Praktikum Jaringan Komputer

giving and caring the world

TELKOM POLYTECHNIC
BANDUNG

Penyusun
Henry Rossi Andrian

Editor
Dahliar Ananda

KATA PENGANTAR

Assalamu'alaikum Wr. Wb

Kami bersyukur atas Izin Allah SWT karena dengan karunia-Nya c*ourseware* ini akhirnya dapat diselesaikan.

Dengan segala kerendahan hati kami mencoba untuk menyusun *courseware* ini . Kami mengharapkan dengan membaca *courseware* ini pembaca memperoleh gambaran apa dan bagaimana menjadi seorang administrator jaringan itu.

Namun tak ada gading yang tak retak, banyak kekurangan dan kesalahan yang dapat ditemui di sini. Untuk pengembangan selanjutnya kami mengharapkan saran dan kritik dari pembaca.

Semoga *courseware* ini dapat memberikan manfaat dan membantu seluruh civitas akademika Politeknik Telkom dalam memahami dan mengikuti materi perkuliahan di Politeknik Telkom

Terakhir kami mengucapkan terima kasih atas segenap perhatiannya

Wassalamu'alaikum Wr. Wb.

Bandung, April 2010

Christanto Triwibisono
Wakil Direktur I
Bidang Akademik & Pengembangan

DAFTAR ISI

1 Pengenalan Jaringan Komputer dan Pengkabelan

Overview

Modul berikut menjelaskan tentang konsep dasar jaringan yang berisi tentang prinsip komunikasi data, koneksi jaringan komputer dan pengkabelan. Dalam materi pengkabelan akan fokus pada kabel UTP untuk membuat kabel straight through, crossover dan rollover.

Tujuan

1. Memahami dasar jaringan komputer
2. Mengenal media transmisi jaringan computer.
3. Mampu membuat kabel jenis straight-through, crossover serta rollover
4. Mempraktikkan pemasangan kabel ke konektor sesuai jenisnya

1.1 Dasar Teori

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama. Tujuan dari jaringan komputer adalah:

- Membagi sumber daya: contohnya berbagi pemakaian printer, CPU, memori, harddisk.
- Komunikasi: contohnya surat elektronik, instant messaging, chatting
- Akses informasi: contohnya web browsing

Agar dapat mencapai tujuan yang sama, setiap bagian dari jaringan komputer meminta dan memberikan layanan (service). Pihak yang meminta layanan disebut klien (client) dan yang memberikan layanan disebut pelayan (server). Arsitektur ini disebut dengan sistem client-server, dan digunakan pada hampir seluruh aplikasi jaringan komputer.
Dengan memasyarakatnya Internet dan dipasarkannya sistem operasi Windows95 oleh Microsoft, menghubungkan beberapa komputer baik komputer pribadi (PC) maupun server dengan sebuah jaringan dari jenis LAN (*Local Area Network*) sampai WAN (*Wide Area Network*) menjadi sebuah hal yang biasa. Demikian pula dengan konsep "downsizing" maupun "lightsizing" yang bertujuan menekan anggaran belanja khususnya peralatan komputer, maka sebuah jaringan merupakan satu hal yang sangat diperlukan. Dalam makalah ini akan dibahas sebagian komponen yang diperlukan untuk membuat sebuah jaringan komputer.

1.2 Prinsip Komunikasi Data

Jaringan komputer digunakan untuk melakukan tukar menukar atau komunikasi data.
Komponen-komponen dalam komunikasi data adalah sebagai berikut:

1.2.1 Komputer Host

Komputer host adalah komputer yang berfungsi sebagai penyebar informasi atau data. Host dapat berupa komputer mainframe atau komputer mini. Host yang berupa mainframe bekerja dengan menggunakan peralatan yang disebut dengan Front and Processor (FEP), yang merupakan komputer mini untuk mengelola komunikasi data dari jaringan

1.2.2 Komputer Receiver

Komputer ini berfungsi sebagai penerima informasi

1.2.3 Data

Data adalah objek dari proses komunikasi yang terjadi pada jaringan.

1.2.4 Protokol Komunikasi

Protokol komunikasi adalah peraturan-peraturan yang diterapkan dalam jaringan dengan tujuan untuk mengatur komunikasi data. Banyaknya protokol komunikasi menyebabkan dibutuhkannya suatu alat (tools) yang disebut dengan Gateway, untuk menterjemahkan protokol sehingga menjadi compatible agar komunikasi data dijaringan dapat berjalan dengan baik.

1.2.5 Komponen Transmisi

Setelah memastikan komputer host dan receiver berjalan dengan baik, serta memilih protokol komunikasi, dilakukan implementtasi terhadap komponen transmisi, seperti kabel penghubung, modem, dan sebagainya.

1.3 Koneksi Jaringan dan Internet

Di akhir milenium kedua perkembangan internet sungguh revolusioner karena internet telah merasuki segala aspek kehidupan manusia. Dengan internet kita dapat melakukan bisnis lebih efisien, melakukan komunikasi antara manusia dengan manusia, manusia dengan komputer atau komputer dengan komputer. Internet sendiri adalah sebuah sistem yang memberikan informasi yang terorganisir dan terkelola dengan baik. Jadi internet itu sendiri adalah sebuah sistem yang terstruktur dan terorganisir.

Untuk memahami bagaimana hubungan internet dengan TCP/IP, mula-mula kita harus mendefinisikan konsep *protokol* dan *standar*. Tentu saja kita dituntut untuk proaktif mengamati dan mempelajari standar-standar yang dikeluarkan oleh organisasiorganisasi yang berkompeten dalam pengembangan internet menjadi suatu standar bersama. Mengapa? Dapat dibayangkan jika ratusan organisasi baik ilmiah maupun komersil membuat standarnya sendiri-sendiri akan menjadi tidak mungkin bila mengaplikasikan perangkat komunikasi yang berbeda standar satu dengan yang lainnya.

Jaringan internet pada dasarnya adalah merupakan jaringan komunikasi data yang terbangun dari komputer individual atau kumpulan-kumpulan jaringan komputer skala kecil yang saling terintegrasi (interkoneksi). Maka dapat disimpilkan agar computer dapat terkoneksi kedalam suatu jaringan baik

secara local area maupun internet maka komponen dasar yang diperlukan adalah :

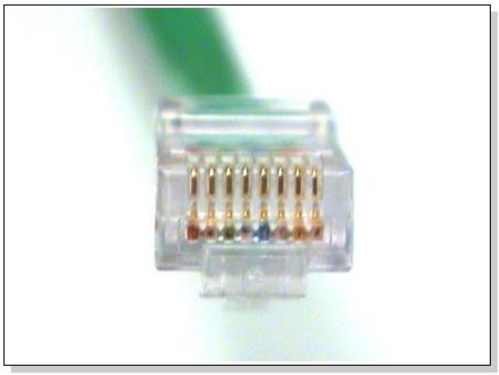
1.3.1 Koneksi Fisik (Physical Connection)

Koneksi fisik sebagai penghubung antara adapter card (Modem, NIC) dari komputer kedalam suatu jaringan. Transfer data yang mengalir dalam koneksi fisik menggunakan transfer sinyal melalui media (kabel atau gelombang)
Komponen yang diperlukan agar terjadinya koneksi fisik adalah :
perangkat keras computer dan perangkat jaringan.

1.3.1.1 Perangkat Keras Komputer

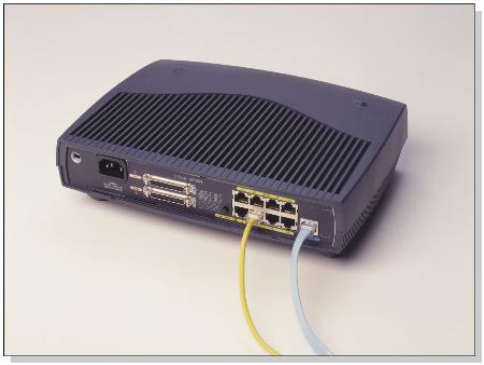
Gambar 1.1 Personal Computer

3.1.1.1 Perangkat Jaringan



Gambar 1.2 RJ 45 Connector

Gambar 1.3 RJ45 jack



Gambar 1.4 HUB

Gambar 1.5 Network Interface Card

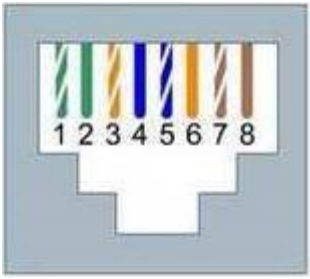
1.4 Pengkabelan

1.4.1 Straight-Through

Jenis kabel ini digunakan untuk menghubungkan antara workstation dengan hub/switch. Kabel ini juga memiliki 4 pairs (8 wire) dimana setiap pin antara ujung satu dengan ujung lainnya harus sama. Maksudnya, bila salah satu ujung memakai standard T568-A maka ujung satunya harus memakai T568-A juga. Begitu pula sebaliknya, jika salah satu ujung menggunakan standard T568-B, ujung satunya juga harus memakai standard yang sama.

