sebagai jalur untuk mentransmisikan data.

Terminologi '*vector'* mengindikasikan arah ke jaringan lain tersebut. Protokol yang tergolong *distance vector* adalah RIP dan IGRP, dua protokol ini mengirimkan seluruh *routing table* ke *router* tetangga yang terhubung langsung.

- *Link State*
  Pada protokol yang bersifat *link state*, atau disebut juga *shortest path protocol*. R*outer* yang menggunakan protokol jenis ini membuat tiga tabel terpisah. Sebuah tabel dialokasikan untuk untuk memantau jalur dari *router* tetangga yang langsung terhubung, sebuah tabel menentukan topologi dari seluruh jaringan, dan sebuah lagi digunakan untuk *routing table*. *Link state protocol* mengirimkan *update* kondisi *router* ke seluruh *router* yang ada di jaringan.
- *Hybrid*
  Hybrid protocol menggunakan aspek – aspek dari *distance vector* dan *link state*, misalnya EIGRP.

2.4.3 *Routing loop*

Routing loop dapat terjadi karena setiap *routing table* dari setiap *router* di jaringan tidak di *update* secara simultan sehingga timbul inkonsistensi dari *routing table* itu sendiri. Contoh fenomena *routing loop* dapat dilihat di Gambar 2.5.



Gambar 2.5. Contoh *routing loop* [5].

Pada Gambar 2.3 semua *router* mengetahui tentang *Network* 5 dari RouterE. RouterA, pada *routing table* yang dimilikinya, memiliki jalur menuju Network 5 yang melalui RouterB. Pada saat Network 5 mengalami kegagalan,

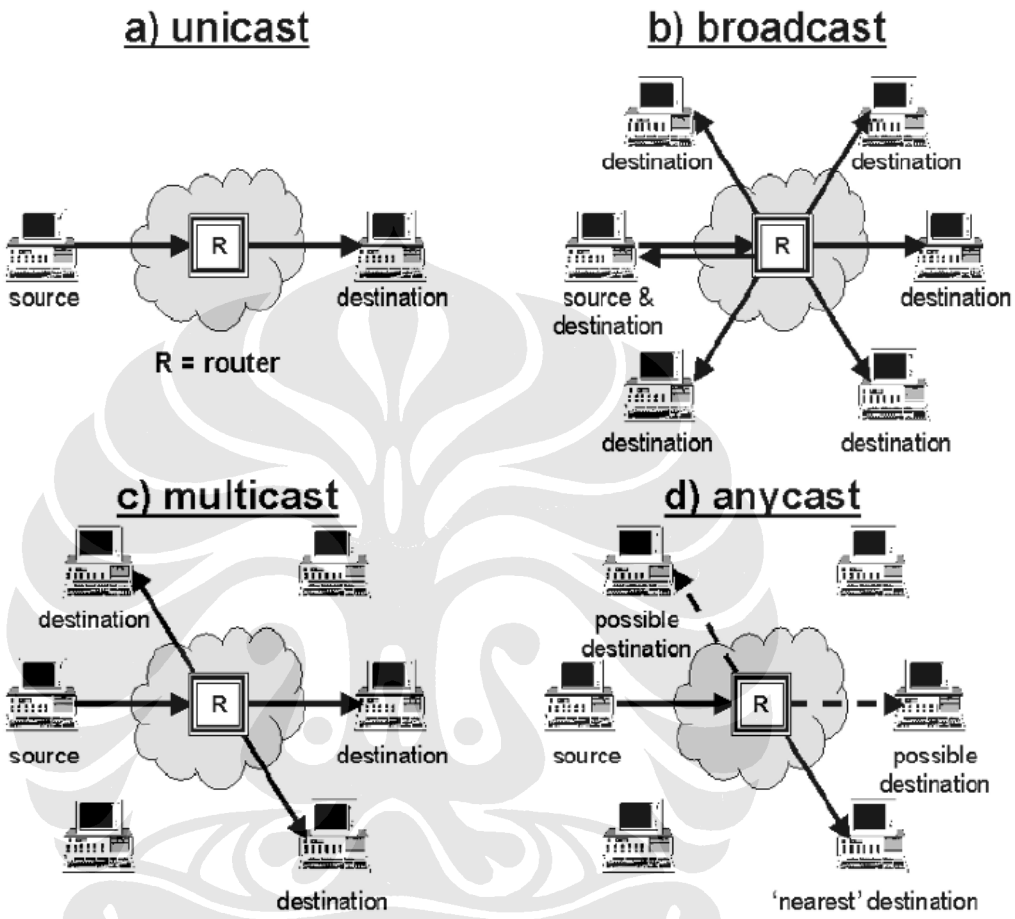
RouterE memberitahu RouterC. Hal ini menyebabkan RouterC untuk menghentikan proses *routing* ke Network 5 melalui RouterE. Tetapi Router A, B, C, dan D belum mengetahui keadaan Network 5 sehingga mereka tetap mengirim *update* informasi. RouterC pada akhirnya akan mengirimkan *update* informasi tentang kegagalan Network 5 dan menyebabkan RouterB berhenti untuk melakukan *routing* ke Network 5, tapi RouterA dan RouterD belum menerima *update* sehingga bagi mereka *Network* 5 masih bekerja dengan jalur *routing* melewati RouterB. Permasalahan lalu terjadi pada saat Router A mengirimkan sinyal *hello* ke RouterA dan RouterD yang secara garis besar memberitahukan bahwa Network 5 masih dapat diakses. Mengetahui hal ini RouterA dan RouterD akan mengirimkan *update* informasi juga bahwa Network 5 dapat diakses. Sehingga setiap paket yang akan menuju *Network* 5 akan menuju ke RouterA ke RouterB lalu ke RouterA lagi dan seterusnya, hal inilah yang disebut *routing loop*. Hal ini dapat dihindari dengan mendefinisikan *maximum hop count*, sehingga paket yang jumlah *hop*-nya melebihi *maximum hop count*, tujuannya akan dinyatakan tak dapat dicapai *(unreachable)* [5].

2.4.4 Komunikasi antar router

Komunikasi antar *router* dapat dilakukan dengan empat cara, yaitu *unicast*, *broadcast*, *multicast*, dan *anycast* [13]. Ilustrasi dari 4 jenis komunikasi ini ditunjukkan pada Gambar 2.6.

- *Unicast*
  Sebuah paket data dikirim oleh sebuah *source* ke sebuah alamat tujuan.
- *Broadcast*
  Paket data sebuah dikirim sebuah *source* dengan beberapa alamat tujuan. Hal ini dilakukan dengan mengirim paket data yang ke *router*, dan nantinya *router* tersebut akan mengirimkan paket data tersebut ke sejumlah alamat yang diinginkan.
- *Multicast*
  Sebuah *source* mengirimkan paket data ke sekelompok tujuan yang telah mempunyai alamat tertentu yang spesifik. Alamat spesifik ini dikeluarkan oleh IANA.

- *Anycast*
  Merupakan variasi dari *multicast*. Pada *anycast*, paket data akan dikirimkan oleh *router* ke tujuan yang dianggap paling dekat dari sebuah kelompok.



Gambar 2.6. Empat macam komunikasi antar *router* [13]

2.5 OSPF *ROUTING PROTOCOL*

2.5.1 Pengenalan OSPF

OSPF merupakan *link-state protocol* yang mengirimkan LSA (*Link-state* Advertisement) ke semua *router* yang terletak dalam satu hierarki area yang sama. Inforrmasi yang terdapat dalam LSA antara lain adalah informasi mengenai *interface* yang digunakan dan *metric* yang digunakan. *Router* OSPF menggunakan algoritma SPF untuk mengkalkulasi jalur terbaik yang dapat dilewati data [4]. Terminologi – terminologi penting yang berhubungan dengan OSPF antara lain :

Link : Jaringan atau *interface* suatu *Router* yang dialokasikan ke sebuah jaringan tertentu. Saat sebuah *interface* ditambahkan ke dalam proses OSPF maka, protokol OSPF menganggapnya sebagai sebuah *link*.

Router ID : Alamat IP yang digunakan untuk mengidentifikasi sebuah *router*.

Neighbor : Dua atau lebih *router* yang mempunyai *interface* yang berada pada *network* yang sama.

Adjacency : Hubungan antara dua *router* OSPF yang mendukung pertukaran langsung *update* informasi.

Hello protocol : Protokol OSPF yang berfungsi melakukan pencarian *neighbor* secara dinamis sekaligus menjaga keterhubungan antara *neighbor*.

Neighborship database : Daftar dari semua *router* OSPF yang dikirimi paket *hello*.

Topological database : Daftar yang menyimpan informasi dari semua LSA yang telah diterima oleh sebuah area.

Link State Advertisement : Paket data OSPF yang mengandung informasi *link-state* dan informasi *routing* yang dipakai bersama antar sejumlah *router* OSPF. Sebuah *router* OSPF hanya akan bertukar paket LSA dengan *router* yang telah membentuk *adjacency*.

Designated Router : Sebuah *DR* dipilih pada saat *router* OSPF dihubungkan ke ke *multi-access network* yang sama.

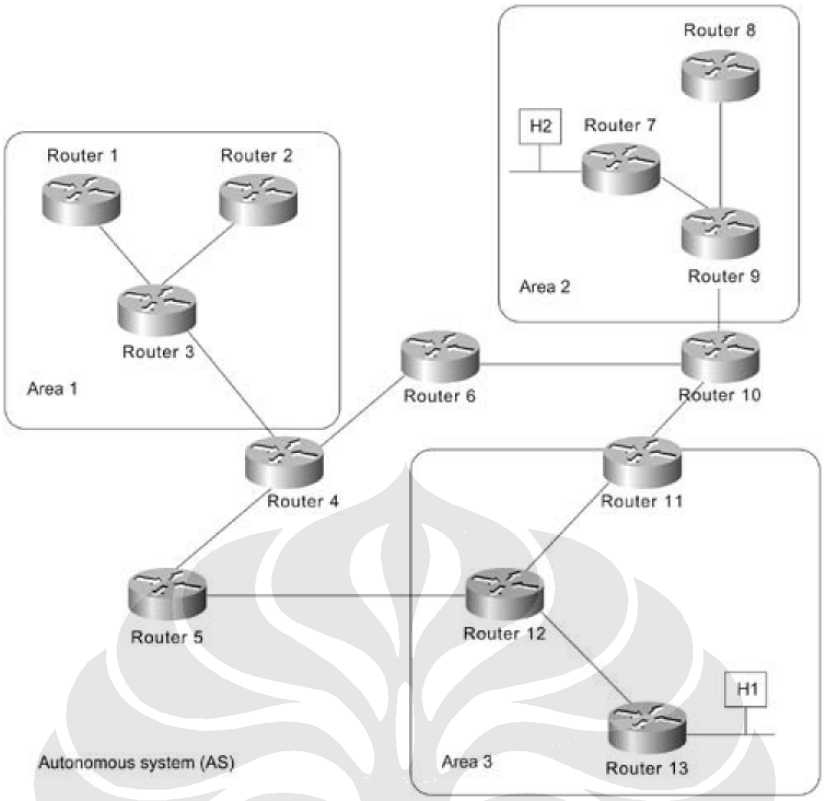
OSPF areas : Merupakan sekelompok jaringan dan *network* yang bersifat *contigous*. Semua *router* yang berada pada satu area akan menggunakan area ID yang sama. Pada sebuah *router*, area ID diperuntukkan bagi *interface*, sehingga memungkinkan dalam satu *router* terdapat *port – port* yang berada pada *interface* yang berbeda.

2.5.2 Hierarki Routing

Pengimplementasian OSPF dianjurkan dalam bentuk hierarkial, sehingga sebuah jaringan yang besar dapat dibagi menjadi sekumpulan jaringan – jaringan yang lebih kecil [4].

OSPF dapat beroperasi dalam hierarki, dimana entitas terbesar dalam sebuah hirarki adalah *autonomus system* (AS), yang merupakan gabungan jaringan yang yang memakai bersama sebuah algoritma *routing*. Sebuah AS dapat dibagi menjadi beberapa area, yang merupakan kumpulan jaringan dan *host*. *Router* dengan banyak *interface* dapat berada pada beberapa area sekaligus dengan mengatur konfigurasi area pada *interface* yang diinginkan. Pertukaran informasi *routing* antar area dilakukan oleh OSPF *backbone*, OSPF *backbone* sendiri terdiri atas sejumlah *Area Border Router* (ABR) yang menjaga *topological database* yang terpisah untuk masing –masing area. dilakukan Gambar 2.7 memperlihatkan contoh desain OSPF dengan susunan hierarkial.

