PERANCANGAN JARINGAN *BACKBONE* DENGAN VLAN DAN PROTOKOL *ROUTING* EIGRP PADA PLN CABANG PALEMBANG

SKRIPSI

OLEH:

RIZKI MAYANDI

04 04 03 0725

DEPARTEMEN TEKNIK ELEKTRO

FAKULTAS TEKNIK UNIVERSITAS INDONESIA

GENAP 2007/2008

PERANCANGAN JARINGAN *BACKBONE* DENGAN VLAN DAN PROTOKOL *ROUTING* EIGRP PADA PLN CABANG PALEMBANG

OLEH:

RIZKI MAYANDI

04 04 03 0725

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 Jaringan *Backbone* dengan VLAN dan Protokol *Routing* EIGRP pada PLN Cabang Palembang

Yang dibuat untuk melengkapi sebagian persyaratan menjadi Sarjana Teknik pada program studi Teknik Elektro Departemen Teknik Elektro Fakultas Teknik Universitas Indonesia, sejauh yang saya ketahui bukan merupakan tiruan atau duplikasi dari skripsi yang sudah 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 dicantumkan sebagaimana mestinya.

Depok, 19 Juni 2008

Rizki Mayandi Hasibuan

NPM. 0404030725

PERSETUJUAN

Skripsi dengan judul :

Perancangan Jaringan *Backbone* dengan VLAN dan Protokol *Routing* EIGRP pada PLN Cabang Palembang

Dibuat untuk melengkapi sebagian persyaratan menjadi Sarjana Teknik pada program studi Teknik Elektro Departemen Teknik Elektro Fakultas Teknik Universitas Indonesia dan disetujui untuk diajukan dalam siding ujian skripsi.

Depok, 19 Juni 2008

Dosen Pembimbing

Prof. Dr. Ir. Dadang Gunawan

NIP. 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 kakak-kakak saya yang telah memberikan doa dan dukungan moril maupun materi sehingga tugas ini dapat diselesaikan dengan baik.
2. Bapak Ari Rahmat IC yang telah memberikan sedikit banyak masukan dalam pengerjaan skripsi ini.
3. Rekan-rekan seperjuangan, Jusril A. Hidayat, M. Ginta Mardalin, Ganis Zulfa S., Aji Teguh P, Dunda A. Nugraha, dan Agung Adi P. atas dukungan dan kebersamaan selama ini.
4. Rekan-rekan elektro khususnya angkatan 2004 atas semangat yang diberikan kepada penulis.

Rizki Mayandi
NPM 04 04 03 0725
Departemen Teknik Elektro

Dosen Pembimbing
Prof. Dr. Ir. Dadang Gunawan.

PERANCANGAN JARINGAN BACKBONE DENGAN VLAN DAN PROTOKOL ROUTING EIGRP PADA PLN CABANG PALEMBANG

ABSTRAK

Perkembangan teknologi telekomunikasi menunjukkan peningkatan yang sangat pesat seiring dengan semakin meningkatnya kebutuhan manusia akan fasilitas komunikasi. Sekarang ini manusia telah mampu melakukan komunikasi tanpa harus tergantung pada waktu dan tempat. Hal ini bisa terwujud berkat ditemukannya teknologi komunikasi.

Sebuah perusahaan membutuhkan sebuah jaringan untuk dapat menghubungkan beberapa kantor yang mereka miliki. Untuk dapat berhubungan antar kantor tersebut maka dibutuhkan jaringan sesuai dengan kebutuhan layanan yang akan dibuat pada jaringan tersebut. Adapun pada penulisan skripsi kali ini, yang dirancang merupakan jaringan yang akan mengakomodir 4 buah layanan yaitu layanan *video conferencing*, IP VPN, IP telepon, serta internet. Sedangkan yang dijadikan *backbone* adalah layanan IP VPN. Layanan ini akan diwakili dengan perancangan *backbone* itu sendiri yang dibagikan menjadi 2 buah layanan pada tingkatan yang ada pada OSI *layer*. Layanan yang diwakili oleh *layer 2* dibuat dengan *backbone* yang tersusun atas beberapa *switch*, sedangkan *layer* 3 disusun oleh *router.*

Untuk membuat sebuah jaringan maka dibutuhkan beberapa metode, yaitu PDIOO, yaitu singkatan dari *Plan- Design- Implementation- Operation- Optimization.* Langkah- langkah ini merupakan rekomendasi dari Cisco. Langkah-langkah inilah yang nantinya yang menjadi dasar untuk perancangan jaringan. Adapun perancangan ini dibuat dengan menggunakan perangkat lunak Packet Tracer. Perangkat lunak ini akan mensimulasikan VLAN dan EIGRP tersebut dan untuk kemudian dapat diuji.

Kata kunci : VLAN, EIGRP, Jaringan,PDIOO

Rizki Mayandi
NPM 04 04 03 0725
Departemen Teknik Elektro

Dosen Pembimbing
Prof. Dr. Ir. Dadang Gunawan.

Designing BACKBONE NETWORK WITH VLAN AND ROUTING PROTOCOL EIGRP IN PLN BRANCH OFFICE IN PALAEMBANG

ABSTRACT

Development of telecommunication technology shows the big increasement and along with the increasement of human need to communicate between each other. Rigth now, people can communicate each other without limitation of place and time. This term can be done by invention of communication technology.

A coorporate need the network to connect their branch office with another. Build a network can be done by look into what services will be build on that office. In this research, the design of network hepefully can accomodate 4 servies, the services are : video conferencing, IPVPN, internet and ip telephony. IP VPN will be an option to build the backbone. This services represent by designing the backbone of layer 2 and layer 3. The backbone in layer 2 represent by switch and named switch, and the backbone in layer 3 represent by router and named the routing protocol with EIGRP.

To build a network, we need some method, the metchod called PDIOO, which recomended by Cisco. The abbreviation of Plan- Design – Implement- operation an Optimization. This step of method that become a foundation of network building. This design of network build by simulation software called Packet Tracer. This software can be simulate EIGRP and VLAN and also test the network.

Kata kunci : VLAN, EIGRP, Jaringan,PDIOO

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi telekomunikasi menunjukkan peningkatan yang sangat pesat seiring dengan semakin meningkatnya kebutuhan manusia akan fasilitas komunikasi. Sekarang ini manusia bisa berkomunikasi dengan jarak yang jauh serta menikmati layanan yang sama dengan bandwidth yang tersedia.

Salah satu kebutuhan perusahaan adalah untuk membangun suatu jaringan pada suatu daerah dengan biaya yang murah dan cepat dengan bantuan sebuah perangkat lunak yang dapat mensimulasikan bagaimana sebuah jaringan akan dibangun nantinya sehingga jalur yang terpasang menjadi dapat menjadi acuan dokumentasi untuk pembangunan ataupun pengembangan jaringan selanjutnya sehingga lebih mudah untuk pengembangan selanjutnya. Data ini juga dapat memberikan petunjuk bagi para pengguna jaringan sehingga tidak salah dalam menggunakan layanan yang tersedia pada sebuah jaringan. Pembangunan jaringan ini juga didasarkan pada mekanisme pembangunan yang direkomendasikan perusahaan jaringan terkemuka, yaitu Cisco. Sedangkan jaringan yang dibangun adalah jaringan yang mempunyai teknologi L2VPN dan L3VPN. L2VPN diwakili dengan VLAN sedangkan L3VPN diwakili dengan EIGRP sebagai protokol *ruting*.

Pembangunan sebuah jaringan juga harus didukung dengan perkembangan teknologi yang ada, seperti perkembangan IOS command yang akan dibuat untuk setiap perangkat keras yang ada serta kabel yang tersedia. Untuk membangun jaringan yang pertama perlu diperhatikan adalah kebutuhan jaringan tersebut akan dibangun untuk pengguna layanan apa saja.

1.2 Perumusan Masalah

Perusahaan icon + akan membangun jaringan untuk kantor- kantor cabang yang ada di kota Palembang yang mana jaringan ini akan digunakan untuk mengakomodasi jaringan yang dapat mendukung layanan *video conferencing*, ip VPN, Internet dan IP Telephony. Dengan kata lain, layanan- layanan inilah yang akan menentukan bagaimana jaringan tersebut akan dibangun.

Dalam skripsi ini akan dicari solusi dari permasalahan di atas, yaitu membangun sebuah jaringan yang dapat mendukung semua layanan tersebut. Permasalahan dalam penelitian ini dapat dirumusakan sebagai berikut :

- Apakah pembangunan jaringan dengan menggunakan metode yang memenuhi PDIOO (*Plan- Design- Implement- Operate- Optimize*) dapat merumuskan sebuah jaringan yang baru akan dibangun pada sebuah perusahaan
- Adapun jaringan yang dibangun dibatasi pada pembangunan kali ini adalah jaringan yang berbasis pada layer 2 dan layer 3. Pada layer 2 dinamakan L2VPN sedangkan pada layer 3 dinamakan L3VPN.
- Bagaimana L2VPN dapat memberikan hasil yang maksimum pada setiap layanan yang akan dibangun dan memberikan akses yang cepat untuk setiap layanan.
- Bagaimana cara mengkonfigurasi beberapa switch sesuai dengan cisco IOS command agar bisa mengakomodasi layanan jaringan yang akan dibuat dengan perangkat lunak packet tracer.

1.3 Tujuan

Tujuan dari penelitian ini adalah untuk membangun jaringan dengan metode PDIOO dan mengimplementasikan jaringan berbasis VLAN dan EIGRP pada sebuah jaringan agar bisa mengakomodasikan layanan- layanan yang ada.

Kegunaan dari penelitian ini adalah sebagai acuan perusahaan icon + untuk membangun jaringan pada kantor- kantor cabangnya yang ada di kota Palembang.

1.4 Batasan Masalah

Pembahasan dalam penelitian ini dibatasi hanya pada perancangan dan pengujian jaringan yang sudah dibangun dengan metode PDIOO dengan mengimplementasikan VLAN pada sebuah jaringan.

1.5 Metodologi Penelitian

Penelitian ini merupakan penelitian pengembangan, yaitu mengembangkan kompresi data berbasis teks dari fasilitas pentransferan data berbasis teks pada teknologi 3G.

Langkah – langkah yang ditempuh dalam melakukan penelitian ini adalah :

- Perumusan masalah
- Mempelajari literatur tentang layanan yang akan dibangun pada jaringan tersebut.
- Perancangan perangkat lunak sistem dengan cisco IOS command menggunakan metode VLAN dan EIGRP.
- Pengujian fungsi – fungsi sistem VLAN dan EIGRP dengan menggunakan software packet tracer.
- Menarik kesimpulan hasil penelitian dan merekomendasikan pembangunan jaringan yang telah dibuat untuk 4 layanan tersebut.

1.6 Sistematika Penelitian

Sistematika penulisan laporan tugas akhir ini meliputi :

Bab I (Pendahuluan)

Dalam bab ini akan dibahas mengenai latar belakang masalah, identifikasi masalah, tujuan dan kegunaan penelitian , metode penelitian dan sistematika penulisan laporan.

Bab II (Pengantar Perancangan Jaringan, VLAN, EIGRP Dan Topologi Serta Elemen Jaringan)

Dalam bab ini akan dibahas mengenai Teknologi VLAN dan EIGRP serta langkah-langkah dalam membangun sebuah jaringan.

Bab III (Perancangan)

Bab ini membahas spesifikasi dari L2VPN yang dalam hal ini adalah VLAN.

Bab ini juga membahas spesifikasi dari L3VPN yang dalam hal ini adalah EIGRP

Bab ini juga membahas mengenai layanan yang akan dibangun pada jaringan tersebut.

BAB IV (Implementasi dan Analisis)

Bab ini akan menganalisis jaringan VLAN dan EIGRP yang telah dibangun dengan cara pemberian data berupa ping untuk melihat bahwa jaringan tersebut sudah dapat digunakan.

Bab ini juga membahas kebutuhan perangkat lunak dan perangkat keras yang digunakan untuk merealisasikan jaringan VLAN dan perbandingannya dengan EIGRP ini.

Disamping itu juga dibahas perancangan perangkat lunak sistem serta pengujian sistem, dalam hal ini kode pemrograman yang berbasis bahasa pemrograman cisco IOS command

BAB II

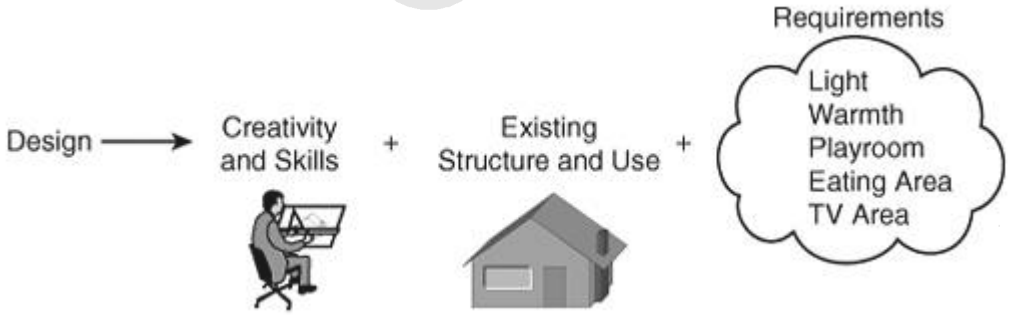
PENGANTAR PERANCANGAN JARINGAN, VLAN, EIGRP DAN TOPOLOGI SERTA ELEMEN JARINGAN

2.1 Merancang Suatu Jaringan

Sebelum lebih jauh menuju perancangan jaringan, maka terdapat suatu cara untuk membangun suatu jaringan. Adapun langkah-langkah tersebut adalah [1]:

- Membuat list kepentingan untuk apa suatu jaringan dibangun
- Mengetahui jenis layanan apa yang akan dibangun pada sebuah jaringan
- Mengerti mengapa sebuah jaringan yang akan dibangun tersebut untuk apa
- Pemilihan perangkat keras yang tepat untuk membangun jaringan tersebut
- Pemilihan perangkat yang lunak apa yang akan digunakan untuk mendukung pembangunan layanan tersebut
- Platform yang tepat untuk pembangunan layanan tersebut

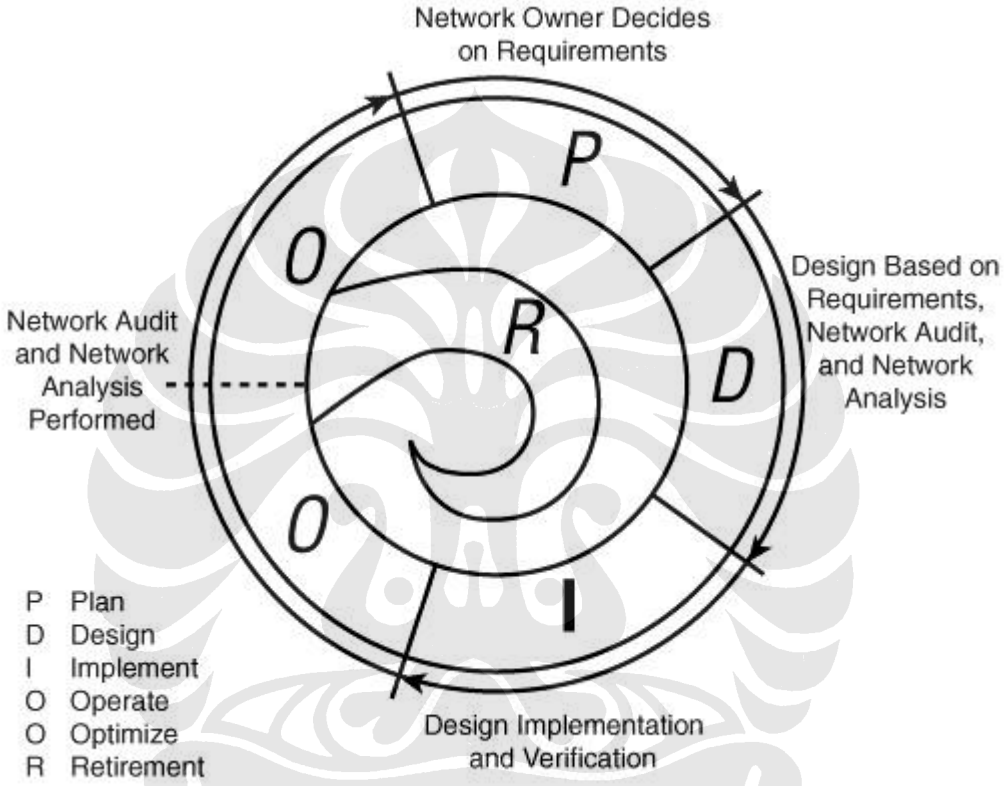
Gambar 2.1 melukiskan tata cara untuk membangun sebuah jaringan untuk membangun sebuah layanan. Gambar di bawah merepresentasikan pembangunan sebuah kebutuhan pembuatan ruangan pada sebuah rumah. Dengan kata lain, pembangunan sebuah jaringan dapat disamakan dengan membangun sebuah rumah dengan ruangan-ruangan yang ada.



Gambar 2.1 Tata cara pembangunan jaringan yang direpresentasikan oleh pembangunan sebuah ruangan [1].

2.1.1 Prinsip Desain

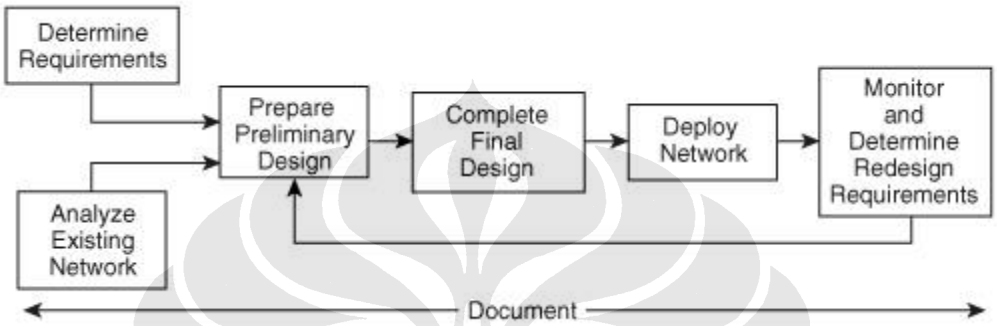
Cisco telah mengembangkan tata cara desain suatu jaringan, tata cara ini dikenal dengan nama PDIOO. PDIOO ini sendiri merupakan singkatan dari *Plan-Design-Implement-Operate-Optimize*. PDIOO ini sendiri menjadi sebuah lingkaran kehidupan dalam pembangunan jaringan dan digunakan untuk menjelaskan beragam fase yang akan dilewati sebuah jaringan. *Life cycle* ini diilustrasikan pada gambar di bawah.