Pin#	Function	Wire Color
1	Transmit	White/Green
2	Receive	Green/White
3	Transmit	White/Orange
4	Not Used	Blue/White
5	Not Used	White/Blue
6	Receive	Orange/White
7	Not Used	White/Brown
8	Not Used	Brown/White

Tabel 1.1 Standar Pengkabelan T568-A

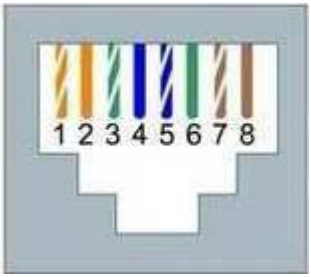


Gambar 1.6 Struktur T568-A

Pin#	Function	Wire Color
1	Transmit	White/Orange
2	Receive	Orange/White

3	Transmit	White/Green
4	Not Used	Blue/White
5	Not Used	White/Blue
6	Receive	Green/White
7	Not Used	White/Brown
8	Not Used	Brown/White

Tabel 1.2 Standar Pengkabelan T568-B



Gambar 1.7 Struktur T568-B

1.4.2 Cross Over

Merupakan jenis kabel yang digunakan untuk menghubungkan antar workstation atau antar hub/switch. Kabel jenis ini menggunakan standard T568-A pada salah satu ujung, dan T568-B pada ujung lainnya.

1.4.3 Roll Over

Digunakan untuk koneksi antara sebuah workstation ke port console pada sebuah router atau switch. Standard yang digunakan adalah T568-A pada salah satu ujung dan ujung lainnya urutan T568-A tinggal di roll (dibalik). Demikian juga jika yang dipakai adalah standard T568-B.

1.5 Praktikum

1. Pembuatan kabel
    a) Siapkan kabel UTP dan RJ 45 sebagai interfacenya
    b) Potong jaket ujung kabel kira-kira 1.5 cm dengan cutter atau gunting, dan buanglah jaket tersebut. Hati-hati dalam mengupas jaket, jangan sampai kabel yang ada di dalamnya ikut terpotong.
    c) Untwist atau buka lilitan masing-masing pasangan kabel

d) Untuk membuat kabel straight-trough, crossover maupun rollover, lihat standard T568-A atau T568-B
e) Sesuaikan masing-masing jenis kabel dengan standardnya, lalu luruskan hingga memungkinkan untuk bisa dimasukkan ke dalam RJ 45
f) Bila sudah dimasukkan ke RJ 45, crimpinglah dengan menggunakan peralatan yang ada agar kabel menjadi permanen dan tidak mudah goyah
g) Periksa terlebih dahulu urutan kabelnya sebelum dicrimping, karena kabel yang sudah dicrimping tidak dapat dicabut lagi. Artinya jika kita salah mengurutkan pasangan atau memasukkan ke RJ 45 nya kurang sempurna, besar kemungkinan kabel tidak dapat dipakai
h) Laporkan hasil kabel yang telah Anda buat

2. Test kabel
   a) Kabel yang sudah dicrimping dapat dideteksi kesalahannya dengan memakai cable tester (misal : Fluke 620 LSN CableMeter)
   b) Bila cable tester tidak ada, pasangkan kabel tersebut dari NIC ke hub (bila jenisnya straight-through) dan antar workstation jika jenis kabelnya adalah crossover.
   c) Pekailah perintah *ping* untuk uji coba kabel. Apabila koneksi dapat terbentuk, berarti pembuatan kabel Anda sudah benar. Sebaliknya, jika koneksi tak dapat terbentuk, berarti ada kesalahan dalam proses cabling.
   d) Amati hasilnya dan catat

3. Pemasangan jaringan menggunakan kabel UTP :
   a) Pasang NIC yang tipe medianya kabel UTP ke slot di motherboard PC yang akan disambungkan
   b) Persiapkan kabel UTP crossover dan straight-trough dan pasang ke NIC masing-masing.
   c) Cobalah pasang UTP straight-trough untuk PC ke hub dan UTP crossover dari PC ke PC
   d) Pastikan bahwa driver LAN card sudah terinstall
   e) Beri IP address yang unik untuk tiap workstation. Address tersebut bisa diisi dengan cara mengklik kanan Network Neighborhood. Tanyakan kepada asisten mengenai pengisian IP lebih lanjut

f) Bila jaringan telah terbentuk, coba jalankan aplikasi yang berhubungan dengan jaringan
g) Amati hasilnya dan catat pada system dengan bagian yang berbeda-beda.

2 Pengenalan dan Pemasangan Jaringan Komputer

Overview

Modul ini berisi pengenalan perangkat yang digunakan dalam jaringan komputer. Contoh sederhana membangun jaringan komputer menggunakan perangkat-perangkat yang sederhana.

Tujuan

1. Memahami cara kerja perangkat jaringan.
2. Mampu mengkonfigurasi perangkat jaringan, dalam bab ini tidak termasuk konfigurasi router.

2.1 Dasar Teori

Untuk mengimplementasikan jaringan komputer kita memerlukan perangkat jaringan. Jaringan komputer melibatkan 3 macam perangkat jaringan antara lain :

- *End devices*
- *Intermediary devices*

2.1.1 End Devices

End devices adalah perangkat jaringan yang menjadi titik awal informasi dibuat dan menjadi akhir dari perjalanan informasi(tujuan pengiriman data). contoh perangkat komputer yang bertype end devices antara lain PC, notebook, Ponsel, PDA phone atau perangkat semisal yang lainnya. Pada end devices ada perangkat yang bertindak sebagai alat yang digunakan end devices untuk berkomunikasi di jaringan, yaitu :

2.1.1.1 Network Interface Card

Dalam memilih network interface card, ada beberapa pertimbangan yang harus diperhatikan. Pertimbangan-pertimbangan ini sangat penting untuk diperhatikan, yaitu :

- Tipe jaringan seperti Ethernet LANs, Token Ring, atau Fiber Distributed Data Interface (FDDI).
- Tipe Media seperti Twisted Pair, Coaxial, Fiber-Optic, dan Wireless.
- Tipe Bus seperti ISA dan PCI.

Gambar 2.1Ethernet Card

Gambar 2.2 Ethernet Card PCMCIA

2.1.2 Intermediary Devices

Perangkat jaringan yang termasuk dalam kategori ini memiliki beberapa sifat antara lain :

- Mampu melakukan *regenerate* dan *retransmit* sinyal data
- Menyimpan informasi tentang jalur pengiriman paket.
- Memberikan pemberitahuan tentang adanya error dan kegagalan dalam jaringan.
- Mengklasifikasikan paket data berdasarkan jenisnya.
- Mengijinkan atau melarang paket yang lewat berdasarkan konfigurasi keamanan.

Tidak semua perangkat intermediary memiliki semua fungsi diatas. Berikut akan dibahas lebih detail tentang beberapa perangkat intermediary.

2.1.2.1 Repeater

Sebuah jaringan komputer mempunyai keterbatasan daya jangkau. Jaringan yang menggunakan kabel dengan tipe UTP (Cat 5) hanya memiliki daya jangkau hingga 100 meter. Oleh karena itu dibutuhkan sebuah alat yang dapat berfungsi untuk memperpanjang jangkauan jaringan dari medium komputer tersebut. Alat yang dimaksud tersebut adalah *repeater*. *Repeater* berguna untuk membangkitkan dan menguatkan sinyal-sinyal yang mengalir pada jaringan komputer sehingga jaringan komputer dapat menjangkau jarak yang lebih jauh.

Gambar 2.3Cable Tester

2.1.2.2 Hub

Hub memiliki prinsip kerja yang sama dengan *repeater* yakni berfungsi untuk menguatkan sinyal-sinyal pada jaringan komputer. Namun yang membedakannya dengan *repeater* adalah pada *hub* terdapat *port-port* yang lebih banyak sehingga *hub* dikenal juga dengan *multiport repeater*. Ada 2 alasan di dalam menggunakan *hub* yakni *hub* digunakan sebagai titik pusat koneksi dari sambungan jaringan (titik pusat dari topologi *star*). Alasan lainnya adalah apabila ada masalah dengan kabel jaringan yang menghubungkan sebuah komputer, maka masalah tersebut tidak akan mempengaruhi jaringan (hal ini berbeda bila menggunakan topologi *bus* dimana apabila ada kabel jaringan yang bermasalah maka akan berdampak pada jaringan). Dengan menggunakan *hub* maka topologi jaringan secara fisik akan berbentuk seperti topologi *star*. Namun topologi jaringan secara logik akan berbentuk seperti topologi *bus.* Hal ini disebabkan cara kerja *hub* yakni dalam satu waktu tidak semua komputer yang terhubung dapat berkomunikasi. Selain itu setiap ada pengiriman data dari satu komputer ke komputer lainnya maka data ini akan di-*broadcast* atau disebarkan ke setiap komputer yang terhubung melalui *hub* ini.

