ST-RK-1.16-082-007/R-
Laboratorium Komputer 132

STIKOM SURABAYA

Modul Praktikum
Jaringan Komputer

LABKOM
laboratorium komputer

MODUL PRAKTIKUM 01

CABLING

I. TUJUAN

Setelah praktikum dilaksanakan, praktikan diharapkan memiliki kemampuan :

1. Membuat susunan konfigurasi T568A dan T568B untuk kabel Unshielded Twisted Pair (UTP)
2. Memasang kabel UTP pada konektor Registered Jack 45 (RJ-45)
3. Membuat kabel UTP Straight-through dan Cross-over

II. Perangkat keras yang digunakan

No	Nama perangkat	Gambar
1.	Kabel UTP Cat 5e	
2.	Konektor RJ 45	
3.	Strain Relief RJ 45	
4.	Tang Crimping	
5.	UTP Tester	
6.	PC / Laptop	
7.	Switch / Hub	

III. Referensi

1. Modul kuliah jaringan komputer STIMIK STIKOM Surabaya
2. Internet

IV. Landasan Teori

4.1. Kabel

Ada beberapa tipe (jenis) kabel yang banyak digunakan dan menjadi standar dalam penggunaan komunikasi data dalam jaringan komputer. Kabel-kabel ini sebelumnya harus lulus uji kelayakan sebelum dipasarkan dan digunakan. Setiap jenis kabel mempunyai kemampuan dan spesifikasi yang berbeda.

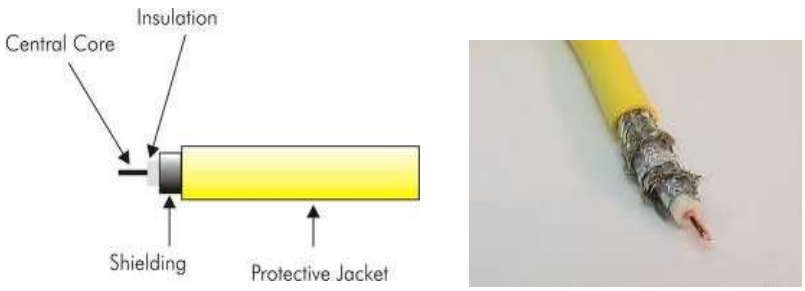
Ada dua jenis kabel yang sering digunakan untuk membangun LAN, yaitu coaxial dan twisted pair (*UTP unshieldedtwisted pair* dan *STP shielded twisted pair*) .

a. Coaxial Cable

Jenis-jenis Coaxial Cable dikenal ada dua jenis, yaitu thick coaxial cable (mempunyai diameter lumayan besar) dan thin coaxial cable (mempunyai diameter lebih kecil).

1. Thick Coaxial Cable

Kabel coaxial memiliki ukuran yang bervariasi. Diameter yang terbesar ditujukan untuk penggunaan kabel backbone Ethernet karena secara histories memiliki panjang transmisi dan penolakan noise yang lebih besar. Kabel coaxial ini seringkali dikenal sebagai thicknet. Kabel coaxial jenis ini dispesifikasikan berdasarkan standar IEEE 802.3 10BASE5, dimana kabel ini mempunyai diameter rata-rata 12mm, dan biasanya diberi warna kuning, kabel jenis ini biasa disebut sebagai standard ethernet atau thick Ethernet, atau hanya disingkat ThickNet, atau bahkan cuman disebut sebagai yellow cable.



Gambar Thick Coaxial cabel

Seperti namanya, jenis kabel ini, karena ukurannya yang besar, pada beberapa situasi tertentu dapat sulit diinstall. Suatu petunjuk praktis menyatakan bahwa semakin sulit media jaringan diinstall, maka semakin mahal media tersebut diinstall. Kabel coaxial memiliki biaya instalasi yang lebih mahal dari kabel twisted pair. Kabel thicknet hampir tidak pernah digunakan lagi, kecuali untuk kepentingan khusus. Kabel Coaxial ini (RG-6) jika digunakan dalam jaringan mempunyai spesifikasi dan aturan sebagai berikut:

a. Setiap ujung harus diterminasi dengan terminator 50-ohm (dianjurkan menggunakan terminator yang sudah dirakit, bukan menggunakan satu buah

resistor 50-ohm 1 watt, sebab resistor mempunyai disipasi tegangan yang lumayan lebar).

b. Maksimum 3 segment dengan peralatan terhubung (attached devices) atau berupa populated segments.
c. Setiap kartu jaringan mempunyai pemancar tambahan (external transceiver).
d. Setiap segment maksimum berisi 100 perangkat jaringan, termasuk dalam hal ini repeaters.
e. Maksimum panjang kabel per segment adalah 1.640 feet (atau sekitar 500 meter).
f. Maksimum jarak antar segment adalah 4.920 feet (atau sekitar 1500 meter).
g. Setiap segment harus diberi ground.
h. Jarang maksimum antara tap atau pencabang dari kabel utama ke perangkat (device) adalah 16 feet (sekitar 5 meter).
i. Jarak minimum antar tap adalah 8 feet (sekitar 2,5 meter).

2. Thin Coaxial Cable

Seiring dengan pertambahan ketebalan atau diameter kabel, maka tingkat kesulitan pengerjaannya pun akan semakin tinggi. Harus diingat pula bahwa kabel jenis ThickNet harus ditarik melalui pipa saluran yang ada dan pipa ini ukurannya terbatas. Oleh karena itu diciptakanlah Thin Coaxial cable untuk mengatasi beberapa masalah diatas.

Kabel coaxial jenis ini banyak dipergunakan di kalangan radio amatir, terutama untuk transceiver yang tidak memerlukan output daya yang besar. Untuk digunakan sebagai perangkat jaringan, kabel coaxial jenis ini harus memenuhi standar IEEE 802.3 10BASE2, dimana diameter rata-rata berkisar 5mm dan biasanya berwarna hitam atau warna gelap lainnya. Setiap perangkat (device) dihubungkan dengan BNC T-connector. Kabel jenis ini juga dikenal sebagai thin Ethernet atau ThinNet.

Gambar thin Coaxial cable

Kabel coaxial jenis ini, misalnya jenis RG-58 A/U atau C/U, jika diimplementasikan dengan Tconnector dan terminator dalam sebuah jaringan, harus mengikuti aturan sebagai berikut:

a. Setiap ujung kabel diberi terminator 50-ohm.

b. Panjang maksimal kabel adalah 1,000 feet (185 meter) per segment.
c. Setiap segment maksimum terkoneksi sebanyak 30 perangkat jaringan (devices)
d. Kartu jaringan cukup menggunakan transceiver yang onboard, tidak perlu tambahan transceiver, kecuali untuk repeater.
e. Maksimum ada 3 segment terhubung satu sama lain (populated segment).
f. Setiap segment sebaiknya dilengkapi dengan satu ground.

Dulu jaringan Ethernet menggunakan kabel coaxial yang diameter luarnya hanya 0,35 cm (kadanag dikenal sebagai thinnet). Kabel ini terutama berguna untuk instalasi kabel yang memerlukan pelilitan dan pembengkokan. Karena mudah diinstall, maka kabel ini juga lebih murah untuk diinstal. Hal ini mendorong beberapa orang menyebutnya sebagai cheapernet. Namun kabel ini memerlukan penanganan khusus. Seringkali pemasang gagal melakukannya. Akibatnya, sinyal transmisi terinterferensi oleh noise. Oleh karena itu, terlepas dari diameternya yang kecil, thinnet sudah jarang digunakan pada jaringan Ethernet. Thicknet dapat menjangkau sampai 500 meter, dan perangkat dihubungkan ke kabel secara langsung dengan menggunakan transceiver Ethernet dengan kabel AUI. Di lain pihk thinnet lebih fleksibel dan dapat menjangkau sampai 185 meter. Komputer dihubungkan ke kabel dengan menggunakan konektor BNC. Thicknet menggunakan spesifikasi Ethernet 10 base 5, sedangkan thinnet menggunakan 10 base 2.

Walapun kabel coaxial sukar di pasang, tetapi ia mempunyai rintangan yang tinggi terhadap ganguan elektromagnet. Dan kabel ini juga mempunyai jarak maksimal yang lebih daripada kabel “twisted pair”. Keunggulan dan kelemahan coaxial cable:

Keunggulan

a. Dapat digunakan untuk menyalurkan informasi sampai dengan 900 kanal telepon
b. Dapat ditanam di dalam tanah sehingga biaya perawatan lebih rendah
c. Karena menggunakan penutup isolasi maka kecil kemungkinan terjadi interferensi dengan sistem lain

Kelemahan

a. Mempunyai redaman yang relatif besar, sehingga untuk hubungan jarak jauh harus dipasang repeater-repeater
b. Jika kabel dipasang diatas tanah, rawan terhadap gangguan-gangguan fisik yang dapat berakibat putusnya hubungan.

b. Twisted Pair Cable

Selain kabel koaksial, Ethernet juga dapat menggunakan jenis kabel lain yakni UTP (Unshielded Twisted Pair) dan Shielded Twisted Pair (STP). Kabel UTP atau STP yang biasa digunakan adalah kabel yang terdiri dari 4 pasang kabel yang terpilin. Dari 8 buah kabel yang ada pada kabel ini, hanya digunakan 4 buah saja yang digunakan untuk dapat mengirim dan menerima data (Ethernet). Perangkat-perangkat lain yang berkenaan dengan penggunaan jenis kabel ini adalah konektor RJ-45 dan HUB.

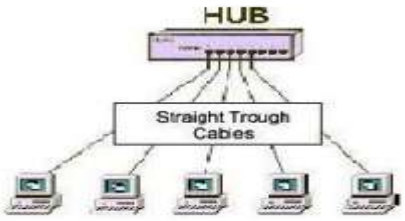
Gambar UTP cable

Ada dua jenis pemasangan kabel UTP yang umum digunakan pada jaringan lokal, ditambah satu jenis pemasangan khusus untuk cisco router, yakni:

1. Straight Through Cable

Untuk pemasangan jenis ini, biasanya digunakan untuk menghubungkan beberapa unit komputer melalui perantara HUB / Switch yang berfungsi sebagai konsentrator maupun repeater.

Penggunaan kabel UTP model straight through pada jaringan lokal biasanya akan membentuk topologi star (bintang) atau tree (pohon) dengan HUB/switch sebagai pusatnya.



Gambar penggunaan kabel *straight throught cable*

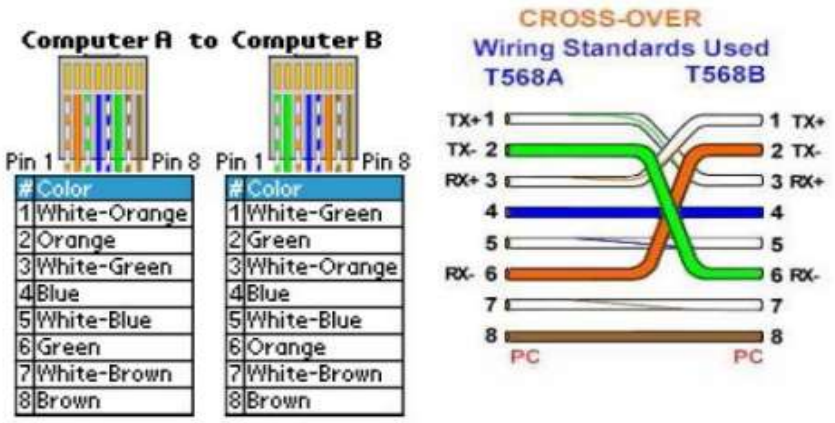
Penggunaan Straight Through Cable

Digunakan untuk menghubungkan dua mesin yang berbeda, seperti :

a. PC – Hub
b. PC – Switch

2. Cross Over Cable

Berbeda dengan pemasangan kabel lurus (straight through), penggunaan kabel menyilang ini digunakan untuk komunikasi antar komputer (langsung tanpa HUB), atau dapat juga digunakan untuk meng-cascade HUB jika diperlukan. Sekarang ini ada beberapa jenis HUB yang dapat di-cascade tanpa harus menggunakan kabel menyilang (cross over), tetapi juga dapat menggunakan kabel lurus.



#	Color
1	White-Orange
2	Orange
3	White-Green
4	Blue
5	White-Blue
6	Green
7	White-Brown
8	Brown

#	Color
1	White-Green
2	Green
3	White-Orange
4	Blue
5	White-Blue
6	Orange
7	White-Brown
8	Brown

Gambar cross over cable

Penggunaan kabel cross over

Digunakan untuk menghubungkan dua mesin yang sama, seperti :

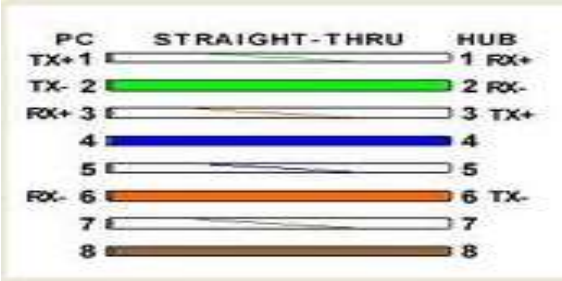
a. Hub – Hub
b. Switch – Router

Pada sistem CISCO, ada satu cara lain pemasangan kabel UTP, yang digunakan untuk menghubungkan sebuah terminal (PC) dan modem ke console Cisco Router atau console switch managible, cara ini disebut dengan Roll-Over. Kabel Roll-Over tersebut sebelumnya terkoneksi dengan DB-25 atau DB-9 Adapter sebelum ke terminal (PC). Anda dapat mengenali sebuah kabel roll-over dengan melihat ke dua ujung kabel. Dimana warna kabel dari sisi yang satu akan berbalik pada sisi kabel di ujung yang lain. Misalnya kabel putih orange yang berada pada pin 1 ujung kabel A, akan berada pada pin 8 ujung kabel B.

V. Praktikum *Cabling*

5.1. Membuat kabel Stright

1. Siapkan perlengkapan praktikum (kabel UTP, conector RJ 45, Strain Relief RJ 45, tang crimping, UTP tester dan switch/ Hub)
2. Kupas ujung kulit kabel UTP secukupnya menggunakan pemotong pada Crimp Tool
3. Buat konfigurasi dengan urutan sebagai berikut (568A) : **putih hijau – hijau-putih orange – biru – putih biru – orage – putih coklat – coklat** antara kedua ujung sama seperti pada gambar di bawah .



Gambar konfigurasi straight cable

4. Jepit kabel yang sudah tersusun dengan ibu jari dan telunjuk agar tetap merata dan terurut, kemudian ratakan ujung kabel dengan pemotong pada Crimp Tool
5. Jangan lepaskan jepitan ibu jari dan telunjuk pada kabel agar susunan tidak bergeser, kemudian masukkan ujung kabel pada konektor RJ-45 dengan posisi Pin-1 sebagai berikut.

Gambar poisisi RJ 45 saat memasukan kabel

7. Pastikan setiap tembaga pada ujung kabel mencapai ujung konektor RJ-45
8. Gunakan Crimp Tool untuk menekan tembaga di ujung konektor RJ-45 agar kabel terpasang pada konektor dengan sempurna.

9. Pasang konektor pada sisi kabel yang lain dengan cara yang sama
    i. Untuk kabel Straight-through, kedua ujung kabel menggunakan susunan T568A atau T568B
    ii. Untuk kabel Cross-over, salah satu ujung kabel menggunakan susunan T568A dan ujung yang lain menggunakan T568B
10. Setelah kedua konektor terpasang dengan baik, gunakan Cable Tester untuk memastikan kondisi konektor terpasang dengan sempurna.

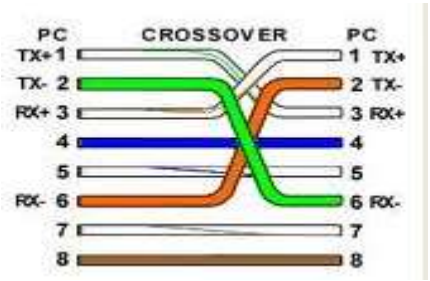
Gambar test koneksi kabel stright

Jika konfigurasi benar maka lampu indikator menyala secara berurutan.

11. Untuk hasil yang maksimal dari gangguan luar (noise), pastikan seluruh kabel tertutup oleh kulit kabel secara sempurna sampai bagian dalam konektor.

5.2. Membuat kabel cross over

1. Untuk membuat kabel cross over lakukan langkah dan 2 seperti pada pembuatan kabel stright cable.
2. Buat konfigurasi yang berbeda antara sisi yang satu dengan sisi yang lain seperti dibawa :



Gambar konfigurasi kabel *cross over*

3. Lakukan langkah yang sama seperti pada langkah 4 s/d 10.

VI. Soal latihan

1. Mintalah bahan-bahan yang diperlukan ke dosen/assisten anda
2. Buatlah kabel *stright* dan *cross over*
3. Lakukan testing dan amati, pastikan nyala lampu secara berurutan.
4. Tunjukan pada dosen/ assisten anda.

Selamat Mencoba, semoga berhasil

MODUL PRAKTIKUM 02

PENGENALAN SOFTWARE SIMULATOR JARINGAN

I. TUJUAN

Setelah praktikum dilaksanakan, praktikan diharapkan memiliki kemampuan :

1. Mengenali komponen-komponen perangkat lunak jaringan berdasarkan fungsinya
2. Menggunakan software Packet Tracer untuk simulasi jaringan sederhana
3. Menjalankan perintah-perintah standar konfigurasi pada masing-masing perangkat jaringan komputer.