Gambar 2.2 Fase-fase Pembangunan Jaringan [1].

- Fase *Plan* (Perencanaan) Kebutuhan jaringan secara terperinci diidentifikasi, dan jaringan yang sudah ada dilihat dan kemudian akan dibandingkan.
- Fase *Design* (Desain) Sebuah jaringan didesain berdasarkan pada kebutuhan awal dan data tambahan dari jaringan yang sudah dibuat/dibangun sebelumnya. Kebutuhan desain kemudian akan didiskusikan dengan klien.
- Fase *Implement* (Implementasi) Sebuah jaringan dibangun berdasarkan pada desain yang sudah disetujui oleh klien.
- Fase *Operate* (Operasi) Sebuah jaringan dioperasikan dan dimonitor. Fase ini merupakan fase terbaik untuk menguji desain yang telah dibuat.

- Fase *Optimize* (Optimalisasi) Selama fase ini, permasalahan yang ada diteliti dan dibetulkan, baik sesudah ada permasalahan atau permasalahan dapat saja dibuat untuk perhitungan kesalahan di masa yang akan dating.
- Fase *Retirement* (Pergantian) Walaupun diluar dari singkatan PDIOO, fase ini merupakan fase yang dibutuhkan ketika bagian dari jaringan yang dibangun sudah usang dan tidak diperlukan lagi untuk mendukung layanan tersebut.



Gambar 2.3 Garis Besar Prinsip Pembangunan Jaringan [1].

Secara garis besar, pembangunan jaringan akan menempuh cara-cara berikut ini :

- Pengumpulan kebutuhan layanan jaringan

  Pengumpulan kebutuhan jaringan adalah bagian dari fase perencanaan PDIOO. Banyak tipe kebutuhan yang harus didefinisikan, termasuk yang berkaitan dengan masalah teknis dan bisnis. Beberapa faktor yang mungkin membatasi desain jaringan harus juga diidentifikasi. Dalam kasus dimana terdapat jaringan yang sudah ada, harus diidentifikasi bahwa desain jaringan yang baru memberikan operasi yang berkelanjutan dan memberikan suatu kontribusi baru pula yang lebih baik dari desain sebelumnya. Kebutuhan teknis terdiri dari :
- Aplikasi layanan yang berjalan pada jaringan
- Mendukung pengalamatan IPV6
- Kebutuhan akan koneksi *Internet*
- Protokol lain yang berjalan pada jaringan (seperti protocol routing)
- Kebutuhan kabel
- Kebutuhan redundansi
- Menggunakan alat-alat dan protokol khusus layanan yang akan dibangun

- Peralatan yang sudah ada sebelumnya
- Layanan jaringan yang dibutuhkan
- Pengaturan jaringan
- Kebutuhan *bandwidth*
- Solusi layanan jaringan (seperti traffic suara, konten jaringan, penyimpanan jaringan)
- Bagaimana keamanan jaringan layanan
- QoS (Quality of Service)
- Faktor keamanan dan QoS bukan merupakan tujuan utama dari aplikasi yang akan dibangun pada jaringan. Kedua factor tersebut hanya factor pelengkap untuk pembangunan sebuah layanan jaringan. Semakin aman jaringan, maka semakin baik jaringan tersebut.

Selain kebutuhan teknis, maka kebutuhan lain yang perlu diperhatikan adalah masalah bisnis. Kebutuhan masalah bisnis antara lain:

- Modal *budget* dan operasi
- Penjadwalan pembangunan dan pemilihan SDM (Sumber Daya Manusia) yang tepat

  Pemilihan orang yang tepat untuk peng-*install*-an dan pengoperasian jaringan, skill apa yang dimiliki oleh masing-masing SDM, apakah SDM tersebut membutuhkan pelatihan, perlu outsourcing dan lain sebagainya
- Faktor jaringan yang sudah dibangun sebelumnya, apa yang perlu ditambahkan atau dikurangi.
- Peraturan pembangunan jaringan
- Kebutuhan jaringan harus dibuat sedetail mungkin, artinya di akhir pembangunan jaringan, tidak ada lagi yang harus dilakukan untuk menutupi kekurangan pada bagian yang krusial. Sebagai contoh, *customer* mungkin akan meminta pembangunan jaringan yang baru harus menekan biaya *overall.* Kebutuhan ini harus diterjemahkan ke dalam kebutuhan teknis sehingga tidak terlalu banyak pemakaian biaya. Pada pembangunan kebutuhan jaringan kali ini, factor biaya bukan merupakan sebuah poin yang penting untuk diperhatikan.

- Jika ada, analisis jaringan yang sudah pernah dibuat sebelumnya
- Membangun persiapan desain jaringan

  Dalam membangun suatu persiapan desain jaringan, maka pendekatan yang paling baik dilakukan adalah pendekatan *top-down*, yaitu pendekatan dimana pembangunan jaringan dimana yang harus disiapkan sebelumnya adalah kebutuhan pembagunan layanan yang akan di-install pada jaringan tersebut, dengan kata lain, yang membuat suatu desain dapat dibuat berdasarkan analisis kebutuhan layanan jaringan, bukan peralatan apa yang akan digunakan untuk membangun jaringan itu terlebih dahulu, lalu menyesuaikannya dengan kebutuhan suatu jaringan itu untuk menjalankan layanan apa saja. Kasus terakhir ini akan berakhir pada pemilihan ulang suatu desain jaringan yang akan dibangun.
- Menyempurnakan pembangunan jaringan
- Membangun jaringan
- Melihat unjuk kerja jaringan, jika perlu desain ulang
- Buat dokumentasi untuk setiap langkah

2.2 TELECOMMUNICATION MANAGEMENT NETWORK

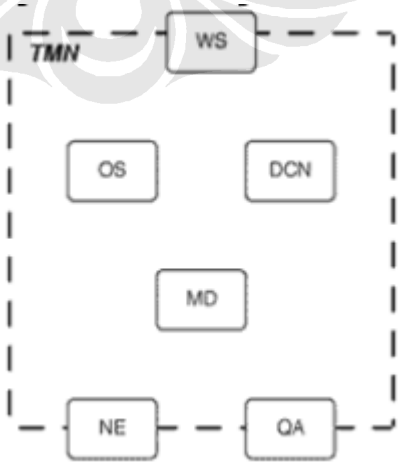
TMN (*Telecommunication Management Network*) dibuat oleh ITU-T (*International Telecommunication Union -Telecommunication)* Sektor layanan (secara formal dinamakan CCITT –*Comite Consultatif Internationale de Telegrapique et Telephonique*-)yang termaktub pada rekomendasi M.3000. Ketika manajemen jaringan telekomunikasi diimplementasikan pada sebuah jaringan, maka jaringan tersebut akan bersifat *interoperable* (dapat dioperasikan/dijalankan), bahkan jika dikomunikasikan / dihubungkan dengan peralatan dan jaringan telekomunikasi lainnya. Antarmuka dari sebuah jaringan yang termaktub dalam rekomendasi ini disebut dengan Q3. Antarmuka dan Jaringan yang dibuat pada rekomendasi M.3000 ini dibangun pada standard OSI (*Open System Interconnection*) yang sudah ada. Standar ini termasuk, tetapi tidak terbatas pada [2] :

- *Common Management Information Protocol* (ICMP) – mengatur pertukaran layanan antar entitas antar dua titik yang berhubungan.

- *Guideline for Definition of Managed* Object (GDMO) – menyediakan *template* untuk mengklasifikasi dan menjelaskan sumber-sumber jaringan.
- *Abstract Syntax Notation One* (ASN.1) – menyediakan aturan syntax untuk tipe data
- *Open System Interconnect Reference Model* – mengatur 7 lapisan OSI

Sejak dibuatnya rekomendasi ini, maka beberapa forum telekomunikasi dunia mulai mengumumkan dengan resmi peraturan baru ini, beberapa forum yang ikut meramaikan pembahasan ini diantaranya : *Network Management Forum* (NMF), Bellcore, dan *European Telecommunication Standard Institute* (ETSI). Secara umum, NMF dan bellcore fokus pada percepatan implementasi dan menyediakan framework untuk membangun kebutuhan manajemen jaringan secara detail. Secara bersamaan, forum-forum teknologi menyiapkan komplian antarmuka manajemen secara mendetail. Forum-forum tersebut antara lain : *Synchronous Optical Network* (SONET), *Interoperability Forum* dan *Asynchoronous Transfer Model*.

Fungsi dari TMN sendiri adalah membuat suatu penyedia layanan dalam bidang telekomunikasi untuk mencapai konektivitas dan komunikasi yang baik melalui sistem operasi dan jaringan. Interkonektivitas didapatkan melalui antarmuka yang standar yang membuat seluruh *resource* sebagai objek. Tabel di bawah menunjukkan komponen-komponen fungsional dari TMN. Gambar di bawah ini menggambarkan blok bangunan dari TMN.



Gambar 2.4 Blok bangunan TMN [2]

Setiap komponen-komponen TMN di atas mempunyai fungsi-fungsi, fungsi dari masing-masing komponen tersebut dapat dilihat pada tabel 2.1:

Penjelasan tabel :

MD = Mediation Table

OS = Operation Systems

QA = Q-Adapters

NE = Network Element

WS = Work Station

MD, menyediakan OS, QA, WS. Sebagai tambahan OS menyediakan QA dan WS.

Tabel 2.1 Komponen Fungsional [2]

System Component	Description
OS	performs operations system functions, including operations monitoring and controlling telecommunications-management functions; the OS can also provide some of the mediation, q-adaption, and WS functions.
MD	performs mediation between local TMN interfaces and the OS information model; mediation function may be needed to ensure that the information, scope, and functionality are presented in the exact way that the OS expects. Mediation functions can be implemented across hierarchies of cascaded MDs.
QA	The QA enables the TMN to manage NEs that have non–TMN interfaces. The QA translates between TMN and non–TMN interfaces. A TL1 Q-adapter, for example, translates between a TL1 ASCII message-based protocol and the CMIP, the TMN interface protocol; likewise, simple network management protocol (SNMP) Q-adapter translates between SNMP and CMIP.
NE	In the scope of TMN, an NE contains manageable information that is monitored and controlled by an OS. In order to be managed within the scope of TMN, an NE must have a standard TMN interface. If an NE does not have a standard interface, the NE can still be managed via a Q-adapter. The NE provides the OS with a representation of its manageable information and functionality (i.e., the MIB). Note that the NE contains NE functionality—that is, the functions required in order to be managed by an OS. As a building block, the actual NE can also contain its own OS function, as well as QA function, MD function, etc.
WS	The WS performs workstation functions. WSs translate information between TMN format and a displayable format for the user.
data communication network (DCN)	The DCN is the communication network within a TMN. The DCN represents OSI layers 1 to 3.

2.2.1 Jaringan logika TMN

Gambar 2.5 di bawah menunjukkan hirarki dari suatu TMN. Semakin ke atas, maka semakin jarang digunakan, Bagian atas dari hirarki TMN merupakan standar yang biasa digunakan pada skala korporat (*enterprise*), sedangkan semakin ke bawah akan sering dijumpai pada jaringan kebanyakan (*rural area*).

Gambar 2.5 Komponen logika TMN

Merupakan suatu sistem untuk mengatur suatu jaringan komputer.

Fungsi dari network management [3]:

- Kesalahan (Fault) : mengenali masalah, mengisolasinya, membuat laporan kesalahan
- Konfigurasi : mengumpulkan , simpan konfigurasi, membuat menjadi sederhanan, mencari perubahan dan menetapkan
- Accounting : Mengumpulkan statistik penggunaan
- Performance : Persiapan kapasitas, determine the efficiency
- Security : Mengontrol akses ke asset

2.3 Elemen Jaringan

Elemen Jaringan adalah sebuah kumpulan alat yang akan digunakan pada sebuah jaringan. Adapun elemen jaringan yang bakal digunakan antara lain:

1. Router
2. Switch

2.3.1 Router

Router merupakan divais pada *network layer* yang berfungsi melakukan forwarding 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 internetwork yang sangat besar, selain itu router juga dapat digunakan untuk menghubungkan jaringan yang berbeda arsitektur seperti Ethernet dengan jaringan *token ring*. Divais ini juga dapat memberikan pilihan jalur terbaik untuk transmisi paket data pada jaringan dengan algoritma routing tertentu. Pada praktisnya router mempunyai banyak modul yang dapat dipasang pada bagian belakang router sesuai dengan interface yang diinginkan seperti *Ethernet*, *Fast Ethernet*, *Gigabit Ethernet*, dan kabel serial. Router dapat dikonfigurasi dengan menggunakan *IOS (Internet Operating System) Command*.Gambar 2.6 menunjukkan contoh sebuah *router*.

Gambar 2.6 *Router[Packet Tracer Software]*

2.3.2 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 MAC (Medium Access Control) address. MAC address sendiri merupakan identitas suatu divais yang terdiri dari 48 bits dimana 24 bi t pertama diberikan oleh IEEE Standard Association sebagai OUI (Organizationally Unique Identifier) dan 24 bit sisanya diberikan ke vendor untuk memperoleh alamat yang bersifat unik untuk setiap network interface yang mereka buat Terdapat dua cara forwarding data pada switch, yaitu store-and-forward dan cut-through. Pada switch, sebuah frame harus diterima secara lengkap dulu baru dapat diteruskan, hal ini menyebabkan adanya latency yang tergantung dari besarnya frame. Switch biasanya disimbolkan sesuai dengan gambar 2.7.

Gambar 2.7 *Switch* [*Packet Tracer Software*]

2.4 Pengkabelan

Jenis dari pengkabelan dari Ethernet adalah :

1. Kabel *Straight- Through*
2. Kabel *Crossover*

2.4.1 Kabel Straight-Through

Pengkabelan ini menghubungkan antara :

- *host* ke *switch* atau *hub*
- *router* ke *switch* atau *hub*

4 kabel digunakan pada pengkabelan *straight-through* yang menghubungkan peralatan *Ethernet*. Keterhubungan 4 kabel tersebut dapat dilihat pada gambar di bawah.

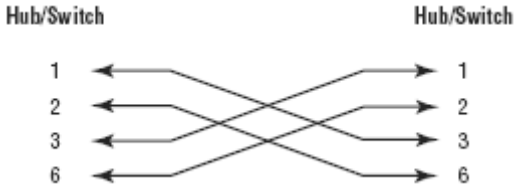
Gambar 2.8 Kabel *Straight-Through*

2.4.2 Pengkabelan Crossover

Kabel crossover biasanya digunakan untuk menghubungkan :

- *Switch* ke *switch*
- *Hub* ke *hub*
- Komputer ke komputer
- *Hub* ke *Switch*
- *Router* ke komputer

Pengkabelan ini digunakan untuk menghubungkan peralatan jaringan dengan hirarki yang sama. Gambar dari hubungan antar kabel ini dapat dilihat dari gambar di bawah.

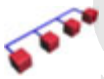


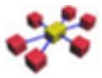
Gambar 2.9 *Crossover*

2.4.3 Komparasi Topologi

Tabel 2.2 menunjukkan komparasi topologi yang terdapat pada beberapa jaringan, setiap topologi jaringan mempunyai kelebihan dan kekurangannya masing- masing. Tabel ini sangat membantu untuk menentukan topologi apa yang akan digunakan dalam pembangunan jaringan kali ini.

Tabel 2.2 Komparasi Topologi

Topologi	Deskripsi
 Bus	Terdiri dari kabel trunk dengan dengan titik yang langsung terhubung dengan titik yang terhubung langsung dengan trunk, atau titik yang terhubung dengan kabel drop secara langsung. • Sinyal berjalan dari titik satu ke titik lainnya pada bus. • Alat yang dinamakan terminator diletakkan pada setiap titik akhir dari kabel trunk.. • Terminator menyerap sinyal dan mencegahnya dari refleksi secara berulang balik pada kabel. Bus Fisik :The physical bus: • Memerlukan kabel lebih sedikit daripada topologi star • Sulit untuk isolasi masalah pengkabelan.
 Ring	Topologi ring berhubungan dengan titik sampai masing- masing titik membentuk cincin. semua peralatan yang terhubung dengan ring berguna sebagai repeater untuk mengirim paket ke peralatan lain.Dengan ring : • Penginstalan memerlukan rencana yang sangat hati- hati untuk membangun sebuah jaringan ring yang bersambung. • Mengisolasi masalah dapat memerlukan pemeriksaan pada setiap bagian dari jaringan tersebut.

	• Sebuah titik yang tidak berfungsi dapat mencegah sinyal dari mencapai titik lain pada jaringan ring tersebut.
 Star	Topologi ini menghubungkan hub atau switch sebagai konsentrasi semua koneksi jaringan untuk lokasi fisik tunggal. • Mudah untuk dikonfigurasi ulang. • Titik- titik dapat ditambahkan ataupun dihilangkan. • Masalah pengkabelan biasanya member efek hanya pada satu titik. • Membutuhkan lebih banyak kabel dari pada topologi yang lain.
 Mesh	Topologi mesh jika ada banyak jalur antar dua titik pada satu jaringan. Topologi ini terhubunga menggunakan jaringan point-to-point. Topologi ini meningkatkan toleransiterhadap kesalahan. Jika satu jalur rusak, maka masih adas jalur lain yang menjadi cadangan untuk berhubungan antar elemen jaringan.Topologi ini terdiri atas dua jenis jaringan, yaitu: • Mesh Parsial – beberapa jalur perulangan ada. • Mesh Penuh – Setiap titik mempunyai koneksi point-to-point dengan titik lainnya. Topologi Mesh penuh tidak biasa digunakan karena terlalu banyaknya kabel yang akan digunakan. Topologi ini biasa digunakan pada jaringan nirkabel yang mempunyai topologi ad-hoc.

2.5 VLAN (VIRTUAL LOCAL AREA NETWORK)

VLAN (*Virtual* LAN) merupakan suatu jaringan dimana pengguna menggunakan suatu jalur virtual yang dibuat dari konfigurasi *port- port switch* yang mengizinkan adanya keterhubungan antar *host* yang ada dan terhubung secara logika walaupun tidak terhubung secara langsung dengan menggunakan media kabel.

2.5.1 Kendali Terhadap Penyiaran (Broadcast Control)

Penyiaran berada pada setiap protocol, tetapi seberapa sering penyiaran ini berlangsung tergantung pada 3 kondisi, yaitu [4]:

- Tipe protokol
- Aplikasi yang berjalan pada jaringan
- Bagaimana aplikasi- aplikasi ini berjalan pada jaringan

Beberapa layanan memerlukan *bandwidth* yang kecil, dan beberapa lagi memerlukan *bandwidth* yang sangat besar, biasanya ini merupakan suatu aplikasi yang besar seperti video conferencing. Disinilah fungsi dari VLAN untuk membagi *bandwidth* yang ada sesuai dengan layanan yang dijalankan pada suatu jaringan. Jika suatu layanan dijalankan, maka switch yang dikonfigurasi dengan VLAN akan menyiarkannya pada pengguna yang menggunakan layanan yang sejenis. Ini merupakan keuntungan yang besar bagi perusahaan untuk mengadopsi VLAN bagi jaringan yang akan dibangun.