Gambar 2.4 HUB

2.1.2.3 Bridge

Bridge merupakan alat yang bekerja untuk menghubungkan 2 segmen LAN atau lebih. Tujuan utama dari penggunaan *bridge* adalah untuk memfilter *traffic* antar kedua segmen LAN. Jadi apabila ada data yang hanya ditujukan untuk komputer yang terletak pada segmen LAN yang sama, maka data tersebut tidak diteruskan ke segmen LAN yang lainnya. *Bridge* dapat melakukan filtrasi terhadap data yang akan melewatinya dengan menggunakan alamat *Media Access Control* (MAC) yang merupakan alamat permanen unik yang ada pada setiap *network interface*. Setiap data yang akan melewati *bridge*, maka *bridge* akan mengecek terlebih dahulu *frame* yang ada pada data. Di dalam *frame* terkandung alamat MAC tujuan, apabila alamat MAC tujuan masih berada di dalam segmen LAN yang sama dengan pengirim data, maka data tersebut tidak akan diteruskan ke segmen lainnya.

Gambar 2.5 Bridge

2.1.2.4 Switch

Switch juga dikenal sebagai *multiport bridge*. *Switch* juga melakukan penyaringan terhadap data yang melewatinya dengan menggunakan alamat MAC. Dengan adanya filtrasi pada *switch* ini maka jaringan komputer akan lebih efisien. Hal ini disebabkan pada *switch*, data akan langsung disalurkan ke *port* yang menghubungkan dengan komputer yang merupakan tujuan dari data tersebut.

Walaupun *switch* memiliki jumlah *port* yang banyak (mirip *hub*) namun *switch* memiliki kelebihan lainnya dibandingkan *hub*. Dalam satu waktu yang sama, hubungan komunikasi dapat terjadi lebih dari satu (pada *hub* hal ini tidak bisa dilakukan). Misalnya komputer A sedang berkomunikasi dengan komputer B, maka pada waktu yang sama pula komputer C dapat berkomunikasi dengan komputer D. Sehingga dengan adanya fasilitas ini, pengiriman data akan lebih cepat dan efisien.

Gambar 2.6 Switch

2.1.2.5 Router

Router bekerja untuk melakukan *routing* yaitu menentukan jalur terbaik yang akan dilalui sebuah paket data berdasarkan pada alamat IP yang terdapat pada data yang melewatinya. Karena kemampuannya mengarahkan (*routing*) paket data berdasarkan pada alamat IP, *router* ini menjadi alat yang cukup penting di dalam sebuah jaringan internet. *Router* bekerja dengan cara menganalisa alamat IP dari paket data yang masuk. Berdasarkan hasil analisa tersebut, *router* memutuskan apakah data tersebut perlu diteruskan atau tidak. Apabila perlu diteruskan, maka *router* juga dapat memilihkan rute terbaik bagi paket data tersebut dan kemudian meneruskan ke *port* yang sesuai. Selain fungsi-fungsi dasar, *router* juga memiliki kelebihan lainnya. Kelebihan lainnya adalah dapat memfiltrasi data yang melewatinya berdasarkan ACL (*Access Control List*), menjembatani komunikasi antar protokol yang berbeda (misalnya antara protokol IP dengan protokol IPX) dan juga antar teknologi yang berbeda-beda (misalnya antara *Token Ring* dengan *Ethernet*).

Gambar 2.7 Router

2.1.2.6 Modem

Suatu perangkat keras yang bertugas merubah suara digital menjadi analog, begitu juga dengan sebaliknya. Modem biasa digunakan untuk komunikasi komputer satu dengan komputer yang lainnya dengan media transmisi jaringan telpon biasa. Selain itu modem indentik digunakan baik dalam personal komputer maupun pada jaringan sebagai alat menyambungkan kepada jaringan MAN, WAN dan internet.

Gambar 2.8 Modem

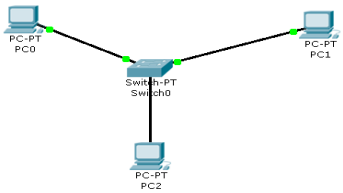
2.2 Praktikum

3.1.2 Peralatan yang dibutuhkan

1) Personal Komputer
2) Switch / Hub

3.1.3 Langkah-langkah praktikum

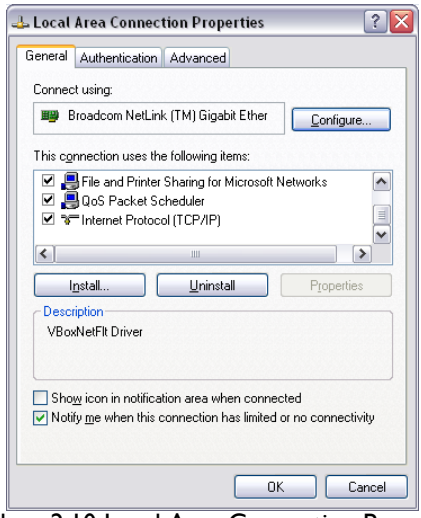
1. Buatlah Jaringan komputer sesuai dengan skema berikut :



Gambar 2.9 Skema Jaringan

2. Buatlah konfigurasi jaringan sesuai dengan langkah-langkah berikut :

Pastikan NIC sudah terpasang dan instalasi driver sudah berhasil. Jika sudah, maka NIC dapat dilihat di Control Panel>>System>>Hardware>>Device Manager. Masuk ke Properties dari My Network Places, sehingga akan keluar tampilan seperti berikut. Pilihan General untuk melakukan pengaturan pokok, Authentification untuk mengatur bagaimana mengenali komputer lain, sedangkan Advanced untuk setting filter dan firewall. Untuk saat ini kita akan mencoba setting pokok, maka pilih General>>Internet Protocol (TCP/IP).



Gambar 2.10 Local Area Connection Properties

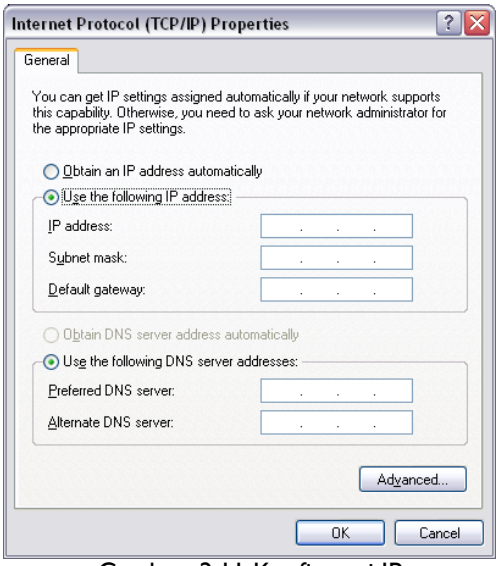
Form yang muncul akan seperti yang terlihat di gambar berikut, isikan ke dalamnya:

- IP Address : alamat komputer Anda pada network
- Subnet Mask : kelas addressing yang dipakai pada network
- Default Gateway : komputer pada jaringan yang berfungsi menghubungkan jaringan intranet dengan segmen jaringan di luar
- Fungsi Advanced juga tersedia untuk pengaturan mendetil, silakan dicoba mempelajarinya sendiri.

Masukkan konfigurasi
PC 1 :

IP Address : 192.168.0.2
Subnet Mask : 255.255.255.0

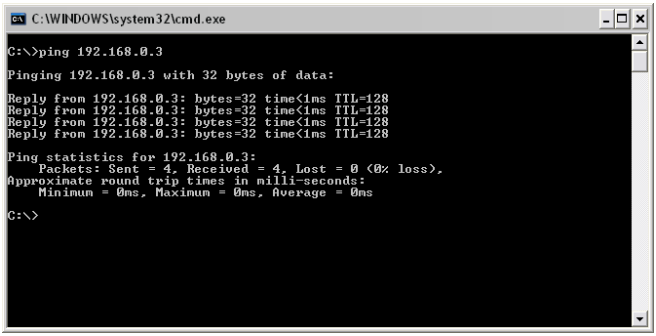
PC 2
IP Address : 192.168.0.3
Subnet Mask : 255.255.255.0



Gambar 2.11 Konfigurasi IP

3. Lakukan Tes koneksi dengan menggunakan perintah ping seperti ilustrasi berikut.

   Dari PC 1 lakukan ping ke PC 2 dengan perintah ”ping 192.168.0.3”