II. MATERI

Pengenalan simulator paket tracer

III. Perangkat keras yang digunakan

Perangkat personal komputer / laptop

IV. Referensi

1. Graziani, R.; Johnson, A. 2008. *Routing Protocols and Concepts– CCNA Exploration Companion Guide* . Cisco Press.
2. Cisco CCNA dan jaringan komputer

V. Landasan Teori

Bermacam-macam software simulator yang dapat membantu kita dalam menganalisa ataupun mendisain jaringan komputer. Dalam masa 1 semester praktikum jaringan komputer kali ini kita akan menggunakan tool yang bisa membantu kita dalam kegiatan praktikum yaitu simulator paket tracer.

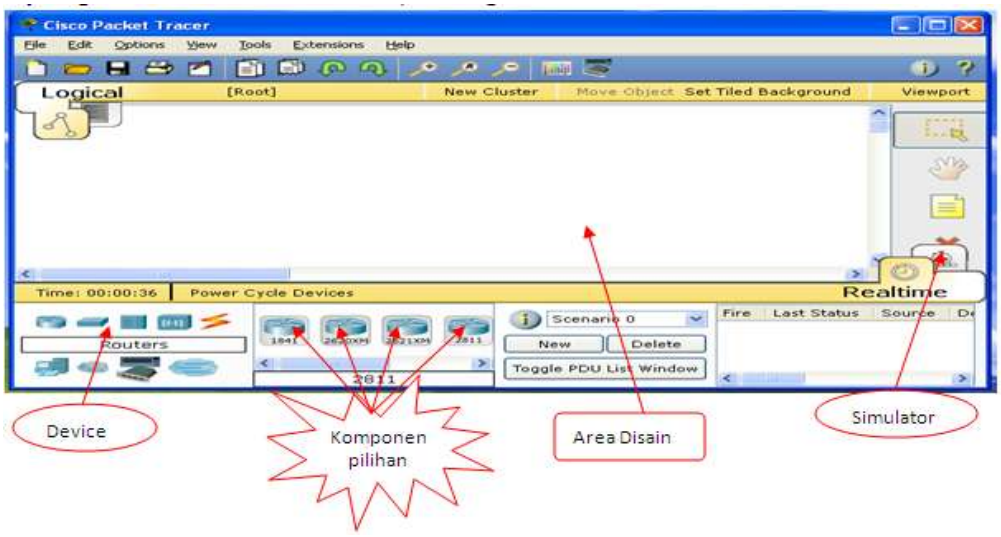
5.1. Packet Tracer

Packet Tracer adalah sebuah simulator protocol jaringan yang dikembangkan oleh Cisco System. Packet Tracer dapat mensimulasikan berbagai macam protocol yang digunakan pada jaringan baik secara realtime maupun dengan mode simulasi. Sebelum melakukan konfigurasi jaringan yang sesungguhnya (mengaktifkan fungsi masing-masing device hardware) terlebih dahulu dilakukan simulasi menggunakan software ini. Simulasi ini

sangat bermanfaat jika membuat sebuah jaringan yang kompleks namun hanya memiliki komponen fisik yang terbatas.

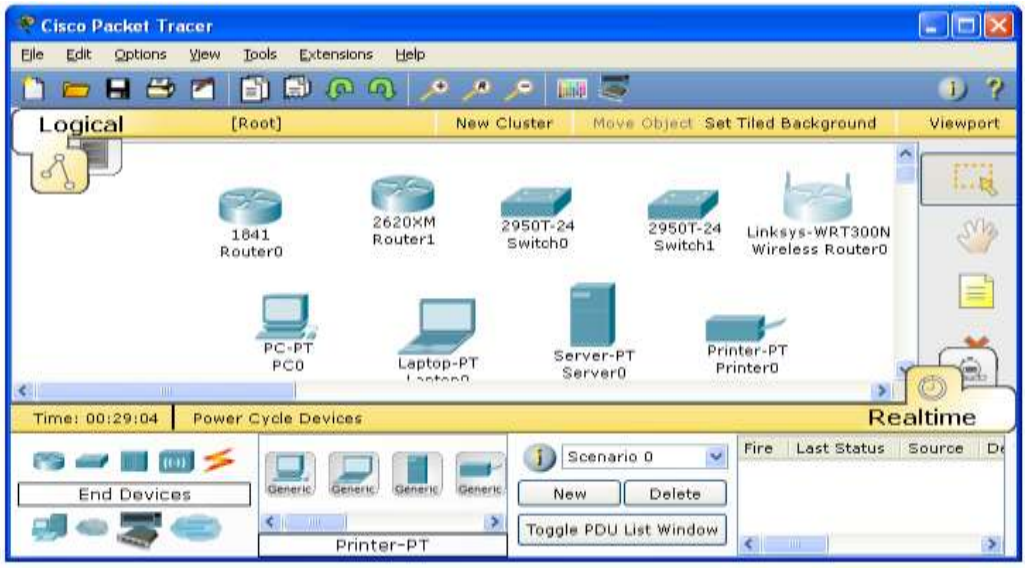
5.1.1. Cara menjalankan Packet Tracer

1. Pastikan software paket tracer sudah terinstall pada komputer /laptop
2. Klik Menu Packet Tracer



Gambar 2.1 tampilan awal paket tracer

3. Pilih Device yang akan digunakan, drag ke area disain / tengah layar.

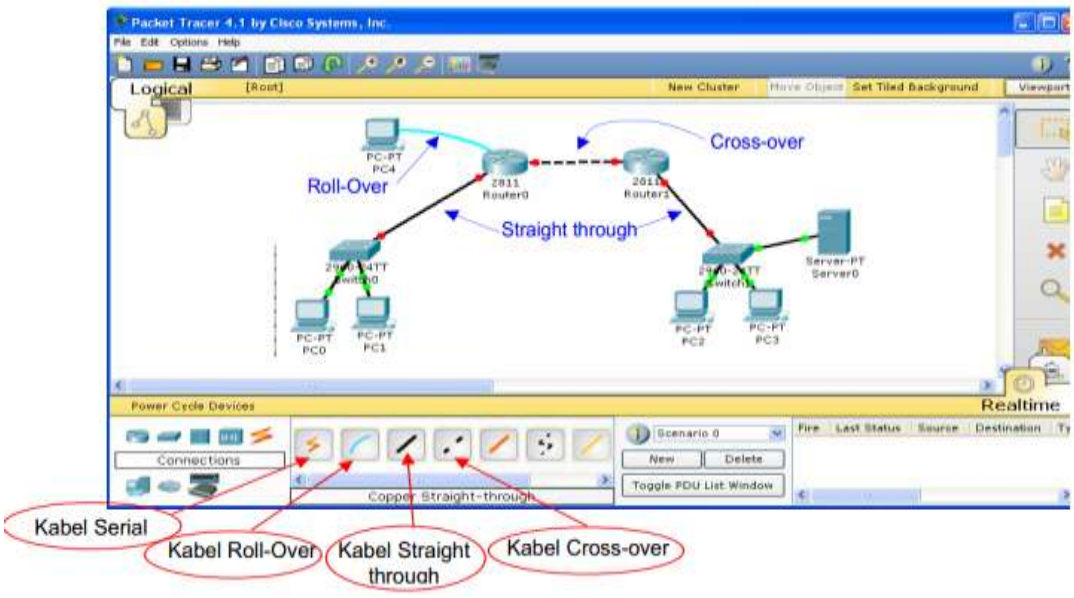


Gambar 2.2 Beberapa jenis device pada paket tracer

4. Hubungkan masing-masing device dengan kabel yang sesuai.

Untuk membuat sebuah konfigurasi jaringan, bagi pemula, sebaiknya ditentukan dulu jenis device yang digunakan, berapa jumlahnya dan bagaimana bentuk konfigurasi jaringan tersebut pada kertas buram. Jenis-jenis kabel penghubung ditentukan berdasarkan aturan sebagai berikut :

a. Untuk mengkoneksikan peralatan yang berbeda, gunakan kabel Straight-through :
    1. Router – Switch
    2. Router – Hub
    3. PC – Switch
    4. PC – Hub
b. Untuk mengkoneksikan peralatan yang sama, gunakan kabel Cross-Over :
    1. Router - Router
    2. Router – PC
    3. Switch - Switch
    4. Switch – Hub
c. Untuk mengkonfigurasi Router melalui PC gunakan kabel Roll-Over



Gambar 2.3 Jenis kabel penghubung

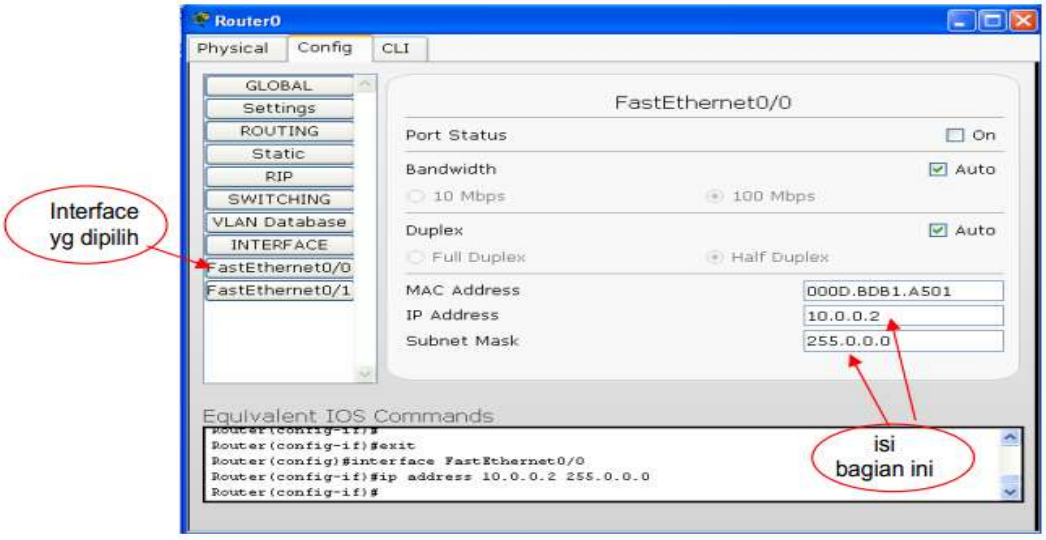
5. Konfigurasi masing-masing device

   Proses konfigurasi merupakan bagian penting dalam mendisain jaringan komputer. Proses konfigurasi di masing-masing device diperlukan untuk mengaktifkan fungsi dari device tersebut. Proses konfigurasi meliputi pemberian IP Address dan subnet mask pada interface-interface device (pada Router, PC maupun Server), pemberian Tabel Routing (pada Router), pemberian label nama dan sebagainya.

   Setelah proses konfigurasi dilakukan, maka tanda bulatan merah pada kabel yang terhubung dengan device tersebut berubah menjadi hijau. Ada 2 mode konfigurasi yang dapat dilakukan : mode GUI (*Config mode*) dan mode CLI (*Command Line Interface*).

Konfigurasi dengan mode GUI

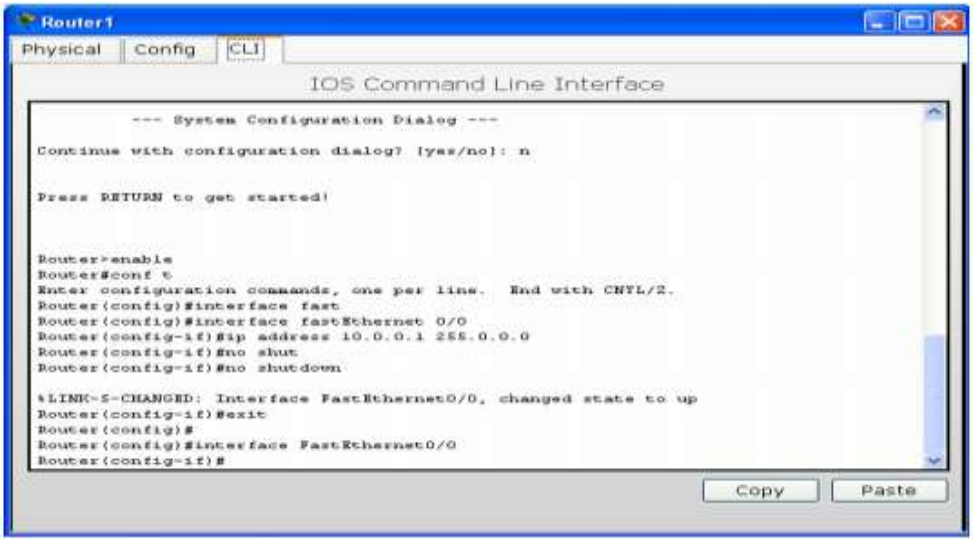
1. Klik device yang akan dikonfigurasi.
2. Pilih menu Config.
3. Klik interface yang diinginkan.
4. Isi IP Address dan subnet mask-nya.
5. Lakukan hal yang sama untuk interface-interface dan device yang lain.



Gambar 2.4 konfigurasi dengan mode GUI

Konfigurasi dengan mode CLI

1. Klik device yang akan dikonfigurasi.
2. Pilih menu CLI.
3. Ketik perintah sesuai dengan format yang disediakan oleh Cisco.



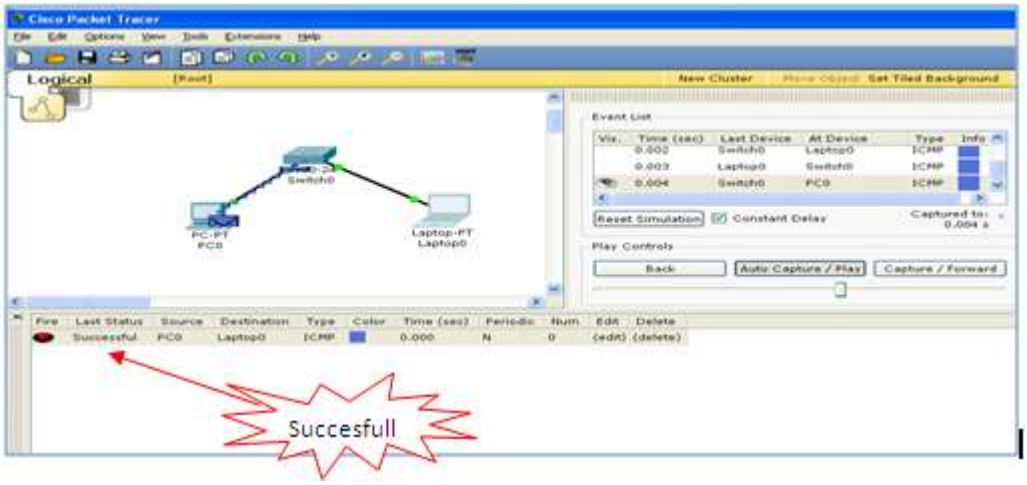
Gambar 2.5 konfigurasi dengan mode CLI

6. Simulasi

Proses simulasi digunakan untuk memastikan apakah jaringan yang sudah dibuat dapat berjalan dengan baik atau tidak. Sebelum menjalankan proses ini, pastikan bahwa antar device sudah terkoneksi dengan benar, yaitu dengan perintah ping ke device tujuan. Contoh : dari device dengan IP address 192.168.10.1 dilakukan ping ke device tujuan 192.168.10.2

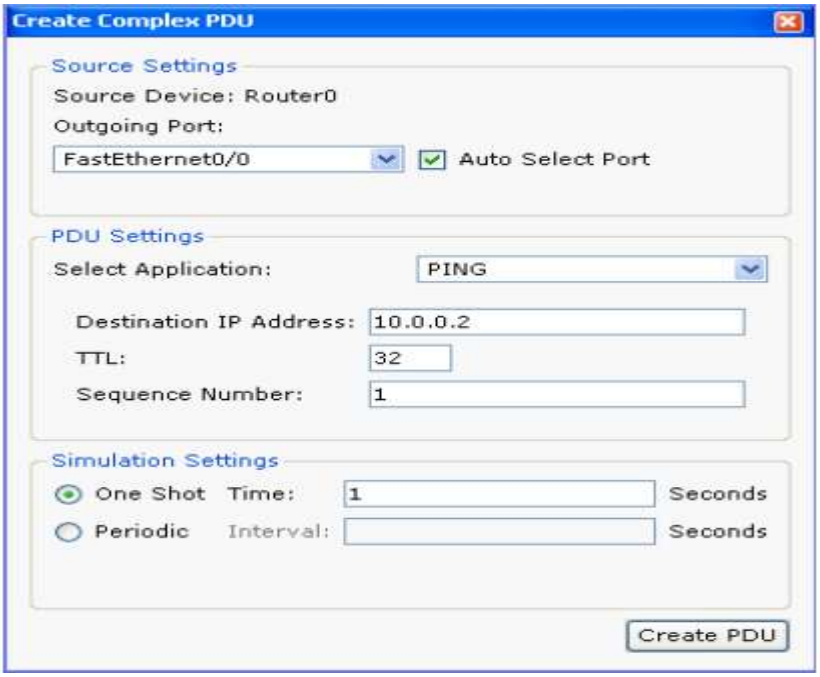
```
ping 192.168.10.2
```

Jika koneksi tersambung dengan baik, akan muncul balasan sebagai berikut :



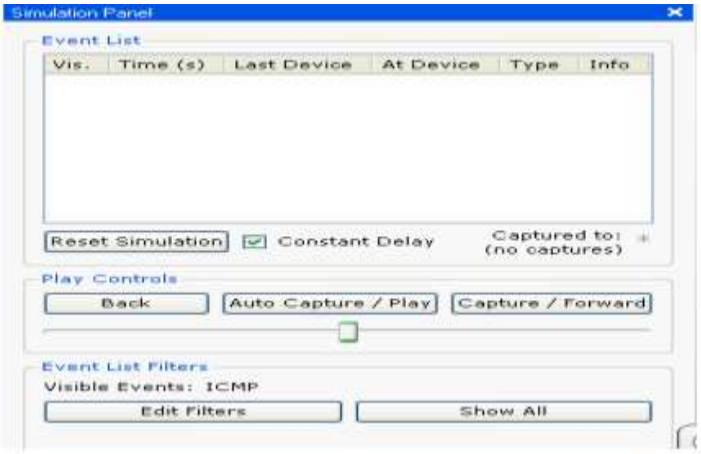
Gambar 2.6 pesan pengiriman paket sukses

Proses simulasi dilakukan dengan mengirim paket dari device pengirim ke device tujuan. Klik gambar paket surat di sebelah kanan tengah meu utama, drag dan klik pada sisi device pengirim. Akan muncul menu Create PDU seperti pada gambar dibawah.