2.5.2 Keamanan

Keamanan menjadi isu yang sangat penting saat ini. Untuk itulah VLAN digunakan untuk mengatasi masalah ini. Dengan VLAN maka hanya yang masuk dalam database VLAN tersebut yang dapat mengakses layanan tersebut. Dengan begini, maka administrator jaringan dapat dengan mudah mengawasi dengan sangat teliti pengguna yang akan mengakses layanan tertentu. Selain itu pengguna tidak dapat seenaknya mengganti port yang tersedia untuk layanan tersebut karena yang menjadi parameter untuk dapat terhubung pada layanan tertentu, maka data IP pengguna juga merupakan sebuah parameter untuk dapat terhubung. Maka dari itu VLAN merupakan pilihan yang baik jika suatu perusahaan menginginkan keamanan pada jaringannya.

2.5.3 Komponen VLAN

Untuk membangun VLAN, maka dibutuhkan beberapa komponen, komponen inilah yang nantinya akan membagi pengguna sesuai dengan kebutuhan layanannya satu per satu. Adapaun komponen tersebut adalah :

1. VLAN database, merupakan kumpulan nama dari VLAN tersebut, contoh, jika ada 3 buah bagian pada sebuah perusahaan, misalnya *marketing*, teknik, keuangan, maka database-nya dibuat sesuai jumlah bagian tersebut. Ini menyebabkan pengguna marketing hanya bisa mengakses bagian tersebut dan tidak diizinkan untuk berhubungan dengan bagian lain.
2. Hubungan *Access*, merupakan *port* pada *switch* yang berhubungan dengan pengguna
3. Hubungan *Trunk* , merupakan hubungan pada *switch* yang berhubungan dengan *switch* yang lain.

2.5.4 Metode Identifikasi VLAN

Identifikasi VLAN adalah switch menggunakan apa untuk memeriksa suatu jejak dari semua frame. Identifikasi ini yang digunakan switch untuk mengenali frame mana yang merupakan bagian dari VLAN yang mana pula. Identifikasi ini sendiri terdiri dari beberapa metode, yaitu:

- *Inter-Switch Link* (ISL) merupakan properti dari switch Cisco, dan hanya digunakan oleh Fast Ethernet dan Gigabit. Hubungan ini tidak mengizinkan layer 3 untuk melewatinya
- IEEE 802.1Q merupakan rekomendasi IEEE yang ditetapkan sebagai standar dari metode frame tagging, yang memasukkan sebuah *field* ke dalam frame untuk identifikasi VLAN. Identifikasi ini baik dilakukan jika yang dihubungkan adalah tipe switch yang berbeda. Cara kerja dari identifikasi ini adalah dengan cara mencalonkan setiap port 802.1Q untuk diasosiasikan dengan VLAN ID tertentu. Port yang berada pada suatu trunk akan membuat grup yang dikenal dengan VLAN asli (native), dan setiap port mendapat tag dengan nomor identifikasi yang merefleksikan VLAN *native*- sebagai defaultnya adalah menjadi VLAN1.

2.5.5 Keanggotaan VLAN

Keanggotaan VLAN sendiri dibagi atas 2, yaitu:

1. VLAN Statis, Merupakan keanggotaan yang tidak dapat diubah sewaktu jaringan VLAN sudah dibagun, semua komponen VLAN tidak dapat secara otomatis diubah kecuali dengan cara manual oleh seorang administrator jaringan. Keanggotaan VLAN ini sangat aman dibandingkan dengan VLAN yang dinamis. Pengguna tidak dapat merubah IP yang sudah diterima dari administrator. Misalnya sebuah VLAN dinamakan marketing, maka hanya pengguna dengan IP dalam range tersebut yang dapat mengakses VLAN tersebut.
2. VLAN dinamis, merupakan VLAN dengan pemberian IP secara otomatis dengan menggunakan perangkat lunak manajemen yang inteligen, VLAN dapat dibuat dengan cara menandai alamat MAC, protokol perangkat keras yang ada atau bahkan aplikasi untuk membuat VLAN dinamis. Sehingga VLAN database akan memuat batasan alamat MAC yang akan dapat mengakses VLAN tersebut. Database bisa berubah secara otomatis sesuai dengan VLAN yang akan dituju oleh pengguna yang baru saja memasukkan kabel yang ada pada suatu port, setelah itu aplikasi pada switch akan membaca alamat MAC pengguna tersebut dan secara otomatis memberikan akses ke suatu VLAN tertentu sesuai kebutuhan.

2.6 EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP merupakan protokol *routing* yang dipakai pada *router* cisco dan pada prosesor internal yang ditemukan pada distibusi cisco.

2.6.1 Fitur dan Cara Kerja EIGRP

Enhaced IGRP merupakan protokol *routing* yang tidak mempunyai kelas, *distance-vector* (merupakan protokol ruting yang mencari jalur dengan memperhitungkan jarak) yang lebih tinggi dari pada IGRP-protokol *ruting* lain dari cisco-. EIGRP menggunakan *autonomous-system* dengan *router* yang ada di sebelahnya untuk menjelaskan kepada router tetangga tersebut yang menjalankan protokol ruting yang sama dengan cara saling tukar informasi *ruting*. Tetapi berbeda dengan IGRP, maka protokol ini mengandung subnet mask pada perbaharuan jalur yang ada. Penyebaran informasi subnet menggunakan VLSM dan sumarisasi untuk desain jaringan kita.

EIGRP terkadang mempunyai protokol *ruting hybrid* (penggabungan antara *distance vector* dan *link state*). Sebagai contoh EIGRP tidak mengirim paket link-state seperti OSPF, malahan mengirim distance-vector update yang berisi informasi tentang jaringan ditambah dengan biaya dari pencapaian mereka dari perspektif *router* yang mengirimkan paket- paket. Dan EIGRP mempunyai karakteristik link state juga, yang menyamakan tabel rute antara router- router yang ada di sebelahnya pada waktu awal dan kemudian mengirim update yang spesifik ketika perubahan topologi berlangsung. EIGRP sangat cocok pada jaringan yang besar. EIGRP mempunyai perhitungan hop yang maksimum sebesar 255. Ada beberapa fitur kuat yang membuat EIGRP berbeda dan lebih baik dari pada IGRP dan protokol lain. Fitur tersebut antara lain :

- Mendukung untuk IP, IPX, dan *Apple Talk* via modul protokol dependen.
- Penemuan tetangga yang efisien
- Komunikasi via RTP (*Reliable Transport Protocol*)
- Jalur terbaik seleksi via *Diffusing Update Algorithm* (DUAL)

2.6.2 Menemukan Router Tetangga

Sebelum router EIGRP akan berpindah ke router lain, router tersebut harus menjadi tetangga. Ada 3 kondisi dimana EIGRP harus bertemu dengan tetangganya, yaitu:

- Penerimaan ACK atau hello
- Kesamaan nomor AS
- Ukuran yang serupa (Nilai K)

Protokol link-state menggunakan pesan Hello untuk membangun tetangga karena biasanya router- router tetangga tidak mengirim perbaharuan secara periodik, dan harus ada mekanisme yang menolong tetangga untuk menyadari bahwa router tersebut merupakan tetangganya., router EIGRP harus terus- menerus melakukan hubungan Hello dengan router tetangganya.

Router- router EIGRP yang mempunyai AS yang berbeda tidak secara otomatis membagi informasi routing dan mereka tidak merupakan tetangga. Hal ini sangat baik untuk mengurangi terlalu banyaknya pertukaran informasi antar router jika semua memiliki nomor AS yang sama. Hanya saja yang menjadi masalah adalah pertukaran informasi ruting dengan jaringan yang mempunyai AS yang berbeda harus dilaksanakan secara manual. Maka jika ada tetangga baru, tabel ruting akan diperbaharui secara berkala.

2.6.3 Konsep Routing

Mempunyai 4 konsep fundamental, yaitu [4]: tabel tetangga, tabel topologi, pernyataan rute, dan tagging rute.

2.6.3.1 Tabel Tetangga

Ketika router menemukan tetangga baru, router tersebut merekam alamat tetangga dan antar muka sebagai masukan pada tabel tetangga. Satu tabel tetangga berisi atas modul protokol keterganrungan. Ketika tetangga mengirim paket Hello, router tersebut menyiarkan waktu tunggu, yang merupakan pemanggilan dari waktu yang menyebabkan router itu merupakan router tetangga.

2.6.3.2 Tabel Topologi

Berisi semua informasi tentang semua alamat destinasi yang disiarkan oleh *router- router* yang bertetangga. Selain itu tabel ini terdiri dari alamat tujuan daftar dari tetangga yang telah disebarkan alamat tujuannya. Untuk setiap tetangga, catatan

menyimpan metrik yang disebarkan, yang disimpan oleh tetangga pada tabel ruting. Jika rute ini disebarkan, maka router EIGRP yang menggunakan protokol *distance-vector* harus mengikuti rute ini untuk meneruskan paket. Tabel terbaik adalah kumpulan-kumpulan dari tabel- tabel yang ada pada *router- router* sekitar untuk menghasilkan rute terbaik.

2.6.3.3 Keadaan Rute

Isi dari tabel topologi untuk tujuan dapat berisi dua pernyataan: aktif atau pasif. Tujuan merupakan pernyataan pasif jika *router* tidak melaksanakan komputerisasi ulang. Rekomputasi terjadi jika tidak ada pengganti yang meyakinkan dan ini adalah saat dimana pernyataan aktif berlangsung. Ketika tujuan berada dalam keadaan aktif maka akan dilakukan rekomputasi. Rekomputasi terjadi bila tujuan yang dituju tidak memiliki pengganti yang memungkinkan. Router menginisiasi proses rekomputasi dengan mengirimkan paket *query* untuk setiap router tetangga. Router tetangga yang dikirimi paket query ini dapat mengirimkan paket balasan sebagai tanda bahwa suatu tujuan mempunyai pengganti yang memungkinkan, atau dapat pula mengirimkan paket *query* yang mengindikasikan bahwa router tersebut termasuk router yang melakukan rekomputasi. Selama sebuah tujuan berada dalam keadaan aktif, maka sebuah router tidak dapat mengganti tujuan yang tercantum dalam tabel *routing*. Setelah router mendapat balasan dari setiap *router* tetangga, maka masukan data pada tabel topology berubah ke keadaan pasif dan sebuah *router* dapat memilih pengganti.

2.6.3.4 Route Tagging

EIGRP mendukung rute internal dan eksternal. Internal route merupakan karakteristik asli dari EIGRP, sehingga jaringan yang terpasang langsung dengan jaringan EIGRP dianggap sebagai *internal route*. Sedangkan *external route* (rute eksternal) merupakan router yang dipelajari routing protokol yang lain dan masih dianggap sebagai *static route.* Rute eksternal ditandai *(tagged)* dengan informasi – informasi sebagai berikut :

- Router ID
- *AS number* dari tujuan
- Penanda (tag) dari administrator yang dapat dikonfigurasi
- ID dari protokol external
- Metric dari protocol external
- *Bit flags* dari protokol routing standar

2.7 PING

Ping (singkatan dari *Packet Internet Groper*) adalah sebuah program utilitas yang digunakan untuk memeriksa konektivitas jaringan berbasis teknologi *Transmission Control Protocol/Internet Protocol* (TCP/IP). Dengan menggunakan utilitas ini, dapat diuji apakah sebuah komputer terhubung dengan komputer lainnya. Hal ini dilakukan dengan cara mengirim sebuah paket kepada alamat IP yang hendak diujicoba konektivitasnya dan menunggu respons darinya. Nama "ping" datang dari sonar sebuah kapal selam yang sedang aktif, yang sering mengeluarkan bunyi *ping* ketika menemukan sebuah objek.

Apabila utilitas ping menunjukkan hasil yang positif maka kedua komputer tersebut saling terhubung di dalam sebuah jaringan. Hasil statistik keadaan koneksi ditampilkan dibagian akhir. Kualitas koneksi dapat dilihat dari besarnya waktu pergi-pulang (*roundtrip*) dan besarnya jumlah paket yang hilang (*packet loss*). Semakin kecil kedua angka tersebut, semakin bagus kualitas koneksinya.

	Bit 0 - 7	Bit 8 - 15	Bit 16 - 23 Bit 24 - 31
IP Header (160 bits OR 20 Bytes)	Version/IHL	Type of service	Length
	Identification		*flags* et *offset*
	Time To Live(TTL)	Protocol	Checksum
	Source IP address		
	Destination IP address		
ICMP Payload (64+ bits OR 8+ Bytes)	Type of message	Code	Checksum
	Quench		
	Data (*optional*)		

Gambar 2.10 Paket ICMP

BAB III
PERANCANGAN JARINGAN

3.1 Pengumpulan Kebutuhan Jaringan

Sebelum membangun jaringan, maka perlu dikumpulkan terlebih dahulu kebutuhan tentang layanan yang akan dibangun pada jaringan tersebut sehingga ketika akan memilih hardware yang akan digunakan pada sebuah topologi jaringan, tidak terjadi kesalahan sedikitpun. Adapun data yang tersedia adalah data wilayah dan *bandwidth* yang tersedia pada masing-masing wilayah. Diharapkan dari data-data tersebut akan diperoleh jaringan sesuai dengan kebutuhan layanan yang ada.

Adapun ke tujuh wilayah tersebut dengan alokasi banyaknya *host* yang ada pada setiap wilayah ditunjukkan pada tabel berikut:

Tabel 4.1 Banyaknya Jumlah Pengguna Jaringan pada Setiap Wilayah

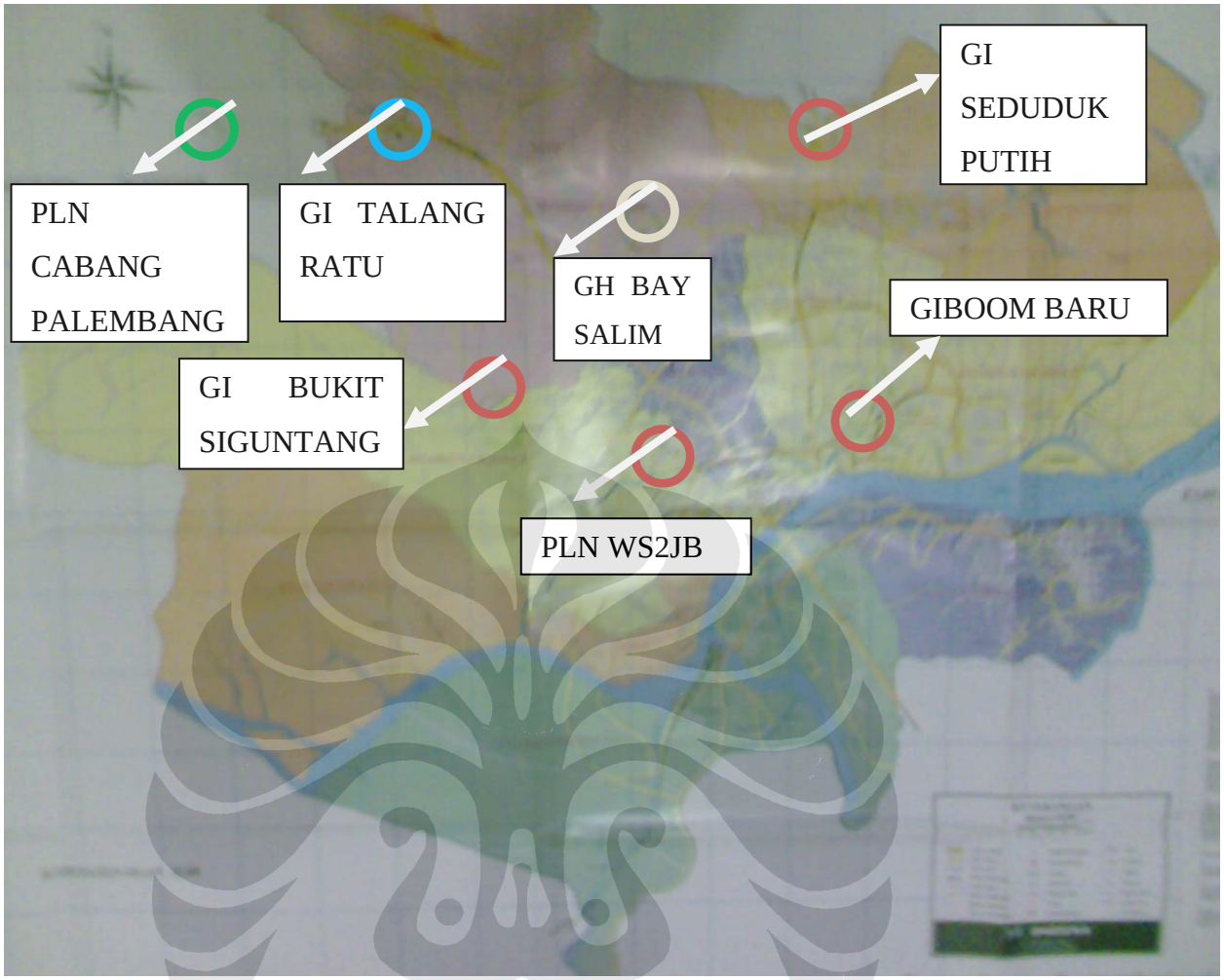
- Tabel 3.1

No	Lokasi	Jumlah *host*	Alokasi *Bandwidth* (Kbps)
1.	GI Talang Kelapa	5	2048
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	64
7.	GI. Bukit Siguntang	5	64

3.2 Pembangunan Jaringan Berdasarkan Area Layanan

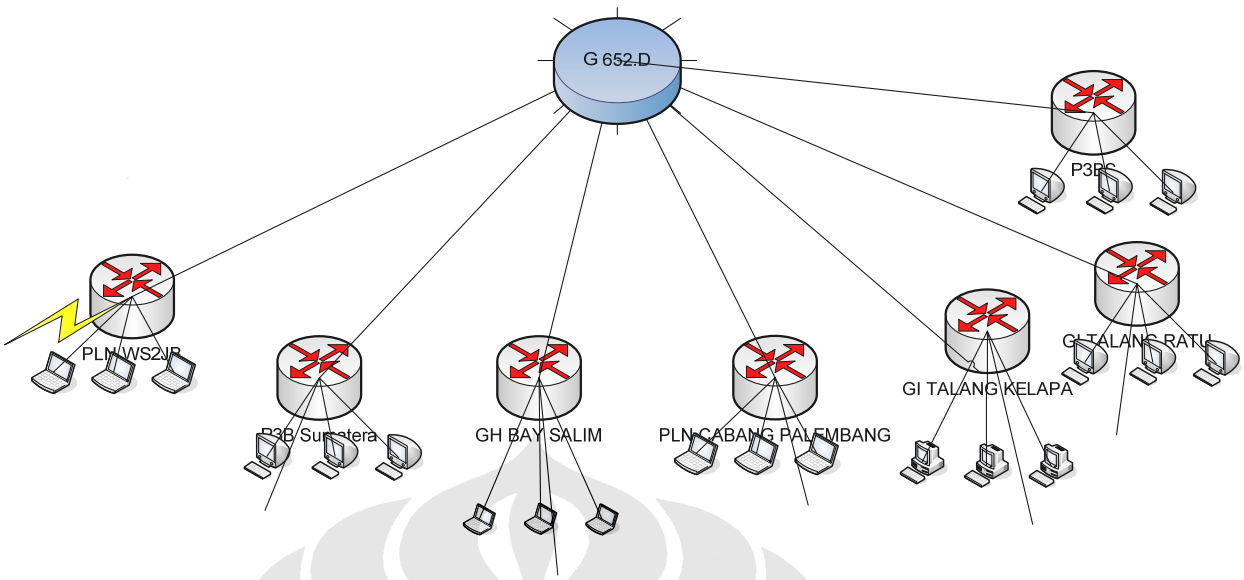
Pembangunan jaringan akan dibangun dengan topologi *ring*. Digunakannya topologi ring karena berdasarkan wilayah yang ada merupakan daerah yang memutar dan, maka diambil kesimpulan bahwa topologi yang paling baik untuk membangun jaringan dengan area layanan yang berbentuk memutar seperti pada peta di bawah adalah dengan topologi *ring*. Topologi ini juga dipilih untuk mengurangi biaya untuk penyediaan kabel sehingga kabel yang dibutuhkan untuk membangun jaringan di Palembang ini dapat dikurangi. Adapun ke tujuh wilayah tersebut dapat dilihat pada Gambar 3.1 di bawah ini.