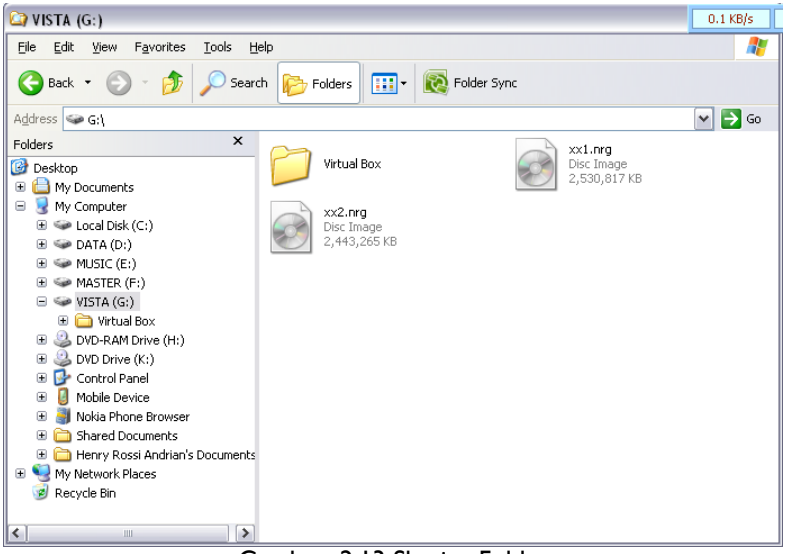
Gambar 2.12 Tes Koneksi

4. Lakukan Sharing Folder

   a. Buka Windows Explorer dengan langkah

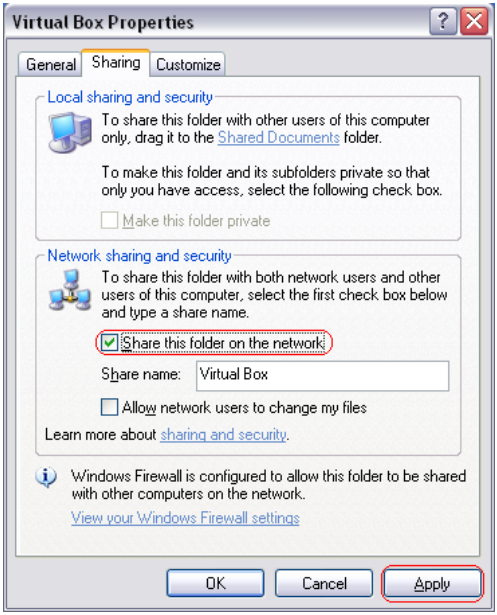
      i. Klik kanan pada start →pilih explore .

      ii. Tekan tombol windows+E secara bersamaan.



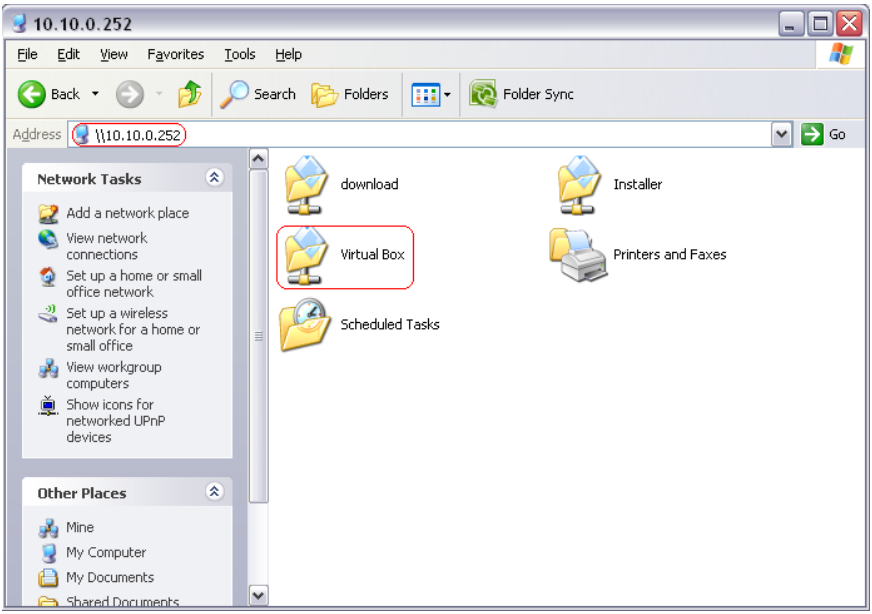
Gambar 2.13 Sharing Folder

b. Klik kanan pada folder yang ingin dishare →pilih sharing and security



Gambar 2.14 Share Folder Properties

c. Klik check box "Share this folder on the network" kemudian klik apply. Folder telah di share dan bisa diakses oleh semua computer di jaringan.
d. Untuk mengakses dari computer yang lain ulangi langkah pertama untuk membuka explorer.
e. Masukkan address dari folder yang di share. Missal IPnya adalah 10.10.0.252 maka masukkan alamat tersebut di address explorer seperti gambar di bawah ini. Folder yang telah dishare akan muncul pada explorer tersebut.



Gambar 2.15 View Shared Folder

3 Monitoring Jaringan

Overview

Modul ini berisi mengenai bentuk bentuk segmen TCP dan UDP yang ada di transport. Untuk melihat bentuk segmen TCP dan UDP yang ada dalam jaringan kita memerlukan tools, di dalam modul ini kita akan membahas salah satu tools jaringan yaitu wireshark.

Tujuan

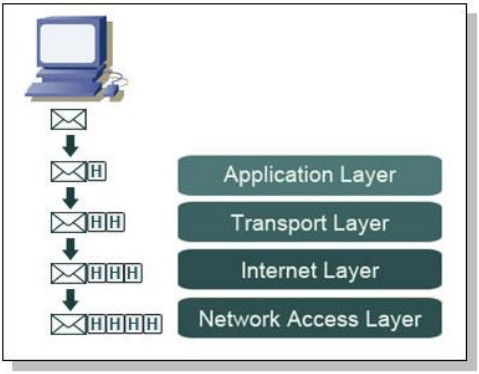
1. Memahami konsep paket TCP dan UDP.
2. Mampu memonitoring paket TCp yang ada di jaringan.

3.1 Dasar Teori

Dalam konsep komunikasi data suatu jaringan komputer, ada mekanisme pengiriman data dari komputer sumber ke komputer tujuan dimana proses pengiriman paket data tersebut sampai dengan benar ke komputer yang dituju. Tentunya dalam proses pengiriman yang terjadi tidak semudah yang dipikirkan. Alasan pertama, komputer tujuan berada jauh dari komputer sumber sehingga paket data yang dikirimkan bisa saja hilang atau rusak di tengah jalan.
Alasan lainnya, mungkin komputer tujuan sedang menunggu/mengirimkan paket data dari/ke komputer yang lain. Tentunya paket data yang akan dikirimkan diharapkan sampai dengan tepat tanpa terjadi kerusakan. Untuk mengatur mekanisme komunikasi data tersebut dibutuhkan pengaturan proses pengiriman data yang dikenal sebagai protocol. Protokol di sini adalah sebuah perangkat lunak yang melekat pada setiap sistem operasi tertentu.

3.2 Layer TCP/IP

Protokol TCP/IP (Transmision Control Protocol / Internet Protocol) merupakan sekumpulan layer yang di desain untuk melakukan fungsi-fungsi komunikasi data pada sebuah jaringan komputer, masing-masing layer bertanggung jawab atas bagian-bagian tertentu dari proses komunikasi data, sehingga masing-masing layer memiliki tugas yang berbeda satu sama lainya, dimana suatu layer tidak perlu mengetahi kerja dari layer yang lain selama masih dapat melakukan proses masing-masing.
Protokol TCP/IP memiliki sifat yang sangat fleksibel, sehingga dapat dengan mudah untuk di implementasikan pada berbagai platform komputer dan interface jaringan. Karena tidak melakukan spesifikasi terhadap suatu platform komputer atau interface jaringan tertentu.



Gambar 3.1TCP/IP Layer

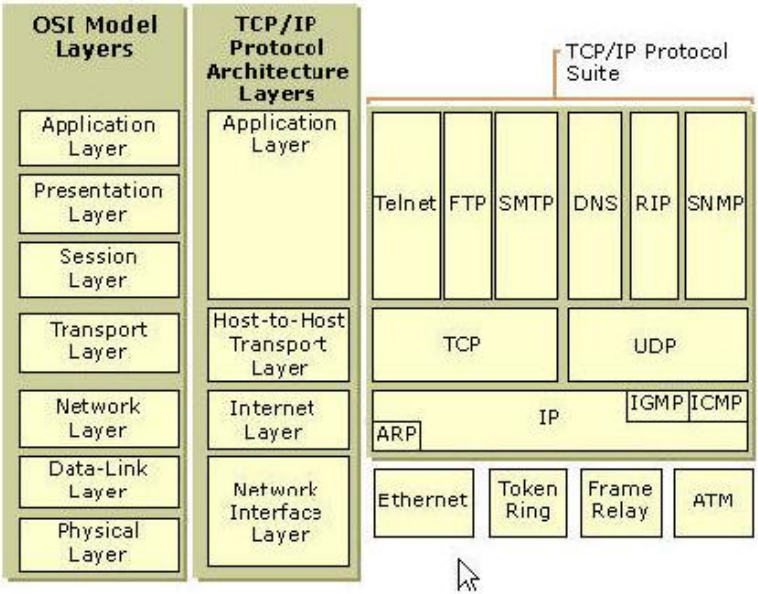
Fungsi dari masing-masing layer :

Aplication Layer, layer ini terdapat pada bagian teratas dari susunan layer, disini semua aplikasi yang mengunakan protokol TCP/IP ditempatkan

Transport Layer, layer ini bertanggung jawab mengadakan komunikasi antara dua host atau komputer. Layer ini mengatur aluran informasi dan mungkin menyediakan pemeriksaan error. Data dibagi kedalam beberapa paket yang dikirim ke internet layer dengan sebuah header. Header mengandung alamat tujuan, alamat sumber dan checksum. Checksum diperiksa oleh mesin penerima untuk melihat apakah paket tersebut ada yang hilang pada rute.