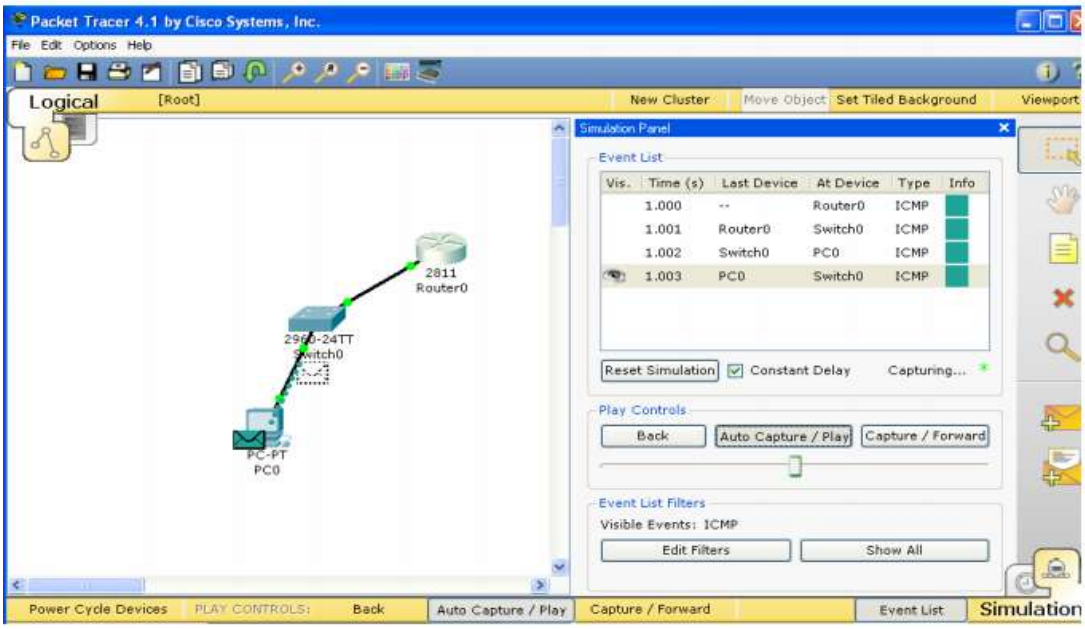
Gambar 2.7 Menu Create Complex PDU

Isilah destination IP Address, sequence number dan One shot time, akhiri dengan menekan tombol Create PDU. Selanjutnya akan muncul informasi tentang PDU yag dibuat pada sisi kanan bawah menu utama. Untuk menghapus dan meng-edit informasi tersebut klik pada bagian yang ingin di-edit atau klik delete untuk menghapus. Untuk menjalankan simulasi, klik panel simulasi pada menu utama Packet Tracer, akan muncul display Simulation Panel.



Gambar 2.8 Menu panel Simulasi

Jenis-jenis paket yang dikirim meliputi paket ARP, Telnet, EIGRP, OSPF, ICMP dan sebagainya. Klik tombol Edit Filters, pilih salah satu dengan me-non aktifkan tanda centang yang ada. Untuk menjalankan simulasi, klik tombol Auto Capture/Play, dan untuk menghentikannya klik tombol yang sama. Hasil simulasi ditunjukkan pada gambar dibawah.

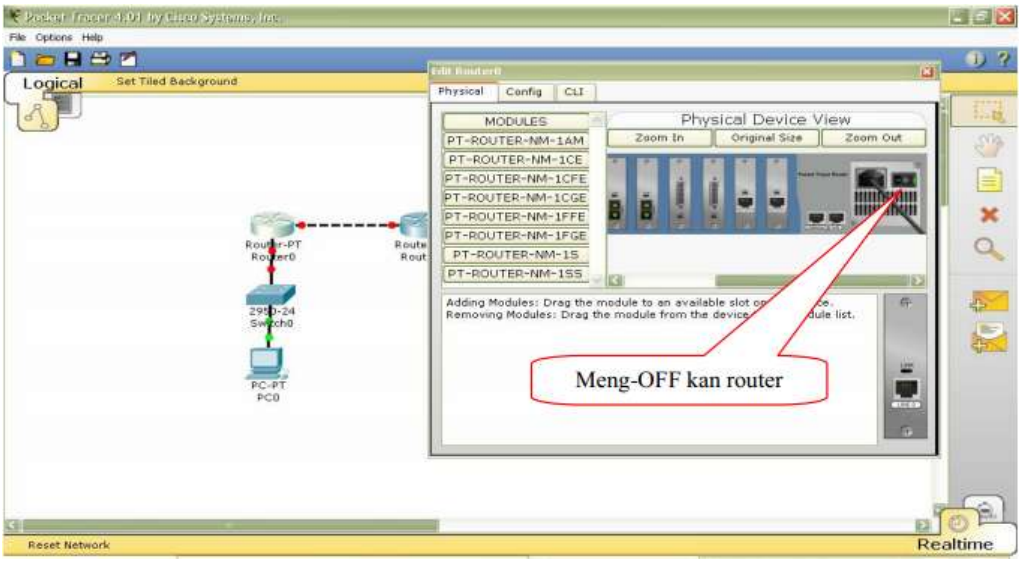


Gambar 2.9 Menu hasil simulasi.

Tambahan :

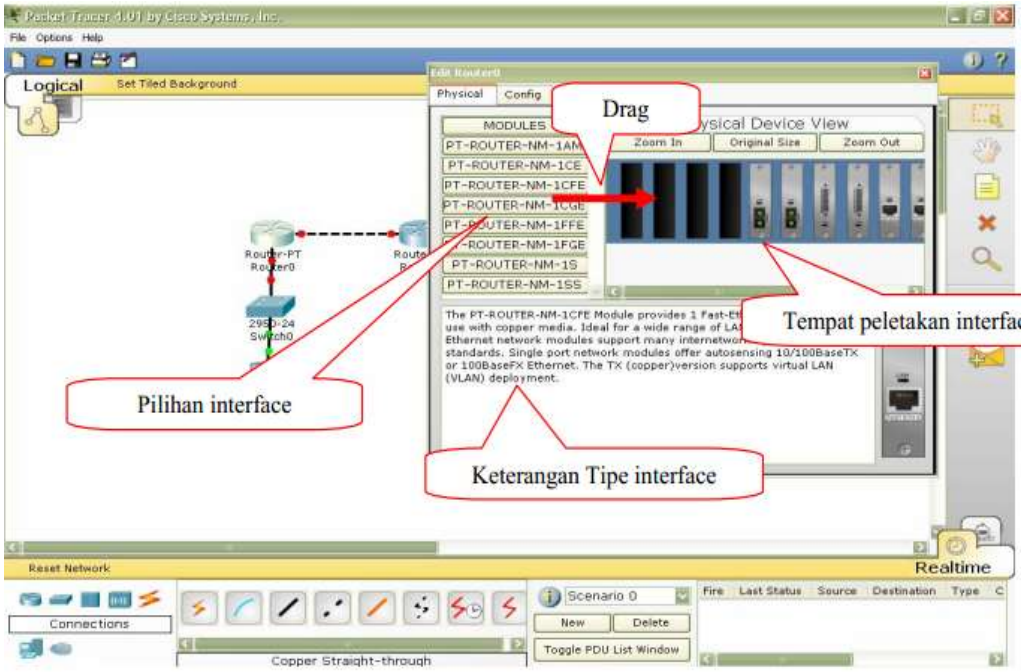
Cisco menyediakan beberapa jenis interface pendukung untuk dipasang di Router, seperti serial card, voip card dsb. Interface-interface tersebut dipasang pada slot-slot kosong yang sudah tersedia. Salah satu jenis Cisco router yang dapat diisi dengan beberapa interface tambahan tersebut adalah tipe 2851. Pembahasan lebih detail tentang interface tambahan diberikan pada materi jenis Cisco Router. Cara menambahkan interface pada slot Router yang kosong adalah sebagai berikut :

1. Off dahulu Router yang anda pasang port serial.



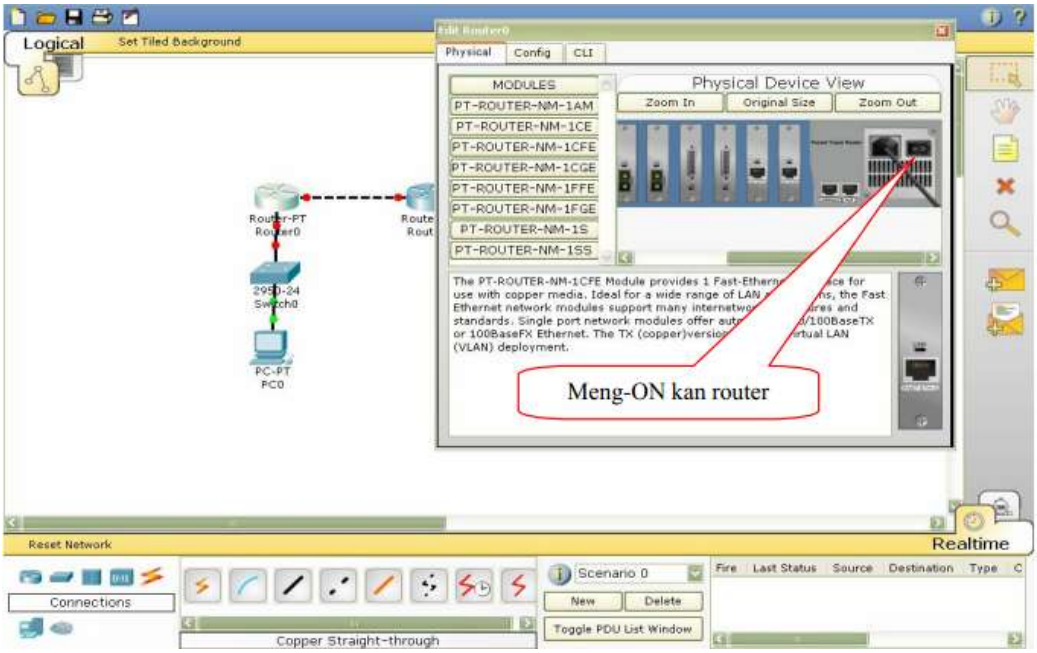
Gambar 2.10 router di Off kan

2. Pilih Interface



Gambar 2.11 Memilih Interface

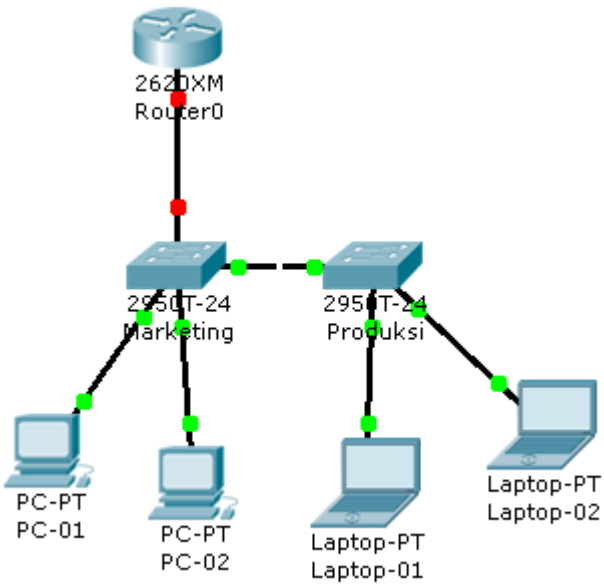
3. Drag interface yang dipilih ketempat interface yang kosong atau bisa juga pada tempat interface yang sudah ada untuk mengganti interface yang sudah ada.



Gambar 2.12 Router di ON kan

VI. Latihan

1. Buatlah Disain jaringan sederhana seperti dibawah
2. Lakukan konfigurasi seperti pada latihan di atas & lakukan uji coba dengan melalukan ping ke ip address tujuan.



Selamat Mencoba, semoga berhasil

MODUL PRAKTIKUM 03
STATIC ROUTING

3.1. TUJUAN

Setelah praktikum dilaksanakan, praktikan diharapkan memiliki kemampuan :

1. Melakukan konfi gurasi das ar Cisco Router
2. Melakukan konfi gurasi Static Routing dengan mo de Command Line (CLI) pada Cisco Router

3.2. PERANGKAT YANG DIBUTUHKAN

Perangk at yang digunak an untuk prak tikum adalah sbb :

1. Windows XP SP3
2. Packet Tracer 53.0.0088

3.3. MATERI

1. Static routing

3.4. REFERENSI

1. Rafiudin, R. (2003). *Mengupas Tuntas Cisco Router.*
2. Jakarta: PT. Elex Media Komputindo, hal. 45
3. http://en.wikipedia.org/wiki/Cisco_IOS

3.5. Landasan Teori

Routing protocol sangat penting dalam mendisain jaringan komputer, sebagai acuan dari penjalur (router) untuk menentukan jalur kemana ia akan meneruskan suatu paket berdasarkan alamat tujuan (*destination address*). Routing protocol diterapkan pada router dimana jalur-jalur routing akan ditentukan lewat *routing table* yang dibuat berdasarkan *routing protokol* yang diaplikasikan. *Routing table* disimpan pada nvram router. Terdapat 2 jenis routing protocol, yaitu *routing protocol static* dan *routing protocol dynamic.* Static routing protocol adalah jenis routing protokol yang statis, maksudnya routing table tidak dipengaruhi oleh update routing table dari router lainnya dan user harus mendefinisikan alur routing yang tetap secara spesifik. Sedangkan pada dynamic routing protocol, routing table dipengaruhi oleh update routing table dari

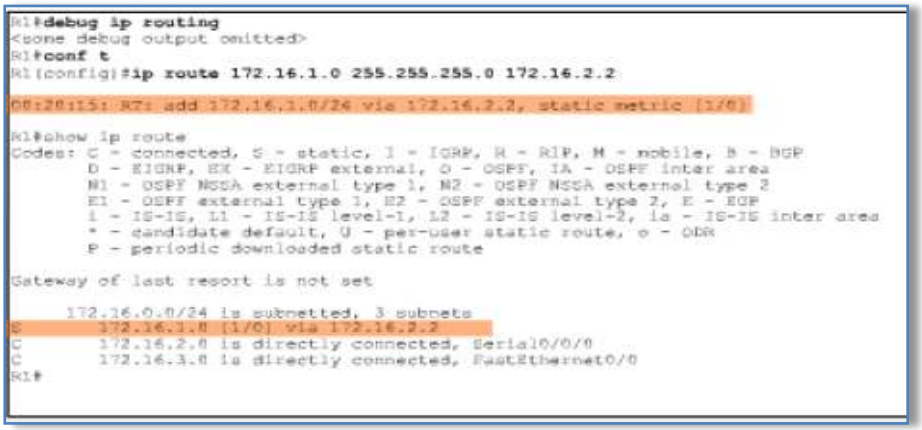
router lainnya dan user tidak perlu mendefinisikan alur routing secara spesifik, tetapi user hanya perlu untuk mendefinisikan alamat-alamat jaringan yang terhubung langsung pada konfigurasi dynamic routing protocol. Modul ini akan membahas static routing protocol pada router Cisco dan cara konfigurasinya. Sedangkan dynamic routing protocol akan dibahas pada modul berikutnya.

3.5.1. Peran Router Dalam Jaringan Komputer

a. Menentukan jalur terbaik untuk mengirimkan paket-paket.
b. Meneruskan paket sesuai dengan alamat jaringan (*network address*) tujuan.

3.5.2. Routing Table

Routing table atau tabel jalur adalah sebuah tabel yang disimpan pada **nvram** sebuah router yang berfungsi sebagai acuan router dalam menentukan jalur terbaik ketika mengirimkan paket-paket dan sebagai acuan kemana router akan meneruskan paket sesuai dengan tujuannya. Routing table berisi alamat network serta interface keluar/alamat next hop untuk masing-masing network tujuan.



Gb. 3.1 Routing table

Gambar diatas adalah contoh routing table, pada routing table terdapat flag, alamat network yang terdaftar dan next hop/exit interface untuk alamat jaringan (network address) tujuan. Flag berfungsi untuk menunjukkan jenis routing protocol yang digunakan, pada contoh di atas flag "S" menunjukkan static routing dan flag "C" menunjukkan network yang langsung terhubung ke *interface router* (*directly connected network*). Untuk menampilkan routing table pada router dapat digunakan syntax : show ip route (pada mode previlege EXEC).

3.5. 3. Konfigurasi Static Routing

Static routing adalah metode dimana network administrator memberitahu router kemana lalulintas data akan dikirimkan. Static routing digunakan jika hanya terdapat sedikit perangkat router atau hanya ada satu route dari satu sumber ke satu tujuan.