- Gambar 0.1

- Gambar 3.0.2 Peta Palembang

Berdasarkan area di atas, maka topologi yang akan dibangun ditunjukkan pada Gambar 3.2 di bawah ini.



- Gambar3.0.3 Topologi Jaringan yang akan dibangun di Palembang

Gambar 3.2 di atas menunjukkan setiap titik daerah yang akan dibangun jaringan dibuat saling berhubungan satu sama lain. Ini dilakukan agar mudah mendeteksi jika terjadi kesalahan di salah satu titik. Kelemahan topologi ring sendiri adalah jika salah satu jaringan terputus, maka akan mengganggu jaringan lainnya sehingga semua jaringan terputus. Untuk mengatasi kelemahan tersebut, maka akan dibuat sebuah protokol *routing* EIGRP pada layanan yang akan dibangun dengan L3VPN, sedangkan yang dibangun dengan L2VPN dengan menggunakan teknologi VLAN. Pembangunan jaringan ring yang menghubungkan setiap titik daerah layanan di daerah Palembang cukup beralasan karena melihat jaringan ini mungkin punya layanan yang akan saling berhubungan satu sama lain di kemudian hari, walaupun untuk saat ini belum dibutuhkan hubungan antar semua titik. Masing-masing daerah di atas memiliki kebutuhan layanan yang berbeda satu sama lain. Layanan yang akan dibangun pada masing-masing titik akan dibangun pada jaringan tersebut adalah sebagai berikut :

- Layanan video conferencing
- Layanan IP VPN
- Layanan Internet
- Layanan suara (IP Telephony)

Sedangkan yang akan dibahas secara terperinci adalah layanan IP VPN. Layanan ini kemudian akan dibagi menjadi dua, yaitu VLAN dan EIGRP.

3.3 Pembangunan Jaringan L2VPN dengan teknologi VLAN

Untuk membangun sebuah jaringan VLAN, maka dibutuhkan sebuah alat yang bernama switch untuk menjamin keterhubungan antara VLAN yang akan dibentuk. Terdapat dua komponen penting untuk membangun sebuah jaringan berbasis VLAN (Virtual Local Area Network). Komponen tersebut adalah trunk dan access. Dua komponen ini masing-masing dapat pada diatur pada port dari switch yang ada. Trunk ialah port yang berhubungan dengan port lain pada switch lain pula. Sedangkan access adalah hubungan antara komputer dengan port pada switch. Pada penelitian kali ini akan dibangun beberapa layanan jaringan antar lokasi yang sudah dijelaskan sebelumnya dengan menggunakan teknologi VLAN. Jaringan VLAN tersebut akan membedakan jalur berdasarkan layanan yang ada. Hanya komputer dengan jalur VLAN yang ada yang akan dapat mengadakan hubungan. Misalnya, jika layanan yang dipunyai pada satu jalur VLAN hanya akan berhubungan dengan komputer lain yang juga terletak pada jalur VLAN tersebut. Dengan kata lain, setiap komputer ditandai dengan suatu nama pada setiap port pada switch untuk melakukan hubungan dengan komputer lain pada port switch. Penandaan port ini diatur oleh sebuah konfigurasi pada sebuah switch. Adapun langkah-langkah untuk membuat tanda pada masing-masing port untuk sebuah jalur adalah sebagai berikut:

1. Membuat sebuah nama baru untuk sebuah vlan, nama ini dapat berupa nama layanan yang akan diberikan. Dalam kasus pembangunan jaringan di Palembang ini, maka nama-namanya akan disamakan dengan nama setiap layanan. Nama VLAN yang ada antara lain: vlan 2 dengan nama vicon, vlan 3 dengan nama ipvpn, vlan 4 dengan nama iptelephony dan vlan 4 dengan nama internet.
2. Setiap *switch* yang akan menggunakan layanan spesifik akan mendapatkan nama yang spesikfik pula untuk setiap port pada switch. Sebagai contoh di daerah bukit siguntang akan dibangun layanan video conferencing dan ip vpn maka database VLAN akan diisi dengan nama vicon dan ipvpn.
3. *Database* tersebut nantinya akan menerima tipe-tipe *port* yang ada (trunk atau akses) dan merubahnya menjadi frame setelah dibandingkan. *Switch* tersebut akan menjatuhkan frame jika :

4. port tersebut merupakan *port* akses jika *frame* mempunyai format enkapsulasi Dot1q
    a. port tersebut merupakan port trunk jika *frame* bukan Dot1q.
    b. jika tidak ada *frame* yang akan dikirim, maka proses pemrosesan *frame* dilaksanakan
5. Switch akan mengenali VLAN mana yang akan menjadi tujuan dari frame
    a. Jika port yang menerima adalah trunk, maka :
        i. port tersebut menerima frame tujuan nomor VLAN dari tag VLAN pada header Dot1q.
        ii. mengecek apakah switch tersebut mempunyai konfigurasi VLAN.
        iii. jika terkonfigurasi, maka *switch* tersebut akan menerima tabel alamat MAC.
        iv. Jika tidak,akan diberi tabel alamat MAC yang baru.
        v. jika VLAN tidak ada, maka switch akan menyiarkan frame pada semua port trunk (kecuali port yang menerima) yang menerima nomor VLAN tersebut.
    b. Jika port yang menerima adalah access, maka switch tersebut akan melanjutkan proses tersebut. Switch tersebut akan mengirimkan paket pada proses yang lebih tinggi, yaitu:
        i. *frame* STP.
        ii. *frame* tujuan merupakan alamat MAC adalah alamat CDP *multicast*.
        iii. alamat MAC yang disiarkan.

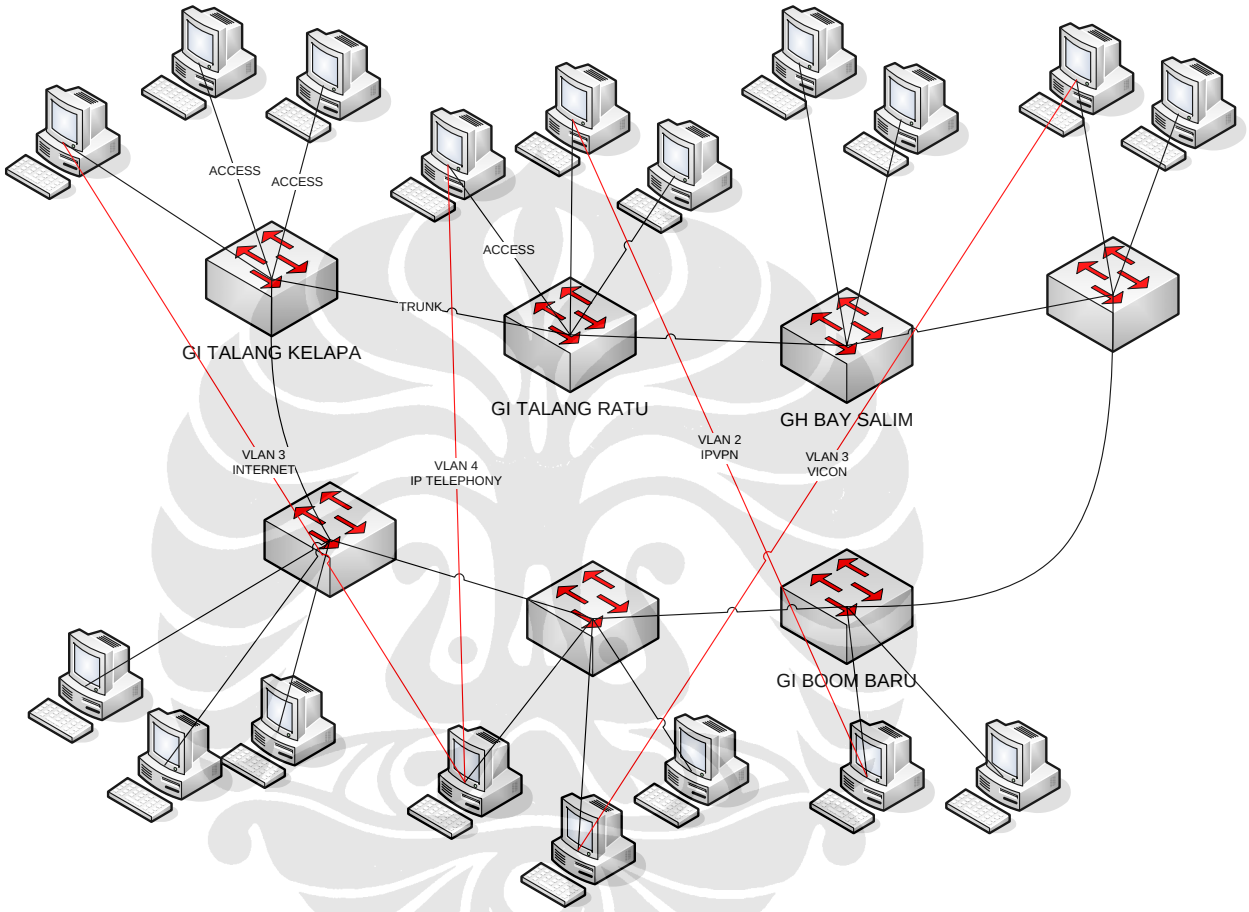
3.4 Desain Jaringan VLAN

Untuk membuat suatu jaringan VLAN, maka diperlukan:

- Desain jaringan logika
- Desain Jaringan fisik
- Desain kebutuhan IP (*Internet Protocol)*
- VLAN *database*
- IOS *command* untuk konfigurasi VLAN

3.4.1 Desain Jaringan logika

Jaringan yang akan dibangun merupakan jaringan dengan topologi *ring*. Adapun desain jaringan logika pada pembangunan kali ini adalah sebagai berikut :



- Gambar3.0.4 Jaringan Logika

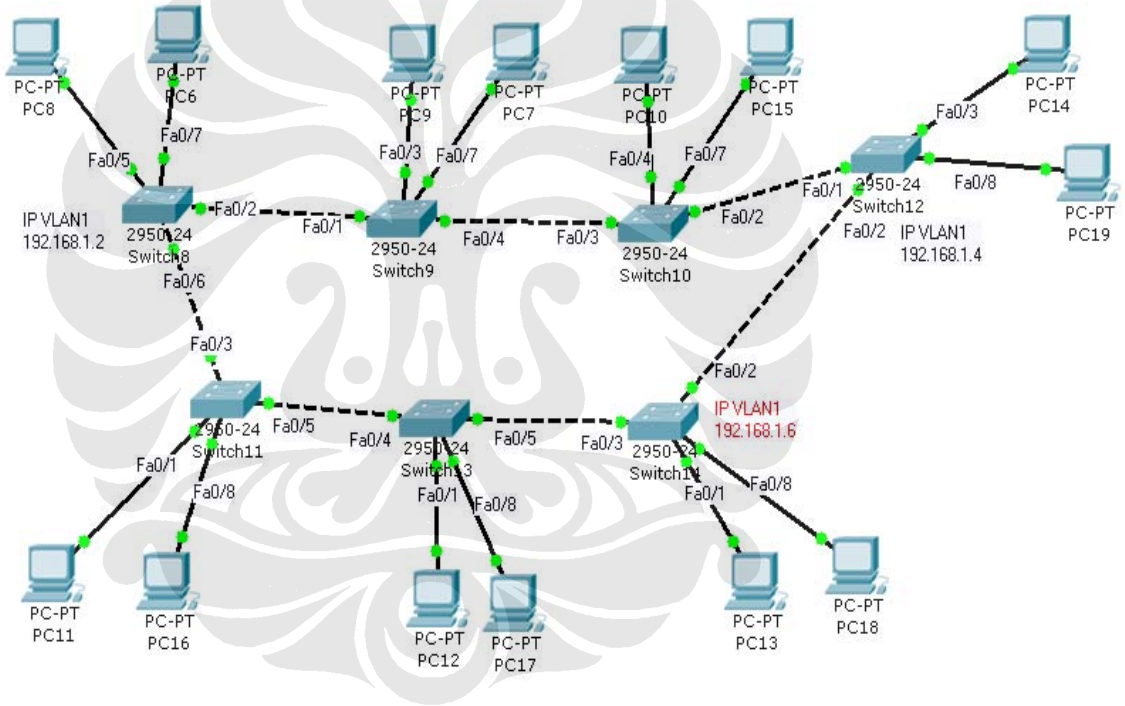
Gambar di atas menunjukkan rancangan jaringan secara logika yang dibentuk masing-masing pengguna dengan menggunakan konfigurasi VLAN. Jaringan ini dibuat dengan topologi *ring* dan direncanakan bahwa sebuah lokasi dapat mengakomodir layanan yang berbeda dan setiap anggota VLAN tersebut hanya dapat mengakses ke tempat lain dengan anggota VLAN yang sama saja. Rangkaian logika ini dijelaskan dengan garis berwarna merah di atas dengan tulisan vlan 3dan sebagainya. Hanya yang termasuk dalam anggota vlan 3 yang dapat mengakses komputer pengguna yang merupakan anggota vlan 3 lainnya tersebut. Jaringan tersebut

sebenarnya merupakan jaringan dengan topologi *full mesh* yang diwakilkan dengan topologi ring.Disebut topologi *full mesh* karena setiap komputer pada masing- masing titik tersebut saling berhubungan secara langsung dengan logika. Oleh karena itulah jaringan tersebut dikatakan jaringan logika

3.4.2 Desain Jaringan Fisik

Kebutuhan Hardware yang akan digunakan antara lain adalah :

- Komputer
- *Switch* Cisco 2950 -24 (memiliki 24 port)

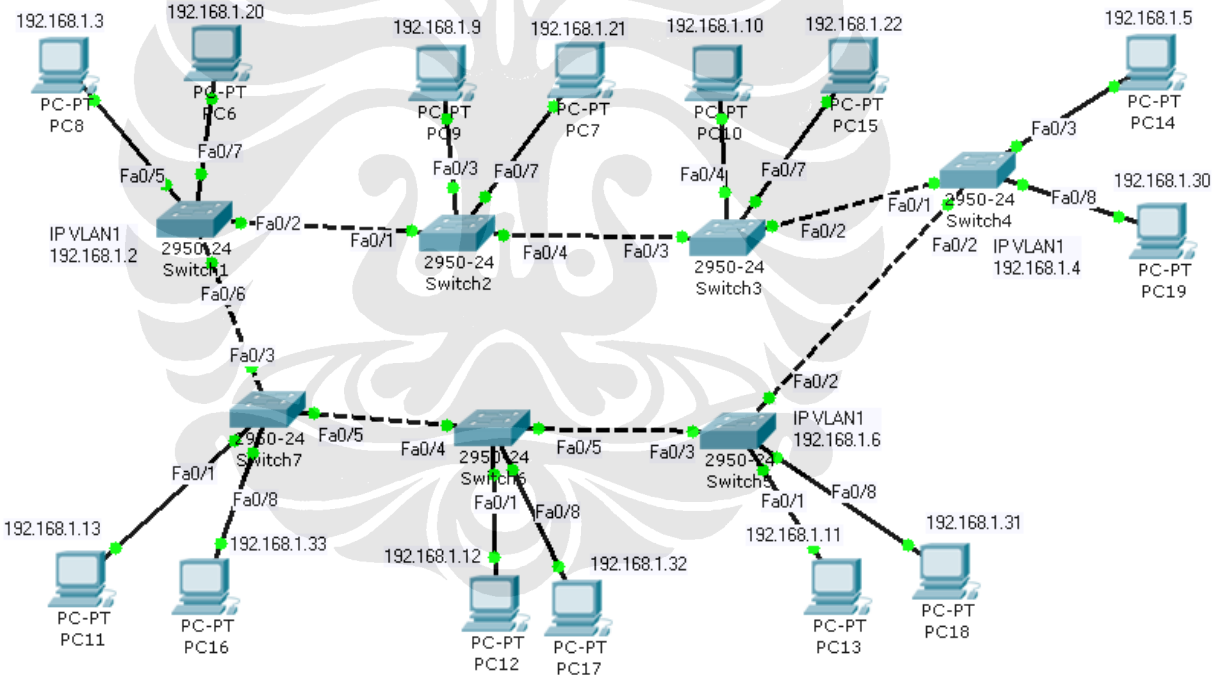


Gambar 3.0.5 Jaringan Fisik

Gambar 3.4 di atas menunjukkan desain jaringan fisik yang dibuat pada perangkat lunak Packet Tracer. Perangkat lunak tersebut dapat mensimulasikan dengan jarignan yang ada dengan jaringan yang akan dibangun pada ke tujuh wilayah tersebut. Jaringan di atas merupakan wujud aplikatif dari jarignan logika yang telah dijelaskan di atas. Jaringan ini akan dirancang dengan menggunakan topologi ring pada hubungan *backbone* yang saling dihubungkan dengan *switch.*

3.4.3 Alokasi IP pada Pengguna

Pembangunan jaringan VLAN ini menggunakan IP pada kelas C. Pemilihan IP kelas C ini tentu sangat berhubungan dengan banyaknya pengguna pada masing- masing tempat. Adapun jumlah pengguna di 7 cabang kantor PLN yang ada di kota Palembang adalah sekitar 90 pengguna. Oleh karena jumlah pengguna ada 90, maka dipilihlah IP kelas C dengan alamat subnet adalah 192.168.1.0/24 dengan subnet mask 255.255.255.0. IP ini mempunyai range dari 192.168.1.1 sampai 192.168.1.254. Dengan alokasi IP pada VLAN1 pada switch 1 (lihat gambar di bawah) 192.168.1.2. IP VLAN1 diberikan di setiap titik dimana VLAN database baru ditambahkan. Setiap port pada sebuah switch adalah merupakan bagian dari VLAN1 sebagai acuan.