Internetwork Layer, layer ini bertanggung jawab untuk komunikasi antara mesin. Layer ini meng-encapsul paket dari transport layer ke dalam IP datagrams dan menggunakan algoritma routing untuk menentukan kemana datagaram harus dikirim. Masuknya datagram diproses dan diperiksa kesahannya sebelum melewatinya pada Transport layer.

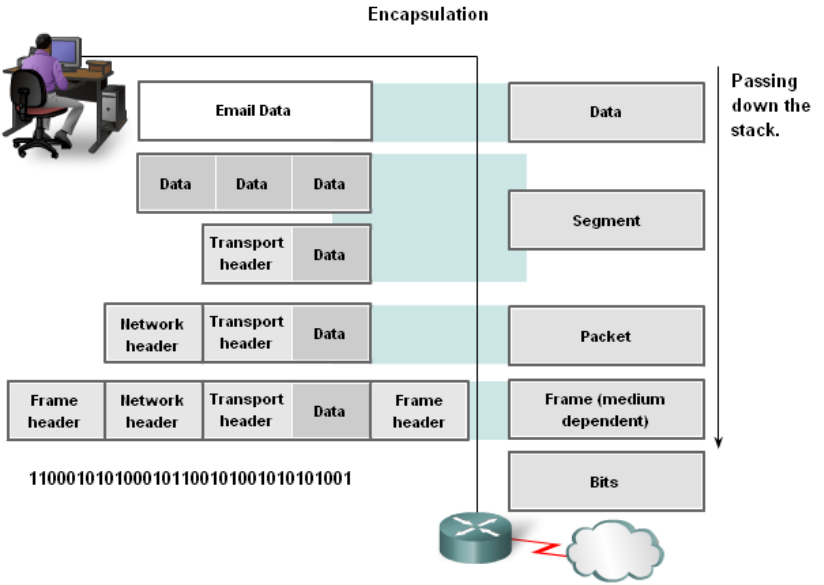
Network Interface Layer, adalah level yang paling bawah dari susunan TCP/IP. Layer ini adalah device driver yang memungkinkan datagaram IP dikirim ke atau dari physical network. Jaringan dapat berupa sebuah kabel, Ethernet, frame relay, Token ring, ISDN, ATM jaringan, radio, satelit atau alat lain yang dapat mentransfer data dari sistem ke sistem. Layer network interface adalah abstraksi yang memudahkan komunikasi antara multitude arsitektur network.



Gambar 3.2 Layer Jaringan Komputer

3.3 Enkapsulasi

Jika suatu protocol menerima data dari protocol lain di layer atasnya, ia akan menambahkan informasi tambahan miliknya ke data tersebut. Informasi ini memiliki fungsi yang sesuai dengan fungsi protocol tersebut. Setelah itu, data ini diteruskan lagi ke protocol pada layer dibawahnya. Hal yang sebaliknya terjadi jika suatu protocol menerima data dari protocol lain yang berada pada layer dibawahnya. Jika data ini dianggap valid, protocol akan melepas informasi tambahan tersebut, yang berada pada layer di atasnya.



Gambar 3.3 Enkapsulasi

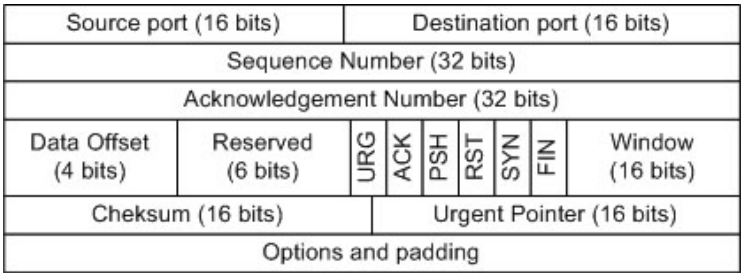
Lapisan/layer terbawah, yaitu *Network Interface layer* bertanggung jawab mengirim dan menerima data ke dan dari media fisik. Media fisiknya dapat berupa kabel,
serta optik atau gelombang radio. Karena tugasnya ini, protocol pada layer ini harus mampu menerjemahkan sinyal listrik menjadi data digital yang dimengerti komputer, yang berasal dari peralatan lain yang sejenis.

Lapisan/layer protocol berikutnya ialah *Internet Layer*. Protocol yang berada pada
layer ini bertanggung jawab dalam proses pengiriman paket ke alamat yang tepat. Pada layer ini terdapat tiga macam protocol, yaitu IP, ARP dan ICMP.
IP (*Internet Protocol*) berfungsi untuk menyampaikan paket data ke lamat yang tepat. ARP (*Address Resolution Protocol*) ialah protocol digunakan untuk menemukan alamat hardware dari host/komputer yang terletak pada network yang sama. Sedangkan ICMP (*Internet Control Message Protocol*) ialah protocol yang digunakan untuk mengirimkan pesan & melaporkan kegagalan pengiriman data Layer berikutnya yaitu *Transport layer* berisi protocol yang bertanggung jawab untuk mengadakan komunikasi antara dua host/komputer. Kedua

protocol tersebut ialah TCP (*Transmission Control Protocol*) dan UDP (*User Datagram Protocol*). Layer teratas, ialah *Application Layer*. Pada layer inilah terletak semua aplikasi yang menggunakan protocol TCP/IP ini.

3.4 Protokol Data Unit TCP

Sebagaimana telah dijelaskan di atas, TCP harus berkomunikasi dengan IP pada lapisan di bawahnya (dengan menggunakan metode IP yang telah dijelaskan pada bab sebelumnya) dan aplikasi pada layer di atasnya (menggunakan ULP TCP).. TCP juga harus berkomunikasi dengan implementasi TCP lainnya dalam jaringan. Untuk melakukan ini, digunakan protocol data unit (PDU), yang telak kita sebut sebagai segman TCP. Layout PDU TCP (biasanya disebut sebagai header) direpresentasikan pada gambar berikut



Gambar 3.4 Segmen TCP

Bidang-bidang tersebut adalah sebagai berikut:

Source port : field 16-bit yang mengidentifikasi pemakai lokal TCP (biasanya sebuah aplikasi upper layer).

Destination port : field 16-bit yang mengidentifikasi mesin remote pemakai TCP.

Sequence number : nomor yang menandakan posisi blok di dalam message secara keseluruhan. Nomor ini juga digunakan antara dua implementasi TCP untuk menyediakan initial sequence number (ISS) yang dikirim.

Acknowledgement number : nomor yang menandai nomor urutan yang berikutnya yang diperlukan. Dengan kata lain, sequence number ini merupakan sequence number data tarakhir yang dikirim kemudian ditambah 1 kemudian dikirim kembali ke mesin pengirim.

Data offset : 32-bit word yang ada di dalam header TCP. Field ini digunakan untuk mengidentifikasi awal field data.

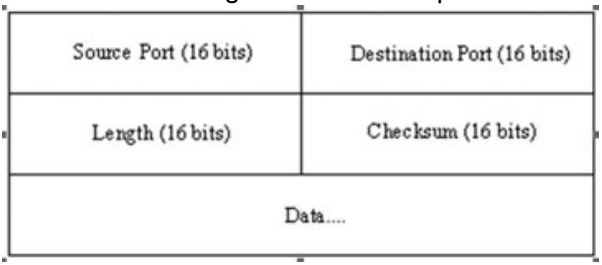
Reserved : field 6-bit digunakan untuk kebutuhan mendatang. Keenam bit

harus di-set menjadi 0.
Urg flag : jika on (nilainya 1), menunjukkan bahwa field urgent pointer significant.
ACK flag : jika on, menunjukkan bahwa field ACK significant.
Psh flag : jika on, menunjukkan bahwa fungsi push akan dilakukan.
Rst flag : jika on, menunjukkan bahwa koneksi akan reset.
Syn flag : jika on, menunjukkan bahwa sequence number akan disinkronisasi. Flag ini digunakan ketika koneksi sedang ditetapkan.
Fin flag : jika on, menunjukkan bahwa pengirim tidak punya lagi data untuk dikirimkan. Ini merupakan pesan bahwa komunikasi akan diakhiri.
Window : sebuah angkan yang menunjukkan banyaknya blok data yang dapat diterima oleh mesin penerima.
Checksum : dihitung dengan mengambil 16-bit satu komplemen dari penjumlahan satu komplemen dari 16-bit word dalam header (termasuk pseudo-header) dan teks. (diperlukan suatu proses yang agak panjang untuk mencocokkan checksum dengan baik dengan header).
Urgent pointer : digunakan jika URG Flag set, ini menandakan porsi message data yang urgent dengan membuat spesifikasi offset dari sequence number dalam header.
Option: sama dengan header option pada IP, field ini digunakan untuk membuat spesifikasi option TCP. Setia option terdiri atas sebuah oprtion number (1 byte)
0 akhir dari option list
1 tidak ada operasi
2 ukuran maksimum segmen
Padding : diisi untuk memastikan bahwa header berukuran multiple 32-bit.