Static routing protocol dapat dikonfigurasi dengan 2 cara, yaitu static routing mendefinisikan **alamat next hop** (alamat IP hop selanjutnya) dan konfigurasi static routing dengan mendefinisikan **exit interface** (interface keluar).

a. Konfigurasi dengan mendefiniskan alamat next hop.

Konfigurasi static routing dengan mendefinisikan alamat next hop dilakukan dengan mendefinisikan alamat network tujuan beserta alamat next hop tujuan untuk alamat tersebut. Dimana alamat next hop adalah alamat interface tujuan untuk meneruskan paket ke alamat tujuan. Syntax untuk melakukan static routing by next hop : (pada global configuration mode).

```
ip route [destination network address] [subnet mask] [next
                    hop address]
```

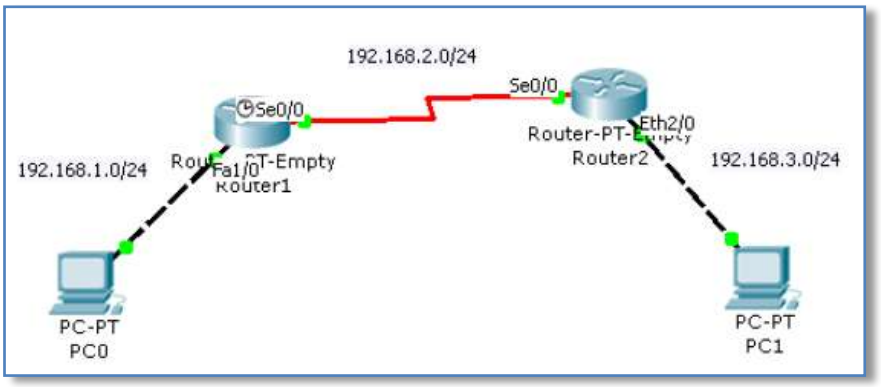
Ip route : perintah untuk membuat static routing

Destination network address : network tujuan yang akan dimasukan kedalam tabel routing

Subnet mask : subnet yang digunakan oleh destination network

Next hop address : ip address yang terhubung langsung (*directy conected*)

Contoh :



Gambar.3.2 Routing dengan 2 router

Konfigurasi static routing untuk alamat network 192.168.1.0/ 24 pada Router2 (catatan: interface se0/0 melalui Router 1 memiliki alamat 192.168.2.1).

```
ip route 192.168.1.0 255.255.255.0 192.168.2.1
```

b. Konfigurasi dengan mendefinisikan exit interface

Konfigurasi static routing dengan mendefinisikan exit interface dilakukan dengan mendefinisikan **alamat network tujuan beserta exit interface** pada router yang dikonfigurasi untuk alamat tersebut. Dimana alamat exit interface adalah interface keluar pada router untuk meneruskan paket sesuai dengan alamat tujuan. Syntax untuk melakukan static routing by exit interface : (pada global configuration mode)

```
ip route [destination network address] [subnet mask] [exit
                    interface]
```

Exit interface : interface router dimana paket akan keluar.

Contoh :

Konfigurasi static routing untuk alamat network 192.168.1.0/24 pada Router2 (catatan: exit interface pada Router2 untuk network 192.168.1.0/24 adalah Se0/0)

```
ip route 192.168.1.0 255.255.255.0 Se0/0
```

c. Delete Static Routing

Pada static routing protocol kita dapat menghapus static routing yang telah kita definisikan sebelumnya. Syntax yang digunakan :

```
no ip route [destination network address] [subnet
    mask] [next hop address/exit interface]
```

d. Default Route

Default route adalah jalur default untuk paket yang mempunyai alamat network tujuan tertentu tapi tidak terdapat di routing table router yang disinggahi. Jika terdapat default route yang di-set pada router tersebut, maka paket tersebut akan mengikuti rute default yang telah ditetapkan, jika tidak ada default route maka paket akan dibuang/discard. Default route didefiniskan dengan alamat : 0.0.0.0/0 . Default route pada routing table ditandai dengan flag “S*”.

3.5.4. Mekanisme Routing

Isi tabel tersebut dapat diatur dan dipelihara sesuai kebutuhan di lapangan. Ada beberapa mekanisme routing yang dapat di gunakan, yaitu :

a. **Static Routing**

Mekanisme pengisian atau pengubahan jalur routing yang dilakukan secara manual pada tiap router. Yang menguntungkan dari mekanisme ini adalah :

- ❖ Kerja processor router lebih ringan.
- ❖ Menghemat bandwith yang dipakai karena tidak ada pertukaran data tabel antar router.

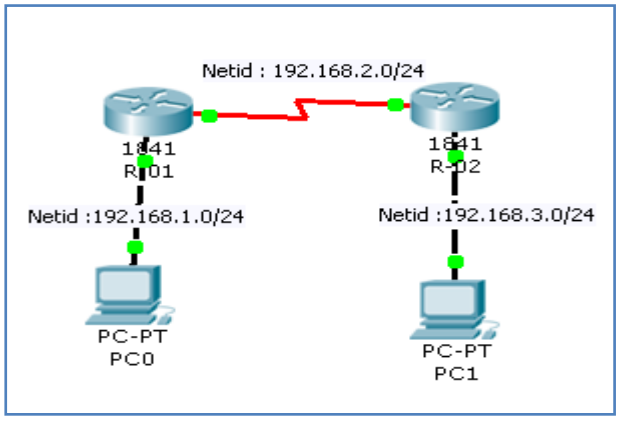
Karena mekanisme ini dilakukan secara manual oleh administrator ,jaringan pasti memiliki kekurangan, antara lain:

1. Jika jaringan besar maka mekanisme ini akan sangat tidak efisien karena harus dilakukan pada setiap router.
2. Apabila ada perubahan atau penambahan sumber daya di dalam jaringan maka tabel routing juga harus segera diubah secara manual.
3. Informasi dari tiap router harus diketahui oleh administrator.

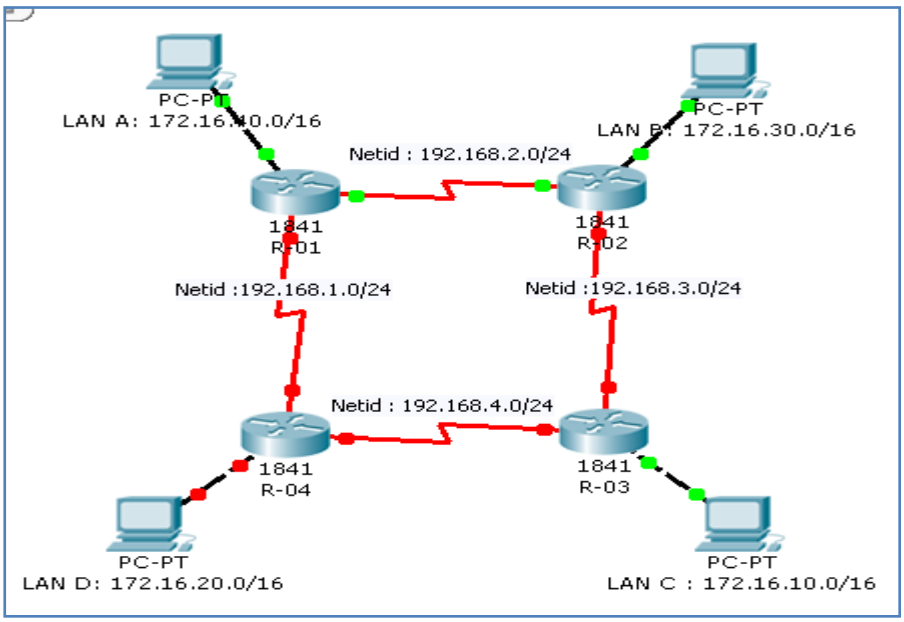
3.5.5. Tugas Praktikum

1. Buat disain seperti gambar dibawah ini, tentukan ip address masing-masing personal komputer serta gatwaynya mengacu pada netid .

   Seting kedua router menggunakan static routing sehingga kedua pc dapat saling terhubung, jangan lupa buattabel routingnya terlebih dahulu.



2. Buatl disain seperti gambar dibawah ini, lakukan langkah seperti pada soal di atas.



MODUL PRAKTIKUM 04
DYNAMIC ROUTING

4.1. TUJUAN

Setelah praktikum dilaksanakan, praktikan diharapkan memiliki kemampuan :

1. Praktikan mengetahui konsep dasar dynamic routing.
2. Praktikan bisa membandingkan kelebihan dan kekurangan dari dynamic Routing dengan static routing.
3. Praktikan dapat melakukan konfigurasi router dengan dynamic routing

4.2. PERANGKAT YANG DIBUTUHKAN

Perangk at yang digunak an untuk prak tikum adalah sbb :

1. Windows XP SP3
2. Packet Tracer 53.0.0088

4.3. MATERI

1. Cisco IOS dengan simulator PAKET TRACER

4.4. REFFERENSI

1. Rafiudin, R. (2003). *Mengupas Tuntas Cisco Router.*
2. Jakarta: PT. Elex Media Komputindo, hal. 45
3. http://en.wikipedia.org/wiki/Cisco_IOS
4. Jaringan Komputer sttelkom Bandung

4.5. Landasan Teori

Dynamic Routing adalah sebuah mekanisme otomatis yang dilakukan oleh router tanpa campur tangan network administrator. Router-router yang terhubung dalam sebuah jaringan akan saling berkomunikasi dan bertukar informasi *routing table* yang ada pada masing-masing router. Hal ini akan berjalan dengan baik pada jaringan yang sudah besar dan beragam. Pada mekanisme ini, **tabel routing tidak di-update secara manual** oleh administrator tetapi router sendiri yang akan memberikan atau bertukar informasi (*routing table*) dengan router lain. Jalur yang dipilih dan digunakan berdasarkan jarak terpendek antara peralatan pengirim dan peralatan penerima.

Untuk merepresentasikan jarak dynamic routing menggunakan nilai metric yang di dalamnya terdapat parameter-parameter untuk menghasilkan nilai metric tersebut. Parameter yang dapat digunakan untuk menghasilkan sebuah nilai metric adalah :

1. *Hop count*, berdasarkan banyaknya router yang dilewati.
2. *Ticks*, berdasarkan waktu yang diperlukan.
3. *Cost,* berdasarkan perbandingan sebuah nilai standart dengan bandwidth yang tersedia.
4. *Composite metric*, berdasarkan hasil perhitungan dari parameter-parameter :
    a. *Bandwitdh*
    b. *Delay*
    c. *Load*
    d. *Reliability*
    e. *MTU*

Beberapa konsep yang digunakan oleh protokol-protokol routing antara lain :

1. Distance Vector

Pada konsep ini setiap router yang terhubung dalam sebuah jaringan akan saling bertukar informasi secara otomatis secara periodik, kurang lebih setiap 30 detik.

Saat pertama kali router terhubung dalam sebuah jaringan komputer maka router tersebut akan memiliki table routing yang berisi data alamat jaringan yang terhubung langsung dengan router tersebut. Misalkan sebuah jaringan dengan network ID 172.25.82.0 terhubung ke [Router1], maka tabel routing akan berisi network ID tersebut. Setelah terhubung kurang lebih 30 detik atau lebih maka daftarnya akan bertambah dengan sendiri, misalkan berhasil mengenali network ID 172.25.83.0 dan 172.25.84.0. Jenis routing yang masuk kategori Distance Vector adalah :

a. Dynamic Routing Protokol

RIP (Routing Information Protocol) mengirimkan *routing table* yang lengkap ke semua interface yang aktif setiap 30 detik, RIP hanya menggunakan jumlah hop untuk menentukan cara terbaik ke sebuah network *remote*, tetapi RIP secara default memiliki jumlah hop maksimum yang di izinkan, yaitu 15 hop. Hal tersebut berarti nilai 16 dianggap tidak terjangkau (*unreachable*). RIP bekerja dengan baik di network-network yang kecil, tetapi RIP tidak efisien pada network yang besar dengan link WAN yang lambat atau pada network yang

memiliki jumlah router yang banyak. RIP versi 1 menggunakan hanya *classful routing*, yang berarti semua alat di network harus menggunakan subnetmask yang sama, hal tersebut dikarenakan RIP versi 1 tidak mengirimkan update dengan informasi subnetmask didalamnya. Kasus pada RIP versi 1 dapat ditanggulangi dengan menggunakan RIP versi 2, pada versi ini menyediakan sesuatu yang disebut *prefix routing*, dan bisa mengirimkan informasi subnetmask bersama dengan update-update dari route.

2. RIP Timers

RIP menggunakan tiga jenis timer yang berbeda untuk mengatur unjuk kerjanya yaitu :

a. **Route Update Timer** , Interval antar update biasanya 30 detik secara periodik dimana router mengirimkan sebuah copy yang lengkap dari routing table-nya ke semua router terdekat.
b. **Route Invalid Timer**, Timer ini menentukan jangka waktu yanga harus lewat (180 detik) sebelum sebuah router menentukan bahwa sebuah rute menjadi tidak valid.
c. **Holddown Timer**, Timer ini men-set interval waktu di mana informasi routing ditahan (*holddown state*) , defaultnya adalah 180 detik.
d. **Route Flish Time**, Timer ini men-set waktu antara sebuah routemenjadi tidak valid dan penghapusannya dari routing table (240 detik).

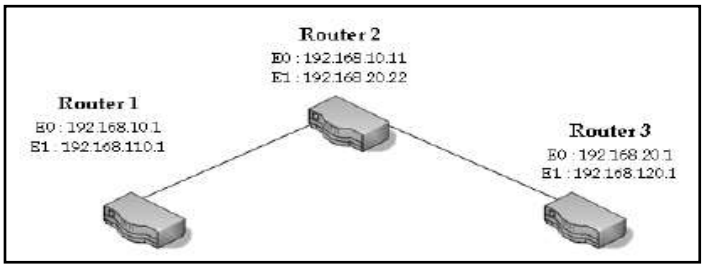
3. Konfigurasi RIP (Routing Information Protocol)

Untuk mengkonfigurasi routing dengan RIP digunakan perintah [***router rip***] dan [***network***] yang dapat Anda masukkan dari mode [***Global Configuration***].

Perintah [***router rip***] digunakan untuk mengaktifkan protocol RIP yang ada pada router dan perintah [**network]** berfungsi untuk menginformasikan kepada protokol routing tentang network mana yang akan diroute. Contoh penggunaannya dapat Anda lihat dibawah ini :

```
Router(config) # router rip
Router(config) # network 172.25.82.0
```

Contoh kasus :



Gambar 3.1 Konfigurasi 3 router

Pada ilustrasi tersebut terdapat 3 (tiga) router yang saling terhubung. [Router1] terhubung ke 2 (dua) network yaitu 192.168.10.0/24 dan 192.168.110/24 untuk [Router2] terhubung ke 2 (dua) network yaitu 192.168.10.0/24 dan 192.168.20.0/24, sedangkan untuk [Router3] terhubung ke 2(dua) network yaitu 192.168.20.0 dan 192.168.120.0. Desain konfigurasi seperti pada gambar diatas, kemudian perhatikan gambar diatas dengan seksama dan teliti, [Router1] terhubung ke [Router2] melalui [ethernet0] sedangkan [Router2] terhubung ke [Router3] melalui [ethernet1].

Berikutnya kita akan mencoba melakukan konfigurasi pada 3 (tiga) router tersebut. Untuk mengkonfigurasi protokol RIP pada [Router1] maka setting yang Anda harus berikan adalah :

1. Setelah masuk pada console Router, ketikkan [enable] pada prompt.
2. Berikan identitas pada router tersebut dengan nama [Router1].
3. Kemudian berikan alamat IP untuk masing-masing interface yang ada pada [Router1].

Interface [ethernet0] alamat IP-nya 192.168.10.1/24 sedangkan interface [ethernet1] alamat IP-nya 192.168.110.1/24.

Pemberian alamat IP pada interface e0 di router1

Pemberian alamat IP pada interface e1 di outer1

4. Setelah pemberian identitas nama dan alamat IP, berikutnya kita akan melakukan konfigurasi protokol RIP pada [Router1].

```
Router1#con t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#int e0
Router1(config-if)#ip address 192.168.10.1 255.255.255.0
Router1(config-if)#no shut
Router1(config-if)#end
Router1#
```

```
Router1(config)#int e1
Router1(config-if)#ip address 192.168.110.1 255.255.255.0
Router1(config-if)#no shut
%LINK-3-UPDOWN: Interface Ethernet1, changed state to up
Router1(config-if)#end
```

5. Masuk pada mode [*Global Configuration*] kemudian ketikkan perintah *router Rip* lanjutkan dengan memasukkan *network ID* yang akan di routing.

   Konfigurasi RIP pada Router1

```
Router1(config)#router rip
Router1(config-router)#network 192.168.110.0
Router1(config-router)#network 192.168.10.0
Router1(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

6. Perintah *router rip* digunakan untuk mengatifkan protokol RIP, sedangkan perintah *network* digunakan untuk menjelaskan network yang dirouting kepada router lain yang terhubung dalam jaringan tersebut.
7. Kemudian coba hasil konfigurasi Anda dengan perintah *show ip route* pada mode [Privileged Configuration].

```
Router1#sh ip ro
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route

Gateway of last resort is not set

     192.168.10.0/24 is subnetted, 1 subnets
C       192.168.10.0 is directly connected, Ethernet0
     192.168.110.0/24 is subnetted, 1 subnets
C       192.168.110.0 is directly connected, Ethernet1
```

   Belum terjadi konfigurasi RIP, karena semua network ID belum terhubung

8. untuk sementara konfigurasi RIP pada Router1 selesai, Berikutnya kita lanjutkan konfigurasi untuk Router2.

   Sedangkan untuk *Router2* konfigurasinya hampir sama dengan Router1 berikan identitas nama dan alamat IP pada router tersebut.