- Gambar3.0.6 Alokasi IP

3.4.4 VLAN database

VLAN database merupakan komponen penting dari suatu jaringan VLAN. Database ini berisi semua nama- nama VLAN yang akan dibuat pada jaringan. Adapun konfigurasi untuk menambah VLAN database adalah dengan menggunakan perintah yang diletakkan pada *switch* seperti dituliskan sebagai berikut :

```
Switch(vlan)#vlan 2 name vicon
VLAN 2 added:
Name: vicon
Switch(vlan)#vlan 3 name ipvpn
VLAN 3 added:
Name: ipvpn
Switch(vlan)#vlan 4 name internet
VLAN 4 added:
Name: internet
Switch(vlan)#vlan 5 name iptelepon
VLAN 5 added:
Name: iptelepon
Switch(vlan)#exit
APPLY completed.
Exiting....
```

Dari konfigurasi di atas maka didapatlah 4 buah VLAN database masing- masing bernama vicon, ipvpn, internet dan iptelepon.

3.4.5 Konfigurasi VLAN dengan IOS (Internetwork Operating System) Command

IOS adalah *operating system* yang berjalan pada sebuah peralatan cisco. Masing- masing switch ataupun router dapat dikonfigurasi menggunakan beberapa instruksi yang dimengerti oleh mesin- mesin tersebut. Dengan instruksi ini, diharapkan alat tersebut dapat berjalan sesuai

dengan apa yang diinginkan oleh *administrator* jaringan. Adapun konfigurasi yang dibuat untuk menjalankan VLAN pada sebuah jaringan adalah sebagai berikut :

```
Switch#
Switch#en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-if)#int f0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#int f0/7
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 4
Switch(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
Switch#
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int f0/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
Switch#
```

konfigurasi di atas merupakan konfigurasi agar *interface Fast Ethernet* 0/5 akan dibuat menjadi hubungan access untuk berhubungan hanya pada VLAN 2 yang bernama vicon. Begitu juga dengan port Fast Ethernet 0/7 akan dibuat terlebih dahulu menjadi hubungan *access* dan hanya diizinkan untuk berhubungan dengan VLAN 4 yang bernama *internet*. Selain itu, antarmuka *fast Ethernet* 0/2 akan berhubungan dengan *switch* lain yang ada di sebelahnya dan diberikan hubungan *trunk*.

3.5 Desain Jaringan EIGRP

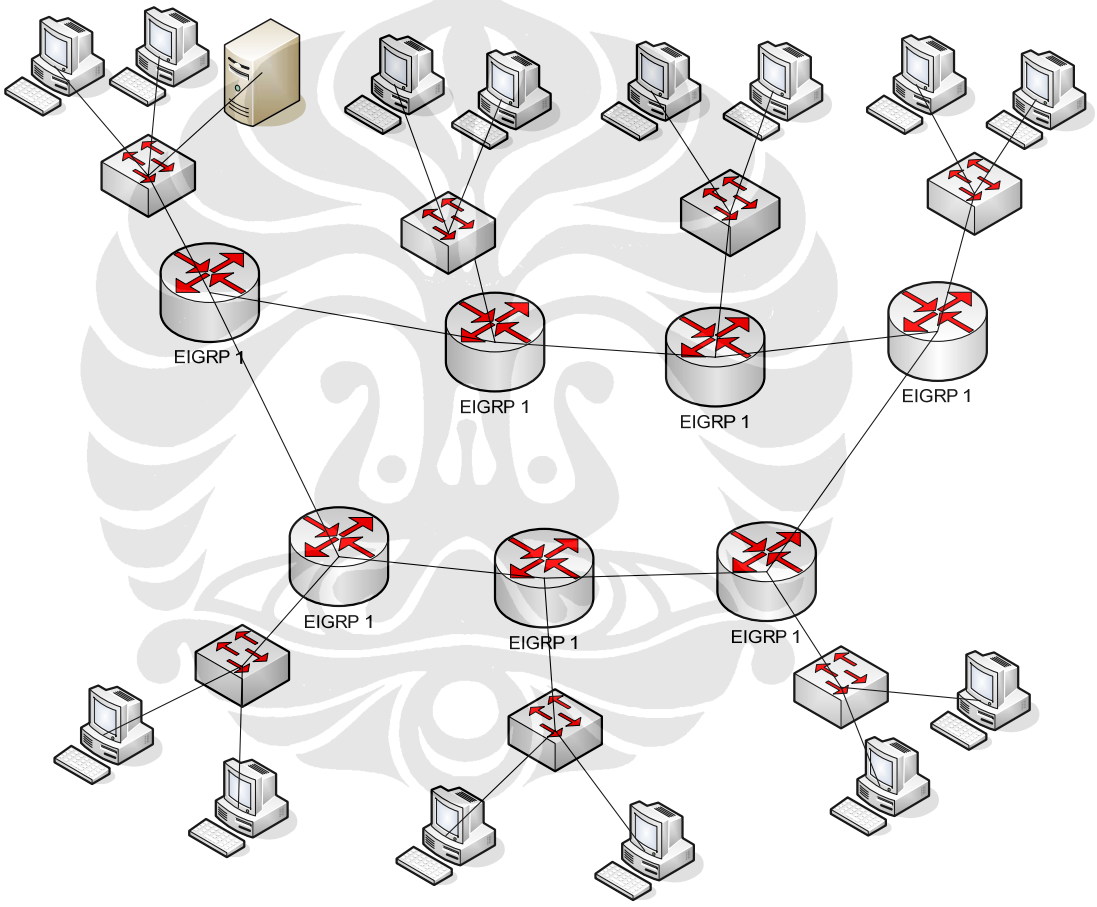
Untuk membuat suatu jaringan EIGRP, maka diperlukan:

- Desain jaringan logika
- Desain Jaringan fisik
- Desain kebutuhan IP (*Internet Protocol*)

- Pembuatan tabel *routing*
- IOS command untuk konfigurasi EIGRP

3.5.1 Desain Jaringan Logika

Untuk membangun jaringan berdasarkan layer 3 atau dinamakan juga L3VPN, maka jaringan *backbone* yang ada diberi protokol EIGRP (*Enhanced Internal Gateway Border Protocol*). Adapun jaringan *backbone* tersebut akan dibangun seperti gambar di bawah.



Gambar 3.0.7 Jaringan Logika EIGRP

Pada Gambar 3.6 di atas dapat dilihat bahwa semua *router* dapat disusun dengan topologi ring dan masing- masing *router* diberikan tulisan EIGRP 1. Angka satu tersebut merupakan nomor *auotonomous system.* Semua dibuat menjadi satu untuk menandakan bahwa semua *router*

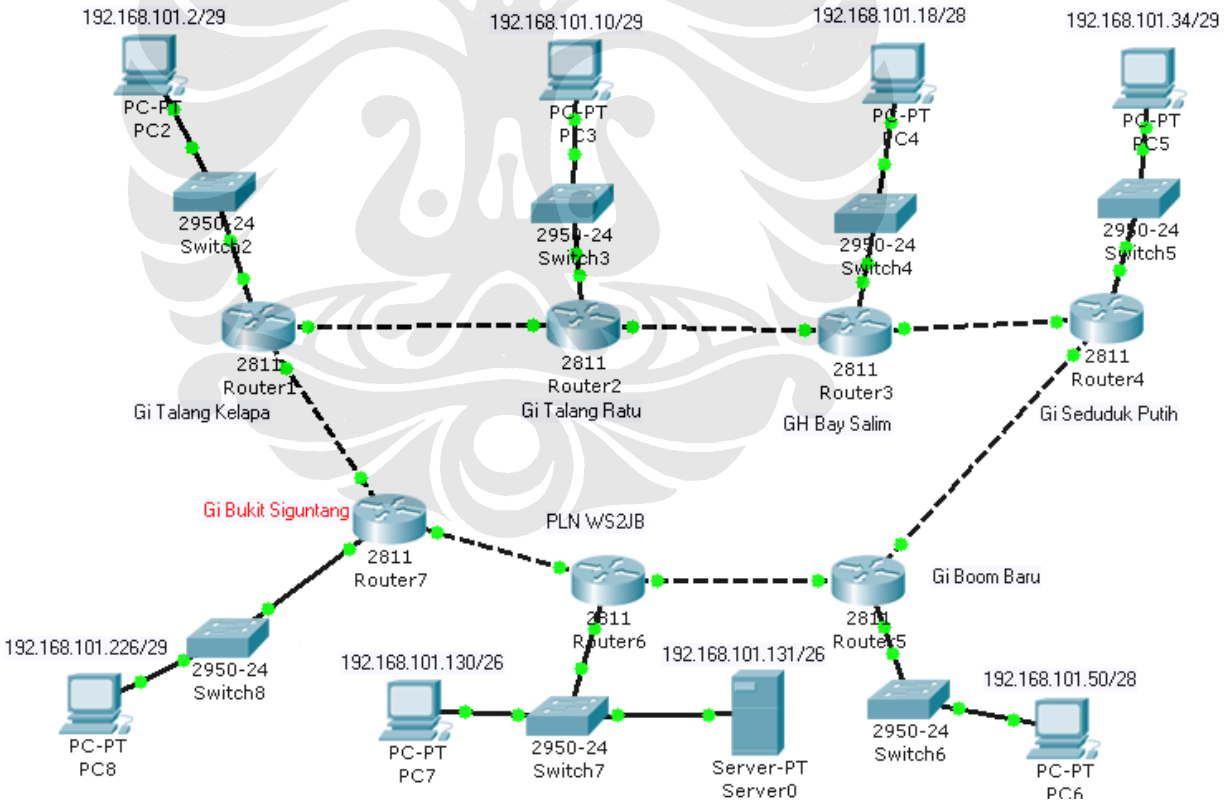
tersebut berada pada *autonomous system number* yang sama. Sebenarnya *autonomous system number* tersebut merupakan nomor pengenal yang unik untuk setiap jaringan yang ada. Pada kasus ini semua router tersebut diberikan nomor yang sama untuk memudahkan komunikasi antar *router*. Memudahkan disini adalah membuat jaringan tersebut dapat dengan cepat memperbaharui tabel *routing* di masing- masing tempat mereka sendiri.

3.5.2 Desain Jaringan Fisik

Untuk membuat jaringan infrastruktur EIGRP, maka dibutuhkan peralatan seperti yang tertera di bawah ini.

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

Adapun gambar dari jaringan fisik untuk jaringan ini dapat dilihat pada gambar di bawah.



- Gambar 3.0.8 Jaringan Fisik EIGRP

Gambar 3.7 di atas menunjukkan jaringan fisik yang dibangun berdasarkan jaringan logika yang ditunjukkan oleh Gambar 3.8. Jaringan mempunyai topologi ring yang artinya ketujuh *router* tersebut dihubungkan satu sama lain tanpa harus berhubungan secara *full mesh.* Walaupun secara logika komputer pada masing- masing tempat secara logika berhubungan secara *full mesh.*

Dapat dilihat pada gambar di atas bahwa untuk menghubungkan router dengan *router* digunakan sebuah kabel serial, sedangkan hubungan antara pengguna dengan *router* dihubungkan dengan sebuah *switch.* Dapat dilihat pula pada gambar di atas bahwa jika *router* dihubungkan dengan *switch,* maka dihubungkan dengan kabel *straight through,* begitu pula dengan hubungan antara pengguna (komputer) dengan *switch.*

3.5.3 Alokasi IP pada *Router* dan Pengguna

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

- Tabel 3.2 Alokasi IP pada Jaringan yang mempunyai protokol routing EIGRP

Nama router	Fast Ethernet 1/1	Fast Ethernet1/0	Fast Ethernet 0/0
Router1	10.100.101.1	10.100.101.50	192.168.101.1/29
Router2	10.100.101.9	10.100.101.2	192.168.101.9/29
Router3	10.100.101.17	10.100.101.10	192.168.101.17/28
Router 4	0.100.101.18	10.100.101.25	192.168.101.33/29
Router 5	10.100.101.33	10.100.101.26	192.168.101.49/28
Router 6	10.100.101.34	10.100.101.41	192.168.101,129/26
Router 7	10.100.101.42	10.100.101.49	192.168.101.225/29

Alokasi IP pad a pengguna menggunakan subnet mask yang sama dengan yang ada pada *port Fast Ethernet* pada setiap router. Untuk setiap pengguna pada setiap wilayah, alokasi IP dapat dilihat pada tabel di bawah ini.

Tabel 4.3 Alokasi IP pada Pengguna

Nama Pengguna	IP
PC2	192.168.101.2/29
PC3	192.168.101.10/29
PC4	192.168.101.18/28
PC5	192.168.101.34/29
PC6	192.168.101.50/28
PC7	192.168.101,130/26
PC8	192.168.101.226/29
Server0	192.168.101.131/26

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

3.5.4 Tabel Routing

Seperti dijelaskan pada BAB II, tabel routing merupakan komponen yang terpenting dari EIGRP. Masing- masing router memiliki tabel routing sendiri. Contoh tabel routing dapat dilihat pada gambar di bawah. Tabel routing ini diambil dari salah satu router yang dibangun di suatu wilayah.

Type	Network	Port	Next Hop IP	Metric
C	10.100.101.0/29	Serial0/0/0	---	0/0
C	10.100.101.48/29	Serial0/0/1	---	0/0
C	192.168.101.0/29	FastEthernet0/0	---	0/0
D	10.100.101.16/29	Serial0/0/0	10.100.101.2	90/3193856
D	10.100.101.24/29	Serial0/0/0	10.100.101.2	90/3705856
D	10.100.101.32/29	Serial0/0/1	10.100.101.49	90/3193856
D	10.100.101.40/29	Serial0/0/1	10.100.101.49	90/2681856
D	10.100.101.8/29	Serial0/0/0	10.100.101.2	90/2681856
D	192.168.101.128/26	Serial0/0/1	10.100.101.49	90/2684416
D	192.168.101.16/28	Serial0/0/0	10.100.101.2	90/2684416
D	192.168.101.224/29	Serial0/0/1	10.100.101.49	90/2172416
D	192.168.101.32/29	Serial0/0/0	10.100.101.2	90/3196416
D	192.168.101.48/28	Serial0/0/1	10.100.101.49	90/3196416
D	192.168.101.8/29	Serial0/0/0	10.100.101.2	90/2172416

- Gambar 3.0.9 Tabel *routing* pada router 1

3.5.5 Konfigurasi EIGRP dengan IOS command

Untuk membuat sebuah jaringan yang mempunyai protokol *routing* EIGRP, maka setiap *router* diberi konfigurasi sebagai berikut:

```
Router1#conf  t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#int Fa1/0
Router1(config-if)#ip add 10.100.101.1 255.255.255.248
Router1(config-if)#no shut
Router1(config)#int Fa0/1
Router1(config-if)#ip add 192.168.101.1 255.255.255.0
Router1(config-if)#no shut

interface Serial1/1
 ip address 10.100.101.50 255.255.255.248
!
router eigrp 1
```

```
 network 192.168.101.0
 network 10.0.0.0
 no auto-summary
!
ip classless
!
!
!
!
```

Dapat dilihat dari konfigurasi di atas, maka yang diberikan clock rate adalah yang memegang *clock* yaitu *port* serial 0/0/1 pada router. *Clock rate* yang diberi pada *port* tersebut adalah sebesar 64000. Pembuatan tabel routing dibuat dengan member perintah *router* eigrp 1, arti 1 pada perintah tersebut adalah memberikan nomor *autonomous system*. Pada pembangunan jaringan kali ini hanya terdapat satu buah autonomous system. Perintah network *IP* merupakan sebuah tanda bahwa setiap *port* pada *router* berisi IP dengan alamat subnet sebesar nilai IP tersebut, sebagai contoh, IP 192.168.101.0, angka 0 pada belakang IP tersebut menunjukkan bahwa *router* tidak melihat angka itu untuk *hop* (jalur tujuan) selanjutnya.

Konfigurasi EIGRP sendiri perlu diberikan pada *router* yang ada pada wilayah GI Talang Kelapa dan pada *router* yang terletak pada wilayah Gi Talang Ratu. Konfigurasi tersebut antara lain sebagai berikut :

```
router eigrp 1
 network 192.168.101.0
 network 10.0.0.0
 no auto-summary
!
```

ip classless

!

Perintah *no auto-summary* berarti *router* tidak akan memperhatikan IP lain yang berbeda dari 10.0.0.0 sampai habis / sampai 255 pengguna tetapi hanya sampai pada subnet mask yang digunakan yaitu sebesar 255.255.255.248 atau IP yang hanya mempunyai jangkauan dari 10.100.101.1 sampai dengan 10.100.101.6 saja. *Router* lain yang perlu diberi konfigurasi yang sama adalah *router* pada wilayah Gi Talang Ratu dengan tujuan agar kedua *router* yang bersebelahan tersebut dapat saling mengenal dan memperbaharui tabel *routing* yang ada. Jika *port router* tetangga dengan IP 10.100.101.0/29 diberikan, maka secara otomatis tabel *routing* akan segera diperbaharui dan router akan memberikan pesan seperti di bawah ini :

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.100.101.2 (FastEthernet1/0) is up: new adjacency

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.100.101.49 (FastEthernet1/1) is up: new adjacency

Petunjuk pada pesan di atas menunjukkan tabel *routing* yang baru pada *router* tersebut dan keterhubungannya pada *router* yang ada di sebelah kanan dan kirinya yaitu *router* pada Gi Bukit Siguntang dan Gi Talang Ratu. *Router* pada kedua jaringan ini tidak boleh mati disebabkan oleh kedua *router* inilah yang membentuk tabel *routing* pada jaringan ini. Jika salah satu dari *router* ini mati, maka jaringan tidak dapat saling berhubungan satu sama lain.