Pada Gambar 2.7, *router* 4, 5, 6, 10, 11, dan 12 membentuk OSPF backbone, semua *router* yang membentuk *backbone* ini merupakan *router – router* OSPF yang berada pada area yang sama, sehingga semua *router* penyusun backbone menggunakan prosedur dan algoritma yang sama. Sementara r*outer* 4, 10, dan 12 merupakan *router* ABR karena bersifat sebagai *gateway* suatu area.



Gambar 2.7. Contoh OSPF dengan susunan hierarkial [4]

2.5.3 Algoritma SPF

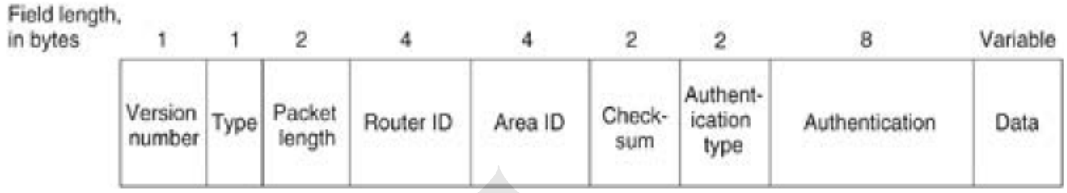
Algoritma *routing* SPF merupakan dasar operasi OSPF, pada saat *router* yang dikonfigurasi dengan OSPF dinyalakan maka, *router* tersebut menginisialisasi *routing protocol* dan menunggu respon dari *interface* yang menyatakan bahwa mereka dalam keadaan fungsional. Setelah r*outer* mendapat respon dari *interface* maka *router* mulai mengirimkan paket *hello* untuk mendapatkan *neighbor*.

Selain untuk mendapatkan *neighbor,* paket *hello* juga digunakan sebagai konfirmasi bahwa *router* lain di jaringan masih dalam keadaan fungsional. Pada *multi-access network* (jaringan yang mendukung lebih dari dua *router)*, paket h*ello* memilih *DR* yang nantinya berfungsi untuk menyebarkan LSA ke seluruh jaringan. Apabila *database link-state* antara dua *router* yang bertetangga telah disinkronisasi makan kedua *router* tersebut dinyatakan telah *adjacent*. Setiap *router* secara periodik mengirimkan LSA untuk menginformasikan *adjacency* dari *router* tersebut atau untuk mengirimkan *update* informasi tentang keadaan r*outer* tersebut. Dengan membandingkan *adjacency* yang ada dengan *link-state*, *router*

yang mengalami kegagalan dapat dideteksi secara cepat dan topologi jaringan pun dapat disesuaikan dengan cepat pula [5].

2.5.4 Paket OSPF

Semua paket OSPF dimulai dengan *header* sepanjang 24 byte, seperti dapat dilihat pada Gambar 2.5.



Gambar 2.8. . Header OSPF [4]

Berikut ini adalah penjelasan dari *header* tersebut :

Version Number : Mengidentifikasi versi yang digunakan

Type : mengidentifikasi tipe paket OSPF, yang terdiri dari:

a. *Hello*—membangun dan mengatur hubungan antar *neighbor*.
b. *Database description*—Menjelaskan isi dari *topology database*. Pesan ini dipertukarkan ketika urutan diinisialisasi
c. *Link-state request*—meminta bagian dari *topology database* dari neighbor. Pesan ini dipertukarkan setelah *router* menemukan bagian itu dari *topology database*.
d. *Link-state update*—Memberikan respon terhadap *link-state request.*
e. *Link-state acknowledgment*—mengkonfirmasi paket *link-state update.*

Packet length : Menetapkan panjang paket, termasuk *header* OSPF, dalam *bytes*.

Router ID : Mengidentifikasi sumber paket

Area ID **:** Mengidentifikasi area dimana paket berasal. Semua paket OSPF diasosiasikan dengan satu buah area

Checksum : Memeriksa semua isi paket untuk semua jenis kerusakan yang terjadi saat transit.

Autenthication type : Berisi tipe autentikasi. Semua protokol pertukaran OSPF diautentikasi. Tipe autentikasi dapat dikonfigurasi pada basis area.

Autenthication : Berisi informasi autentikasi

Data : Berisi informasi layer teratas yang dienkapsulasi.

2.6 EIGRP *ROUTING PROTOCOL*

2.6.1 Pengenalan EIGRP

EIGRP merupakan *routing protocol* yang dikembangkan dari IGRP, dan hanya dapat digunakan oleh *router* yang diproduksi oleh Cisco, Inc. EIGRP menggunakan konsep *autonomous system* untuk menggambarkan sekelompok *router* yang beroperasi dengan menggunakan protokol yang sama dan berbagi informasi *routing* yang sama. EIGRP merupakan protokol yang bersifat *hybrid* yang menggunakan aspek – aspek yang bersifat *distance vector* dan *link state*, dimana EIGRP mengirimkan *update* informasi tentang jaringan sekaligus *cost* untuk mencapai suatu tujuan, dimana hal ini merupakan karakteristik *distance vector,* namun di sisi lain EIGRP mengsinkronisasi *routing table* antara *neighbor* dan mengirim *update* informasi pada saat terjadi perubahan topologi. EIGRP mempunyai *maximum hop* sebesar 255, dengan *default* sebesar 100 [5]. Terminologi – terminologi yang digunakan pada EIGRP antara lain :

Feasible distance : Rute terbaik yang dapat ditemui pada *routing table.*

Neighbor table : Tabel yang berisi alamat dan *interface* dari suatu *router* yang bersifat *adjacent.*

Topology table : Tabel yang menyimpan informasi semua tujuan yang diberitahukan *(advertised)* oleh *neighbor* sekaligus daftar semua *neighbor* yang telah melakukan pemberitahuan *(advertising)*

Feasible successor : Jalur yang jaraknya kurang dari *feasible distance* dan dianggap sebagai rute cadangan. EIGRP akan

menyimpan sampai dengan enam buah *feasible successor* dalam *topology table*.

Successor : Rute terbaik ke suatu jaringan yang terpisah. Rute ini digunakan oleh EIGRP untuk meneruskan trafik data ke suatu tujuan dan rute ini akan disimpan di *routing table.*

2.6.2 Teknologi Pendukung EIGRP

Untuk mendukung proses *routing* yang cepat dan handal, EIGRP menggunakan empat teknologi kunci, yaitu *neighbor discovery/recovery*, *Reliable Transport Protocol* (RTP), *Diffusing Update Algorithm* (DUAL), dan *protocol dependent modules.*

- *Neighbor Discovery/Recovery*

Mekanisme *neighbor discover/ recovery* memungkinkan *router* untuk secara dinamis mempelajari *router* lain yang terdapat dalam jaringan yang sama. *Router* harus dapat mengetahui kondisi bila *neighbor* mereka tak dapat dijangkau *(unreachable)* atau tidak beroperasi. Proses ini dilakukan dengan secara periodik mengirimkan paket *hello*, sehingga selama suatu *router* menerima paket *hello* dari *neighbor* maka *router* akan mengasumsikan bahwa *neighbor*-nya masih dalam keadaan aktif [5].

- *Reliable Transport Protocol (RTP)*

RTP bertanggung jawab untuk menjamin sampainya paket EIGRP dari suatu *router* ke semua *neighbor*-nya. Pada proses *routing* dengan EIGRP suatu *router* menyebarkan paket secara multicast, maka *router* EIGRP akan mencatat *neighbor* mana saja yang memberikan balasan. Apabila ada *neighbor* yang terdaftar dalam *routing table* namun tidak member balasan, maka *router* tersebut akan mengirim ulang paket data secara *multicast* hanya ke *neighbor* yang tidak memberi balasan [4].

- *Diffusing Update Algorithm (DUAL)*

EIGRP menggunakan DUAL utnuk mencari dan menjaga *(maintaining)* jalur terbaik yang dapat dilewati data ke setiap jaringan terpisah. Algoritmanya meliputi hal – hal berikut [5] :

  - Membuat rute cadangan
  - Mendukung VLSM *(Variable Length Subnet Masking)*
  - Pembuatan ulang rute dinamis
  - Membuat sejumlah rute alternatif bila tak ada rute yang bisa ditemukan.

- *Protocol Dependent Modules (PDM)*

EIGRP mendukung pelaksanaan *routing* untuk bermacam protokol *Network layer* seperti : IP, IPX, dan Apple Talk, dengan penggunaan PDM. Setiap PDM akan menetapkan seri tabel yang terpisah untuk informasi *routing* bagi setiap protokol tersebut.

2.6.3 Tipe – tipe Paket EIGRP

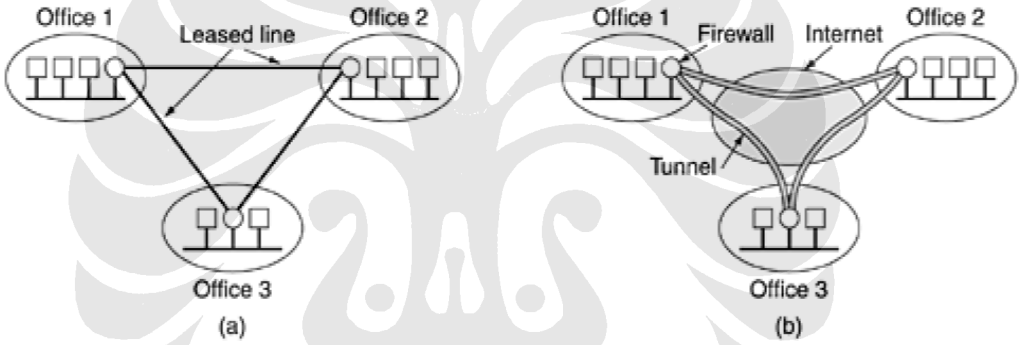
EIGRP menggunakan empat tipe paket data untuk komunikasi divais – divasis penyusun jaringan, yaitu *hello, acknowledgement, update, query,* dan *reply* [5].

- *Hello* : Paket data yang disebarkan secara *multicast* untuk mencari *router* yang akan dijadikan *neighbor*
- *Acknowledgement* : Merupakan paket *hello* yang tidak berisi data dan dikirimkan secara unicast ke satu alamat tertentu.
- *Update* : Digunakan untuk memverifikasi *reachability* dari suatu alamat tujuan
- *Query* dan *reply* : Paket *query* dan *reply* dikirimkan pada saat alamat yang ingin dituju tidak mempunyai *feasible successor*. Paket *query* dikirimkan secara multicast, dan paket *reply* dikirim dikirm sebagai response untuk meminta pemilihan jalur ulang.

2.7 VPN

Terminologi VPN *(Virtual Private Network)* merujuk kepada hubungan antara sejumlah lokasi pelanggan dengan menggunakan suatu infrastruktur berupa VPN *backbone* yang digunakan bersama oleh sejumlah pelanggan. Dari sudut pandang pelanggan, *backbone* tersebut seolah – olah diperuntukkan hanya untuk pelanggan tersebut [12. Dalam skala institusi atau organisasi, kebutuhan – kebutuhan komunikasi yang menjadi pendorong digunakannya VPN, antara lain [12] :

- Komunikasi *intra-organizational (intranet)*
- Komunikasi dengan organisasi lain *(extranet)*
- Akses oleh *mobile user* dan *home workers* yang ingin terhubung dengan *internal network* suatu organisasi melalui jaringan publik.



Gambar 2.9. (a) Leased line; (b) VPN [8]

Sebelum VPN digunakan biasanya organisasi atau perusahaan yang mempunyai kantor cabang, menyewa jalur komunikasi *(leased line)* dari perusahaan telepon setempat, hal ini sangat aman karena tidak ada trafik data yang dapat keluar dari jalur ini. Namun hal ini dirasakan tidak efektif dari segi biaya karena mahalnya biaya sewa ini. VPN dikembangkan untuk menjadi solusi karena jaringan yang digunakan merupakan jaringan publik namun tetap menjamin aspek keamanan dari transfer data[8]. Pada Gambar 2.9 pengimplementasian VPN dilakukan dengan menggunakan jaringan publik berupa jaringan internet. Dengan alternatif pengimplementasian seperti ini aspek keamanan dicapai dengan mekanisme VPN *tunnel.* VPN *tunnel* adalah jalur logika antara dua divais misalnya *router* PE yang membawa trafik data *customer* melewati backbone. Penggunaan VPN tunnel ini penting untuk menjamin keamaman trafik data dan

untuk menyediakan QoS yang berbeda antar *custome.* Pada Gambar 2.9 VPN *tunnel* misalnya dilakukan oleh *office 1* dan *office 2* untuk melakukan pertukaran data melewati jaringan internet publik dengan menggunakan VPN *label* sebagai identitas agar suatu paket data dapat dilewatkan di VPN *tunnel* tersebut [12].