```
Router>enable
Router#con t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Router2
```

Berikutnya lakukan konfigurasi RIP pada [Router2].

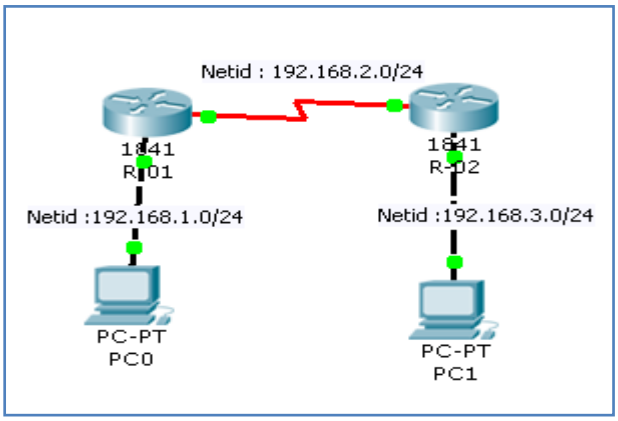
```
Router2#con t
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#router rip
Router2(config-router)#network 192.168.10.0
Router2(config-router)#network 192.168.20.0
Router2(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

9. Apabila Anda lakukan pengecekan konfigurasi RIP maka hasilnya akan sama seperti pada Router1 karena belum semua network ID terhubung.
10. Coba Anda lakukan tes koneksi ke 192.168.10.1 dan ke 192.168.110.1 yang ada di Router1.
11. Sampai disini konfigurasi untuk Router2 selesai.

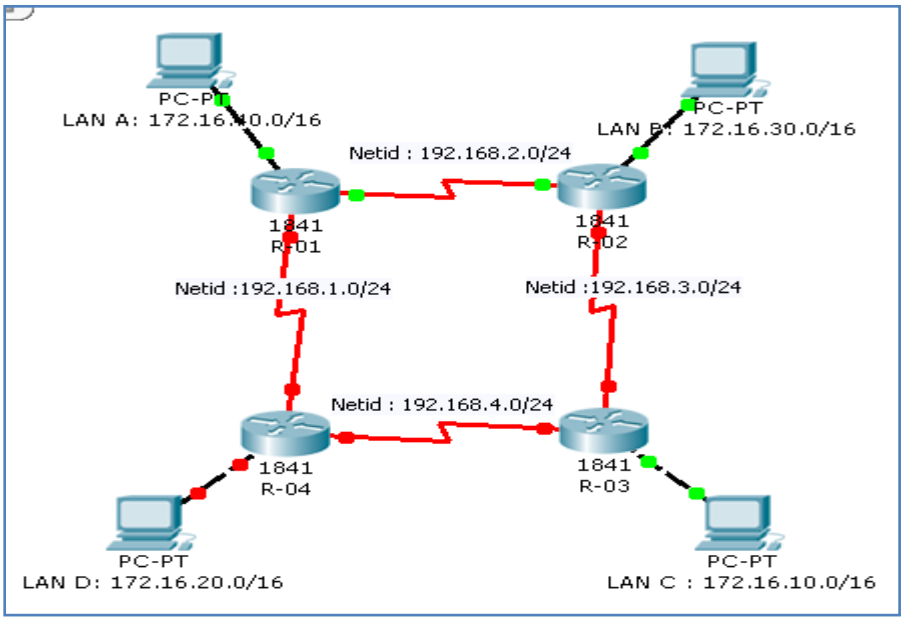
3.5.5. Tugas Praktikum

1. Buat desain seperti gambar dibawah ini, tentukan ip address masing-masing personal komputer serta gatwaynya mengacu pada netid .

   Seting kedua router menggunakan ***Dynamic routing*** sehingga kedua pc dapat saling terhubung, jangan lupa buattabel routingnya terlebih dahulu.



2. Buatl disain seperti gambar dibawah ini, lakukan langkah seperti pada soal di atas.



MODUL PRAKTIKUM 05

ROUTING EIGRP *(Enhanced Interior Gateway Routing Protocol)*

5.1. Tujuan :

1. Mengenal dan mempelajari EIGRP serta fitur-fiturnya
2. Melakukan konfigurasi dasar EIGRP pada router Cisco

5.2. PERANGKAT YANG DIBUTUHKAN

Perangk at yang digunak an untuk praktikum adalah sbb :

1. Windows XP SP3
2. Packet Tracer 53.0.0088

5.3. MATERI

ROUTING EIGRP *(Enhanced Interior Gateway Routing Protocol)* dengan simulator PAKET TRACER

5.4. Referensi

1. Rafiudin, R. (2003). *Mengupas Tuntas Cisco Router.*
2. Jakarta: PT. Elex Media Komputindo, hal. 45
3. http://en.wikipedia.org/wiki/Cisco_IOS

5.5. LANDASAN TEORI

Enhanced Interior Routing Protocol (EIGRP) adalah salah satu *routing protocol* yang bersifat *proprietary* dari Cisco System yang di rilis pada tahun 1992. Disebut sebagai proprietary karena routing protocol EIGRP ini hanya bisa digunakan sesama router cisco, tidak untuk router yang lain. Dilihat dari namanya dapat disimpulkan, EIGRP adalah "pengkayaan" dari IGRP *(Interior Gateway Routing Protocol).* EIGRP menggunakan formula berbasis bandwidth dan delay untuk menghitung metric yang sesuai untuk rute. EIGRP melakukan konvergensi secara tepat ketika menghindari loop. EIGRP tidak melakukan perhitungan – perhitungan rute seperti yang dilakukan oleh protocol link state. Hal ini membuat EIGRP tidak memputuhkan dIsain extra, sehingga hanya memerlukan lebih sedikit memori dan proses dibandingkan dengan protocol link state. Konvergensi EIGRP lebih cepat dibandingkan protocol distant vector lainnya, hal ini di sebabkan karena EIGRP

tidak memerlukan loop-avoidance yang pada kenyataannya menyebabkan protocol distant vector melambat. EIGRP mengurangi pembebanan di jaringan karena hanya mengirim sebagian dari routing update, EIGRP tidak akan mengirimkan update jika tidak ada perubahan. Jika ada perubahan, langsung update dilakukan, akan tetapi hanya mengirim update kepada yang terkena imbas update.

EIGRP sering pula disebut *hybrid-distant vector routing protocol*, hal ini dikarenakan EIGRP seperti memiliki dua tipe routing protocol yang di gunakan yaitu distant vector dan link state. Akan tetapi walaupun EIGRP mempunyai kemampuan seperti link-state routing protocol, EIGRP tetaplah distant vector routing protocol. Dalam perhitungan untuk menentukan jalur mana yang terpendek, EIGRP menggunakan algoritma DUAL (Diffusing Update Algorithm) dalam menentukannya, DUAL juga memiliki fungsi menyiapkan backup dan memastikan backup loop-free.

5.5.1. EIGRP memiliki karakteristik sebagai berikut:

1. Reliable Transport Protocol (RTP)
2. Bounded Updates
3. Diffusing Update Algorithm (DUAL)
4. Establishing Adjacencies
5. Neighbor and Topology Tables

5.5.2. Kelebihan EIGRP dibanding routing protocol lainnya:

1. Satu – satunya routing protocol yang menggunakan route backup.
2. Mudah di konfigurasi, semudah RIP
3. Summarization dapat dilakukan dimana saja dan kapan saja
4. EIGRP satu satunya routing protocol yang dapat melakukan unequal load balancing
5. Kombinasi terbaik dari protocol distant vector dan link-state

5.5.3. Konfigurasi Dasar EIGRP

A. Process ID

Pada EIGRP, digunakanlah process ID untuk merepresentasikan routing protocol yang sedang berjalan pada router.

Contoh:

Router (config) #router eigrp 1

Angka “1” merepresentasikan proses EIGRP yang berjalan pada router ini. Sederhananya, untuk membangun jaringan dengan router tetangga, EIGRP

mengharuskan semua router di konfigurasi dengan process ID yang sama. Hanya satu process ID dari semua routing protocol yang dapat dikonfigure pada sebuah router.

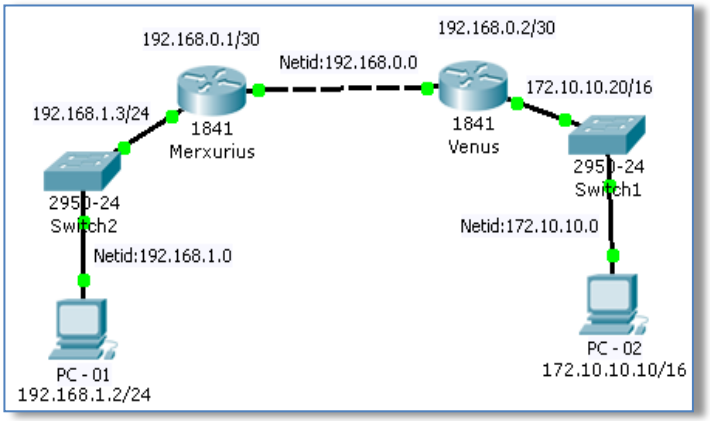
B. EIGRP Networks

Setelah memberikan process ID, langkah selanjutnya yang harus dilakukan adalah memberikan network address dengan menggunakan perintah "network".

Perintahnya adalah:
Router(config-ruter)#network
(network address)

Ket: Network address yang diisikan, adalah classful network address pada interface.

Contoh:



Gb. 5.1 Routing EIGRP dengan 2 router

C. Langkah-langkah Konfigurasi :

1. Atur ip address PC01 menjadi 192.168.1.2 dengan subnet mask 255.255.255.0 gateway 192.168.1.3
2. Atur ip address PC02 menjadi 172.10.10.10 dengan subnet mask 255.255.0.0 gateway 172.10.10.20
3. Klik 2x router dan atur setiap interfacenya dengan masuk pada tab CLI

4. Misal pada router Merxurius :

a. Jika ada pertanyaan awal ketik 'no'
b. Kemudian Enter dan Enter sampai muncul seperti ini
c. Router>enable
d. Router#configure terminal
e. Router(config)#interface fa 0/0
f. Router(config-if)#ip address 192.168.1.3 255.255.255.0
g. Router(config-if)#no shutdown
h. Router(config-if)#exit
i. Router(config)#interface fa 0/1
j. Router(config-if)#ip address 192.168.0.1 255.255.255.252
k. Router(config-if)#no shutdown
l. Router(config-if)#exit
m. Router(config)#exit
n. Router#write --> 'menyimpan perintah-perintah sebelumnya agar router dapat berjalan normal'

5. Lakukan hal yang sama pada router Venus :
   a. Jika ada pertanyaan awal ketik 'no'
   b. Kemudian Enter dan Enter sampai muncul seperti ini
   c. Router>enable
   d. Router#configure terminal
   e. Router(config)#interface fa 0/0
   f. Router(config-if)#ip address 172.10.10.20 255.255.0.0
   g. Router(config-if)#no shutdown
   h. Router(config-if)#exit
   i. Router(config)#interface fa 0/1
   j. Router(config-if)#ip address 192.168.0.2 255.255.255.252
   k. Router(config-if)#no shutdown
   l. Router(config-if)#exit
   m. Router(config)#exit
   n. Router#write

6. Pengaturan ip addres pada setiap router sudah dilakukan, namun, hal ini tidak serta merta PC01 dan PC02 langsung terhubung, coba diping, pasti RTO alias (Request Time Out)

```
PC>ping 172.10.10.10

Pinging 172.10.10.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

7. Selanjutnya adalah konfigurasi EIGRP
8. Pada router Merxurius
   a. Router>enable
   b. Router#configure terminal
   c. Router(config)#**router eigrp 10**
   d. Router(config-router)#**network 192.168.1.0** --> 'atur network gateway atau fa 0/0'
   e. Router(config-router)#**network 192.168.0.0** --> 'atur network fa 0/1'
   f. Router(config-router)#exit --> 'keluar dari konfigurasi router eigrp'
   g. Router(config)#exit
   h. Router#write --> 'lakukan penyimpanan'

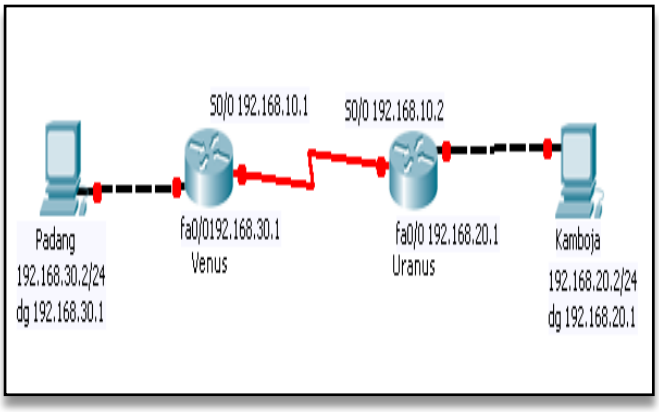
9. Lanjut pada router Venus
   a. Router>enable
   b. Router#configure terminal
   c. Router(config)#router eigrp 10
   d. Router(config-router)#network 172.10.0.0
   e. Router(config-router)#network 192.168.0.0
   f. Router(config-router)#exit
   g. Router(config)#exit
   h. Router#write
10. Kalo sudah, sekarang coba kita ping dari pc01 ke pc02.

```
PC>ping 172.10.10.10

Pinging 172.10.10.10 with 32 bytes of data:

Reply from 172.10.10.10: bytes=32 time=125ms TTL=126
Reply from 172.10.10.10: bytes=32 time=94ms TTL=126
Reply from 172.10.10.10: bytes=32 time=93ms TTL=126
Reply from 172.10.10.10: bytes=32 time=94ms TTL=126
```

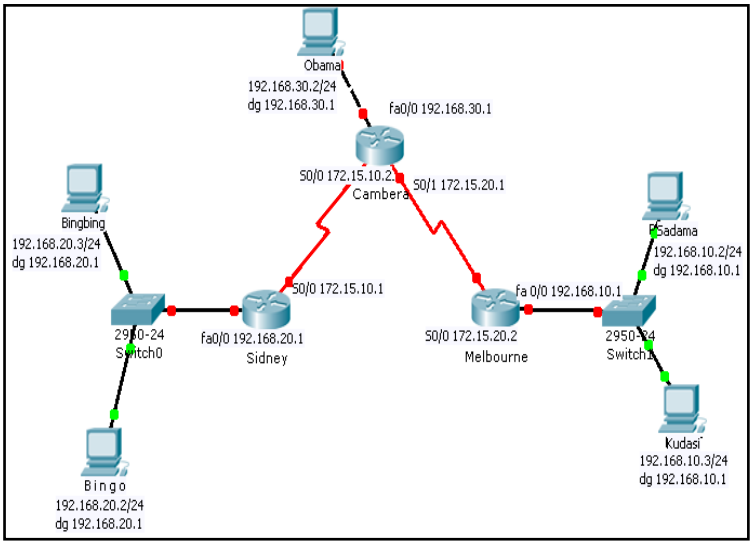
Jika sudah reply indikasinya koneksi sudah betul.

Latihan :

1. Desainlah seperti gambar dibawah ini, kemudian seting kedua router menggunakan EIGRP routing sehingga kedua pc dapat saling terkoneksi.



2. Desain seperti gambar dibawah, konfigur dengan EIGRP routing hinggasemua PC dapat saling terhubung, coba koneksinya dengan *ping*.



Selamat mencoba

MODUL PRAKTIKUM 06
VIRTUAL LOKAL AREA NETWORK (VLAN)

6.1. TUJUAN

1. Mahasiswa mampu memahami aplikasi VLAN.
2. Mahasiswa mampu mengkonfigurasi VLAN dengan switch CISCO
3. Mahasiswa mampu mengkonfigurasi inter-VLAN dengan Cisco Router

6.2. PERANGKAT YANG DIBUTUHKAN

Perangk at yang digunak an untuk prak tikum adalah sbb :

1. Windows XP SP3
2. Packet Tracer 53.0.0088
3. Switch managable

6.3. MATERI

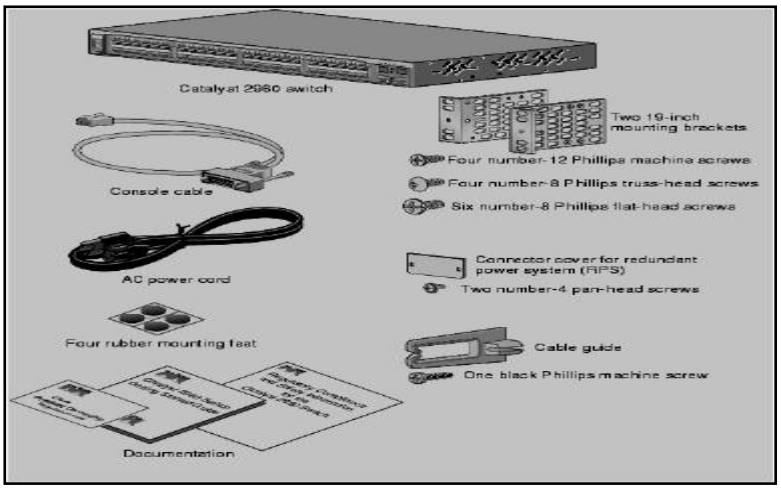
1. Virtual LAN

6.4. REFFERENSI

1. http://en.wikipedia.org/wiki/Vlan
2. http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/switch_c/xcvlan.htm
3. Wijaya, H. (2003). *Cisco Switch Pedoman untuk mendesain LAN.* Jakarta: PT. Elex Media Komputindo.
4. http://www.cramsession.com/articles/files/vlan-trunking-protocol-ba-9172003-0937.asp

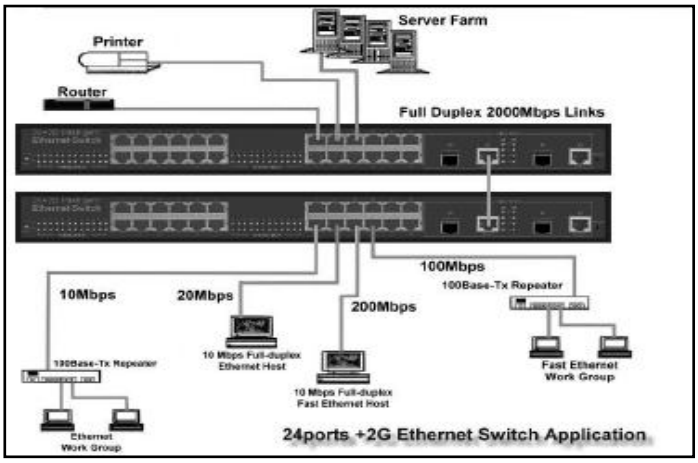
6.5. LANDASAN TEORI

Pengertian Switch Salah satu peralatan yang banyak digunakan dalam sebuah jaringan computer. Switch bekerja di layer 2 data link pada OSI model. Switch mempunyai ”otak” yang dapat mencatat daftar alamat MAC dari semua komputer yang terhubung dalam sebuah jaringan . Sehingga switch dapat mengurangi lalu lintas jaringan dengan hanya menyampaikan pesan tentang paket-paket yang tidak dikenali oleh tabel daftar alamat MAC.



Gambar 6.1. switch seri 2811 dengan perlengkapannya

Setiap port yang dimiliki oleh switch memiliki ”jalur” sendiri-sendiri sehingga tidak akan mengganggu port yang lainnya. Dan switch dapat menciptakan sebuah segmen jaringan tersendiri yang bersifat *private*. Sehingga sebuah switch dapat membentuk sebuah *Virtual Private Network* (VPN) dari port pengirim dan penerima sehingga jika ada sebuah komputer yang saling berkomunikasi lewat jalur VPN tersebut maka segmen lainnya tidak akan terganggu.



Gambar 6.2. Penggunaan switch dalam sebuah jaringan

Sebuah switch juga mempunyai sistem operasi seperti halnya Router, dan di dalamnya juga terdapat tingkatan akses seperti router. Tingkatan akses yang ada pada sebuah switch adalah :

1. **User Exec Mode**

   Tingkatan pertama yang kita jumpai saat terhubung dengan switch. Fasilitas yang disediakan hanya untuk melihat status dan konfigurasi switch.

2. **Privileged Exec Mode**

   Pada mode ini Anda dapat memeriksa konfigurasi yang ada pada sebuah switch.

3. **Global Configuration Mode**

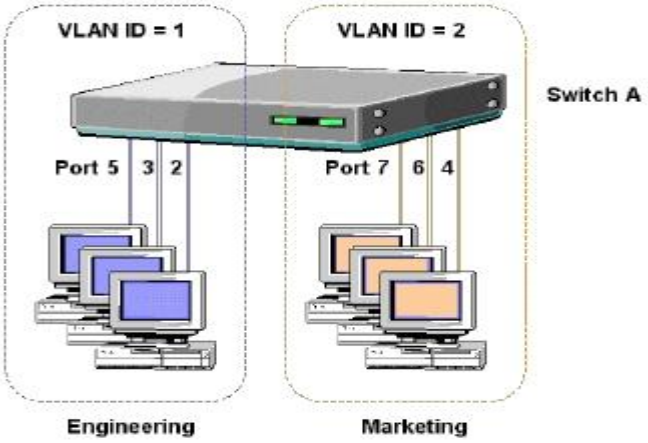
   Pada mode ini Anda dapat melakukan pengubahan konfigurasi pada sebuah switch.

4. **Interface Configuration Mode**

   Mode ini adalah mode konfigurasi untuk setiap interface yang ada pada sebuah switch, untuk memberikan alamat IP pada sebuah switch Anda dapat melakukannya dari sini. Secara garis besar perintah yang digunakan tidak jauh berbeda dengan perintah yang ada pada sebuah router .

6.5.1. Virtual LOKAL AREA NETWORK (VLAN)

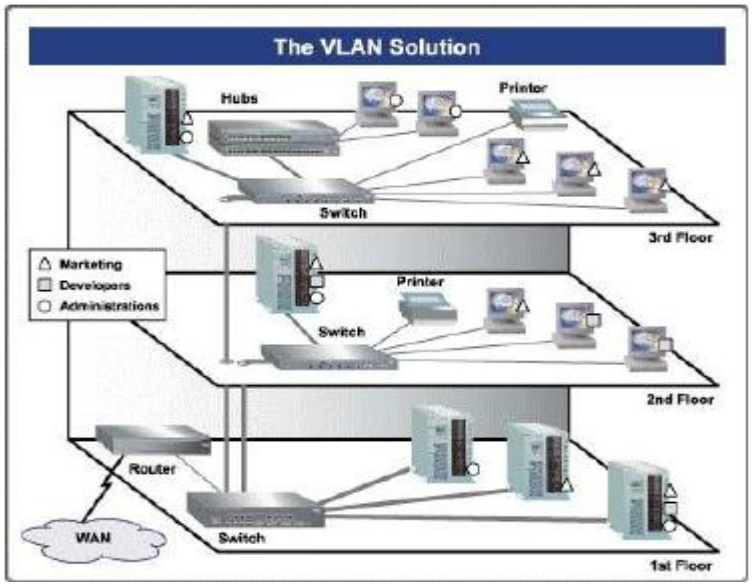
Sebuah fasilitas menarik disediakan oleh Cisco switch yakni Virtual LAN (VLAN) dimana port-port yang tersedia dalam sebuah switch dapat dibagi menjadi beberapa segmen virtual yang mempunyai ”tempat” dan ”jalur” sendiri. Fasilitas tersebut dapat di gunakan untuk mengurangi sinyal broadcast yang dipancarkan oleh masing-masing komputer untuk memperkenalkan dirinya ke dalam sebuah jaringan komputer. Apabila jaringan yang Anda kelola semakin berkembang dan besar maka sinyal broadcast ini akan sangat mengganggu lalu lintas paket di jaringan tersebut. Untuk itu Anda harus dapat menguranginya dengan membaginya menjadi kelompok yang lebih kecil, seperti *subnetting*. Jika subnetting membagi jaringan berdasarkan netwok ID-nya maka VLAN membagi jaringan secara **logika** berdasarkan **port** yang ada pada sebuah switch.



Gambar 6.3. Pembagian port pada switch untuk VLAN

Keuntungan menggunakan VLAN :

1. Meningkatkan jumlah sinyal broadcast tetapi mengurangi ukuran sinyal broadcast yang beredar dalam sebuah jaringan.
2. Mengurangi usaha yang harus Anda keluarkan untuk membuat sub jaringan baru.
3. Tidak perlu menambah peralatan jaringan baru karena jarigan dapat dibagi secara logika.
4. Meningkatkan kualitas kontrol pada lalu lintas di dalam jaringan.



Gambar 6.4. Penerapan VLAN dalam sebuah gedung

Pada ilustrasi diatas coba kita perhatikan pada lantai 1 disana terdapat 3 (tiga) buah server untuk masing-masing departemen (Marketing, Developers, dan Administrative). Ketiga server tersebut dapat dihubungi oleh komputer yang berada pada lantai yang

berbeda. Masing-masing komputer dikelompokkan dalam sebuah grup tersendiri dan masuk dalam VLAN. Antar komputer yang berbeda bagian mereka tidak dapat saling berhubungan tetapi semuanya dapat mengakses jaringan luar, dalam ilustrasi tersebut digambarkan sebagai WAN. Untuk yang masuk pada VLAN Marketing diberi tanda segitiga, yang masuk VLAN Developers diberi tanda segiempat, dan VLAN Administrative diberi tanda lingkaran. Sekalipun berbeda lantai komputer yang masuk dalam satu VLAN tetap bisa berhubungan begitu juga jika ada komputer yang berada dalam satu lantai tapi beda VLAN maka mereka tidak dapat saling berhubungan.

6.5.2. CARA KERJA VLAN

VLAN diklasifikasikan berdasarkan metode (tipe) yang digunakan untuk mengklasifikasikannya, baik menggunakan port, MAC addresses dsb. Semua informasi yang mengandung penandaan/pengalamatan suatu vlan (tagging) di simpan dalam suatu database (tabel), jika penandaannya berdasarkan port yang digunakan maka database harus mengindikasikan port-port yang digunakan oleh VLAN. Untuk mengaturnya maka biasanya digunakan switch/bridge yang manageable atau yang bisa di atur. Switch/bridge inilah yang bertanggung jawab menyimpan semua informasi dan konfigurasi suatu VLAN dan dipastikan semua switch/bridge memiliki informasi yang sama.

Switch akan menentukan kemana data-data akan diteruskan dan sebagainya atau dapat pula digunakan suatu software pengalamatan (bridging software) yang berfungsi mencatat/menandai suatu VLAN beserta workstation yang didalamnya untuk menghubungkan antar VLAN dibutuhkan router.

6.5.3. TIPE-TIPE VLAN

Keanggotaan dalam suatu VLAN dapat di klasifikasikan berdasarkan port yang di gunakan, MAC address, tipe protokol.

1. *Berdasarkan Port*

   Keanggotaan pada suatu VLAN dapat di dasarkan pada port yang di gunakan oleh VLAN tersebut. Sebagai contoh, pada switch dengan 8 port, port 1, 2, 3 dan 4 merupakan VLAN 1, port 5, 6 VLAN 2 dan port 7,8 VLAN 3

Tabel 6.1 Port dan VLAN

Port	1	2	3	4	5	6	7	8
VLAN	1	2	3	4	2	2	2	2

Kelemahannya adalah user tidak bisa untuk berpindah-pindah, apabila harus berpindah maka Network administrator harus mengkonfigurasikan ulang.

2. **Berdasarkan MAC Address**

Keanggotaan suatu VLAN didasarkan pada MAC address dari setiap workstation/computer yang dimiliki oleh user. Switch mendeteksi/mencatat semua MAC address yang dimiliki oleh setiap Virtual LAN. MAC address merupakan suatu bagian yang dimiliki oleh NIC (Network Interface Card) di setiap workstation.

Tabel 6.2. MAC address dan VLAN

MAC address	132516617738	272389579355	536666337777	24444125556
VLAN	1	2	2	1

Kelebihannya apabila user berpindah pindah maka dia akan tetap terkonfigurasi sebagai anggota dari VLAN tersebut.Sedangkan kekurangannya bahwa setiap mesin harus di konfigurasikan secara manual , dan untuk jaringan yang memiliki ratusan workstation maka tipe ini kurang efissien untuk dilakukan.

3. **Berdasarkan tipe protokol yang digunakan**

Keanggotaan VLAN juga bisa berdasarkan protocol yang digunakan.

Tabel 6.3. Protokol dan VLAN

Protokol	IPX	IP	IP	IPX	IPX
VLAN	1	2	2	1	1

4. Berdasarkan Alamat Subnet IP

   Subnet IP address pada suatu jaringan juga dapat digunakan untuk mengklasifikasi suatu VLAN.

Tabel 6.4. IP Subnet dan VLAN

IP subnet	202.10.10	110.10.12	23.12.10
VLAN	2	1	3

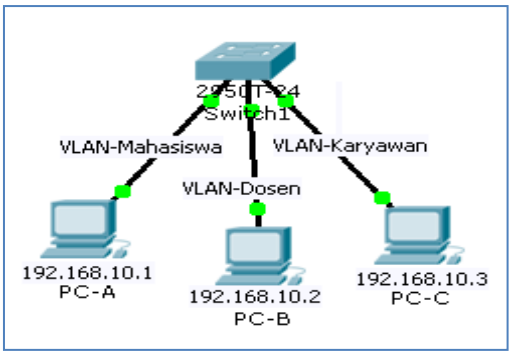
Konfigurasi ini tidak berhubungan dengan routing pada jaringan dan juga tidak mempermasalahkan funggsi router. IP address digunakan untuk memetakan keanggotaan VLAN. Keuntungannya seorang user tidak perlu mengkonfigurasikan ulang alamatnya di jaringan apabila berpindah tempat, hanya saja karena bekerja di layer yang lebih tinggi maka akan sedikit lebih lambat untuk meneruskan paket di banding menggunakan MAC addresses.

6.5.4. Mengkonfigurasi VLAN

Untuk mengkonfigurasi sebuah VLAN Anda harus masuk dalam mode *Global Configuration*. Urutan perintah yang harus Anda lalui untuk memasukkan sebuah port ke dalam VLAN adalah :

1. Beri nomor dan nama pada VLAN yang akan dibentuk.
2. Tentukan port yang akan di VLAN.
3. Masukkan port ke dalam VLAN.

1. Amati desain jaringan dibawah .



Gambar 6.1. Konfigurasi switch dengan 3 VLAN tanpa Router

2. Setting IP address PC-A, PC-B dan PC-C dengan NetID yang sama seperti pada gambar di atas.
3. Lakukan tes koneksi sebelum dilakukan VLAN
4. Setting switch, untuk membuat VLAN-Mhs, VLAN-Dosen dan VLAN-Karyawan seperti pada gambar di atas. (bila perlu buat catatan), dengan perintah sbb:

a. Penamaan vlan

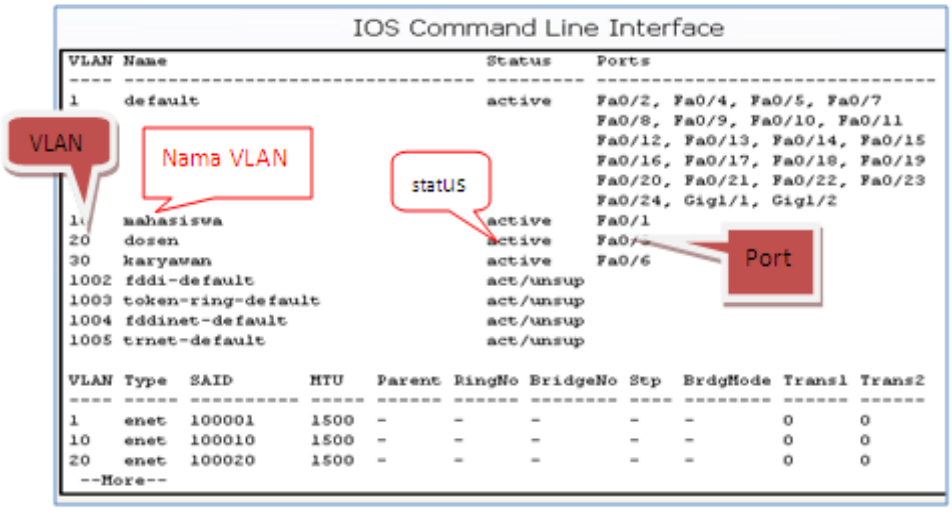
Dalam hal ini akan dibuat 3 buah VLAN yaitu VLAN-A, VLAN-B dan VLAN-C .

```
Switch>en
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#name VLAN-Mahasiswa
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name VLAN-Dosen
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name VLAN-Karyawan
Switch(config-vlan)#exit
Switch(config)#
```

Lihat hasil konfigurasi dengan perintah

```
Switch#show vlan
```

Hasilnya seperti pada gambar di bawah :



Gambar 6.2. VLAN sdh mahasiswa, dosen dan karyawan

b. Setting masing-masing interface Switch(config)#interface fastEthernet 0/1

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/6
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
```

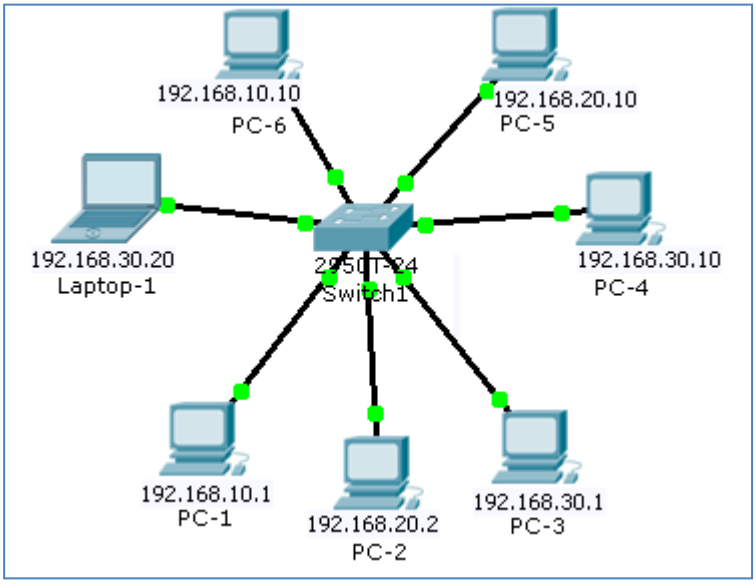
c. Untuk melihat konfigurasi, catat hasilnya

```
# show run
# show vlan
```

d. Tes koneksi antara PC-A, PC-B & PC-C, bandingkan dengan langkah 3. Sebelum dilakukan VLAN , buat kesimpulan sementara hasil percobaan anda.