3.5 Protokol Data Unis UDP

TCP merupakan protokol berorientasi connection. Ada kalanya dimana protokol berorientasi connectionless dibutuhkan, makanya UDP digunaka. UDP digunakan untuk *trivial file transfer protocol* (TFTP) dan *remote call procedure* (RCP). Komunikasi connectionless tidak mendukung reliabilitas, artinya tidak ada informasi yang yang diterima oleh mesin pengirim yang mengindikasikan data diterima oleh mesin penerima dengan benar. Protokol connctionless juga tidak memiliki kemampuan untuk melakukan recover terhadap data yang mengalami error. UDP lebih sederhana dinbanding TCP. UDP berhubungan langsung dengan IP tanpa adanya mekanisme flow control dan error-recovery.
Header message UDP lebih sederhana dibandingkan TCP. Sebagaimana

terlihat pada gambar 6.10. Field padding dapat ditambahkan ke datagram untuk memastikan bahwa message terdiri atas multiple 16-bit.



Gambar 3.5 Layer UDP

Field-fieldnya adalah sebagai berikut:

Source port: field optional dengan nomor port. Jika tidak ada nomor port yang ditentukan, field tersebut diset menjadi 0.

Destination port: nomor port mesin tujuan.

Length: panjang datagram, termasuk header dan data.

Checksum: field dengan 16-bit komplement satu dari jumlah komplemen satu dari datagram, termasuk pseudoheadewr yang sama dengan TCP.

Field checksum pada UDP hanya merupakan optional, tetapi jika tidak digunakan, maka tidak akan ada checksum pada segmen data karena checksum IP hanya digunakan pada header IP. Jika checksum tidak digunakan, field ini akan diset menjadi 0.

UDP adalah protokol transport yang digunakan secara luas pada lapisan di atas IP. Seperti TCP, UDP menggunakan port dan menyediakan konektivitas end-to-end antara aplikasi client dan server. UDP merupakan protokol yang kecil dan efisien. Tetapi, berbeda dengan TCP, UDP tidak menjamin pengiriman – aplikasi harus mengimplementasikan mekanisme error recovery-nya sendiri — jika memerlukan mekanisme tersebut. Hal ini membuatnya cocok untuk beberapa aplikasi, tetapi tidak untuk beberapa yang lain.

Dalam beberapa hal, UDP mirip dengan TCP :

UDP adalah protokol transport : UDP hanya berhubungan dengan komunikasi antara dua end point (misalnya aplikasi client pada mesin Anda, dan aplikasi server pada mesin remote). Intermediate router tidak berhubungan dengan data UDP dalam paket yang dikirimkannya – router hanya beroperasi pada layer IP atau network lower-down.

UDP menggunakan port untuk membedakan antara trafic dari banyak aplikasi UDP pada mesin yang sama, dan untuk mengirim paket yang tepat ke aplikasi

yang sesuai (ini disebut demultiplexing). UDP dan port-nya menyediakan interface antara program aplikasi dan layar networking IP.
UDP berbeda dari TCP dalam beberapa hal penting, karena:
UDP adalah "*datagram oriented*", TCP adalah "*session-oriented*". Datagram adalah paket informasi self-contained; UDP berhubungan dengan datagram atau paket individu yang dikirim dari client ke server, atau sebaliknya.
UDP adalah *connectionless*. Client tidak membangun koneksi ke server sebelum mengirim data – client hanya mengirim data secara langsung.
UDP "tidak andal" dalam pengertian jaringan formal :
Paket dapat hilang. UDP tidak dapat mendeteksinya.
Program aplikasi – client atau server – (sebagai kebalikan TCP/IP stack sendiri) harus mendeteksi paket yang hilang dan menangani transmisi ulang, dan lain-lain. Aplikasi sering menunggu hingga timeout habis, dan kemudian mencoba lagi.
Paket dapat mengalami kerusakan. Paket UDP berisi checksum semua data dalam paket. Checksum ini memungkinkan UDP mendeteksi kapan suatu paket mengalami kerusakan. Jika hal ini terjadi, maka paket tersebut dikeluarkan, dan sebagaimana biasa aplikasi-lah yang harus mendeteksi hal ini dan melakukan transmisi ulang sepenuhnya.
Operasi checksum ini dapat dihentikan, dan beberapa aplikasi melakukannya untuk alasan unjuk kerja. Akan tetapi hal ini dapat berarti paket yang rusak tidak terdeteksi atau layer aplikasi harus melakukan pemeriksaan integritas data sendiri, hal ini merupakan false economy (penghematan finansial yang sebenarnya menuju pada pengeluaran yang lebih besar)
Karena UDP adalah datagram-oriented dan pada level protokol setiap paket berdiri sendiri, maka UDP tidak memiliki konsep paket sesuai urutan, yang selanjutnya berarti tidak memerlukan nomor urut pada paket tersebut.
Sejak pertama kali dikembangkan, TCP telah dilengkapi dengan mekanisme yang sangat canggih untuk mengendalikan kecepatan aliran dalam koneksinya, untuk menghindari kemacetan dan kehilangan paket yang berlebihan. Karena UDP hanya mengirim paket tunggal, yang berdiri sendiri, maka UDP tidak memerlukan mekanisme kontrol yang rumit. Hal ini membuat UDP lebih mudah dan lebih kecil (dalam baris data dan memori) untuk diimplementasikan, tetapi juga membuatnya tidak cocok untuk sejumlah besar data.
Jika suatu aplikasi diimplementasikan menggunakan UDP, bukannya TCP, maka aplikasi tersebut harus memiliki sendiri deteksi paket-hilang, retry, dan lain sebaginya.
UDP mewarisi sifat IP, yaitu connectionless dan tidak andal. UDP sebagai layer transport sangat tipis di atas IP untuk memberikan akses aplikasi ke

fasilitas networking dasar IP, tanpa menambahkan fungsionalitas tambahan yang sangat banyak selain port dan checksum. (sebaliknya, TCP juga merupakan layer transport tetapi tidak melakukan banyak hal selain komunikasi paket IP dasar)
Pada kehidupan sehari-hari UDP dianalogikan seperti proses pengiriman pesan pada alat komunikasi telepon selular dengan menggunakan fasilitas SMS (Short Messsage Service) dimana kita tidak harus selalu berada ditempat untuk menunggu pesan karena pesan yang dikirim melalui fasilitas SMS akan sampai sekalipun telepon selular itu tidak diaktifkan. Sedang TCP dianalogikan seperti proses komunikasi langsung pada telepon dimana kita harus berada ditempat untuk menjawab langsung telepon dari seseorang yang berada ditempat lain.

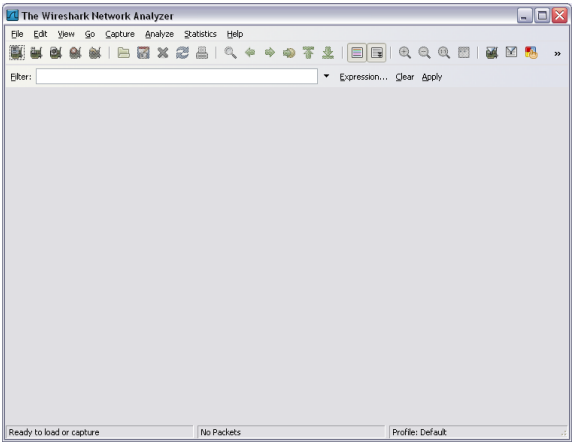
3.6 Melihat Segmen TCP

Melihat Segment TCP yang ada dalam jaringan bisa dilakukan dengan beberapa aplikasi, salah satu contohnya adalah wireshark. Berikut adalah syarat-syarat yang harus dipenuhi untuk melakukan penangkapan paket di jaringan menggunakan wireshark :

1. Mempunyai/bertindak sebagai user administrator.
2. Memiliki network card untuk melakukan penangkapan paket dan memilih network card yang tepat untuk melakukan penangkapan paket.
3. Menentukan tempat atau jaringan yang tepat untuk melakukan penangkapan paket.