BAB IV
IMPLEMENTASI DAN PENGUJIAN LAYANAN JARINGAN

4.1 Implementasi Jaringan

Implementasi jaringan akan dilakukan menggunakan sebuah *software* yang bernama Packet Tracer yang merupakan perangkat lunak yang digunakan untuk simulasi sebuah jaringan yang akan dibangun pada 7 wilayah di daerah Palembang tersebut. Perangkat lunak ini akan digunakan juga digunakan untuk pengujian jaringan yang akan dibangun. Untuk membangun jaringan ini, maka diperlukan beberapa perangkat keras yang terdapat pada perangkat lunak packet tracer tersebut. Inti dari penelitian ini adalah membangun jaringan berdasarkan pada teknologi L2VPN yang diwakili dengan VLAN dan teknologi L3VPN yang diwakili dengan pembangunan protokol ruting dengan EIGRP. Pembangunan jaringan ini akan dibagi menjadi dua buah jaringan, yaitu:

1. Pembangunan VLAN
2. Pembangunan EIGRP

4.1.1 Kebutuhan Perangkat Keras untuk Pembangunan Jaringan VLAN dengan Packet Tracer

Pembangunan jaringan ini akan dibangun dengan menggunakan perangkat lunak Packet Tracer yang akan mensimulasikan VLAN seperti akan dibangun dengan hardware yang sesuai dengan kebutuhan pembangunan VLAN itu sendiri. Pada pembangunan VLAN ini sendiri maka dibutuhkan beberapa hardware yang akan digunakan, diantaranya adalah sebagai berikut:

1. Cisco Catalyst 2950-24, merupakan switch yang diproduksi oleh Cisco yang mempunyai spesifikasi 24 port Fast Ethernet. Alat ini mempunyai spesifikasi sebagai berikut :

Cisco WS-C2950-24 (RC32300) processor (revision C0) with 21039K bytes of memory.
Processor board ID FHK0610Z0WC
Last reset from system-reset
Running Standard Image
24 FastEthernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 000B.BE53.C109
Motherboard assembly number: 73-5781-09
Power supply part number: 34-0965-01
Motherboard serial number: FOC061004SZ
Power supply serial number: DAB0609127D
Model revision number: C0
Motherboard revision number: A0
Model number: WS-C2950-24
System serial number: FHK0610Z0WC
Configuration register is 0xF

Alat ini mempunyai spesifikasi sebagai berikut :

- Memori sebesar 21.039 Kilo bytes
- 24 port Fast Ethernet
- 32 Kbytes Memori flash

Gambar 4.1 Cisco Catalyst 2950-24

2. Komputer yang digunakan untuk pengguna pada perangkat lunak Packet Tracer. Komputer ini sendiri mempunyai spesifikasi sebagai berikut:

IP Address.....: 192.168.1.3

Subnet Mask.....: 255.255.255.0

Default Gateway.....: 0.0.0.0

Spesifikasi ini dapat dilihat pada packet tracer dengan mengetikkan perintah *ipconfig*

Selain itu, komputer ini juga mempunyai sebuah port yang dapat menghubungkannya dengan port Fast Ethernet pada switch yang digunakan di atas. Gambar port yang digunakan adalah sebagai berikut:

Gambar 4.2 Port PT-HOST-NM-1CFE

Port ini menyediakan sebuah antarmuka Fast Ethernet dan dihubungkan dengan switch menggunakan kabel UTP *straight through*. Kabel ini dapat digunakan untuk LAN yang berjarak jauh. Modul ini juga mendukung banyak fitur dan standar internetworking. Port single ini mendukung autosensing 10/100BaseTX ataupun 100BaseFX Ethernet. Mendukung juga buat pembangunan Virtual Local Area Network (VLAN).

Gambar 4.3 Komputer dengan Hubungan port Fast Ethernet

Kedua komponen tersebut akan dijalankan pada sebuah komputer dengan spesifikasi sebagai berikut:

- Prosesor : AMD Turion 64 bit X2
- Memory : DDR RAM 1 Giga Byte

4.1.2 Kebutuhan Perangkat Keras untuk Pembangunan Jaringan EIGRP dengan Packet Tracer

Pembangunan jaringan ini akan dibangun dengan menggunakan perangkat lunak Packet Tracer yang akan mensimulasikan VLAN seperti akan dibangun dengan hardware yang sesuai dengan kebutuhan pembangunan VLAN itu sendiri. Pada pembangunan VLAN ini sendiri maka dibutuhkan beberapa hardware yang akan digunakan, diantaranya adalah sebagai berikut:

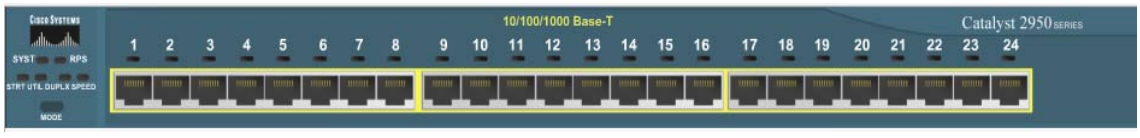
1. Cisco Catalyst 2950-24, merupakan switch yang diproduksi oleh Cisco yang mempunyai spesifikasi 24 port Fast Ethernet. Alat ini mempunyai spesifikasi sebagai berikut :

```
Cisco WS-C2950-24 (RC32300) processor (revision C0) with 21039K bytes of memory.
Processor board ID FHK0610Z0WC
Last reset from system-reset
Running Standard Image
24 FastEthernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 000B.BE53.C109
Motherboard assembly number: 73-5781-09
Power supply part number: 34-0965-01
Motherboard serial number: FOC061004SZ
Power supply serial number: DAB0609127D
Model revision number: C0
Motherboard revision number: A0
Model number: WS-C2950-24
System serial number: FHK0610Z0WC
Configuration register is 0xF
```

Alat ini mempunyai spesifikasi sebagai berikut :

- Memori sebesar 21.039 Kilo bytes
- 24 port Fast Ethernet
- 32 Kbytes Memori flash



Gambar 4.4 Cisco Catalyst 2950-24 [*Packet Tracer 4.11*]

2. Komputer yang digunakan untuk pengguna pada perangkat lunak Packet Tracer. Salah satu komputer ini sendiri mempunyai spesifikasi sebagai berikut:

   IP Address.....: 192.168.101.2

   Subnet Mask.....: 255.255.255.248

   Default Gateway.....: 192.168.101.1

   Spesifikasi ini dapat dilihat pada packet tracer dengan mengetikkan perintah *ipconfig*

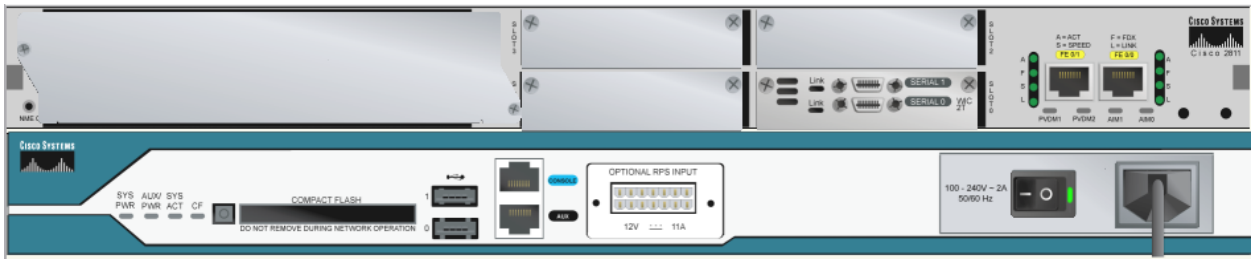
   Selain itu, komputer ini juga mempunyai sebuah port yang dapat menghubungkannya dengan port Fast Ethernet pada switch yang digunakan di atas. Gambar port yang digunakan adalah sebagai berikut:

Gambar 4.5 Port PT-HOST-NM-1CFE [*Packet Tracer 4.11*]

Port ini menyediakan sebuah antarmuka *Fast Ethernet* dan dihubungkan dengan *switch* menggunakan kabel *straight through*. Kabel ini dapat digunakan untuk LAN yang berjarak jauh. Modul ini juga mendukung banyak fitur dan standar internetworking. Port single ini mendukung autosensing 10/100BaseTX ataupun 100BaseFX *Ethernet*. Mendukung juga buat pembangunan *Virtual Local Area Network* (VLAN).

Gambar 4.6 Komputer dengan Hubungan *port Fast Ethernet* [*Packet Tracer 4.11*]

3. *Router* 2811 merupakan *router* yang dikeluarkan oleh cisco, *router* ini mempunyai spesifikasi 4 buah slot kecil dan sebiah slot yang besar untuk dapat diisi dengan beberapa modul yang juga disediakan oleh cisco. *Router* yang digunakan pada penelitian ini menggunakan modul WIC-2T yang mempunyai 2 buah *port serial* dan 2 buah *port fast ethernet*



Gambar 4.7 Router 2811 [*Packet Tracer 4.11*]

Ketiga komponen tersebut akan dijalankan pada sebuah komputer dengan spesifikasi sebagai berikut:

- Prosesor : AMD Turion 64 bit X2
- Memori : DDR RAM 1 Giga Byte

4.2 Pengujian Jaringan VLAN pada Packet Tracer

Jaringan yang telah dibangun dengan langkah-langkah tersebut yang telah dijelaskan sebelumnya, akan diuji dengan beberapa pengujian. Untuk menguji suatu jaringan, maka diperlukan beberapa IOS command. IOS command yang mendukung untuk pengujian jaringan VLAN ini antara lain:

- sho vlan brief
- ping antar pengguna
- tracert antar pengguna
- akses internet pada server0

4.2.1 Perintah sho vlan brief

Perintah sho vlan brief pada 7 buah switch akan menghasilkan data sebagai berikut:

a. switch 1 :