Latihan :

1. Buat desain VLAN seerti dibawah ini



2. Lakukan konfigurasi seperti pada tabel di bawah :

   Tabel 6.5. konfigurasi jaringan VLAN

VLAN	Nama VLAN	No Port	Alokasi
10	Sales	1, 2, 3	Pc-1, Pc-6 & laptop-1
20	Admin	6, 9	Pc-2, Pc-5
30	Manajer	10, 15	Pc-4, Pc-5

3. Tunjukan pada dosen/ assisten, jika anda sudah selesai melakukan konfigurasi seperti pada tanel di atas.

MODUL PRAKTIKUM 07
INTER VIRTUAL LOKAL AREA NETWORK (INTER VLAN)

7.1. Tujuan

1. Memahami konsep Trunking pada VLAN
2. Memahami konsep VTP
3. Praktikan mampu mengkonfigurasi inter-VLAN dengan Cisco Router

7.2. PERANGKAT YANG DIBUTUHKAN

Perangk at yang digunak an untuk prak tikum adalah sbb :

1. Windows XP SP3
2. Simulator Packet Tracer 53.0.0088

7.3. MATERI

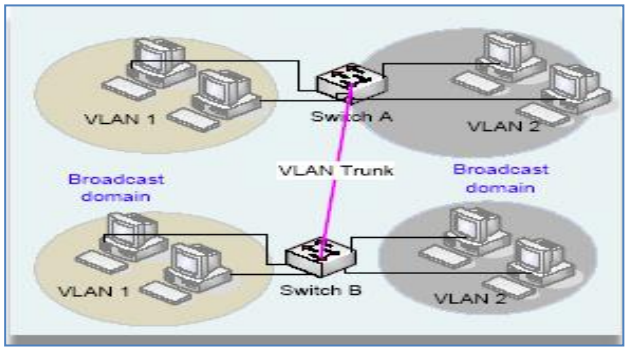
1. Inter Virtual LAN

7.4. REFFERENSI

1. Wijaya, H. (2003). *Cisco Switch Pedoman untuk mendesain LAN.* Jakarta: PT. Elex Media Komputindo.

7.5. LANDASAN TEORI INTER VLAN (Trunking VLAN)

Jika menggunakan VLAN dalam jaringan yang mempunyai beberapa Switch yang saling berhubungan antar VLAN, maka dibutuhkan VLAN Trunk. Switch memerlukan cara untuk mengidentifikasikan VLAN dari mana frame tersebut dikirim saat mengirim sebuah frame ke Switch lainnya. VLAN Trunking mengijinkan Switch memberikan tagging setiap frame yang dikirim antar switches sehingga switch penerima mengetahui termasuk dari VLAN mana frame tersebut dikirim. Idenya bisa digambarkan pada gambar diagram berikut ini:



Gambar 7.1. VLAN

Beberapa VLAN yang mempunyai anggota lebih dari satu Switch dapat didukung dengan adanya VLAN Trunking. Misal, saat Switch1 menerima sebuah broadcast dari sebuah piranti didalam VLAN1, ia perlu meneruskan broadcast ke Switch B. Sebelum mengirim frame, Switch A menambahkan sebuah header kepada frame Ethernet aslinya; heder baru tersebut mengandung informasi VLAN didalamnya. Saat Switch B menerima frame tersebut, ia mengetahui dari headernya bahwa frame tersebut berasal dari piranti pada VLAN1, maka SwitchB mengetahui bahwa ia seharusnya meneruskan broadcast frame hanya kepada port-port pada VLAN1 saja dari Switch tersebut.

Switch Cisco mendukung dua VLAN trunking protocol yang berbeda, Inter-Switch Link (ISL) dan IEEE 802.1q. keduanya memberikan Trunking dasar, seperti dijelaskan pada gambar diatas. Akan tetapi pada dasarnya keduanya sangatlah berbeda.

7.1.1. Best Practices jika menggunakan Virtual LAN

VLAN bukanlah harus diterapkan ke setiap jaringan LAN, akan tetapi bisa diterapkan pada jaringan dengan skala yang sangat besar pada jaringan enterprise dimana populasi host sangat besar – ratusan jumlahnya atau diperlukan suatu kelayakan adanya suatu alasan keamanan. Kalau memang harus digunakan VLAN maka haruslah diusahakan sesederhana mungkin, intuitive dan dukungan dokumentasi yang sangat rapi. Pendekatan yang dianjurkan dalam penggunaan VLAN adalah berdasarkan lokasi atau fungsi departemen. Hal ini dilakukan untuk membatasi *traffic broadcast* (broadcast domain) kedalam hanya masing2 segment VLAN saja. Jumlah VLAN yang didefinisikan pada Switch LAN seharusnya mencerminkan kebutuhan fungsional dan manajemen dalam suatu jaringan tertentu.

Beberapa *switches* dapat secara *transparent* saling dihubungkan dengan menggunakan VLAN Trunking. VLAN Trunking memberikan mekanisme tagging untuk mentransport VLAN secara transparent melewati beberapa Switches. VLAN didefinisikan dalam standards IEEE 802.3 dan IEEE 802.1q.

Seksi berikut ini memnjelaskan beberapa informasi tambahan mengenai protocol VLAN Trunking. Ada dua protocol VLAN Trunking utama saat ini, yaitu IEEE 802.1q dan Cisco ISL. Pemilihan protocol VLAN Trunking normalnya berdasarkan piranti platform Hardware yang digunakan. IEEE 802.1q adalah standard protocol VLAN Trunking yang memberikan tagging internal kedalam frame Ethernet yang ada sekarang. Hal ini dilakukan dalam hardware dan juga meliputi kalkulasi ulang header checksumnya. Hal

ini mengjinkan sebuah frame di tagging dengan VLAN dari mana datagram tersebut berasal dan menjamin bahwa frame dikirim kepada port didalam VLAN yang sama. Hal ini untuk menjaga kebocoran datagram antar VLAN yang berbeda.

ISL (*Inter Switch Link*) memberikan suatu *tagging external* yang dikemas disekitar frame asalnya.

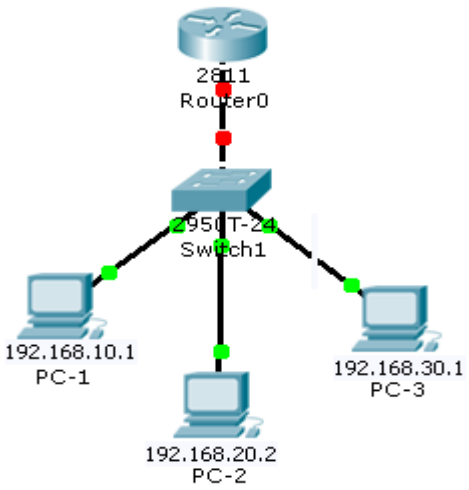
Saat menghubungkan beberapa Switch lewat sebuah Trunk perlu dipastikan bahwa kedua Switch yang terhubung VLAN Trunking tersebut mempunyai protocol VLAN Trunling yang sama. Penggunaan negosiasi automatis dari protocol VLAN Trunking adalah tidak dianjurkan karena bisa terjadi kemungkinan salah konfigurasi.

Untuk penerapan VLAN dengan Switch yang berskala besar sebuah protocol manajemen VLAN diperlukan misal VTP (*VLAN Trunking Protocol*). Protocol VTP memungkinkan VLAN didefinisikan sekali didalam suatu lokasi tunggal dan disinkronkan kepada Switch2 lainnya di dalam administrative domain yang sama.

Penerapan VLAN setidaknya dirancang dengan sangat bagus dan mudah dimanage. Dokumentasinya haruslah sangat rapi dan akurat dan dijaga selalu update agar membantu kegiatan support jaringan. Normalnya VLAN tidaklah dianjurkan untuk jaringan kecil (kurang dari 100 user pada satu lokasi), akan tetapi untuk **business dengan skala menengah dan besar,** VLAN adalah sangat mendatangkan keuntungan yang besar. Satu hal yang pelu diingat bahwa dalam penerapan VLAN ini, komunikasi antar VLAN yang berbeda haruslah di *routed*. Dan jika dibutuhkan suatu interkoneksi VLAN kecepatan tinggi maka penggunaan **Switch Layer 3 yang sangat performa** adalah sangat diperlukan. Menghubungkan beberapa VLAN antara Switch yang berbeda, penggunaan protocol VLAN Trunking seperti ISL atau IEEE802.1q adalah diperlukan. Pastikan bahwa Switch2 tersebut mempunyai dukungan protocol VLAN Trunking yang sama.

7.6. Konfigurasi Trunking VLAN

1. lakukan setting IP address di masing-masing PC dan tambahkan .



Gambar 7.1. VLAN dengan Router

Nama PC	Ip Address	Gateway	Netmask
PC A	192.168.1.2	192.168.1.1	255.255.255.0
PC B	192.168.2.2	192.168.2.1	255.255.255.0

2. Lakukan tes koneksi antara PC-1, PC-2 & PC-3 sebelum anda membagi VLAN pada switch & catat hasilnya.
3. Tambahkan setting di Switch untuk kabel yang terhubung ke Router (trunk) dengan instruksi :

```
Switch#conf t
Switch(config)#interface fastEthernet 0/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#
```

3. Setting router, agar bisa dilakukan interkoneksi antar VLAN.

a. **Konfigurasi pada satu interface di Router**

```
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>
```

```
Router>enable
Router#conf t
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#exit
```

b. Penambahan sub-interface, ini sesuai dengan banyaknya VLAN yang akan ditangani. Berhubung pada kasus di atas hanya 3 VLAN, maka perlu dibuat 3 sub-interface .

```
Router(config)#interface fastEthernet 0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.11
Router(config-subif)#encapsulation dot1Q 11
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.12
Router(config-subif)#encapsulation dot1Q 12
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#exit
Router(config)#^Z
```

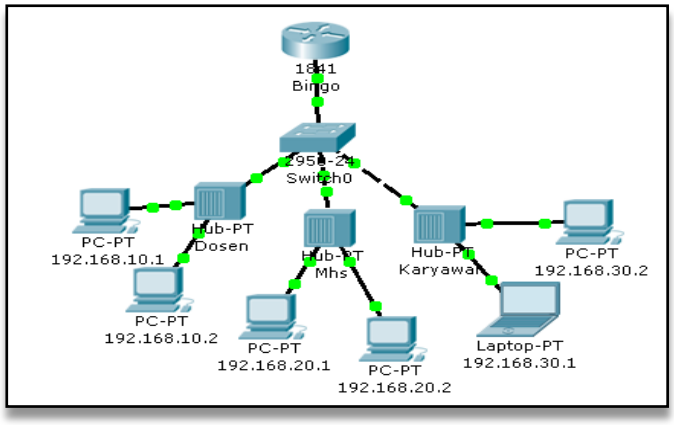
c. Cek konfigurasi

```
Router# show run
Router# show ip interface brief
Router# show ip route
```

4. Lakukan tes koneksi dari PC A ke PC B dengan perintah ping dan traceroute,

Latihan

1. Amati gambar dibawah ini dan lakukan konfigurasi sehingga antar VLAN bisa saling berhubungan.



Ujilah dengan menggunakan perintah ping ke masing-masing VLAN.

MODUL PRAKTIKUM 08

Access Control Lists (ACLs)

8.1. Tujuan

Setelah melakukan kegiatan ini, praktikan di harapkan memiliki kemampuan :

1. Memahami aplikasi access-list.
2. Mampu mengkonfigurasi access-list dengan Cisco Router
3. Mampu menerapkan access-list pada suatu jaringan
4. Menggambarkan fungsi dari firewall

8.2. Perangkat keras yang digunakan

1. Perangkat personal komputer / laptop

8.3. Materi

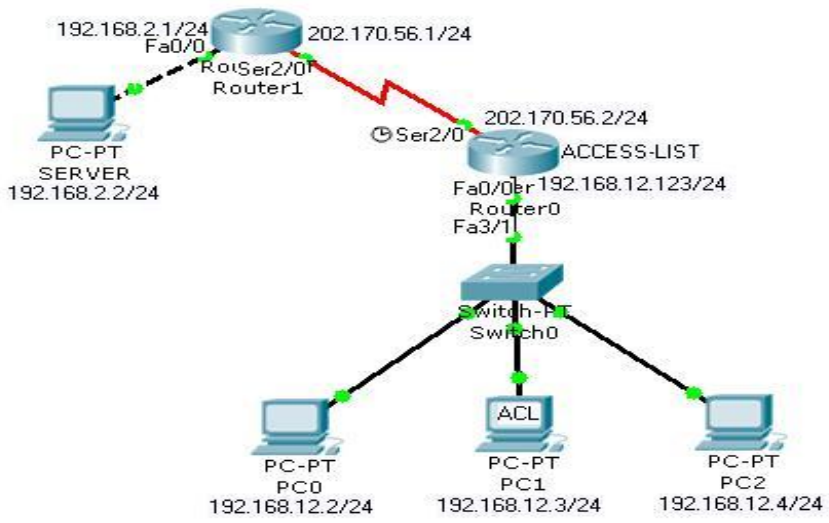
1. Access List Control (ACL)

8.4. Referensi

1. Graziani, R.; Johnson, A. 2008. *Routing Protocols and Concepts– CCNA Exploration Companion Guide* . Cisco Press.
2. Cisco CCNA dan jaringan komputer

8.5. LANDASAN TEORI

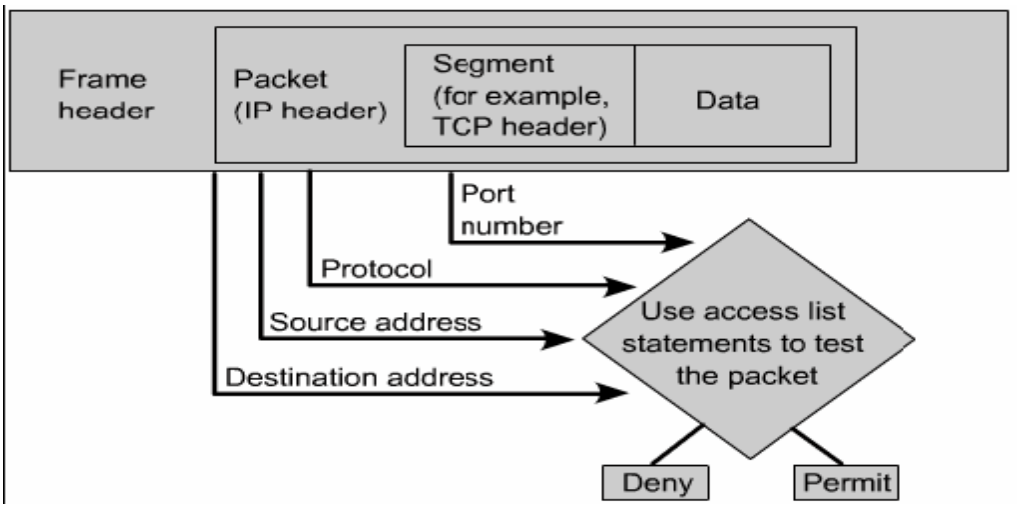
ACL (Access List Control) merupakan daftar kondisi yang digunakan untuk mengetes trafik jaringan yang mencoba melewati interface router. Daftar ini memberitahu router paket-paket mana yang akan diterima atau ditolak. Penerimaan dan penolakan berdasarkan kondisi tertentu.



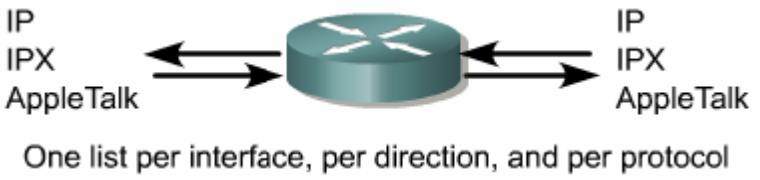
Gambar 8.1 Acces Control List

Untuk mem-filter trafik jaringan, ACL menentukan jika paket itu dilewatkan atau diblok pada interface router. Router ACL membuat keputusan berdasarkan alamat asal, alamat tujuan, protokol, dan nomor port.

ACL harus didefinisikan berdasarkan protokol, arah atau port. Untuk mengontrol aliran trafik pada interface, ACL harus didefinisikan setiap protokol pada interface. ACL kontrol trafik pada satu arah dalam interface. Dua ACL terpisah harus dibuat untuk mengontrol trafik inbound dan outbound. Setiap interface boleh memiliki banyak protokol dan arah yang sudah didefinisikan. Jika router mempunyai dua interface diberi IP, AppleTalk dan IPX, maka dibutuhkan 12 ACL. Minimal harus ada satu ACL setiap interface.