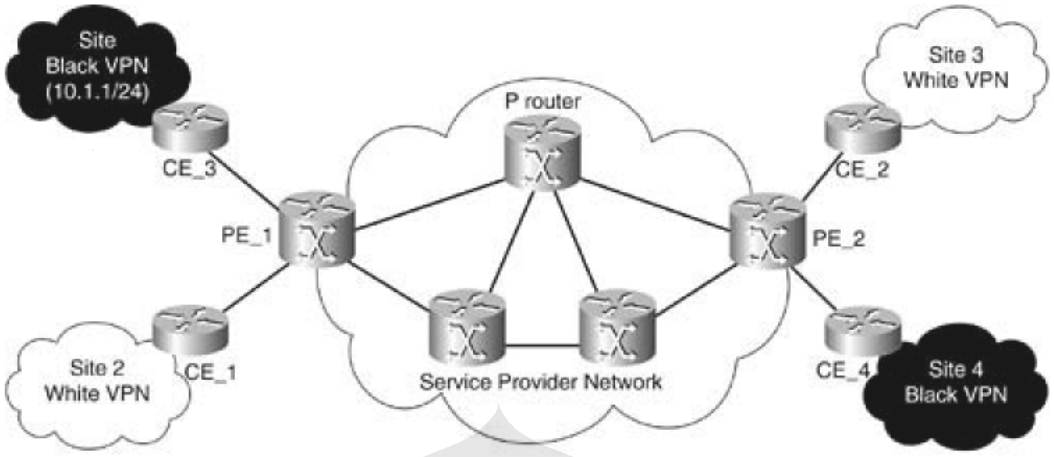
2.7.1 Komponen – komponen VPN

Dalam aplikasinya, VPN mempunyai komponen – komponen sebagai berikut [12] :

- *Service Provider* : Organisasi yang memiliki infrastruktur pelaksana layanan VPN. Infrastruktur berupa perlengkapan dan media transmisi yang menyediakan hubungan ke pelanggan.
- Divais CE : Divais yang digunakan *customer* untuk menghubungkan diri dengan jaringan milik *service provider*.
- Divais PE : Merupakan divais yang bersifat *lastmile* di sisi *service provider* yang akan akan dihubungkan dengan divais CE.
- P-*devices* : Peralatan tambahan milik *service provider* yang ditempatkan di *core network.*
- *Site* : Sisi terluar dari jaringan milik customer yang akan dihubungkan dengan jaringan milik *service provider*.

2.7.2 Pengimplementasian VPN dengan L3VPN

Pada pengimplementasian L3VPN, divais *backbone* menerima paket data dari *customer* lalu menentukan cara untuk meneruskan paket data tersebut dengan mempertimbangkan alamat asal datangnya paket data tersebut dan informasi *network layer* (*Layer 3*) yang ada pada header paket tersebut [12]. Hal ini dilakukan oleh divais yang bekerja di *Layer 3* dalam hal ini *router,* sehingga dalam hal ini *backbone* L3VPN akan tersusun dari sejumlah *router* dengan topologi tertentu, seperti ditunjukkan pada Gambar 2.10. Pengimplementasian L3VPN dilakukan dengan menggunakan BGP/MPLS VPN, seperti dideskripsikan pada *draft* IETF RFC 2547 [4].



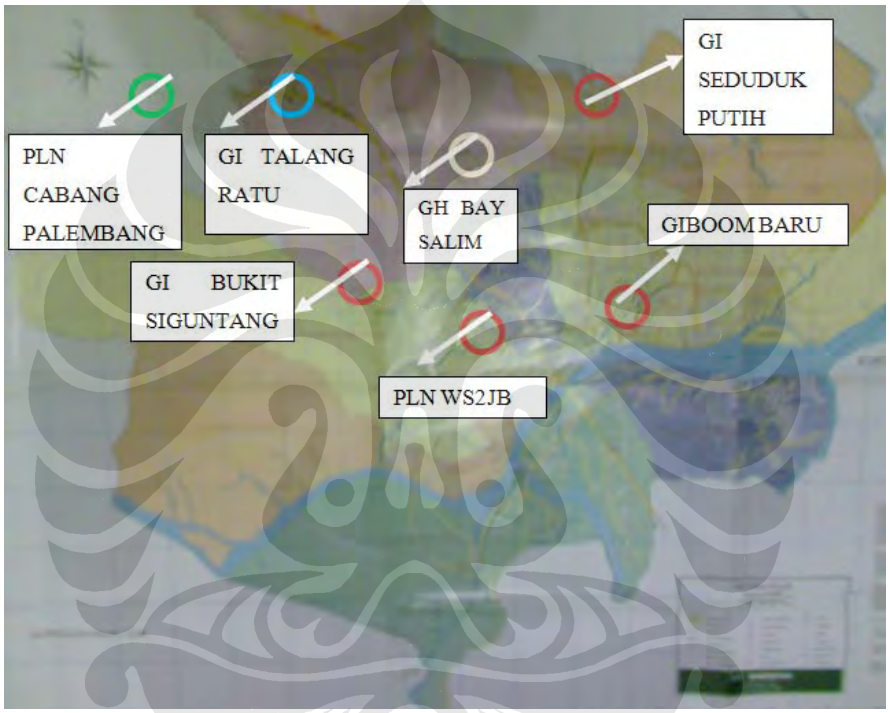
Gambar 2.10. Contoh pengimplementasian L3VPN [12]

Pada pengimplementasian L3VPN seperti yang ditunjukkan pada Gambar 2.10 diperlukan *routing protocol* yang akan bekerja pada *backbone* yang berfungsi untuk melakukan *advertise* terhadap topologi jaringan, melakukan pertukaran informasi *routing* melalui pertukaran *routing table*, dan melakukan perhitungan untuk menentukan jalur yang paling *feasible* untuk mencapai tujuan. *Routing protocol* yang dapat digunakan untuk fungsi ini antara lain RIP, OSPF, IGRP, dan EIGRP. Setelah pengimplementasian *routing protocol*, protokol yang selanjutnya diimplementasikan adalah MPLS *signaling protocol*, yang dapat berupa BGP, LDP, dan RSVP. MPLS *signaling protocol* ini berfungsi untuk menetapkan dan menghapus jalur yang dipakai sebagai VPN *tunnel*.

BAB III PERANCANGAN DAN PENGIMPLEMENTASIAN JARINGAN

3.1 AREA PERANCANGAN JARINGAN

Penelitian ini didasarkan pada studi kasus pada PT. Indonesia Comnetss Plus (PT. ICON +), dimana PT. ICON + bermaksud menghubungkan unit – unit usaha PLN yang berlokasi di kota Palembang. Adapun lokasi – lokasi yang ingin dihubungkan ditunjukkan pada Gambar 3.1.



Gambar 3.1. Lokasi unit – unit usaha PLN di kota Palembang

Pada Gambar 3.1, “GI” adalah kependekan dari gardu induk, sementara “GH” adalah kependekan dari gardu hubung. Pada tujuh lokasi yang ditunjukkan pada Gambar 3.1, masing – masing mempunyai alokasi jumlah *host* dan *bandwidth* seperti ditunjukkan pada Tabel 3.1 berikut.

Tabel 3.1. Distribusi *host* dan alokasi *bandwidth* untuk masing – masing lokasi

No	Lokasi	Jumlah *host*	Alokasi Bandwidth (Kbps)
1.	GI Talang Kelapa	5	64
2.	GI. Talang Ratu	5	64
3.	GH. Bay Salim	10	64
4.	GI. Seduduk Putih	5	64
5.	GI. Boom Baru	10	64
6.	Kantor PLN WS2JB	50	2048
7.	GI. Bukit Siguntang	5	64

3.2 LAYANAN PADA JARINGAN

Langkah awal untuk mendesain jaringan adalah mengidentifikasi layanan yang akan dijalankan pada jaringan. Untuk kasus pada PT. ICON + ini, jaringan yang akan dibangun harus dapat mendukung layanan berikut :

- VPN

Salah satu alternatif cara untuk membangun VPN adalah dengan menggunakan L3VPN [1]. Untuk mendesain jaringan dengan cara ini maka divais – divais yang membentuk *backbone* jaringan adalah divais yang bekerja pada *layer* 3 atau *network layer*. Divais yang memenuhi spesifikasi ini adalah *router* sehingga *backbone* jaringan yang akan dibangun akan berupa terdiri dari rangkaian *router*. Jaringan yang akan mendukung diimplementasikannya L3VPN pertama – tama harus dipastikan tersambung dahulu, dan ketersambungan ini dicapai dengan penggunaan *routing protocol*. Sehingga keberadaan *routing protocol* menjadi sesuatu yang penting sebelum pengimplementasian L3VPN. Dari sejumlah alternatif *routing protocol* yang ada, yang akan digunakan untuk

menyiapkan jaringan adalah OSPF dan EIGRP. Dua *routing protocol* ini dipilih karena paling populer dan paling banyak digunakan dewasa ini [5]. Perbandingan karakteristik *routing protocol* OSPF dan EIGRP ditunjukkan pada Tabel 3.2.

- Akses Internet

Ketersambungan dengan internet dapat dilihat dari kemampuan *host* untuk mengakses halaman web yang dapat berbasis HTTP serta melakukan *upload* dan *download file* menggunakan protokol TFTP sebuah *web server*.

Tabel 3.2. Perbandingan Karakteristik OSPF dan EIGRP [5].

Karakteristik	**OSPF**	**EIGRP**
Tipe protokol	***Link State***	***Hybrid***
Mendukung IP *classless*	**Ya**	**Ya**
Mendukung VLSM	**Ya**	**Ya**
Menggunakan *auto-summarization*	**Tidak**	**Ya**
Metric	***Bandwidth***	**Jumlah *hop***
Jumlah *hop* maksimum	**Tidak ada**	**255**

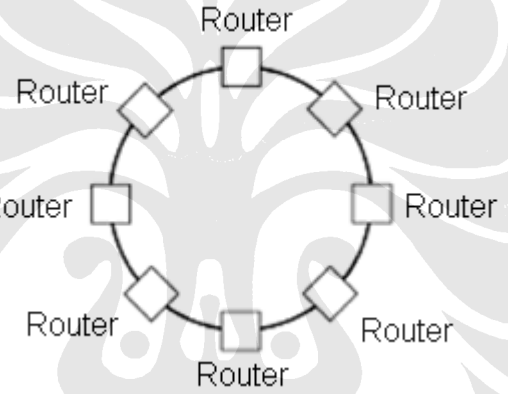
3.3 PEMILIHAN TOPOLOGI JARINGAN

Hal penting yang harus dilakukan dalam perancangan jaringan adalah pemilihan topologi yang akan dipakai, karena topologi akan menentukan hubungan fisik antar divais – divais jaringan.. Topologi yang akan digunakan untuk jaringan pada area yang ditunjukkan pada Gambar 3.1 adalah topologi *ring.* Berikut ini adalah poin – poin alasan dipilihnya topologi *ring* :

- Area layanan yang secara geografis berbentuk memutar.
- Mendukung redundansi, sehingga pada saat satu jalur mengalami kegagalan masih ada jalur alternatif [10].

- Jaringan tergolong jaringan kecil, karena hanya terdiri 7 lokasi [9].
- Ekonomis dari segi pengkabelan [9].
- Mendukung *fault tolerant. Fault tolerant* adalah kemampuan jaringan untuk dapat mengantisipasi kegagalan yang terjadi [9].
- Mempunyai tingkat availibilitas yang tinggi [10].

Dengan penggunaan topologi *ring* dan disesuaikan dengan kebutuhan layanan yang telah dispesifikasikan pada sub-bab 3.2, maka akan ditempatkan *router* pada lokasi – lokasi yang ditunjukkan pada Gambar 3.1, sehingga membentuk *backbone* yang akan melayani keperluan *host – host* di setiap unit – unit usaha PLN. Ilustrasi penggunaan *router* yang disusun dengan topologi *ring* ditunjukkan pada Gambar 3.2.