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24
2    vicon                             active    Fa0/5
4    internet                          active    Fa0/1, Fa0/7
1002 fddi-default                      active
```

1003 token-ring-default active

1004 fddinet-default active

1005 trnet-default active

b. switch 2 :

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/5, Fa0/6, Fa0/8
			Fa0/9, Fa0/10, Fa0/11, Fa0/12
			Fa0/13, Fa0/14, Fa0/15, Fa0/16
			Fa0/17, Fa0/18, Fa0/19, Fa0/20
			Fa0/21, Fa0/22, Fa0/23, Fa0/24
2	vicon	active	Fa0/3
4	internet	active	Fa0/7
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

c. switch 3 :

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/8, Fa0/9
			Fa0/10, Fa0/11, Fa0/12, Fa0/13
			Fa0/14, Fa0/15, Fa0/16, Fa0/17
			Fa0/18, Fa0/19, Fa0/20, Fa0/21
			Fa0/22, Fa0/23, Fa0/24
2	vicon	active	Fa0/4
4	internet	active	Fa0/1, Fa0/7
1002	fddi-default	active	

1003 token-ring-default active

1004 fddinet-default active

1005 trnet-default active

d. switch 4 :

VLAN	Name	Status	Ports
1	default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7
			Fa0/9, Fa0/10, Fa0/11, Fa0/12
			Fa0/13, Fa0/14, Fa0/15, Fa0/16
			Fa0/17, Fa0/18, Fa0/19, Fa0/20
			Fa0/21, Fa0/22, Fa0/23, Fa0/24
3	ipvpn	active	Fa0/3
5	iptelepon	active	Fa0/8
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

e. switch 5 :

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/9
			Fa0/10, Fa0/11, Fa0/12, Fa0/13
			Fa0/14, Fa0/15, Fa0/16, Fa0/17
			Fa0/18, Fa0/19, Fa0/20, Fa0/21
			Fa0/22, Fa0/23, Fa0/24
3	ipvpn	active	Fa0/1
4	internet	active	Fa0/4
5	iptelepon	active	Fa0/8

1002 fddi-default active

1003 token-ring-default active

1004 fddinet-default active

1005 trnet-default active

f. switch 6 :

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/6, Fa0/7 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
3	ipvpn	active	Fa0/1
5	iptelepon	active	Fa0/8
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

g. switch 7 :

VLAN	Name	Status	Ports
1	default	active	Fa0/4, Fa0/6, Fa0/7, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24
3	ipvpn	active	Fa0/1
4	internet	active	Fa0/2

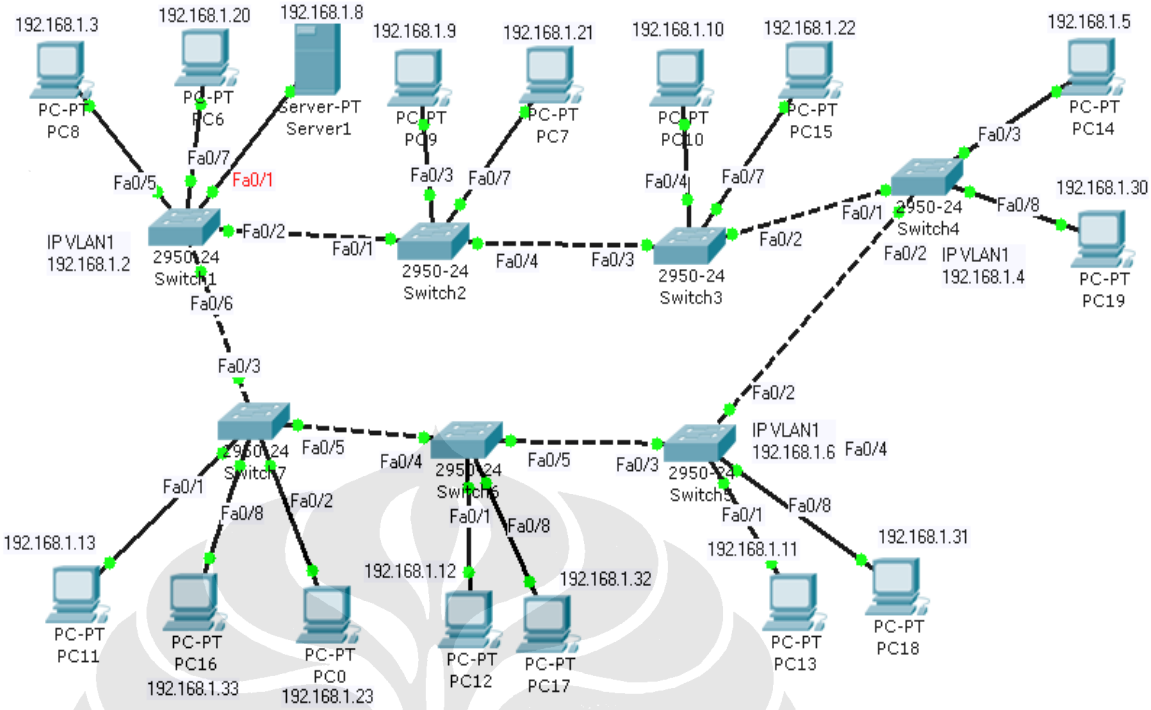
5 iptelepon active Fa0/8
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

Dari perintah sho vlan brief tersebut dapat dilihat bahwa setiap switch memiliki vlan database sendiri yang tersimpan pada memori switch tersebut. Database vlan inilah yang akan menentukan port mana saja yang dapat berhubungan dengan vlan itu sendiri. Sebagai contoh untuk switch 7, terdapat vlan 5 yang bernama iptelepon pada port FastEthernet 0/8, maka port ini hanya bisa berhubungan dengan port lain pada switch yang lain pula dengan nama vlan yang sama seperti pada port Fa0/8 pada switch 6. Selain dari port yang tidak diberi nama vlan yang sama, maka pengguna tidak dapat saling berhubungan.

Simulasi ini hanya melibatkan 2 pengguna pada setiap titik, setiap titik ini diwakili oleh satu buah switch. Alokasi IP untuk setiap VLAN database adalah sebagai berikut:

- VLAN 2 : bernama vicon terdapat pada switch 1, switch 2, dan switch 3. Penggunanya mempunyai IP sebagai berikut : PC 8 : 192.168.1.3, PC 9 : 192.168.1.9, PC 10 : 192.168.1.10.
- VLAN 3 : bernama ipvpn terdapat pada switch 4, 5, 6, dan 7. Penggunanya memiliki IP sebagai berikut : PC 14, PC 13, PC 12, dan PC 11.
- VLAN 4 : bernama internet terdapat pada switch 1, 2, 3, dan 7. Penggunanya adalah sebagai berikut : PC 0, 6, 7, 15 dan Server1.
- VLAN 5 : bernama iptelepon terdapat pada switch 4, 5 ,6 , dan 7. Penggunanya adalah sebagai berikut : PC 16, 17, 18, dan 19

  Alokasi IP pada setiap pengguna dapat dilihat pada gambar di bawah ini:



Gambar 4.8 Alokasi IP pada setiap pengguna

4.2.2 Perintah Ping antar Pengguna

Perintah ping merupakan perintah untuk menguji keterhubungan antar pengguna yang dalam simulasi kali ini dinamakan PC. Setiap PC pada VLAN yang sama dapat saling mengirim paket ping, sedangkan PC yang tidak terdapat dalam VLAN yang sama tidak dapat terhubug sama sekali atau mendapatkan perintah ping yang gagal.

Contoh perintah ping yang berhasil pada simulasi kali ini adalah perintah ping dari PC 8 ke PC 9 dan PC 10. Jika perintah ping dituliskan pada PC 8 menuju PC 9 dan 10 akan menghasilkan data sebagai berikut :

- Ping dari PC 8 ke PC 9 :

  PC>ping 192.168.1.9

  Pinging 192.168.1.9 with 32 bytes of data:

Reply from 192.168.1.9: bytes=32 time=205ms TTL=128
Reply from 192.168.1.9: bytes=32 time=107ms TTL=128
Reply from 192.168.1.9: bytes=32 time=100ms TTL=128
Reply from 192.168.1.9: bytes=32 time=108ms TTL=128

Ping statistics for 192.168.1.9:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 100ms, Maximum = 205ms, Average = 130ms

- Ping dari PC 8 ke PC 10 :

PC>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=220ms TTL=128
Reply from 192.168.1.10: bytes=32 time=143ms TTL=128
Reply from 192.168.1.10: bytes=32 time=146ms TTL=128
Reply from 192.168.1.10: bytes=32 time=136ms TTL=128

Ping statistics for 192.168.1.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 136ms, Maximum = 220ms, Average = 161ms

- ping dari PC 10 ke PC 9 :

PC>ping 192.168.1.9

Pinging 192.168.1.9 with 32 bytes of data:

Reply from 192.168.1.9: bytes=32 time=199ms TTL=128

Reply from 192.168.1.9: bytes=32 time=122ms TTL=128

Reply from 192.168.1.9: bytes=32 time=171ms TTL=128

Reply from 192.168.1.9: bytes=32 time=140ms TTL=128

Ping statistics for 192.168.1.9:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 122ms, Maximum = 199ms, Average = 158ms

Ketiga PC di atas terdapat dalam satu VLAN yang sama yaitu VLAN 2 yang bernama vicon. Kesimpulan yang bisa diambil dari pengujian ping ini adalah bahwa jika salah satu host ingin berhubungan dengan host yang lain, maka kedua host tersebut harus berada pada vlan database yang sama seperti harus dalam VLAN 2. Jika yang diakses merupakan PC dengan VLAN yang berbeda, maka pengujian dengan ping ini gagal, ini menunjukkan keterbatasan akses pada setiap layanan yang ada, PC dengan VLAN vicon hanya bisa mengakses PC yang masuk dalam database VLAN vicon saja. Begitu pula dengan PC yang masuk dalam VLAN iptelepon hanya bisa mengakses PC yang terhubung dalam VLAN iptelepon saja. Di bawah ini diperlihatkan contoh ping yang gagal dari PC 8 ke PC 6 yang terhubung dengan VLAN 4 yang bernama internet:

PC>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

Request timed out.

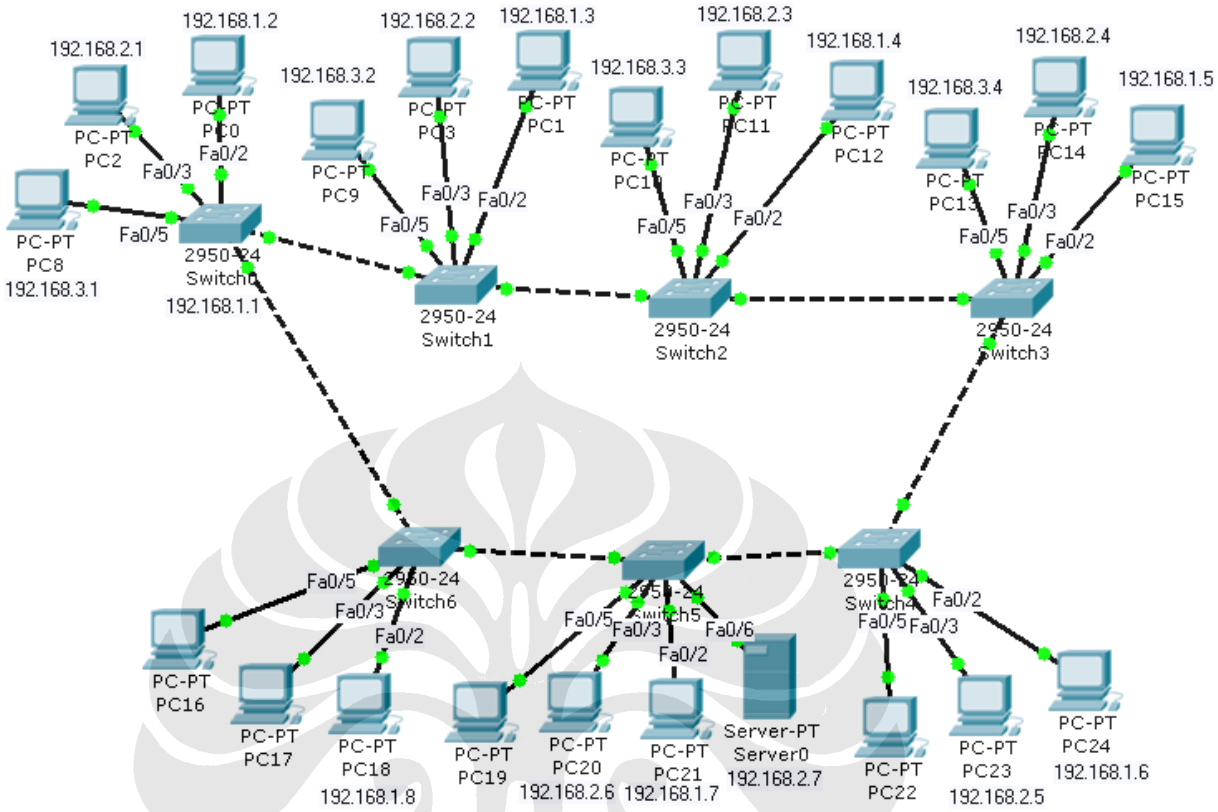
Request timed out.

Request timed out.

Request timed out.

Ping statistics for 192.168.1.20:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),



Gambar 4.9 Alokasi IP yang berbeda untuk setiap VLAN

Gambar 4.9 di atas menunjukkan konfigurasi baru dari VLAN dengan pengalokasian IP yang berbeda untuk setiap VLAN. Tabel 4.1 di bawah ini akan menunjukkan alokasi IP yang baru untuk setiap VLAN.

Tabel 4.1 Alokasi IP VLAN

VLAN *database*	Alokasi IP
VLAN 2/ IPVPN	192.168.1.2 s/d 192.168.1.255 atau 192.168.1.0/24
VLAN 3/INTERNET	192.168.2.1 s/d 192.168.2.255 Atau 192.168.2.0/24
VLAN 4/IPTELEPON	192..168.3.1 s/d 192.168.3.255 Atau 192.168.3.0/24

Tabel 4.1 menunjukkan bahwa satu buah jaringan VLAN dapat mengandung banyak *database* VLAN dan masing-masing VLAN dapat mengandung *subnet* IP yang berbeda untuk lebih mudah dikenali

serta memudahkan untuk pengembangan jaringan di masa depan. Hal ini dikarenakan masih banyaknya IP yang tersedia untuk ditambahkan. Untuk menunjukkan untjuk kerja dari VLAN ini, maka data yang diambil adalah data ping. Data yang diambil berasala dari ping pada VLAN 2 yang bernama ipvpn. Berikut ini merupakan hasil data ping yang diambil dari PC0.

- ping dari PC0 (192.168.1.2) ke PC 1(192.168.1.3) :
  PC>ping 192.168.1.3

  Pinging 192.168.1.3 with 32 bytes of data:

  Reply from 192.168.1.3: bytes=32 time=191ms TTL=128
  Reply from 192.168.1.3: bytes=32 time=170ms TTL=128
  Reply from 192.168.1.3: bytes=32 time=77ms TTL=128
  Reply from 192.168.1.3: bytes=32 time=123ms TTL=128

  Ping statistics for 192.168.1.3:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
  Minimum = 77ms, Maximum = 191ms, Average = 140ms
  kecepatan rata- rata = 32 bytes / 140 ms = **228,57 bps**

- ping dari PC0 (192.168.1.2) ke PC 12(192.168.1.4) :

  PC>ping 192.168.1.4

  Pinging 192.168.1.4 with 32 bytes of data:

  Reply from 192.168.1.4: bytes=32 time=152ms TTL=128
  Reply from 192.168.1.4: bytes=32 time=195ms TTL=128
  Reply from 192.168.1.4: bytes=32 time=176ms TTL=128
  Reply from 192.168.1.4: bytes=32 time=170ms TTL=128

  Ping statistics for 192.168.1.4:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
  Minimum = 152ms, Maximum = 195ms, Average = 173ms
  Kecepatan rata- rata = 32 bytes / 173 ms = **184,97 bps**

- ping dari PC0 (192.168.1.2) ke PC 15(192.168.1.5) :

  PC>ping 192.168.1.5

  Pinging 192.168.1.5 with 32 bytes of data:

  Reply from 192.168.1.5: bytes=32 time=379ms TTL=128
  Reply from 192.168.1.5: bytes=32 time=259ms TTL=128
  Reply from 192.168.1.5: bytes=32 time=236ms TTL=128
  Reply from 192.168.1.5: bytes=32 time=272ms TTL=128

  Ping statistics for 192.168.1.5:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
  Minimum = 236ms, Maximum = 379ms, Average = 286ms
  kecepatan rata- rata = 32 bytes / 286 ms = **111,888 bps**

- ping dari PC0 (192.168.1.2) ke PC 24(192.168.1.6) :

  PC>ping 192.168.1.6

  Pinging 192.168.1.6 with 32 bytes of data:

  Reply from 192.168.1.6: bytes=32 time=320ms TTL=128
  Reply from 192.168.1.6: bytes=32 time=156ms TTL=128
  Reply from 192.168.1.6: bytes=32 time=193ms TTL=128
  Reply from 192.168.1.6: bytes=32 time=203ms TTL=128

  Ping statistics for 192.168.1.6:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
  Minimum = 156ms, Maximum = 320ms, Average = 218ms
  kecepatan rata- rata = 32 bytes / 218 ms = **146,789 bps**

- ping dari PC0 (192.168.1.2) ke PC 21(192.168.1.7) :

  PC>ping 192.168.1.7

Pinging 192.168.1.7 with 32 bytes of data:

Reply from 192.168.1.7: bytes=32 time=242ms TTL=128
Reply from 192.168.1.7: bytes=32 time=120ms TTL=128
Reply from 192.168.1.7: bytes=32 time=116ms TTL=128
Reply from 192.168.1.7: bytes=32 time=212ms TTL=128

Ping statistics for 192.168.1.7:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 116ms, Maximum = 242ms, Average = 172ms
kecepatan rata- rata = 32 bytes / 172 ms = **186,0465 bps**

- ping dari PC 0 (192.168.1.2) ke PC 24 (192.168.1.6)

PC>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time=291ms TTL=128
Reply from 192.168.1.6: bytes=32 time=208ms TTL=128
Reply from 192.168.1.6: bytes=32 time=190ms TTL=128
Reply from 192.168.1.6: bytes=32 time=230ms TTL=128

Ping statistics for 192.168.1.6:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 190ms, Maximum = 291ms, Average = 229ms
kecepatan rata- rata = 32 bytes / 229 ms = **139,73 bps**

- ping dari PC0 (192.168.1.2) ke PC 18(192.168.1.8) :
PC>ping 192.168.1.8

Pinging 192.168.1.8 with 32 bytes of data:

Reply from 192.168.1.8: bytes=32 time=122ms TTL=128
Reply from 192.168.1.8: bytes=32 time=75ms TTL=128
Reply from 192.168.1.8: bytes=32 time=114ms TTL=128
Reply from 192.168.1.8: bytes=32 time=140ms TTL=128

Ping statistics for 192.168.1.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 75ms, Maximum = 140ms, Average = 112ms
Kecepatan rata- rata = 32 bytes / 112 ms = **285, 71 bps**

Selain unjuk kerja jaringan untuk mendapatkan kecepatan akses antar komputer pada VLAN, pengujian dengan menggunakan perintah ping juga membuktikan berhasil tidaknya sebuah konfigurasi VLAN itu sendiri. Tabel 4.2 di bawah ini menunjukkan hasil pengujian ping antar komputer yang ada pada jaringan.

Tabel 4.2 Ping dari VLAN 2 KE VLAN 2

	VLAN 2						
VLAN 2	PC0	PC1	PC12	PC15	PC24	PC21	PC18
PC0	V	V	V	V	V	V	V
PC1	V	V	V	V	V	V	V
PC12	V	V	V	V	V	V	V
PC15	V	V	V	V	V	V	V
PC24	V	V	V	V	V	V	V
PC21	V	V	V	V	V	V	V
PC18	V	V	V	V	V	V	V

Tabel 4.3 Ping dari VLAN 2 ke VLAN 3

	VLAN 3					
VLAN 2	PC2	PC3	PC11	PC14	PC23	PC20
PC0	X	X	X	X	X	X
PC1	X	X	X	X	X	X
PC12	X	X	X	X	X	X
PC15	X	X	X	X	X	X
PC24	X	X	X	X	X	X
PC21	X	X	X	X	X	X
PC18	X	X	X	X	X	X

4.2.3 Perintah traceroute antar Pengguna

PC>tracert 192.168.1.3
Tracing route to 192.168.1.3 over a maximum of 30 hops:
 1 *   117 ms   115 ms   192.168.1.3

Trace complete.

PC>tracert 192.168.1.4
Tracing route to 192.168.1.4 over a maximum of 30 hops:
 1 307 ms   277 ms   269 ms   192.168.1.4

Trace complete.

PC>tracert 192.168.1.5
Tracing route to 192.168.1.5 over a maximum of 30 hops:
 1 171 ms   188 ms   199 ms   192.168.1.5

Trace complete.

PC>tracert 192.168.1.6
Tracing route to 192.168.1.6 over a maximum of 30 hops:
 1 98 ms   194 ms   211 ms   192.168.1.6

Trace complete.

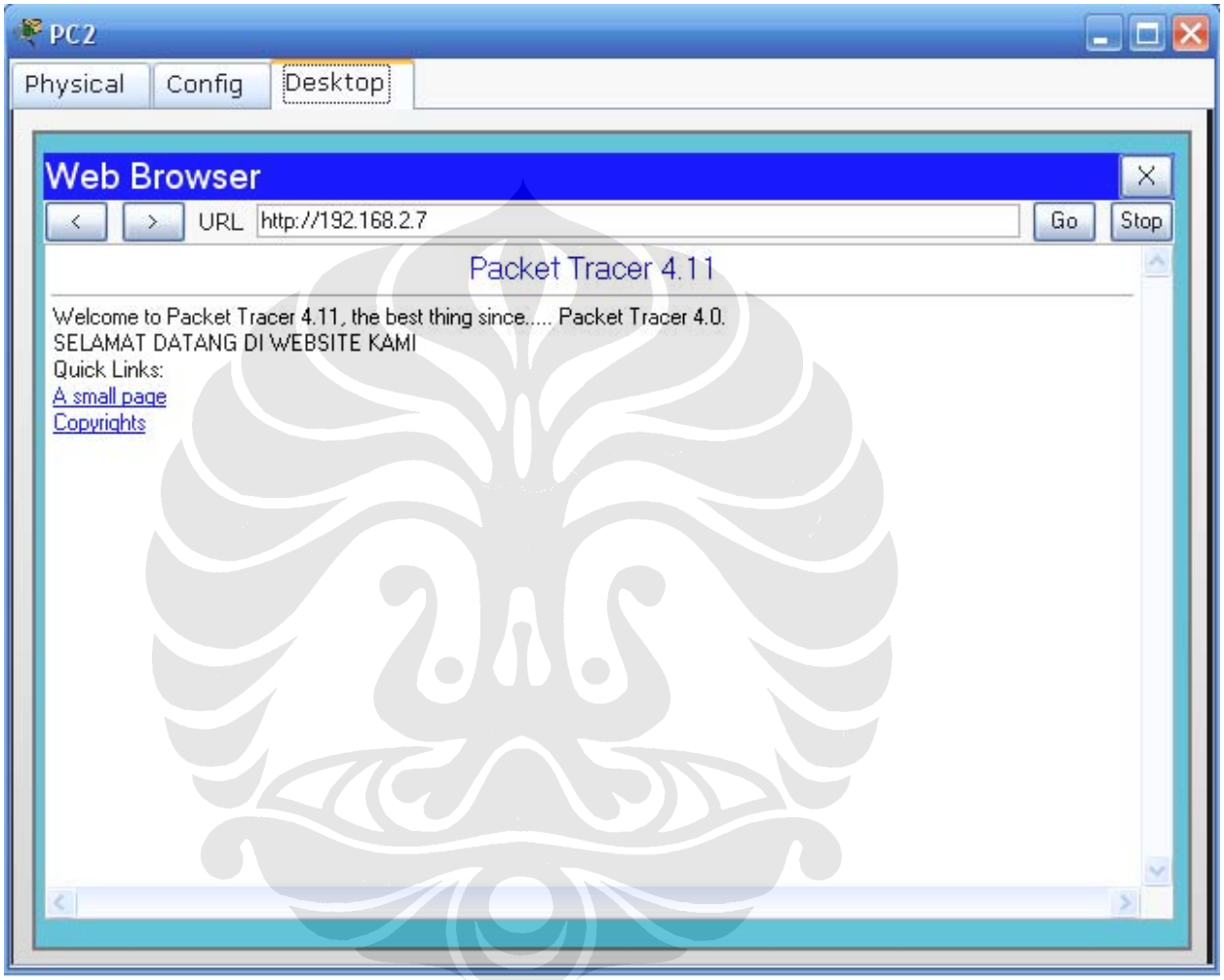
PC>tracert 192.168.1.7
Tracing route to 192.168.1.7 over a maximum of 30 hops:
 1 114 ms   155 ms   134 ms   192.168.1.7

Trace complete

4.2.4 Pengujian Internet

Pengujian kali ini akan mensimulasikan akses internet dari vlan 4 yang bernama internet. Pengguna yang terdapat pada VLAN 3 yang bernama internet akan dicoba untuk mengakses *server website* yang ada pada server0 yang terdapat pada daerah PLN WS2JB. Jika berhasil

maka tampilan dari hasil pengaksesan HTTP pada alamat IP 192.168.2.7 akan terlihat seperti gambar 4.6 di bawah ini. Gambar 4.6 memperlihatkan hasil dari pengaksesan dari PC 2 yang terdapat pada daerah GI TALANG RATU menuju *server web* yang ada di server0 pada PLN WS2JB.



Gambar 4.10 Akses Internet dari PC2 ke Server0

Karena ini merupakan jaringan VLAN, maka semua PC dengan IP 192.168.2.0/24 dapat mengakses website tersebut dan menunjukkan hasil yang sama. tetapi PC lain yang terdapat pada VLAN *database* yang berbeda tidak dapat mengaksesnya.

4.3 Pengujian Jaringan EIGRP pada Packet Tracer

Jaringan yang telah dibangun dengan langkah-langkah tersebut yang telah dijelaskan sebelumnya, akan diuji dengan beberapa pengujian. Untuk menguji suatu jaringan, maka

diperlukan beberapa IOS command. IOS command yang mendukung untuk pengujian jaringan EIGRP ini antara lain:

- ping antar pengguna
- tracert antar pengguna
- akses internet pada server0

4.3.1 Perintah ping antar Pengguna

Seperti yang dilakukan pada pengujian VLAN, maka pengujian protokol *routing* ini diuji juga dengan sebuah pengujian ping. Pengujian ini bertujuan untuk mencari kecepatan dari pengiriman pesan ping dari pengguna pada suatu wilayah menuju wilayah lainnya. Cara mencari kecepatan rata- rata transfer dari suatu jaringan dapat dicari dengan membagi antara besar data yang ada dengan waktu rata- rata yang didapat pada pengujian ping ini. Hasil pengujian ping dapat dilihat pada daftar ping di bawah ini.

- Ping dari PC 2 ke PC3

  PC>ping 192.168.101.10

  Pinging 192.168.101.10 with 32 bytes of data:

  Reply from 192.168.101.10: bytes=32 time=181ms TTL=126
  Reply from 192.168.101.10: bytes=32 time=104ms TTL=126
  Reply from 192.168.101.10: bytes=32 time=78ms TTL=126
  Reply from 192.168.101.10: bytes=32 time=183ms TTL=126

  Ping statistics for 192.168.101.10:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
  Minimum = 78ms, Maximum = 183ms, Average = 136ms
  Kecepatan rata- rata = 32 bytes / 136 ms = **235,29 bps**

- Ping dari PC 2 ke PC4

  PC>ping 192.168.101.18

  Pinging 192.168.101.18 with 32 bytes of data:

  Reply from 192.168.101.18: bytes=32 time=190ms TTL=125
  Reply from 192.168.101.18: bytes=32 time=226ms TTL=125
  Reply from 192.168.101.18: bytes=32 time=221ms TTL=125
  Reply from 192.168.101.18: bytes=32 time=197ms TTL=125

  Ping statistics for 192.168.101.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 190ms, Maximum = 226ms, Average = 208ms
  Kecepatan rata- rata = 32 bytes / 208 ms = **153,846 bps**

- Ping dari PC 2 ke PC5

  PC>ping 192.168.101.34

  Pinging 192.168.101.34 with 32 bytes of data:

  Reply from 192.168.101.34: bytes=32 time=207ms TTL=124
  Reply from 192.168.101.34: bytes=32 time=233ms TTL=124
  Reply from 192.168.101.34: bytes=32 time=271ms TTL=124
  Reply from 192.168.101.34: bytes=32 time=302ms TTL=124

  Ping statistics for 192.168.101.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:

Minimum = 207ms, Maximum = 302ms, Average = 253ms
Kecepatan rata- rata = 32 bytes / 253 ms = **126,48 bps**

- Ping dari PC 2 ke PC6

PC>ping 192.168.101.50

Pinging 192.168.101.50 with 32 bytes of data:

Reply from 192.168.101.50: bytes=32 time=283ms TTL=123
Reply from 192.168.101.50: bytes=32 time=265ms TTL=123
Reply from 192.168.101.50: bytes=32 time=313ms TTL=123
Reply from 192.168.101.50: bytes=32 time=291ms TTL=123

Ping statistics for 192.168.101.50:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 265ms, Maximum = 313ms, Average = 288ms
Kecepatan rata- rata = 32 bytes / 288 ms = **111,111 bps**

- Ping dari PC 2 ke PC7

PC>ping 192.168.101.130

Pinging 192.168.101.130 with 32 bytes of data:

Reply from 192.168.101.130: bytes=32 time=336ms TTL=122
Reply from 192.168.101.130: bytes=32 time=298ms TTL=122
Reply from 192.168.101.130: bytes=32 time=344ms TTL=122
Reply from 192.168.101.130: bytes=32 time=303ms TTL=122

Ping statistics for 192.168.101.130:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 298ms, Maximum = 344ms, Average = 320ms
kecepatan rata- rata = 32 bytes / 320 ms = **100 bps**

- Ping PC 2 ke PC 8

PC>ping 192.168.101.226

Pinging 192.168.101.226 with 32 bytes of data:

Reply from 192.168.101.226: bytes=32 time=249ms TTL=126

Reply from 192.168.101.226: bytes=32 time=169ms TTL=126

Reply from 192.168.101.226: bytes=32 time=119ms TTL=126

Reply from 192.168.101.226: bytes=32 time=194ms TTL=126

Ping statistics for 192.168.101.226:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 119ms, Maximum = 249ms, Average = 182ms

Kecepatan rata- rata = 32 bytes / 182 ms = **175,824 bps**

- Ping dari PC 2 ke server0

PC>ping 192.168.101.131

Pinging 192.168.101.131 with 32 bytes of data:

Reply from 192.168.101.131: bytes=32 time=244ms TTL=122
Reply from 192.168.101.131: bytes=32 time=401ms TTL=122
Reply from 192.168.101.131: bytes=32 time=465ms TTL=122
Reply from 192.168.101.131: bytes=32 time=257ms TTL=122

Ping statistics for 192.168.101.131:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 244ms, Maximum = 465ms, Average = 341ms
Kecepatan rata- rata = 32 bytes / 341 ms = **93,84bps**

4.3.2 Perintah *tracert* antar Pengguna

Daftar di bawah ini menunjukkan data dari pengguna menggunakan perintah traceroute:

- Dari PC2 ke PC3

  PC>tracert 192.168.101.10

  Tracing route to 192.168.101.10 over a maximum of 30 hops:

  1 65 ms 110 ms 115 ms 192.168.101.1
  2 134 ms 141 ms 140 ms 10.100.101.2
  3 184 ms 198 ms 171 ms 192.168.101.10

  Trace complete.
- Dari PC2 ke PC4

  PC>tracert 192.168.101.18

  Tracing route to 192.168.101.18 over a maximum of 30 hops:

  1 60 ms 101 ms 33 ms 192.168.101.1
  2 160 ms 156 ms 71 ms 10.100.101.2
  3 131 ms 128 ms 193 ms 10.100.101.10
  4 184 ms 265 ms 265 ms 192.168.101.18

  Trace complete.
- Dari PC2 ke PC5

  PC>tracert 192.168.101.34

  Tracing route to 192.168.101.34 over a maximum of 30 hops:

  1 126 ms 80 ms 87 ms 192.168.101.1
  2 105 ms 106 ms 131 ms 10.100.101.2
  3 152 ms 182 ms 180 ms 10.100.101.10
  4 156 ms 220 ms 168 ms 10.100.101.18
  5 304 ms 185 ms 281 ms 192.168.101.34

  Trace complete.
- Dari PC2 ke PC6

PC>tracert 192.168.101.50

Tracing route to 192.168.101.50 over a maximum of 30 hops:

```
  1   77 ms     88 ms     119 ms    192.168.101.1
  2   127 ms    133 ms    89 ms     10.100.101.49
  3   *         134 ms    124 ms    10.100.101.41
  4   203 ms    173 ms    220 ms    10.100.101.33
  5   283 ms    305 ms    272 ms    192.168.101.50
```

Trace complete.

- Dari PC2 ke PC7

  PC>tracert 192.168.101.130

  Tracing route to 192.168.101.130 over a maximum of 30 hops:

```
  1   59 ms     50 ms     71 ms     192.168.101.1
  2   158 ms    138 ms    123 ms    10.100.101.49
  3   184 ms    167 ms    199 ms    10.100.101.41
  4   269 ms    242 ms    296 ms    192.168.101.130
```

  Trace complete.

- Dari PC2 ke PC8

  PC>tracert 192.168.101.226

  Tracing route to 192.168.101.226 over a maximum of 30 hops:

```
  1   92 ms     89 ms     68 ms     192.168.101.1
  2   87 ms     150 ms    150 ms    10.100.101.49
  3   212 ms    191 ms    209 ms    192.168.101.226
```

  Trace complete.

- Dari PC2 ke server0

  PC>tracert 192.168.101.131

  Tracing route to 192.168.101.131 over a maximum of 30 hops:

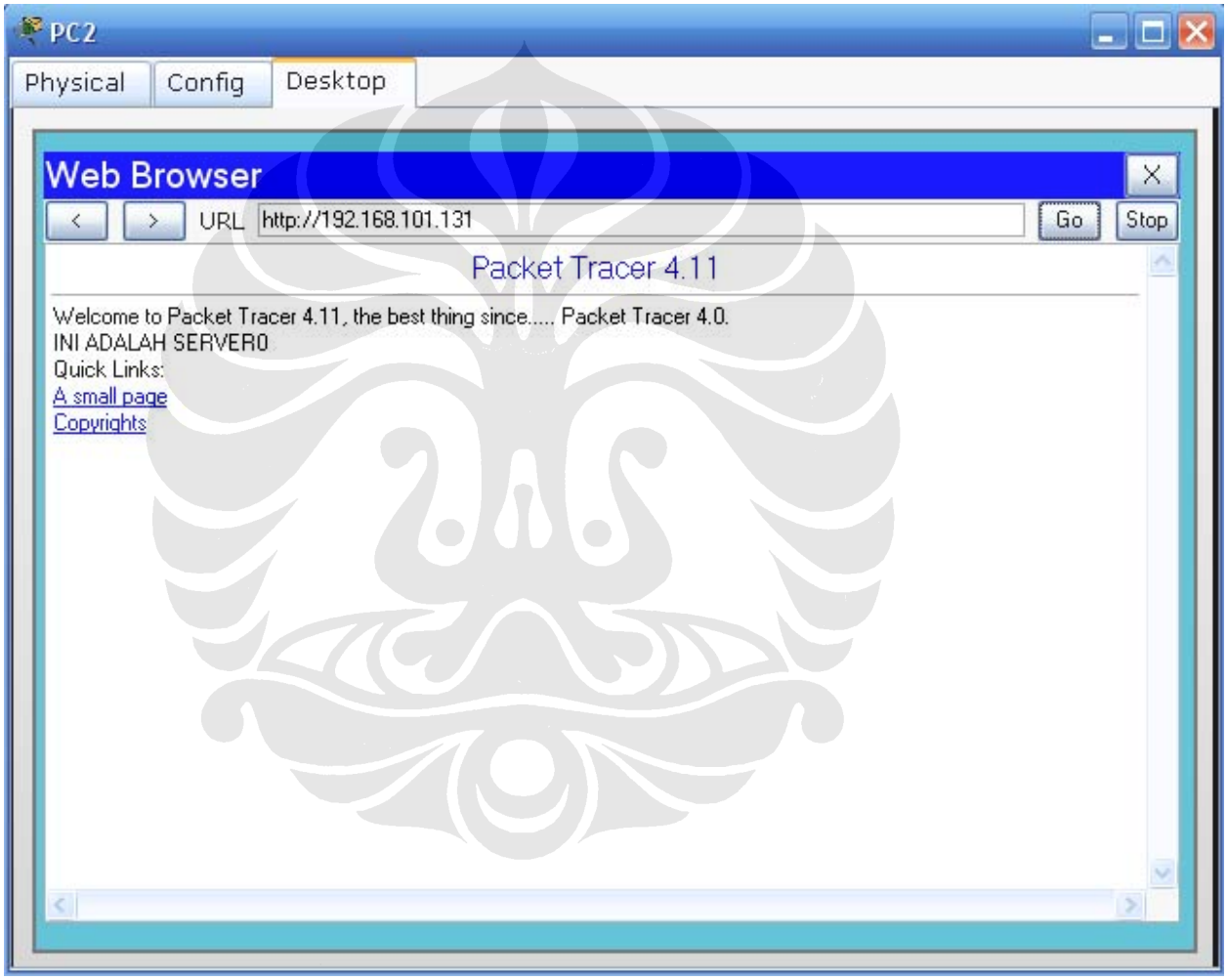
```
  1   88 ms     100 ms    90 ms     192.168.101.1
  2   124 ms    82 ms     109 ms    10.100.101.49
  3   123 ms    87 ms     165 ms    10.100.101.41
```

4 203 ms 264 ms 297 ms 192.168.101.131

Trace complete.

4.3.3 Pengujian *Internet*

Pengujian internet dilakukan dengan mengakses data pada server0 yang mempunyai IP 192.168.101.131.



Gambar 4.11 Akses Internet dari PC2 ke server0

4.4 Perbandingan Unjuk Kerja VLAN dengan EIGRP

Setelah melakukan pengujian dengan perintah ping dan tracert maka diambillah kesimpulan sebagai berikut:

Tabel 4.4 ping antar VLAN2

VLAN 2	PC0	PC1	PC12	PC15	PC24	PC21	PC18
PC0	X	**228,57 bps**	**184,97 bps bps**	**146,789 bps**	**139,73 bps**	**186,0465 bps**	**285, 71 bps**

Tabel 4.5 ping antar VLAN 3

VLAN 3	PC2	PC3	PC11	PC14	PC23	PC20	server0
PC2	X	84 ms	305 ms	279 ms	230 ms	204 ms	189 ms

Tabel 4.6 ping antar VLAN 4

VLAN 4	PC8	PC3	PC10	PC13
PC8		171 ms	188 ms	200 ms

Dari ketiga tabel di atas bahwa arah pergerakan pengiriman paket ataupun pesan antar pengguna dapat berubah sesuai dengan jarak antar pengguna. Ini dapat dilihat dari tabel kecepatan dan waktu untuk sampai pada pengguna tersebut. Semakin dekat jarak antar pengguna, maka semakin cepat pula proses transfer data ataupun paket tersebut.

Tabel 4.6 di bawah ini menunjukkan hasil ping antar pengguna pada protokol *routing* pada EIGRP :

Tabel 4.7 Hasil ping pada jaringan Protokol *routing* EIGRP

	PC3	PC4	PC5	PC6	PC7	PC8	Server0
PC2	**235,29 bps**	**153,846 bps**	**126,48 bps**	**111,111 bps**	**100,00 bps**	**175,824 bps**	**93,84 bps**

	PC2	PC3	PC4	PC5	PC6	PC7	PC8	Server 0
PC2	V	V	V	V	V	V	V	V

Dari tabel di atas dapat disimpulkan bahwa semakin dekat pengguna dengan pengguna lainnya maka semakin cepat pesan tersebut sampai. Maka dapat disimpulkan bahwa EIGRP mengambil jalan tersekat jika ingin mengirimkan pesannya.

Dari pengiriman ping antar pengguna baik pada VLAN dan EIGRP menunjukkan gejala yang sama dan juga menunjukkan kecepatan yang hampir sama besar pula. Hanya jika dilihat lebih teliti lagi, maka kecepatan yang diperoleh dari perintah ping akan lebih cepat jika digunakan switch ataupun teknologi VLAN walaupun perbedaan kecepatannya tidak begitu besar. Perbedaan yang tidak begitu signifikan ini karena alasan paket yang dikirim merupakan paket ping.

Sedangkan perintah tracert menunjukkan bahwa *router* yang dalam hal ini EIGRP menggunakan *hop* yang lebih panjang daripada *backbone* yang menggunakan *switch* yang dalam hal ini menggunakan teknologi VLAN. Hop itu sendiri merupakan banyaknya perpindahan antar IP yang terdapat pada jaringan tersebut. Terlihat juga pada hasil uji *tracert* bahwa EIGRP akan memilih jalur yang paling cepat untuk dapat sampai kepada tujuannya.

BAB V
KESIMPULAN

1. Untuk membangun sebuah jaringan diperlukan tahap- tahap dari awal sampai akhir hingga jaringan itu dapat dipergunakan dengan baik tanpa ada kesalahan sedikitpun. Rangkaian perjalanan dalam pembuatan jaringan tersebut dikenal dengan metode PDIOO, yaitu Plan- *Desain- Implement- Operation- Optimization*. Langkah- langkah ini merupakan rekomendasi Cisco. Sedangkan dalam skripsi ini, yang dilakukan hanya sampai pada perancangan jaringan
2. Adapun pembangunan jaringan ini didasarkan beberapa kebutuhan pelayanan yang akan dibangun di masing- masing daerah tersebut, yaitu : *video conferencing*, internet, ip teleponi, dan IP VPN.
3. Dari keempat layanan tersebut yang menjadi basis utama perancangan jaringan tersebut adalah IP VPN dengan pembagian pembangunan diacukan pada layer, yaitu *layer* 2 dan *layer* 3. *Layer 2* diwakili oleh *backbone* yang dibangun dengan 7 buah *switch*, sedangkan pada *layer 3* dibangun dengan *backbone* yang terdiri oleh *router*.
4. Jaringan *layer 2* tersebut dinamakan VLAN dan terdiri atas komponen sebagai berikut:*database* VLAN, hubungan *access*, dan hubungan *trunk*. Hubungan *access* merupakan hubungan antara *switch* dengan pengguna, sedangkan hubungan *trunk* merupakan hubungan antar *switch* yang ada. Hubungan *access* tersebut dibuat berdasarkan *port fast Ethernet* yang ada. Untuk vlan 2 yang bernama ipvpn diletakkan pada *port fast Ethernet* 2, vlan 3 pada *port fast Ethernet 3* yang bernama internet, sedangkan vlan 4 pada *port fast Ethernet* 5 bernama iptelepon. Masing – masing berturut-turut dari vlan 2 ke vlan 3 dengan IP 192.168.1.0/24, 192.168.2.0/24, dan 192.168.3.0/24.
5. Jaringan *layer 3* tersebut diwakili dengan protokol *routing* EIGRP, yang merupakan cikal bakal L3VPN, dengan basis ini maka yang diperlukan adalah *router*. Adapun komponen EIGRP adalah tabel *routing*, tabel topologi, *route tagging*, dan keadaan rute.
6. Pengujian yang dilakukan merupakan pengujian untuk memeriksa apakah jaringan tersebut dapat berjalan atau tidak dengan perintah ping yang ditujukan dari pengguna ke pengguna lainnya. Setelah diuji, maka didapatkan kesimpulan bahwa yang paling cepat

dengan parameter waktu ping, maka jaringan yang paling cepat adalah jaringan dengan basis *backbone* switch, yaitu VLAN dengan kecepatan masing- masing pada vlan 2 adalah sebagai berikut : 228,57 bps, 184,97 bps, 146,789 bps, 139,73 bps, 186,0465 bps, 285, 71 bps, sedangkan untuk EIGRP adalah sebagai berikut: 235,29 bps, 153,846 bps, 126,48 bps, 111,111 bps, 100,00 bps, 175,824 bps, 93,84 bps

7. Selain pengujian ping, maka diadakan juga pengujian tracert, yaitu untuk melihat akan melewati alat apa saja untuk mengirimkan sebuat paket data yang ada. Pengujian ini akan memperlihatkan bahwa EIGRP merupakan pilihan yang tepat untuk mendapatkan data berupa hitungan *hop*. Sedangkan jaringan VLAN tidak menunjukkan adanya jalur mana yang dilewati oleh paket data tersebut. Ini dapat dilihat dari hanya satu *hop* yang dilewati oleh jaringan tersebut.

DAFTAR ACUAN

[1] Diane Teare, Catherine Paquet, Campus Network Design Fundamentals, Indianapolis, 2005

[2] Tony Allen, Matt Carling, Telecommunication Management Network, Amsterdam, 2006

[3] World Wide Packet Team, OAM Operations, Administration and Maintenance, White Paper, 2007

[4] John Kane, Internetworking Technologies Handbook, Fourth Edition, San Jose, 2004

[5] Todd Lammle, CCNA ™ Cisco Certified Network Associate Study Guide Fourth Edition, Marina Village Parkway Alameda, 2005