Gb. 8.1 Cisco ACL memeriksa paket pada header upper-layer



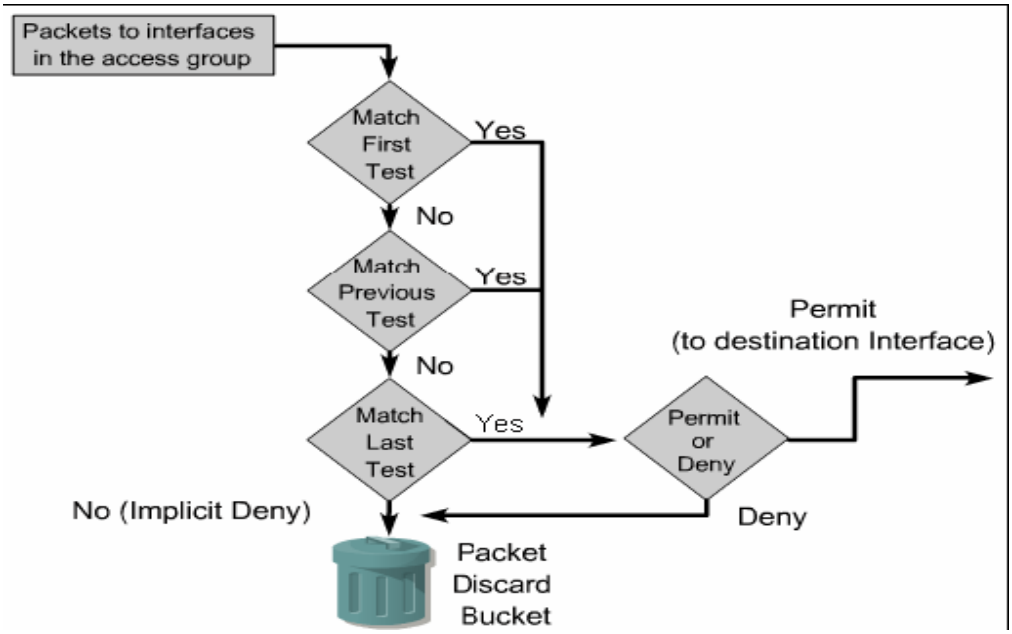
Gb.8.2 Grup access list dalam Router

Berikut ini adalah fungsi dari ACL:

1. Membatasi trafik jaringan dan meningkatkan unjuk kerja jaringan. Misalnya, ACL memblok trafik video, sehingga dapat menurunkan beban jaringan dan meningkatkan unjuk kerja jaringan.
2. Mengatur aliran trafik. ACL mampu memblok update routing. Jika update tidak dibutuhkan karena kondisi jaringan, maka bandwidth dapat dihemat.
3. Mampu membrikan dasar keamanan untuk akses ke jaringan. Misalnya, host A tidak diijinkan akses ke jaringan HRD dan host B diijinkan.
4. Memutuskan jenis trafik mana yang akan dilewatkan atau diblok melalui interface router. Misalnya, trafik email dilayani, trafik telnet diblok.
5. Mengontrol daerah-daerah dimana klien dapat mengakses jaringan.

6. Memilih host-hots yang diijinkan atau diblok akses ke segmen jaringan. Misal, ACL mengijinkan atau memblok FTP atau HTTP.

1.2 Cara kerja ACL



Gambar 8.4 Cara kerja ACL

Keputusan dibuat berdasarkan pernyataan/statement cocok dalam daftar akses dan kemudian menerima atau menolak sesuai apa yang didefinisikan di daftar pernyataan. Perintah dalam pernyataan ACL adalah sangat penting, kalau ditemukan pernyataan yang cocok dengan daftar akses, maka router akan melakukan perintah menerima atau menolak akses. Pada saat frame masuk ke interface, router memeriksa apakah alamat layer 2 cocok atau apakah frame broadcast. Jika alamat frame diterima, maka informasi frame ditandai dan router memeriksa ACL pada interface inbound. Jika ada ACL, paket diperiksa lagi sesuai dengan daftar akses. Jika paket cocok dengan pernyataan, paket akan diterima atau ditolak. Jika paket diterima di interface, ia akan diperiksa sesuai dengan table routing untuk menentukan interface tujuan dan di-switch ke interface itu. Selanjutnya router

memriksa apakah interface tujuan mempunyai ACL. Jika ya, paket diperiksa sesuai dengan daftar akses. Jika paket cocok dengan daftar akses, ia akan diterima atau ditolak. Tapi jika tidak ada ACL paket diterima dan paket dienkapsulasi di layer 2 dan di-forward keluar interface device berikutnya.

1.3 Membuat ACL

Ada dua tahap untuk membuat ACL. Tahap pertama masuk ke mode global config kemudian memberikan perintah **access-list** dan diikuti dengan parameter-parameter. Tahap kedua adalah menentukan ACL ke interface yang ditentukan.

Dalam TCP/IP, ACL diberikan ke satu atau lebih interface dan dapat memfilter trafik yang masuk atau trafik yang keluar dengan menggunakan perintah **ip access-group** pada mode configuration interface. Perintah **access-group** dikeluarkan harus jelas dalam interface masuk atau keluar. Dan untuk membatalkan perintah cukup diberikan perintah **no access-list list-number**.

Aturan-aturan yang digunakan untuk membuat access list:

- Harus memiliki satu access list per protokol per arah.
- Standar access list harus diaplikasikan ke tujuan terdekat.
- Extended access list harus harus diaplikasikan ke asal terdekat.
- Inbound dan outbound interface harus dilihat dari port arah masuk router.
- Pernyataan akses diproses secara sequencial dari atas ke bawah sampai ada yang cocok. Jika tidak ada yang cocok maka paket ditolak dan dibuang.
- Terdapat pernyataan **deny any** pada akhir access list. Dan tidak kelihatan di konfigurasi.
- Access list yang dimasukkan harus difilter dengan urutan spesifik ke umum. Host tertentu harus ditolak dulu dan grup atau umum kemudian.
- Kondisi cocok dijalankan dulu. Diijinkan atau ditolak dijalankan jika ada pernyataan yang cocok.
- Tidak pernah bekerja dengan access list yang dalam kondisi aktif.
- Teks editor harus digunakan untuk membuat komentar.

- Baris baru selalu ditambahkan di akhir access list. Perintah **no access-list x** akan menghapus semua daftar.
- Access list berupa IP akan dikirim sebagai pesan ICMP host unreachable ke pengirim dan akan dibuang.
- Access list harus dihapus dengan hati-hati. Beberapa versi IOS akan mengaplikasikan default deny any ke interface dan semua trafik akan berhenti.
- Outbound filter tidak akan mempengaruhi trafik yang asli berasal dari router local.

Protocol	Range
IP	1-99, 1300-1999
Extended IP	100-199, 2000-2699
AppleTalk	600-699
IPX	800-899
Extended IPX	900-999
IPX Service Advertising Protocol	1000-1099

Gb. **8.5** protokol dengan ACL berdasar nomor

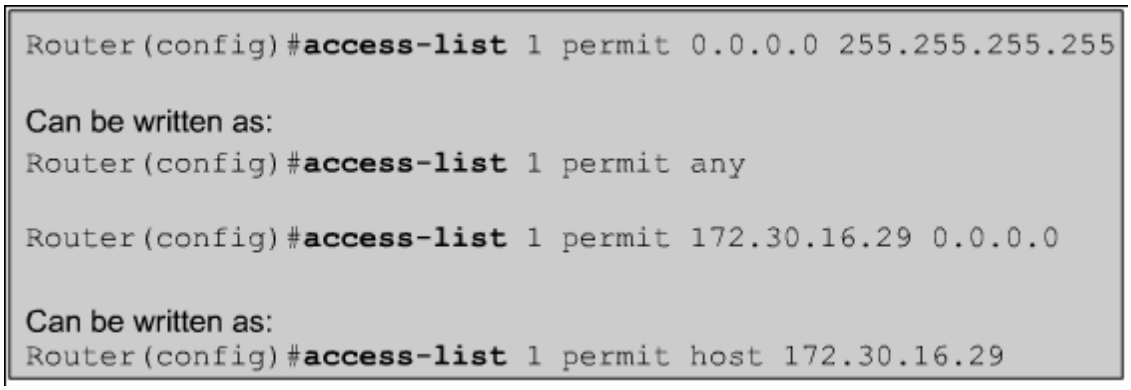
```
Router(config)#access-list 2 deny 172.16.1.1
Router(config)#access-list 2 permit 172.16.1.0 0.0.0.255
Router(config)#access-list 2 deny 172.16.0.0 0.0.255.255
Router(config)#access-list 2 permit 172.0.0.0
0.255.255.255
Router(config)#interface e0
Router(config-if)#ip access-group 2 in
```

Gambar 8.6 perintah access-group

1.4 Fungsi dari wildcard mask

Wildcard mask panjangnya 32-bit yang dibagi menjadi empat octet. Wildcard mask adalah pasangan IP address. Angka 1 dan 0 pada mask digunakan untuk mengidentifikasikan bit-bit IP address. Wildcard mask mewakili proses yang cocok dengan ACL mask-bit. Wildcard mask tidak ada hubungannya dengan subnet mask.

Wildcard mask dan subnet mask dibedakan oleh dua hal. Subnet mask menggunakan biner 1 dan 0 untuk mengidentifikasi jaringan, subnet dan host. Wildcard mask menggunakan biner 1 atau 0 untuk memfilter IP address individual atau grup untuk diijinkan atau ditolak akses. Persamaannya hanya satu dua-duanya sama-sama 32-bit.



Gambar 8.7 any dan host Option

Ada dua kata kunci di sini yaitu **any** dan host. **Any** berarti mengganti 0.0.0.0 untuk IP address dan 255.255.255.255 untuk wildcard mask. **Host** berarti mengganti 0.0.0.0 untuk mask. Mask ini membutuhkan semua bit dari alamat ACL dan alamat paket yang cocok. Opsi ini akan cocok hanya untuk satu alamat saja.

1.5 Verifikasi ACL

Untuk menampilkan informasi interface IP dan apakah terdapat ACL di interface itu gunakan perintah **show ip interface**. Perintah **show access-lists** untuk menampilkan isi dari ACL dalam router. Sedangkan perintah **show running-config** untuk melihat konfigurasi access list.

```
Router#show ip interface
FastEthernet0/0 is up, line protocol is down
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 2
Serial0/0 is down, line protocol is down
  Internet address is 200.200.2.1/24
  Broadcast address is 255.255.255.255
  MTU is 1500 bytes
```

Gambar 8.8 standar ACL

```
Router#show access-lists
Standard IP access list 2
 deny   172.16.1.1
 permit 172.16.1.0, wildcard bits 0.0.0.255
 deny   172.16.0.0, wildcard bits 0.0.255.255
 permit 172.0.0.0, wildcard bits 0.255.255.255
Extended IP access list 101
 permit tcp 192.168.6.0 0.0.0.255 any eq telnet
 permit tcp 192.168.6.0 0.0.0.255 any eq ftp
 permit tcp 192.168.0.0 0.0.0.255 any eq ftp-data
Router#
```

Gambar 1.9 pernyataan standar ACL

2. Access Control Lists

Standar access-list digunakan untuk mendefinisikan standar ACL dengan nomor antara 1 sampai 99 (dan juga antara 1300 sampai 1999 pada IOS yang baru).

```
access-list 2 deny   172.16.1.1
access-list 2 permit 172.16.1.0  0.0.0.255
access-list 2 deny   172.16.0.0  0.0.255.255
access-list 2 permit 172.0.0.0   0.255.255.255
```

- Access list number range of 1 - 99 and 1300 - 1999
- Filter only on source IP address
- Wildcard masks
- Applied to interface closest to destination

Gambar 2.1 Pernyataan standar ACL

Untuk Cisco IOS Software Release 12.0.1, standar ACL dimulai dengan 1300 sampai 1999 untuk menyediakan kemungkinan ACL 798. Pada gambar di atas ACL pertama, menunjukkan tidak ada wildcard mask. Dan default mask 0.0.0.0 diguanakan. Sintak lengkap perintah ACL adalah:

Router(config)#**access-list** *access-list-number* **deny permit remark** *source* [*source-wildcard*] [**log**]

Kata kunci remark membuat access list lebih muda untuk dimengerti. Setiap remark dibatasi sampai 100 karakter. Sebagai contoh:

Router(config)#access-list 1 permit 172.69.2.88

Lebih mudah lagi dengan entri yang lebih spesifik:

Router(config)#access-list 1 remark Permit only Jones workstation through access-list 1 permit 171.69.2.88

Perintah no untuk menghapus ACL:

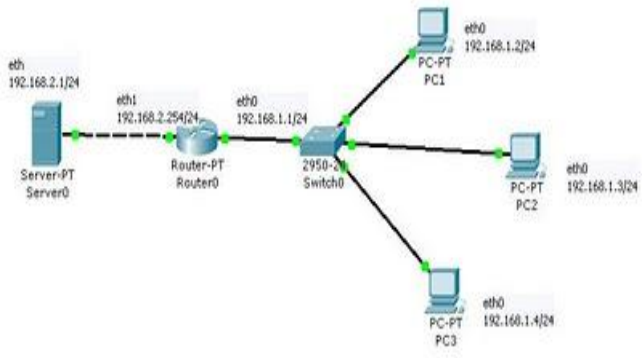
Router(config)#no access-list *access-list-number*

Perintah ip access-group ACL dihubungkan dengan interface:

Router(config-if)#ip access-group {*access-list-number* | *access-list-name*} {*in* | *out*}

Latihan

Desainlah seperti gambar di bawah



kita akan membuat rule bahwa untuk client dengan nama pc1 dan pc3 dapat melakukan koneksi dengan server tetapi untuk client dengan nama pc2 dilarang untuk melakukan koneksi degan server. dengan adanya masalah diatas dapat dipecahkan dengan menggunakan access-list.

Berikut detail dari konfigurasi komputer client dan cisco router.

Konfigurasi pc1

Ethernet adapter Local Area Connection:

IP Address. . . . . : 192.168.1.2

Subnet Mask . . . . . : 255.255.255.0

Default Gateway . . . . . : 192.168.1.1

Konfigurasi pc2

Ethernet adapter Local Area Connection:

IP Address. . . . . : 192.168.1.3

Subnet Mask . . . . . : 255.255.255.0

Default Gateway . . . . . : 192.168.1.1

Konfigurasi pc3

Ethernet adapter Local Area Connection:

IP Address. . . . . : 192.168.1.4

Subnet Mask . . . . . : 255.255.255.0

Default Gateway . . . . . : 192.168.1.1

Konfigurasi server

Ethernet adapter Local Area Connection:

IP Address. . . . . : 192.168.2.1

Subnet Mask . . . . . : 255.255.255.0

Default Gateway . . . . . : 192.168.2.254

Konfigurasi cisco router

Router>

Router>enable

Router#configure terminal

Router(config)#interface ethernet0

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#no shut

Router(config-if)#exit

Router(config)#interface ethernet1

Router(config-if)#ip address 192.168.2.254 255.255.255.0

Router(config-if)#no shut

Router(config-if)#^Z (Ctrl+z)

Router#ping 192.168.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Router#ping 192.168.2.254

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.254, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Konfigurasi ACL

Router#configure terminal

Router(config)#interface fastethernet 0/0

Router(config-if)#ip access-group 1 in

Router(config-if)#exit

Router(config)#access-list 1 deny 192.168.1.3 255.255.255.0

Router(config)#access-list 1 permit any

Router(config)#exit

Router#show access-list

Standard IP access list 1

deny 0.0.0.3 255.255.255.0 (2 match(es))

permit any (8 match(es))

untuk mengembalikan access seperti sebelumnya :

Router#no access-list 1

Hasil uji coba

dari pc1

Router#ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=60ms TTL=241

Reply from 192.168.2.1: bytes=32 time=60ms TTL=241

Reply from 192.168.2.1: bytes=32 time=60ms TTL=241

Reply from 192.168.2.1: bytes=32 time=60ms TTL=241

Reply from 192.168.2.1: bytes=32 time=60ms TTL=241

Ping statistics for 192.168.2.1: Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),

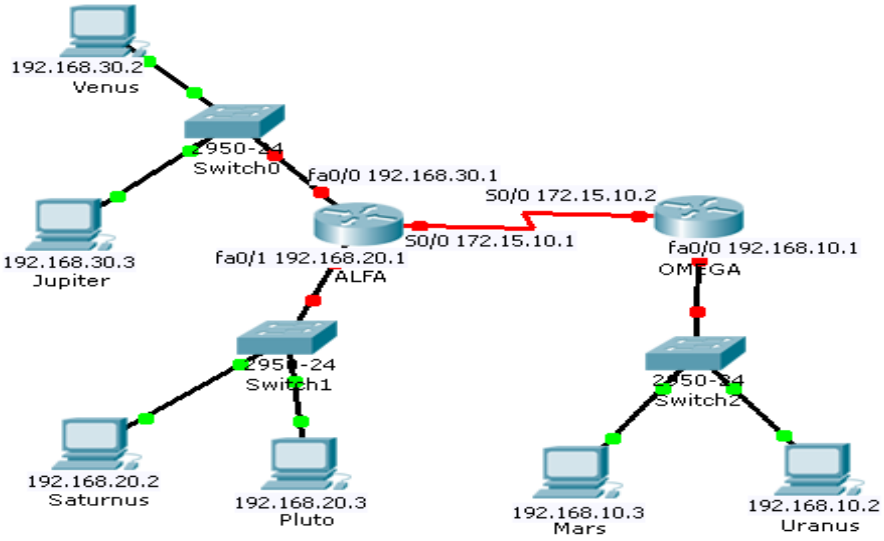
Approximate round trip times in milli-seconds:
Minimum = 50ms, Maximum = 60ms, Average = 55ms

dari pc2
Router#ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.2.1:
Packets: Sent = 5, Received = 0, Lost = 5 (100% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

dari pc3
Router#ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=60ms TTL=241
Reply from 192.168.2.1: bytes=32 time=60ms TTL=241
Reply from 192.168.2.1: bytes=32 time=60ms TTL=241
Reply from 192.168.2.1: bytes=32 time=60ms TTL=241
Reply from 192.168.2.1: bytes=32 time=60ms TTL=241
Ping statistics for 192.168.2.1: Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 50ms, Maximum = 60ms, Average = 55ms

Tugas Pratikum

1. Desainlah seperti gambar dibawah ini. Kemudian setinglah kedua router menggunakan dynamic routing sehingga semua pc dapat saling terkoneksi.



2. Bisakah semua koneksi tersebut .
3. Cobalah *ping* ke router **OMEGA** dari semua **HOST**. Bisakah?
4. Buat access-list standar, agar semua host dengan **network ID 192.168.30.0/24 tidak bisa terkoneksi** ke router **OMEGA**.
5. Buat **extended access-list**, agar yang bisa konek ke router **OMEGA hanya saturnus.**