Gambar 3.2. *Router – router* yang disusun dengan topologi *ring* untuk *backbone*

3.4 DESAIN JARINGAN

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

- Mendesain jaringan logika
- Mengimplementasikan dengan *software,* dengan *software* yang digunakan pada penelitian ini adallah PacketTracer v4.11

3.4.1 Mendesain Jaringan Logika

Jaringan logika jaringan hanya memfokuskan pada konektivitas secara logika dan tidak memperhitungkan hal – hal yang menunjang konektivitas sevara fisik, misalnya panjang kabel yang digunakan. Jaringan logika dibuat untuk

memberikan gambaran tentang seperti apa jaringan yang akan dibangun nantinya. Gambar 3.3 memperlihatkan desain jaringan logika yang untuk area yang ditunjukkan pada Gambar 3.1. Pada tahapan desain ini yang dipentingkan adalah pengaplikasian topologi yang telah dipilih beserta divais – divais yang ingin digunakan. Pada Gambar 3.3 dapat dilihat bahwa lokasi – lokasi unit usaha PLN dihubungkan dengan menggunakan *router – router* yang disusun dengan topologi *ring.*

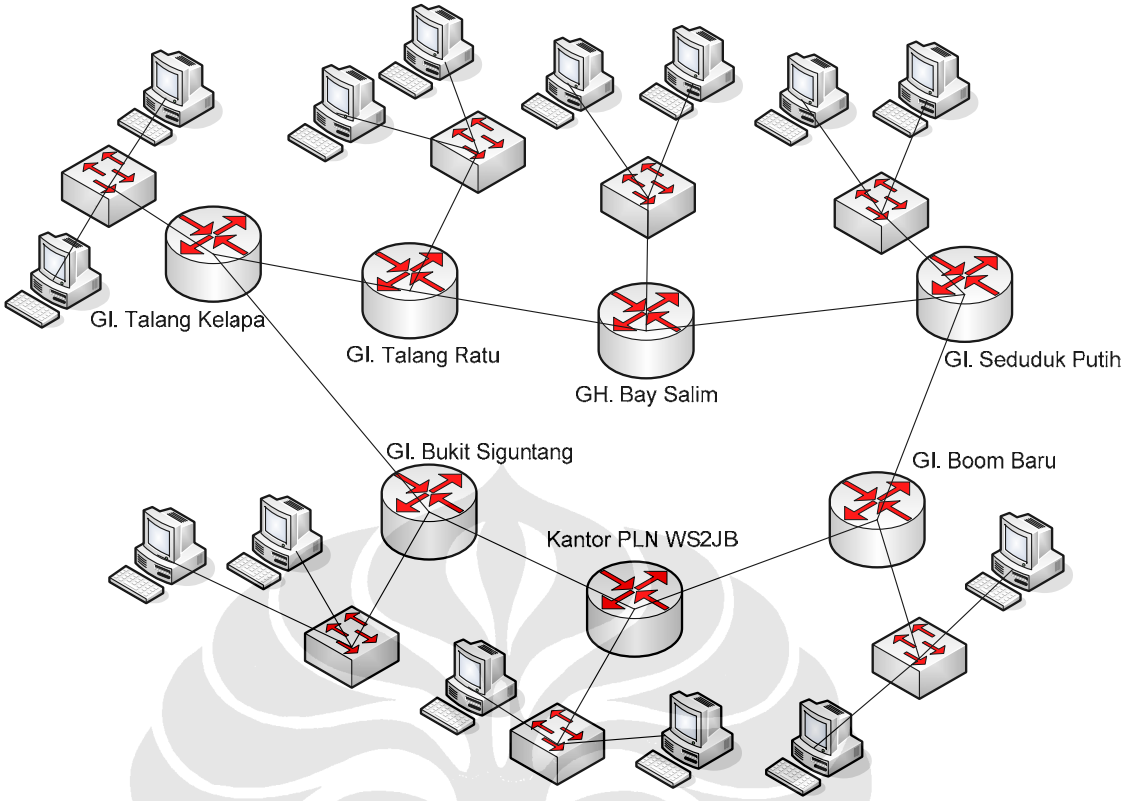
Pengaplikasian topologi ring dapat dilihat dari koneksi antar *router – router* yang ditempatkan di lokasi - lokasi unit usaha PLN yang berbentuk *loop* tertutup. *Router – router* yang tersusun dengan topologi *ring* tersebut akan bertindak sebagai *backbone*. Penempatan *switch* sebagai divais perantara antara host dengan *router* dimaksudkan sebagai pembagi koneksi, dalam hal ini koneksi *Fast Ethernet* yang *interface*-nya terdapat pada *router*. Dengan susunan seperti ini, *router* pada sebuah lokasi, misalnya pada GI. Talang Ratu akan bertindak sebagai *gateway* yang akan memberikan akses bagi *host* untuk menggunakan layanan yang tersedia pada jaringan.

3.4.2 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 dengan *routing protocol* OSPF dan EIGRP.



Gambar 3.3. Desain jaringan logika

3.4.2.1. Pemilihan Divais

Untuk membuat jaringan yang dapat mendukung penggunaan *routing protocol* OSPF dan EIGRP dan dapat diujicoba, digunakan divais – divais berikut :

1. Komputer *(PC)*

   Komputer ini berfungsi untuk mewakili *host – host* pada unit – unit usaha PLN yang akan mengakses jaringan.

Gambar 3.4. . *Host PC* [7]

Komputer yang digunakan mempunyai *port Fast Ethernet* dengan kode PT-*HOST*-NM-1CFE, seperti ditunjukkan pada Gambar 3.5.

Gambar 3.5. . *Port Fast Ethernet* PT-*HOST*-NM-1CFE [7]

2. *Switch*

Berfungi sebagai divais untuk membagi koneksi dari *backbone* ke *host – host*, hal ini dilakukan untuk efisiensi. *Switch* yang digunakan adalah Cisco Catalyst 2950-24.

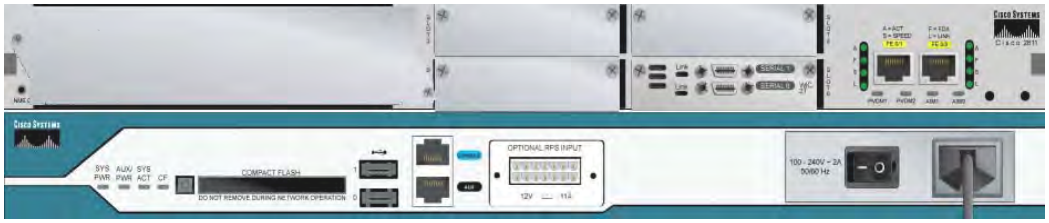
Gambar 3.6. Cisco Catalyst 2950-24 [7]

3. *Router*

Untuk membuat jaringan *backbone* OSPF dan EIGRP, *router* yang dipilih adalah *router* Cisco tipe 2811 dengan modul *Fast Ethernet*. Pemilihan *modul Fast Ethernet* ini dilakukan untuk mengakomodasi keperluan akan *backbone* yang ingin dibangun dengan koneksi *Fast Ethernet*.

4. Pengkabelan

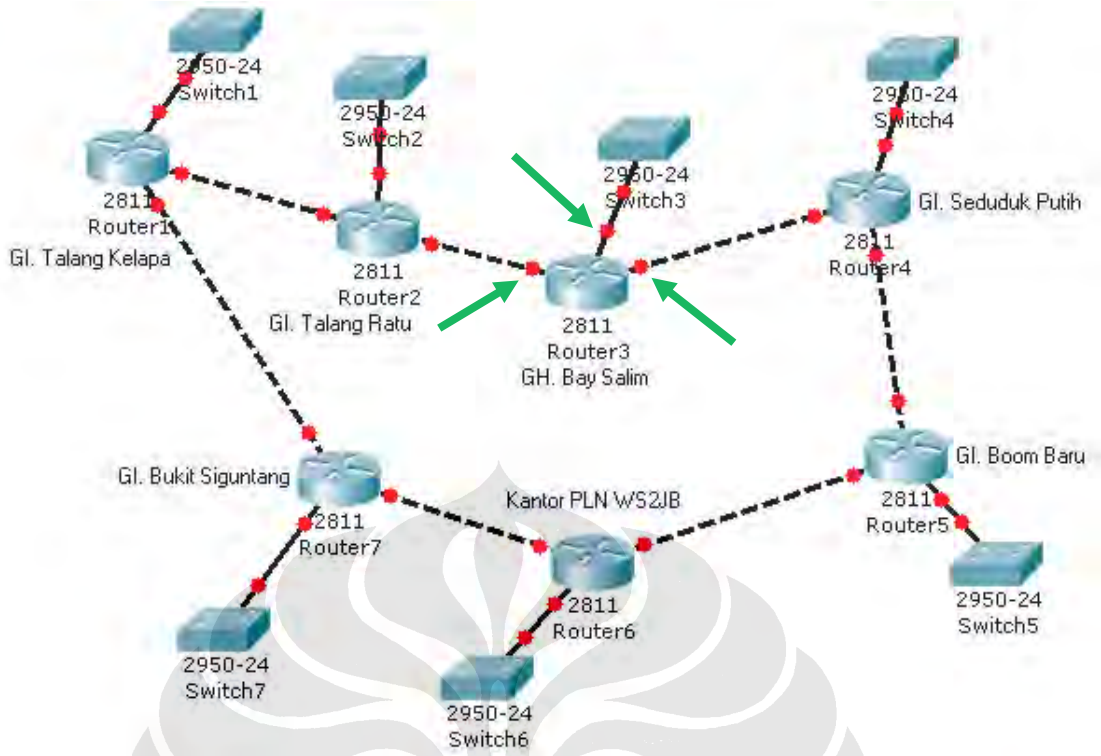
Digunakan kabel RJ-45 dengan konfigurasi *straight-through* dan *cross-over* untuk menghubungkan *interface Fast Ethernet* .



Gambar 3.7. *Router* 2811 [7]

Setelah pemilihan divais – divais penyusun jaringan dilakukan, maka desain jaringan logika seperti yang ditunjukkan pada Gambar 3.3 akan direalisasikan dengan menngunakan *software* simulasi Packet Tracer v4.11. Gambar 3.8 memperlihatkan jaringan yang dibangun dengan menggunakan Packet Tracer v4.11 dengan menggunakan divais – divais yang sudah dipilih.

Pada Gambar 3.8 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]. Pemilihan *interface Fast Ethernet* karena kebutuhan akan jaringan *backbone* yang berkecepatan tinggi, dan setidaknya mendukung *bandwidth* tertinggi yang berada pada kantor PLN WS2JB sebesar 2048 Kbps. 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 [5]. Pada Gambar 3.8 dapat dilihat, pada *router – router backbone*, misalnya *router* di GH. Bay Salim mempunyai bulatan berwarna merah yang ditunjukkan dengan anak panah berwarna hijau pada Gambar 3.8. Bulatan berwarna merah tersebut menunjukkan bahwa *interface Fast Ethernet* pada *router* di GH. Bay Salim masih dalam keadaan *shutdown* dan belum aktif.



Gambar 3.8. Jaringan yang direalisasikan menggunakan Packet Tracer v4.11

3.4.2.2. Pengalokasian IP

Pengalokasian alamat IP untuk *interface* sebuah *router* harus direncanakan dengan baik agar dapat menghubungkan *router* dan tetap efisien dalam penggunaan sumber daya berupa alamat IP. Tabel 3.3 memperlihatkan distribusi alamat IP untuk *interface – interface* yang ada pada *router*.

Alokasi IP dipilih berdasarkan karakteristik dari *router* dimana pada pada koneksi pada *interface* suatu *router* ke *router* lain harus berada pada *subnet* yang sama [5]. Sebagai contoh, *port Fast Ethernet* 1/0 dari *Router*1 dengan alamat IP 10.100.101.1 dihubungkan dengan *Fast Ethernet* 1/0 dari *Router*2 dengan alamat IP 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 lokasi unit usaha PLN. Pengalamatan IP di masing – masing lokasi disesuaikan dengan jumlah *host* yang ada. Hal ini dilakukan untuk mengefisiensikan penggunaan sumber daya berupa alamat IP.