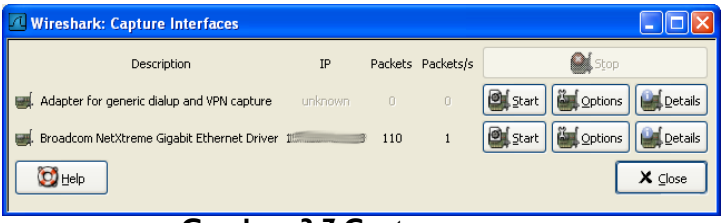
Berikut adalah langkah-langkah penggunaan Wireshark untuk menangkap paket yang ada di jaringan :

1. Buka aplikasi wireshark



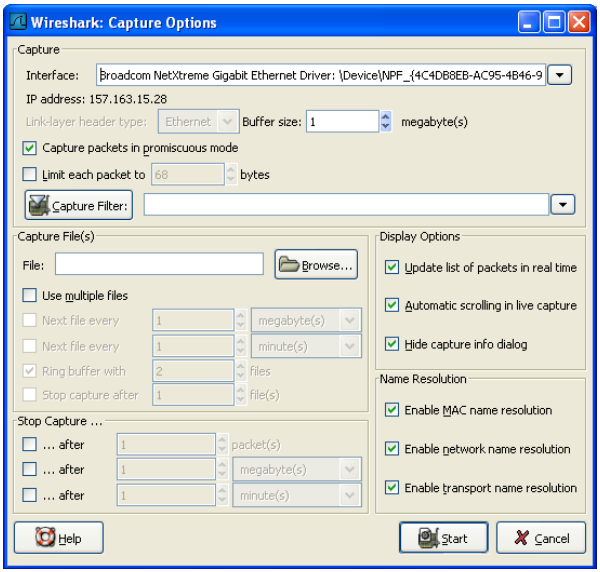
Gambar 3.6 Wireshark Main Window

2. Pilih menu ”capture” atau 



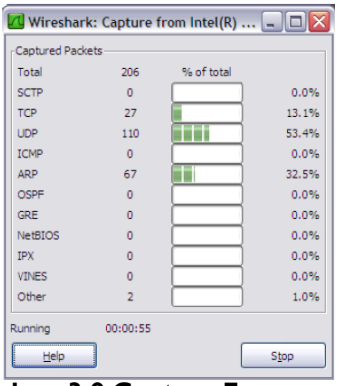
Gambar 3.7 Capture

3. Buka ”Capture Option Dialog”



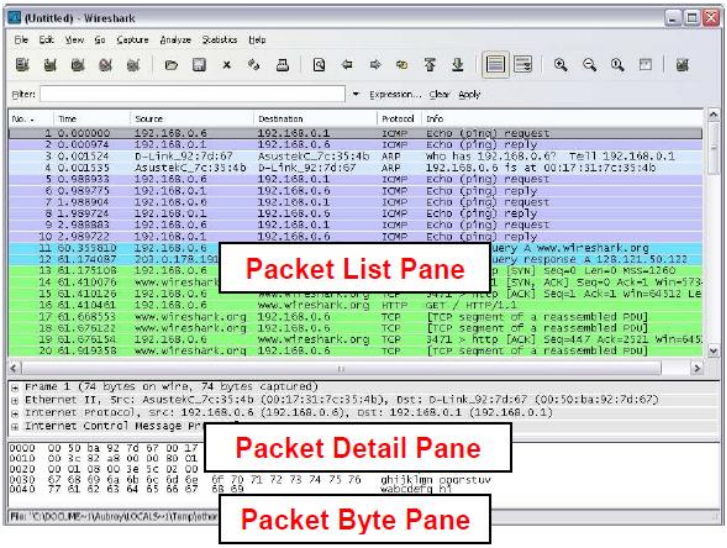
Gambar 3.8 Capture Option

4. Klik Start Capture



Gambar 3.9 Capture Form

5. Setelah slesei hasil capture dapat dilihat sebagai berikut :



Gambar 3.10 Detail View

Dari hasil capture tersebut kita bisa melihat data apa saja yang ditangkap oleh ethernet card kita.

4 IP dan Subnetting

Overview

Modul ini membahas tentang pengalamatan IP. Bagaimana kita membagi jaringan dengan menggunakan subnetting serta menggabungkan jaringan menggunakan supernetting.

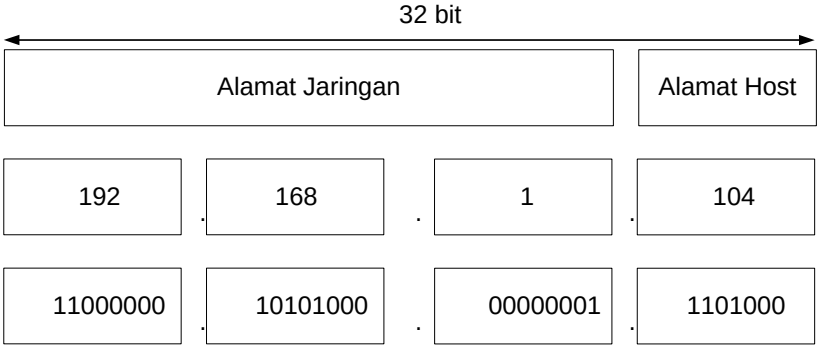
Tujuan

1. Memahami konsep IP
2. Memahami konsep subnetting dan superneting

4.1 Format IP Address

IPv4 memiliki 32 bit menggunakan angka biner dalam penggunaannya. Terbagi kedalam 4 oktet yang dipisahkan oleh tanda . (titik), yang

direpresentasikan dengan notasi desimal. Seperti yang diilustrasikan pada gambar
8.1



Gambar 4.1 Alamat IP

Gambar 8.1 Alamat IP dengan 32 bit yang terbagi kedalam 4 oktet dan representasi dalam bentuk binernya

4.2 Kelas-kelas Alamat IP

Pengalamatan dalam IPv4 memiliki 5 jenis kelas, A,B,C,D dan E. Tetapi hanya kelas A, B, dan C yang digunakan secara umum. Tabel 8.1 menggambarkan informasi tentang skema kelas-kelas yang ada pada IPv4.

Kelas	Format	Range alamat	Jumlah Host maks
A	N.H.H.H	1.0.0.0 - 126.0.0.0	2^{24} - 2
B	N.N.H.H	128.1.0.0 - 191.254.0.0	2^{16} - 2
C	N.N.N.H	192.0.1.0 - 223.255.254.0	2^{8} - 2
D	-	224.0.0.0 - 239.255.255.255	-
E	-	240.0.0.0 - 254.255.255.255	-

Tabel 4.1Kelas IP

Keterangan : N = alamat jaringan, H = alamat host

4.3 Subnet Mask

Seperti yang telah dijelaskan sebelumnya, bahwa alamat IP terdiri dari 2 bagian, yaitu alamat jaringan dan alamat host. Subnet mask atau netmask digunakan untuk menentukan bagian manakah dari sebuah alamat

yang merupakan alamat jaringan dan bagian manakah yang merupakan alamat host. Subnet mask direpresentasikan dengan nilai 1 dan 0 dimana bagian dengan nilai 1 merepresentasikan alamat jaringan sedangkan yang memiliki nilai 0 merupakan alamat hostnya, untuk mempermudah maka direpresentasikan dalam bentuk desimal.

Tidak semua jaringan membutuhkan subnet, dalam hal ini berarti jaringan tersebut menggunakan sebuah subnet mask default. Table 8.2 akan menunjukkan subnet mask default untuk masing-masing kelas A, B, dan C. Subnet default untuk masing-masing kelas ini tidak dapat diubah. Maksudnya adalah kita tidak bisa menggunakan sebuah subnet 255.0.0.0 untuk sebuah kelas B, jika kita mencobanya maka alamat tersebut akan menjadi tidak valid dan bahkan biasanya tidak akan diperbolehkan mengetikkan subnet mask yang salah tersebut. Tidak bisa juga kita set semua nilai dengan 1 atau menjadi 255.255.255.255, dimana alamat tersebut sebenarnya merupakan alamat broadcast.

Kelas	Format	Subnet mask default
A	N.H.H.H	255.0.0.0
B	N.N.H.H	255.255.0.0
C	N.N.N.H	255.255.255.0

Tabel 4.2 Subnet Mask

Sebagai contoh, untuk alamat IP 192.168.1.10 dengan subnet mask 255.255.255.0, berarti alamat jaringan dari IP tersebut adalah 192.168.1.0, sedangkan alamat hostnya adalah 0.0.0.10.

Subnet mask juga bisa direpresentasikan dengan notasi CIDR (*Classless Inter-Domain Routing*), yang akan menggunakan tanda "/" dibelakang sebuah alamat IP dan dibelakangnya terdapat jumlah angka 1 dari netmasknya. Jika kita lihat dari contoh diatas, maka notasi CIDR-nya adalah 192.168.1.10/24.

4.4 CIDR

CIDR (*Classless Inter-Domain Routing*) merupakan sebuah metode yang digunakan untuk mengkategorikan alamat IP dengan tujuan untuk mengalokasikan lamat IP kepada user dan untuk efisiensi dalam proses routing paket-paket IP didalam internet. Metode ini biasanya digunakan oleh ISP (*Internet Service Provider*) untuk mengalokasikan alamat kepada sebuah rumah, perusahaan atau ke seorang pelanggan.

Ketika kita menerima sebuah blok alamat dari ISP, umumnya kita akan menerima dalam bentuk 192.168.1.10/28. Maksud dari angka-angka tersebut adalah menjelaskan bahwa kita berada pada subnet 28. Hal ini berarti

kita menggunakan sebanyak 28 nilai 1, atau berarti subnet mask kita adalah menjadi 255.255.255.240.

Alasan adanya CIDR adalah seperti yang telah dijelaskan sebelumnya, yaitu hanya ada 3 kelas penggolongan alamat IP. Dimana masing-masing kelas memiliki jumlah maksimal alamat tertentu. Ambil sebuah contoh dimana sebuah organisasi dengan jumlah komputer yang harus terhubung ke jaringan adalah 1000 komputer. Jika digunakan kelas C, yang maksimal adalah 256 host, maka jumlah tersebut terlalu kecil untuk digunakan. Jika kita gunakan kelas B, yang maksimal jumlah hostnya adalah 65536, maka sisanya akan menjadi terbuang percuma. Hal ini akan menjadi tidak efisien pada masalah routingnya.