Tabel 3.3. Distribusi alamat IP untuk *interface – interface router*

Nama *router*	*Fast Ethernet* 1/0	Fast Ethenet1/1	*Fast Ethernet* 0/0
*Router*1	10.100.101.1/29	10.100.101.50/29	192.168.101.1/29
*Router*2	10.100.101.2/29	10.100.101.9/29	192.168.101.9/29
*Router*3	10.100.101.17/29	10.100.101.10/29	192.168.101.17/29
*Router*4	0.100.101.18/29	10.100.101.25/29	192.168.101.49/29
*Router*5	10.100.101.33/29	10.100.101.26/29	192.168.101.65/28
*Router*6	10.100.101.34/29	10.100.101.41/29	192.168.101.129/26
*Router*7	10.100.101.49/29	10.100.101.42/29	192.168.101.225/29

Tabel 3.4. Tabel alokasi alamat IP pada masing – masing lokasi

No	Lokasi	Jumlah *host*	Alokasi IP
1	GI. Talang Kelapa	5	192.168.101.1 - 192.168.101.7
2	GI. Talang Ratu	5	192.168.101.8 - 192.168.101.14
3	GI. Bay Salim	10	192.168.101.17 - 192.168.101.30
4	GI. Seduduk Putih	5	192.168.101.49 - 192.168.101.54
5	GI. Boom Baru	10	192.168.101.65 - 192.168.101.78
6	Kantor PLN WS2JB	50	192.168.101.129 -192.168.101.190
7	GI. Bukit Siguntang	5	192.168.101.225 -192.168.101.231

3.5 Konfigurasi dengan Protokol OSPF dan EIGRP

Konfigurasi akan dilakukan dengan menggunakan IOS *command* pada *router* yang – *router* yang menjadi *backbone*. IOS *command* sendiri merupakan bahasa pemrogaman yang digunakan untuk mengkonfigurasi divais – divais jaringan. Berikut ini adalah IOS *command* yang digunakan untuk mengalokasikan

IP pada tiap *port*, menghidupkan *port* tersebut, mengkonfigurasi *router – router* yang membentuk *backbone* tersebut.

3.5.1 Konfigurasi dengan protokol OSPF

Berikut ini adalah konfigurasi OSPF sekaligus pengalokasian alamat IP untuk *interface - interface* yang dilakukan untuk *router-router* yang menyusun *backbone*. Perintah – perintah konfigurasi ini diketikkan pada CLI dari *router*.

1. Konfigurasi di lokasi GI. Talang Kelapa

Konfigurasi 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
```

2. Konfigurasi di lokasi GI. Talang Ratu

Konfigurasi Router2 :

```
Router2>ena
Router2#conf t
Router2(config)#inter fa1/0
Router2(config-if)#ip add 10.100.101.2 255.255.255.248
Router2(config-if)#no shut
Router2(config-if)#inter fa1/1
Router2(config-if)#ip add 10.100.101.9 255.255.255.248
Router2(config-if)#no shut
Router2(config-if)#inter fa0/0
Router2(config-if)#ip add 192.168.101.9 255.255.255.248
Router2(config-if)#no shut
Router2(config-if)#router ospf 1
Router2(config-router)#netw 10.100.101.0 0.0.0.7 area 0
Router2(config-router)#netw 10.100.101.8 0.0.0.7 area 0
Router2(config-router)#netw 192.168.101.8 0.0.0.7 area 0
Router2(config-router)#^Z
```

3. Konfigurasi di lokasi GH. Bay Salim

Konfigurasi Router3 :

```
Router3>ena
Router3#conf t
```

```
Router3(config)#inter fa1/0
Router3(config-if)#ip add 10.100.101.17 255.255.255.240
Router3(config-if)#no shut
Router3(config-if)#inter fa1/1
Router3(config-if)#ip add 10.100.101.10 255.255.255.240
Router3(config-if)#no shut
Router3(config-if)#inter fa0/0
Router3(config-if)#ip add 192.168.101.17 255.255.255.240
Router3(config-if)#no shut
Router3(config-if)#router ospf 1
Router3(config-router)#netw 10.100.101.8 0.0.0.7 area 0
Router3(config-router)#netw 10.100.101.16 0.0.0.7 area 0
Router3(config-router)#netw 192.168.101.16 0.0.0.15 area 0
Router3(config-router)#^Z
```

4. Konfigurasi di lokasi GI. Seduduk Putih

Konfigurasi Router4 :

```
Router4>ena
Router4#conf t
Router4(config)#inter fa1/0
Router4(config-if)#ip add 10.100.101.18 255.255.255.248
Router4(config-if)#no shut
Router4(config-if)#inter fa1/1
Router4(config-if)#ip add 10.100.101.25 255.255.255.248
Router4(config-if)#no shut
Router4(config-if)#inter fa0/0
Router4(config-if)#ip add 192.168.101.49 255.255.255.248
Router4(config-if)#no shut
Router4(config-if)#router ospf 1
Router4(config-router)#netw 10.100.101.16 0.0.0.7 area 0
Router4(config-router)#netw 10.100.101.8 24.0.0.7 area 0
Router4(config-router)#netw 192.168.101.48 0.0.0.7 area 0
Router4(config-router)#^Z
```

5. Konfigurasi di lokasi GI. Boom Baru

Konfigurasi Router5 :

```
Router5>ena
Router5#conf t
Router5(config)#inter fa1/0
Router5(config-if)#ip add 10.100.101.33 255.255.255.240
Router5(config-if)#no shut
Router5(config-if)#inter fa1/1
Router5(config-if)#ip add 10.100.101.26 255.255.255.240
Router5(config-if)#no shut
Router5(config-if)#inter fa0/0
Router5(config-if)#ip add 192.168.101.65 255.255.255.240
Router5(config-if)#no shut
Router5(config-if)#router ospf 1
Router5(config-router)#netw 10.100.101.24 0.0.0.7 area 0
Router5(config-router)#netw 10.100.101.32 0.0.0.7 area 0
Router5(config-router)#netw 192.168.101.64 0.0.0.15 area 0
Router5(config-router)#^Z
```

6. Konfigurasi di lokasi Kantor PLN WS2JB

Konfigurasi Router6 :

```
Router6>ena
Router6#conf t
Router6(config)#inter fa1/0
Router6(config-if)#ip add 10.100.101.34 255.255.255.248
Router6(config-if)#no shut
Router6(config-if)#inter fa1/1
Router6(config-if)#ip add 10.100.101.33 255.255.255.248
Router6(config-if)#no shut
Router6(config-if)#inter fa0/0
Router6(config-if)#ip add 192.168.101.129 255.255.255.192
Router6(config-if)#no shut
Router6(config-if)#router ospf 1
Router6(config-router)#netw 10.100.101.32 0.0.0.7 area 0
Router6(config-router)#netw 10.100.101.40 0.0.0.7 area 0
Router6(config-router)#netw 192.168.101.128 0.0.0.7 area 0
Router6(config-router)#^Z
```

7. Konfigurasi di lokasi GI. Bukit Siguntang

Konfigurasi Router7 :

```
Router7>ena
Router7#conf t
Router7(config)#inter fa1/0
Router7(config-if)#ip add 10.100.101.49 255.255.255.248
Router7(config-if)#no shut
Router7(config-if)#inter fa1/1
Router7(config-if)#ip add 10.100.101.42 255.255.255.248
Router7(config-if)#no shut
Router7(config-if)#inter fa0/0
Router7(config-if)#ip add 192.168.101.65 255.255.255.248
Router7(config-if)#no shut
Router7(config-if)#router ospf 1
Router7(config-router)#netw 10.100.101.40 0.0.0.7 area 0
Router7(config-router)#netw 10.100.101.48 0.0.0.7 area 0
Router7(config-router)#netw 192.168.101.224 0.0.0.15 area 0
Router7(config-router)#^Z
```

Setelah proses konfigurasi untuk masing – masing lokasi selesai maka harus diverifikasi untuk meyakinkan bahwa konfigurasi OSPF yang telah dilakukan berhasil. Proses verifikasi akan dilakukan dengan perintah *"sho ip ospf route"*. Berikut ini adalah hasil pengeksekusian perintah *"sho ip ospf route"* yang diketikkan pada CLI Router1:

```
10.0.0.0/29 is subnetted, 7 subnets
C  10.100.101.0 is directly connected, FastEthernet1/0
O  10.100.101.8 [110/2] via 10.100.101.2, 00:01:29,
FastEthernet1/0
O  10.100.101.16 [110/3] via 10.100.101.2, 00:01:29,
FastEthernet1/0
O  10.100.101.24 [110/4] via 10.100.101.2, 00:01:29,
FastEthernet1/0
O  10.100.101.32 [110/3] via 10.100.101.49, 00:01:29,
FastEthernet1/1
O  10.100.101.40 [110/2] via 10.100.101.49, 00:01:39,
FastEthernet1/1
```

```
C  10.100.101.48 is directly connected, FastEthernet1/1
     192.168.101.0/24 is variably subnetted, 7 subnets, 3 masks
C  192.168.101.0/29 is directly connected, FastEthernet0/0
O  192.168.101.8/29 [110/2] via 10.100.101.2, 00:01:29,
     FastEthernet1/0
O  192.168.101.16/28 [110/3] via 10.100.101.2, 00:01:29,
     FastEthernet1/0
O  192.168.101.48/29 [110/4] via 10.100.101.2, 00:01:29,
     FastEthernet1/0
O  192.168.101.64/28 [110/4] via 10.100.101.49, 00:01:29,
     FastEthernet1/1
O  192.168.101.128/26 [110/3] via 10.100.101.49, 00:01:29,
     FastEthernet1/1
O  192.168.101.224/29 [110/2] via 10.100.101.49, 00:01:39,
     FastEthernet1/1
```

Kode "C" pada bagian paling kiri hasil eksekusi perintah *"sho ip ospf route"* menunjukkan bahwa *Router*1 terhubung langsung dengan suatu *network*, sementara kode "O" menunjukkan bahwa *Router*1 terhubung dengan suatu *network* menggunakan OSPF sehingga status *network* tersebut adalah *neighbor* bagi *Router*1.

3.5.2 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, yaiut di GI. Talang Kelapa dan GI. Talang Ratu. Hanya diberikan konfigurasi pada dua lokasi ini karena konfigurasi pada unit – unit usaha PLN yang lain akan sama dengan konfigurasi kedua lokasi ini

1. Konfigurasi lokasi GI. Talang Kelapa

```
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 lokasi GI. Talang Ratu

```
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
```

Pada konfigurasi yang telah dilakukan, *network* yang terhubung dengan *router* tidak perlu dispesifikasikan jumlah *subnet*-nya sehingga hanya perlu ditulis

"netw 192.168.101.0" dan *"netw 10.0.0.0"*. Perintah *"no auto-summary"* digunakan karena secara *default* konfigurasi EIGRP menganggap *network* yang terhubung dengan suatu interface adalah *classful network* dimana pengalamatannya mencakup 254 alamat IP, sementara yang digunakan pada jaringan adalah *classless network* dimana alamat IP-nya kurang dari 255 untuk tiap *network* yang digunakan.

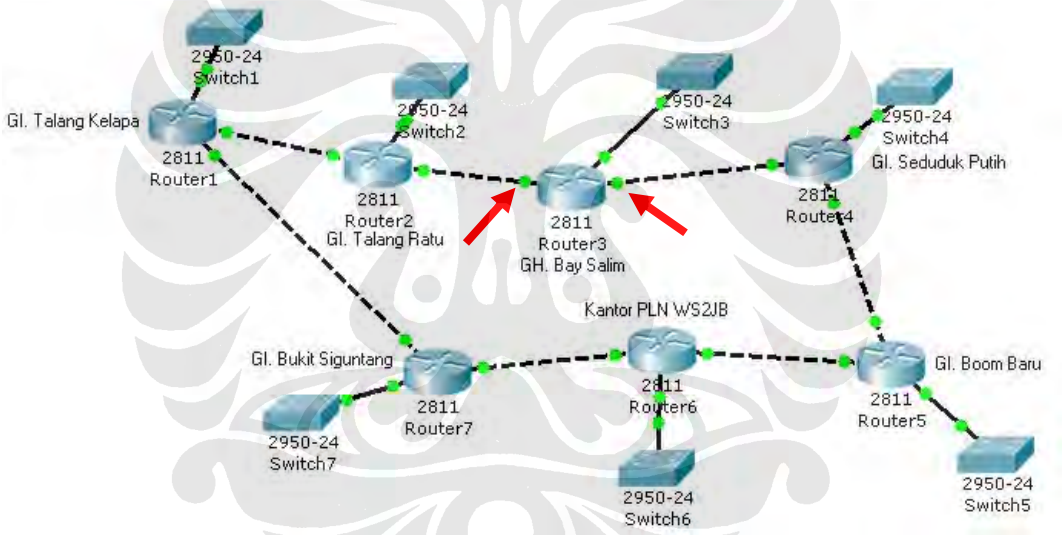
Setelah dikonfigurasi dengan EIGRP maka harus dilakukan verifikasi untuk memastikan bahwa *router – router* yang membentuk *backbone* telah saling mengenali. Verifikasi dilakukan dengan menggunakan perintah *"sho ip route"*. Berikut ini adalah hasil eksekusi yang dilakukan pada *Router*4.

```
D 10.100.101.0 [90/33280] via 10.100.101.17, 00:00:52,
     FastEthernet1/0
D 10.100.101.8 [90/30720] via 10.100.101.17, 00:00:52,
     FastEthernet1/0
C 10.100.101.16 is directly connected, FastEthernet1/0
C 10.100.101.24 is directly connected, FastEthernet1/1
D 10.100.101.32 [90/30720] via 10.100.101.26, 00:00:52,
     FastEthernet1/1
D 10.100.101.40 [90/33280] via 10.100.101.26, 00:00:51,
     FastEthernet1/1
D 10.100.101.48 [90/35840] via 10.100.101.17, 00:00:52,
     FastEthernet1/0
192.168.101.0/24 is variably subnetted, 7 subnets, 3 masks
D 192.168.101.0/29 [90/35840] via 10.100.101.17, 00:00:52,
     FastEthernet1/0
D 192.168.101.8/29 [90/33280] via 10.100.101.17, 00:00:52,
     FastEthernet1/0
D 192.168.101.16/28 [90/30720] via 10.100.101.17, 00:00:52,
     FastEthernet1/0
C 192.168.101.48/29 is directly connected, FastEthernet0/0
D 192.168.101.64/28 [90/30720] via 10.100.101.26, 00:00:52,
     FastEthernet1/1
D 192.168.101.128/26 [90/33280] via 10.100.101.26, 00:00:52,
     FastEthernet1/1
D 192.168.101.224/29 [90/38400] via 10.100.101.17, 00:00:52,
     FastEthernet1/0
```

Dari hasil verifikasi yang telah dilakukan dengan perintah *"sho ip eigrp route"*, kode "C" menunjukkan bahwa *Router*4 terhubung langsung secara fisik dengan suatu *network* menggunakan *interface* tertentu. Sedangkan kode "D" menunjukkan *Router*4 terhubung ke suatu *network* dengan menggunakan protokol EIGRP.

3.5.3 Jaringan Siap Uji coba

Setelah melewati proses – proses berupa pengaktifan interface, pengalokasian IP, dan pengkonfigurasian routing protocol berupa OSPF atau EIGRP, maka jaringan yang semula belum aktif seperti ditunjukkan pada Gambar 3.8 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 divais lain telah terbangun, seperti ditunjukkan pada Gambar 3.9 dengan anak panah berwarna merah.. Jaringan yang sudah aktif ini akan diujicoba untuk melihat unjuk kerja jaringan yang menggunakan *routing protocol* OSPF dan EIGRP dengan pengujian berupa *ping*, *traceroute*, kemampuan akses internet, dan kemampuan *fault tolerant*.



Gambar 3.9. Jaringan yang telah aktif dan akan diuji coba

BAB IV
UJICOBA DAN ANALISIS

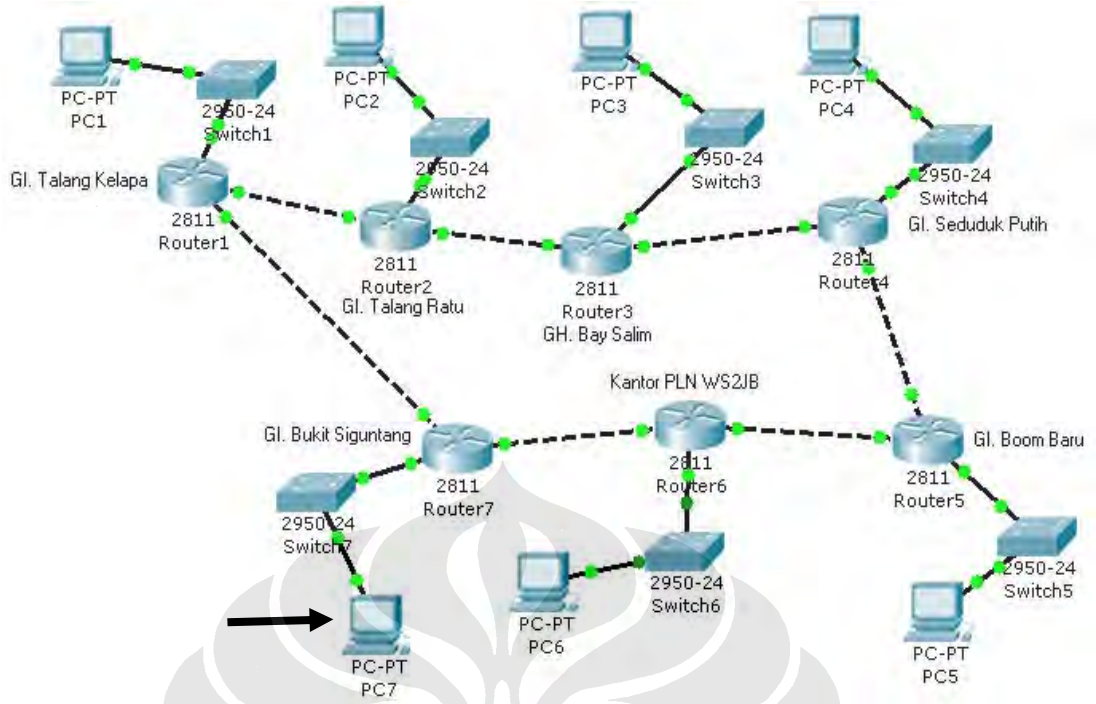
4.1 SKENARIO PENGUJIAN

Ujicoba unjuk kerja jaringan dilakukan pada jaringan *Fast Ethernet* yang sudah dibangun dengan Packet Tracer v4.11 yang menggunakan *routing protocol* OSPF dan EIGRP. Ujicoba unjuk kerja akan dilakukan dengan menggunakan skenario – skenario yang didukung oleh Packet Tracer v4.11 sebagai berikut :

- *Tracert*
- *Ping*
- Akses internet
- *Fault tolerant*

4.2 UJICOBA *TRACERT*

Perintah *tracert* digunakan untuk mencari jalur yang akan dilalui paket data. *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. Cara kerja *tracert* adalah dengan mengirimkan 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 dibutuhkan untuk mencapai alamat yang dituju ini melebihi *timeout*, maka alamat tersebut akan dinyatakan tak dapat dicapai *(unreachable)* [5]. Jaringan yang akan diujicoba dengan perintah *tracert* sama seperti pada Gambar 3.9 namun dimodifikasi dengan ditambahkan *host* berupa PC1, PC2, PC3, PC4, PC5, PC6, dan PC7 seperti dapat dilihat pada Gambar 4.1 dimana sebuah *host* yaitu PC7 ditunjukkan dengan anak panah hitam. Pada pengujian ini, *host* pada suatu unit usaha akan menggunakan *tracert* untuk mencari jalur menuju *host* pada unit usaha lain. Tabel 4.1 menunjukkan alamat IP dan lokasi *host*. 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 4.1. Jaringan untuk ujicoba dengan *tracert*

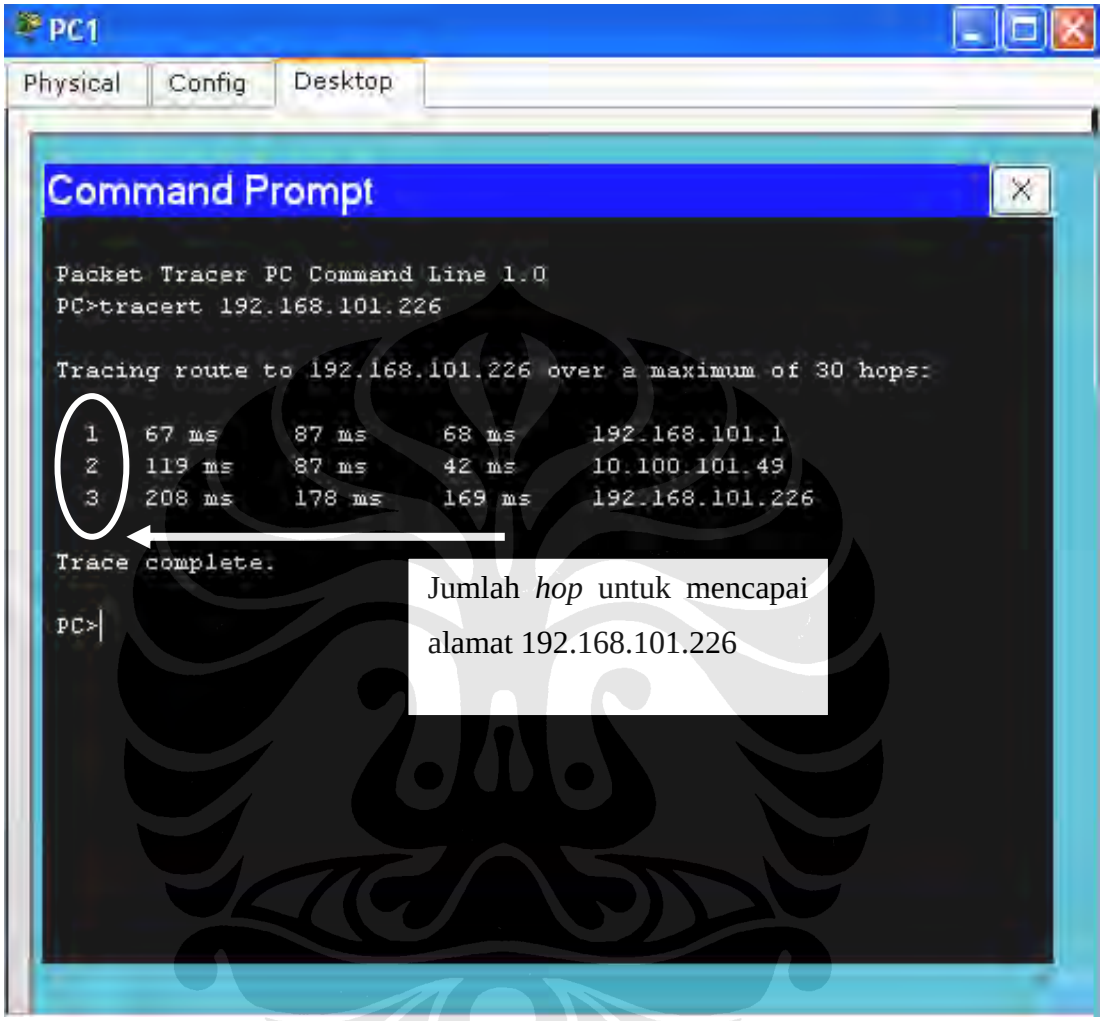
Tabel 4.1. Daftar alamat IP untuk *host* di masing –masing lokasi

No	Lokasi	Nama *host*	Alamat IP
1	GI. Talang Kelapa	PC1	192.168.101.2
2	GI. Talang Ratu	PC2	192.168.101.10
3	GH. Bay Salim	PC3	192.168.101.18
4	GI. Seduduk Putih	PC4	192.168.101.50
5	GI. Boom Baru	PC5	192.168.101.66
6	Kantor PLNWS2JB	PC6	192.168.101.130
7	GI. Bukit Siguntang	PC7	192.168.101.226

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 4.2, dimana diperlukan tiga kali hop bagi PC1 untuk menemukan alamat IP 192.168.101.226.



Gambar 4.2. Tampilan hasil eksekusi perintah *tracert*

4.2.1 Perbandingan *tracert* pada OSPF dan EIGRP

Untuk melihat perbandingan pencarian jalur tempat lewat dengan perintah *tracert* pada protokol OSPF dan EIGRP, maka diambil sampel dua *host* yang akan melakukan *tracert*. Dua *host* tersebut adalah PC1 dan PC4. *Host* PC1akan melakukan *tracert* ke PC2, PC3, PC4, PC5, PC6, dan PC7. Sementara itu PC4 akan melakukan *traceorute* ke PC5, PC6, PC7, PC1, PC2, dan PC3.

Jumlah *hop* dan *interface* yang dilalui oleh PC1 untuk mencapai *host* tujuan akan ditunjukkan pada Tabel 4.2, Tabel 4.3, Tabel 4.4, Tabel 4.5, Tabel 4.6, dan Tabel 4.7. Sementara jumlah *hop* dan *interface* yang dilewati PC4 untuk mencapai *host*

tujuan 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	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	192.168.101.2	5	192.168.101.2

Tabel 4.12. *Tracert* dari PC4 ke PC2

OSPF		EIGRP	
hop	*Interface* yang dilewati	*hop*	*Interface* 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	192.168.101.10	4	192.168.101.10

Tabel 4.13. *Tracert* dari PC4 ke PC3

OSPF		EIGRP	
hop	*Interface* yang dilewati	*hop*	*Interface* yang dilewati
1	192.168.101.49	1	192.168.101.49
2	10.100.101.17	2	10.100.101.17
3	192.168.101.18	3	192.168.101.18

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 4.11 dapat dilihat bahwa saat PC4 berusaha mencapai PC1, jumlah *hop* yang dilakukan adalah sebanyak 5 kali. Pada *hop* pertama, paket IP *datagrams* 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 *datagrams* sampai ke alamat yang dituju. Dengan mengacu pada

Gambar 4.1, maka secara visual jalur terpendek yang antara PC4 dan PC1 adalah melewati Router3, Router2, dan Router1. Hal ini sesuai dengan jalur yang digunakan protokol OSPF dan EIGRP untuk mencapai PC1, sehingga untuk pengujian ini dapat disimpulkan bahwa OSPF dan EIGRP dapat diaplikasikan di jaringan karena dapat memilih jalur paling pendek untuk mencapai tujuan.

4.3 UJICOBA DENGAN *PING*

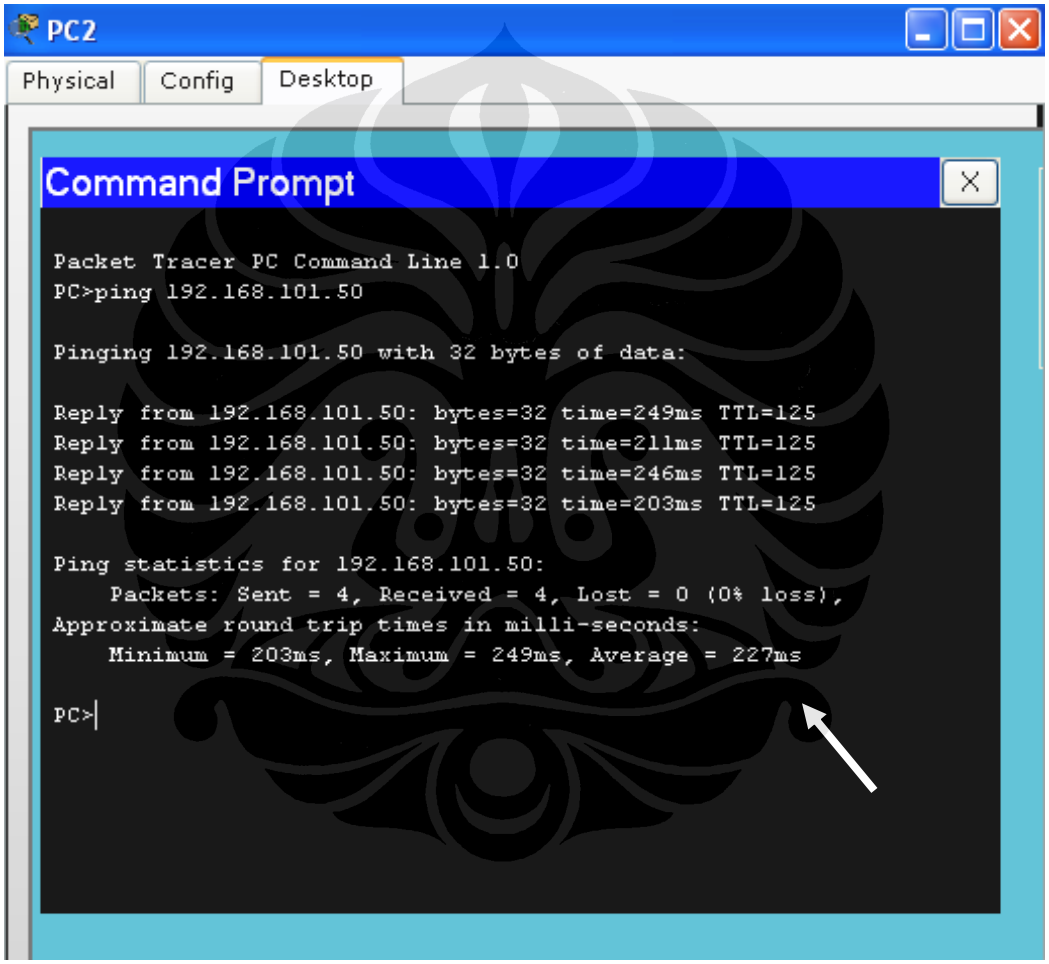
Ping merupakan kependekan dari *Packet Internet Groper*. Perintah *ping* digunakan untuk memeriksa ketersambungan sebuah *interface* pada suatu jaringan dengan cara mengirimkan paket data ICMP *echo request* kepada *interface* tersebut lalu menunggu balasan paket data yang disebut ICMP *echo response*. 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 [5]. Pengujian *ping* dilakuakan 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* PC2 ditunjukkan pada Gambar 4.3. Pada Gambar 4.3 dapat dilihat bahwa PC2 melakukan *ping* kealamat IP 192.168.101.50 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 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 menghubungkan *host* yang berada pada unit –unit usaha PLN.



Gambar 4.3. Tampilan hasil eksekusi perintah *ping* oleh PC2

4.3.1 Hasil pengujian *ping* pada OSPF dan EIGRP

Hasil pengujian *ping* antara seluruh *host* yang berada di lokasi – lokasi unit usaha PLN 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".

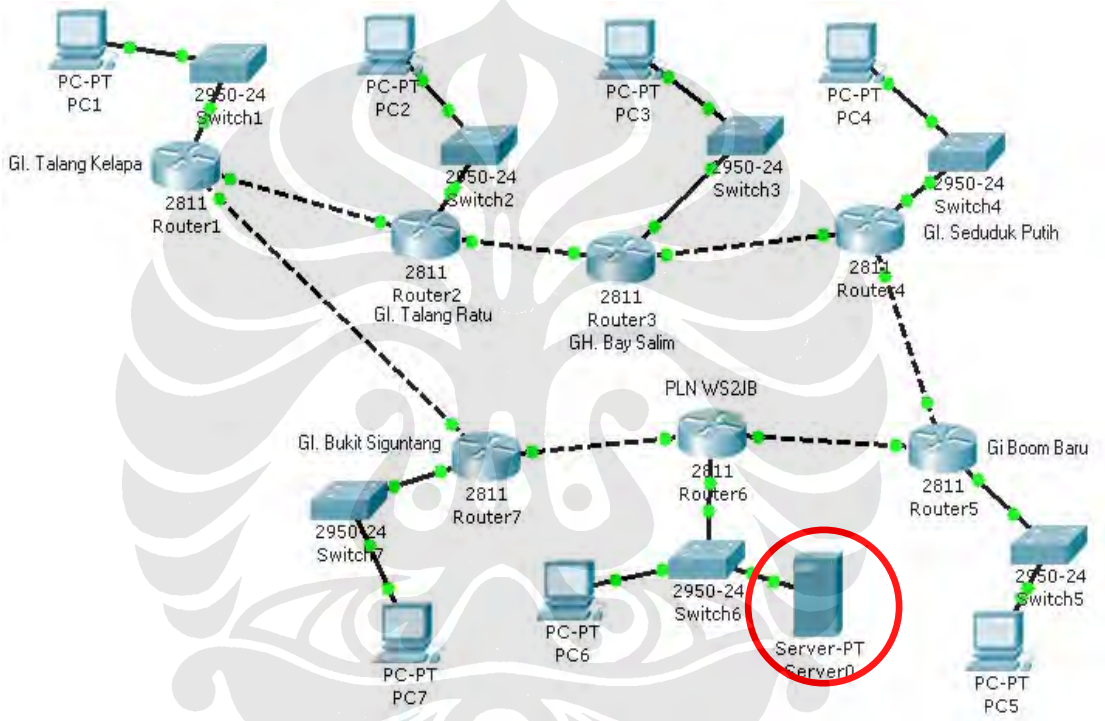
Tabel 4.14. *Ping* antar *host* dengan protokol OSPF dan EIGRP

	PC1 (tujuan)	PC2 (tujuan)	PC3 (tujuan)	PC4 (tujuan)	PC5 (tujuan)	PC6 (tujuan)	PC7 (tujuan)
PC1 (pengirim)		OK	OK	OK	OK	OK	OK
PC2 (pengirim)	OK		OK	OK	OK	OK	OK
PC3 (pengirim)	OK	OK		OK	OK	OK	OK
PC4 (pengirim)	OK	OK	OK		OK	OK	OK
PC5 (pengirim)	OK	OK	OK	OK		OK	OK
PC6 (pengirim)	OK	OK	OK	OK	OK		OK
PC7 (pengirim)	OK	OK	OK	OK	OK	OK	

4.4 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, TFTP

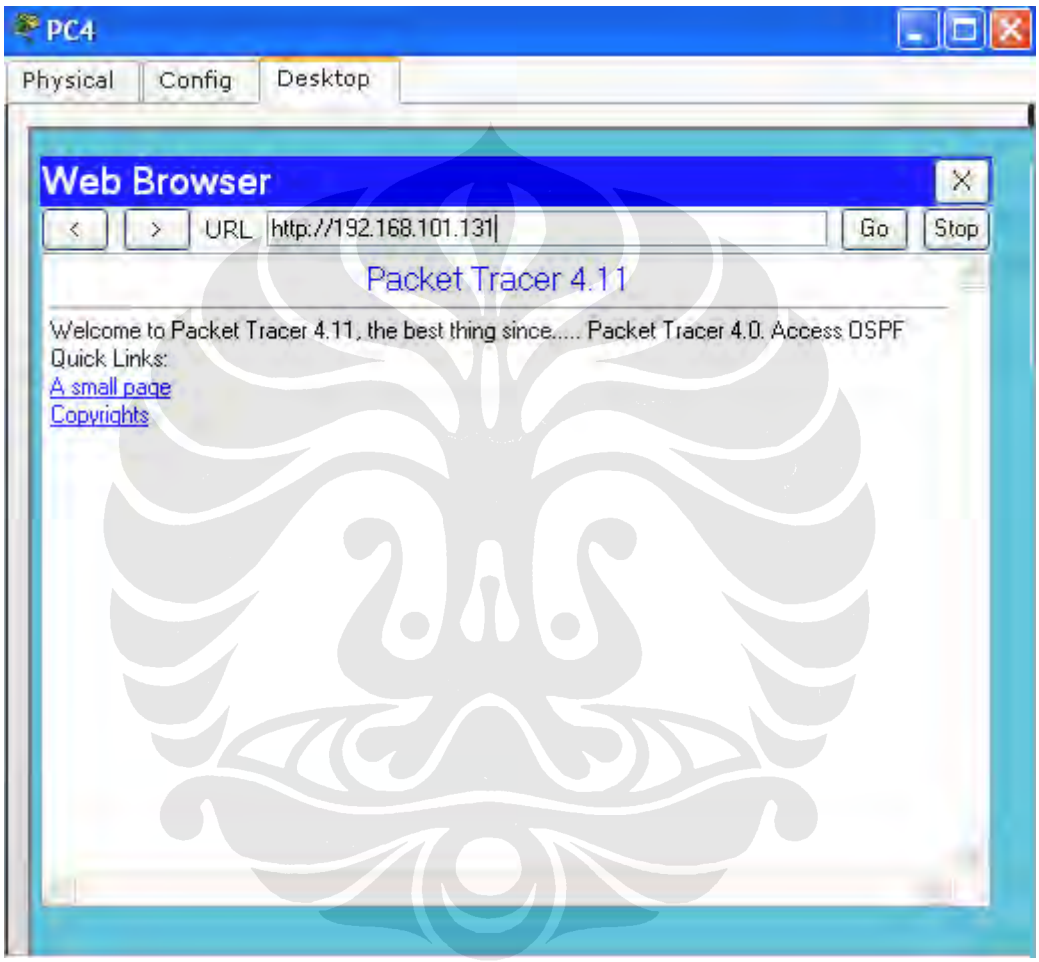
akan menjadi protokol yang mengakomodasi penyimpanan konfigurasi *router* di sebuah *server* yang ditempatkan di kantor PLNWS2JB. Parameter yang akan dibandingkan antara jaringan yang menggunakan protokol OSPF dan EIGRP adalah *bit rate* pada saat *upload* dan *download* konfigurasi *router* ke *server*. Jaringan yang digunakan untuk pengujian ini mirip dengan yang ditunjukkan pada Gambar 4.1, hanya saja pada ditambahkan *web server* yang ditempatkan di lokasi kantor PLNWS2JB seperti ditunjukkkan pada Gambar 4.4. Pada Gambar 4.4 *web server* ditandai dengan lingkaran merah.



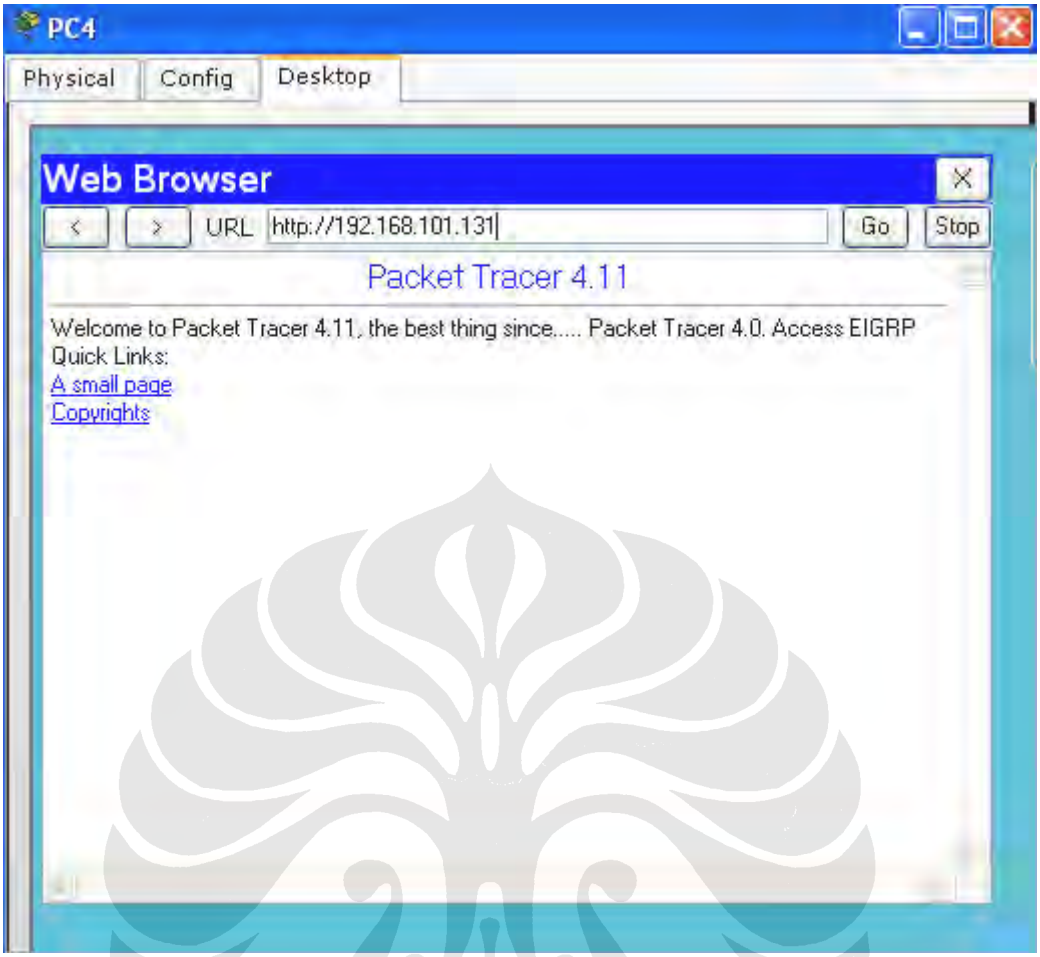
Gambar 4.4. Jaringan untuk ujicoba akses internet

4.4.1 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 4.4 dan Gambar 4.5.



Gambar 4.5. Tampilan halaman *web* (jaringan OSPF)



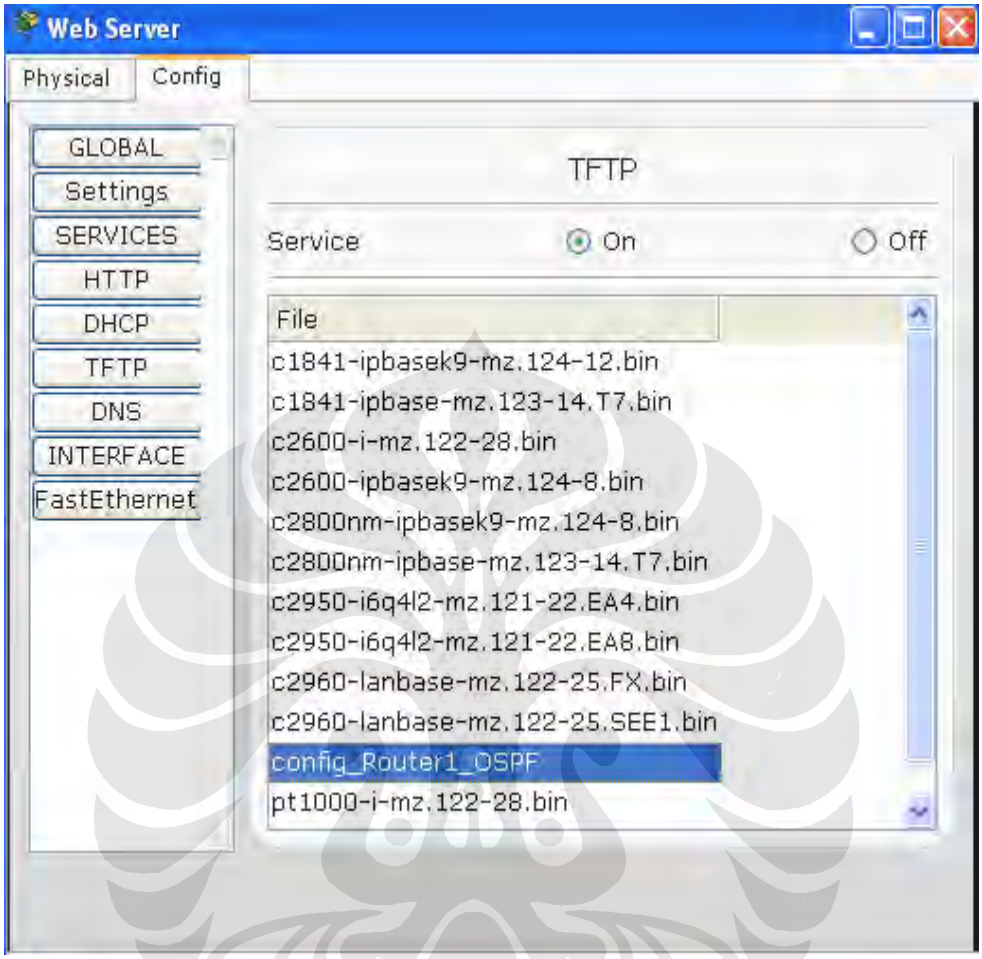
Gambar 4.6. Tampilan halaman *web* (jaringan EIGRP)

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

4.4.2 Perbandingan transfer *file* pada jaringan OSPF dan EIGRP

Pada ujicoba ini *file* yang akan ditransfer adalah konfigurasi dari *router* yang ditempatkan di unit – unit usaha PLN, yaitu Router1, Router2, Router3, Router4, Router5, Router6, dan Router7. Parameter yang akan diamati pada uji coba 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 dapat dilihat pada Tabel 4.14 dan Tabel 4.15.

Tabel 4.15. *Bit rate upload* ke *web server*

	OSPF (bps)	EIGRP (bps)
Router1	2000	2000
Router2	1000	3000
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	3910
Router2	5341	2799
Router3	2867	4338
Router4	4237	3422
Router5	6444	11622
Router6	8822	8118
Router7	6900	5609

Dengan informasi dari Tabel 4.13 dan Tabel 4.14 dapat dicari rata – rata *bit rate* dari 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

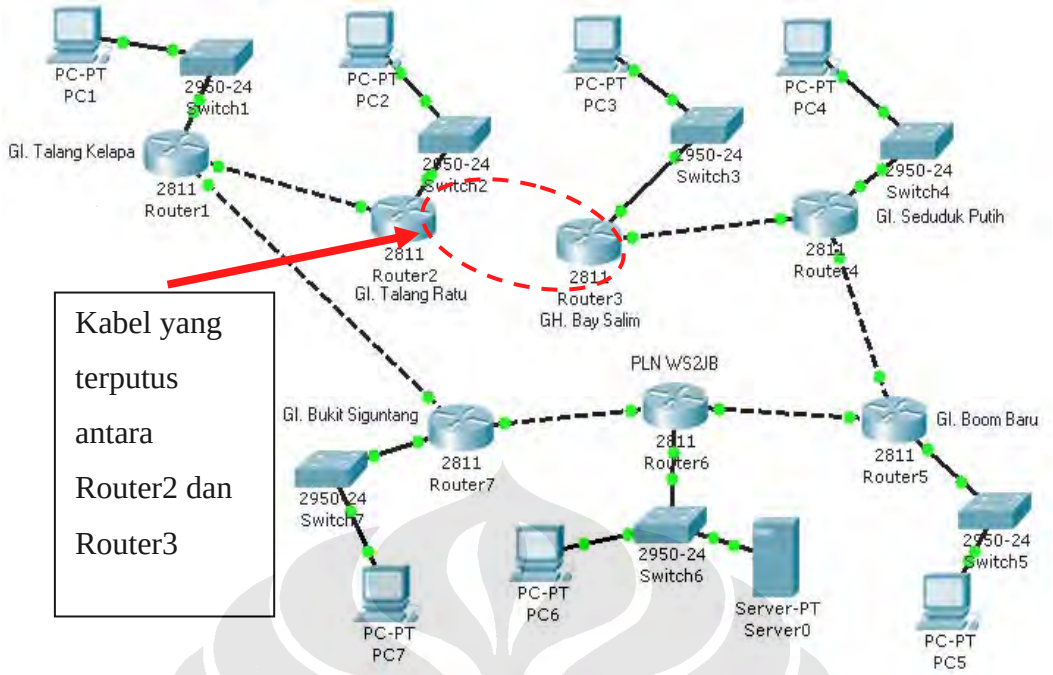
Rata – rata *bit rate download* : 5688.3 bps

Dari perhitungan yang telah dilakukan didapatkan hasil bahwa rata – rata *bit rate upload* adalah sama untuk jaringan yang menggunakan protokol OSPF dan EIGRP. 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 dimaksudkan untuk men-*download* konfigurasi dari server, maka jaringan yang memakai protokol OSPF akan lebih cepat terkonfigurasi.

4.5 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 – tama 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 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 Router2 dan Router3 putus.



Gambar 4.8. Ilustrasi kegagalan jaringan

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

1. Tracert dari PC1 ke PC4, lalu ditengah berjalannya proses *tracert* kabel antara Router2 dan Router3 dihilangkan.
2. Tracert dari PC4 ke PC6, lalu ditengah berjalannya proses *tracert* kabel antara Router4 dan Router5 dihilangkan.

4.5.1 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.

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*.

Tabel 4.17. *Tracert* dari PC1 ke PC4 dengan adanya *fault*

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	10.100.101.41	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	*Interface* yang dilewati	*hop*	*Interface* 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	10.100.101.49	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

4.6 PENGEMBANGAN JARINGAN

Pengembangan jaringan yang sudah dirancang ini adalah untuk menjadi jaringan L3VPN seperti sudah dijelaskan Bab 1 pada bagian tujuan penelitian, dimana tujuan dari penelitian ini adalah merancang jaringan yang dapat

mendukung pengimplementasian L3VPN. Untuk mengimplementasikan L3VPN maka harus dibuah VPN *routing* dengan menggunakan *routing protocol* BGP. Hal ini dilakukan dengan mengkonfigurasi *router* – router penyusun *backbone* dengan *routing protocol* BGP, dimana sebelumnya router – router yang sebelumnya telah dikonfigurasi dengan *routing protocol* OSPF atau EIGRP [11].

BAB V
KESIMPULAN

Dari pengujian dan analisis terhadap jaringan *Fast Ethernet* yang dibangun dengan *software* Packet Tracer v4.11, didapat kesimpulan sebagai berikut.

1. Syarat konektivitas jaringan telah dipenuhi, baik oleh jaringan yang menggunakan *routing protocol* OSPF maupun EIGRP, dimana *host – host* yang berada pada unit – unit usaha PLN 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 paling pendek untuk mencapai alamat tujuan yang diinginkan.
3. *Host* pada unit – unit usaha PLN telah dapat mengakses internet, yang disimulasikan dengan menggunakan dengan kemampuan mengakses *web server*.
4. Pada ujicoba tranfer file konfigurasi *router* dengan protokol TFTP, OSPF dan EIGRP sama – sama mampu untuk melakukan *upload* dan *download* . EIGRP memberikan hasil sedikit lebih baik dari pada OSPF dimana *bit rate* EIGRP mencapai 5688.3 bps sedangkan *bit rate* 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*.

DAFTAR ACUAN

[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.

[7] Packet Tracer v4.11

[8] Andrew S. Tannenbaum,"*Computer Networks*", Pearson Education, Inc, 2003.

[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,"Fault Tolerant IP and MPLS Networks", Cisco Press, 2004.

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

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