CIDR menggunakan VLSM (*Variable-Length Subnet Masks*) untuk mengalokasikan alamat IP sesuai dengan kebutuhannya, daripada menggunakan mengikuti aturan-aturan kelas-kelas A, B dan C dalam jaringan. Sehingga pembagian jaringan atau host dapat dilakukan dengan menggunakan pada semua bit yang ada pada alamat. Seperti yang terdapat pada table 8.2.

Perlu diingat bahwa penggunaan subnet mask maksimal adalah /30, karena sebuah jaringan paling tidak harus menyimpan dua buah bit sebagai bit dari host. Dan dalam sebuah jaringan, tidak semua alamat bisa kita gunakan sebagai alamat host. Setidaknya terdapat dua buah alamat tidak bisa kita gunakan, yaitu alamat pertama yang akan menjadi alamat jaringan tersebut dan alamat terakhir yang akan menjadi alamat broadcast dari jaringan tersebut.

IP/CIDR	Subnet Mask	Jumlah Hosts	Ukuran Class
a.b.c.d/30	255.255.255.252	4	1/64 C
a.b.c.d/29	255.255.255.248	8	1/32 C
a.b.c.d/28	255.255.255.240	16	1/16 C
a.b.c.d/27	255.255.255.224	32	1/8 C
a.b.c.d/26	255.255.255.192	64	1/4 C
a.b.c.d/25	255.255.255.128	128	1/2 C
a.b.c.0/24	255.255.255.000	256	1 C
a.b.c.0/23	255.255.254.000	512	2 C
a.b.c.0/22	255.255.252.000	1,024	4 C
a.b.c.0/21	255.255.248.000	2,048	8 C
a.b.c.0/20	255.255.240.000	4,096	16 C
a.b.c.0/19	255.255.224.000	8,192	32 C

a.b.c.0/18	255.255.192.000	16,384	64 C
a.b.c.0/17	255.255.128.000	32,768	128 C
a.b.0.0/16	255.255.000.000	65,536	256 C = 1 B
a.b.0.0/15	255.254.000.000	131,072	2 B
a.b.0.0/14	255.252.000.000	262,144	4 B
a.b.0.0/13	255.248.000.000	524,288	8 B
a.b.0.0/12	255.240.000.000	1,048,576	16 B
a.b.0.0/11	255.224.000.000	2,097,152	32 B
a.b.0.0/10	255.192.000.000	4,194,304	64 B
a.b.0.0/9	255.128.000.000	8,388,608	128 B
a.0.0.0/8	255.000.000.000	16,777,216	256 B = 1 A
a.0.0.0/7	254.000.000.000	33,554,432	2:00 AM
a.0.0.0/6	252.000.000.000	67,108,864	4:00 AM
a.0.0.0/5	248.000.000.000	134,217,728	8:00 AM
a.0.0.0/4	240.000.000.000	268,435,456	16 A
a.0.0.0/3	224.000.000.000	536,870,912	32 A
a.0.0.0/2	192.000.000.000	1,073,741,824	64 A
a.0.0.0/1	128.000.000.000	2,147,483,648	128 A
0.0.0.0/0	000.000.000.000	4,294,967,296	256 A

Tabel 4.3 Ukuran Kelas

4.5 Subnetting

Dalam sebuah jaringan komputer, sekelompok komputer dan peralatan jaringan yang memiliki routing prefix IP address yang sama dinamakan sebuah subnetworks atau subnet. Dengan menggunakan subnetting, sebuah jaringan yang besar bisa dipecah dan dibentuk menjadi sebuah jaringan-jaringan yang lebih kecil. Proses tersebut dinamakan dengan subnetting. Subnetting memberikan beberapa keuntungan, antara lain:

a. Berkurangnya lalu lintas jaringan. Untuk mengkomunikasikan beberapa subnet dalam sebuah jaringan, maka kita harus menggunakan sebuah router. Dengan adanya router, maka semua lalu lintas hanya akan berada didalam jaringan tersebut,

kecuali jika paket tersebut ditujukan kepada jaringan yang lainnya.

b. Kerja jaringan yang optimal. Hal ini disebabkan oleh berkurangnya lalu lintas jaringan.
c. Pengelolaan yang sederhana. Akan lebih mudah bagi kita untuk mengelola sebuah jaringan kecil-kecil yang saling terisolasi jika dibandingkan dengan mengelola sebuah jaringan tunggal yang sangat besar.
d. Membantu pengembangan jaringan dengan jarak geografis yang jauh. Karena jalur dalam WAN yang lebih lambat dan mahal, maka sebuah jaringan yang mencakup jarak yang jauh akan menciptakan masalah masalah diatas. Sehingga menghubungkan banyak jaringan kecil akan menjadi lebih efisien.

Pada sebuah jaringan yang besar, tanpa adanya subnetting, lalu lintas paket dalam jaringan bisa mencapai nilai rata-rata yang cukup tinggi, yang banyak disebabkan oleh terjadinya collision pada sebuah jaringan Ethernet (CSMA/CD). Oleh karena itu subnetting digunakan untuk membentuk jaringan-jaringan yang lebih kecil. Disini router digunakan untuk mengelola lalu lintas data dan memisahkan batas antar subnet.

Selain itu. subnetting membantu juga dalam mengatasi masalah keterbatasan jumlah host dalam IPv4, dimana jumlah maksimal alamat IP yang dimungkinkan adalah sebanyak 2^{32} alamat IP. Mengingat bahwa setiap mesin yang terhubung kedalam internet haruslah memiliki alamat yang unik, maka jika dilihat maka jumlah tersebut tidak mungkin akan cukup untuk seluruh mesin yang ada di dunia ini.

Oleh karena itu, jika dilihat dari posisinya didalam sebuah jaringan, sebuah alamat IP dibagi menjadi 2 golongan, yaitu:

a. IP publik yaitu alamat IP yang langsung terhubung kedalam internet, dimana IP tersebut bersifat unik di keseluruhan jaringan internet.
b. IP private yaitu alamat IP yang bersifat tidak umum, yang hanya dikenali oleh jaringan lokal saja. Agar dapat terhubung ke internet dibutuhkan beberapa server yang bisa digunakan untuk mengkonversi alamat kita sehingga terhubung kedalam internet.

3.1.4 Perhitungan Subnetting

Ketika sudah diputuskan untuk memilih sebuah subnet mask, maka kita perlu untuk menentukan beberapa hal yaitu: jumlah subnet, host yang valid, dan alamat broadcast. Maka dari subnet yang telah dipilih tadi perlu dijawab 5 buah pertanyaan mendasar berikut:

a. Berapa jumlah subnet yang dihasilkan?
b. Berapa jumlah host yang valid untuk setiap subnet?
c. Mana sajakah subnet-subnet yang valid?
d. Alamat broadcast dari setiap subnet adalah?
e. Manakah host-host yang valid untuk setiap subnet?

3.1.5 Contoh untuk kelas C.

Misal untuk melakukan subnetting pada alamat jaringan 192.168.1.0 dengan subnet mask 255.255.255.192 maka bentuk dari subnet mask tersebut adalah 11111111 . 11111111 . 11111111 . 11000000
Jawaban untuk masing-masing pertanyaan diatas adalah

a. Berapa jumlah subnet yang dihasilkan?

   Jumlah subnet = 2^x-2. Dimana x adalah jumlah bit 1(satu) dalam subnet mask terakhir. Akan kita ambil oktet terakhirnya, 11000000. Sehingga dapat kita tentukan bahwa jumlah subnet dengan x=2, adalah $2^2 – 2 = 2$ subnet.

b. Berapa jumlah host yang valid untuk setiap subnet?

   Jumlah host per-subnet=2^y-2. Dimana y adalah jumlah angka 0 (nol). Dari oktet terakhir 11000000, dapat kita tentukan jumlah host valid/subnet dengan y=6 adalah $2^6 – 2 = 62$ host/subnet.

c. Mana sajakah subnet-subnet yang valid?

   Sebelumnya harus kita tentukan ukuran blok subnetnya. Dari contoh diatas maka ukuran blok per subnet adalah 256 – 192 = 64. Kita mulai dari 0 dengan menambahkannya dengan ukuran bloknya, hingga mencapai angka subnet masknya (dari contoh diatas adalah 192).
   0 + 64 = 64 ← valid
   64 + 64 = 128 ← valid
   128 + 64 = 192 ← tidak valid

Tetapi blok 192 akan menjadi tidak valid karena semua bit-nya adalah 1. Sehingga dua subnet yang valid adalah 64 dan 128.

d. Alamat broadcast dari setiap subnet adalah?
Adalah nomor yang tepat sebelum subnet yang selanjutnya (subnet selanjutnya - 1). Sehingga alamat broadcast dari tiap subnet adalah
Subnet 64 →127
Subnet 128 → 191

e. Manakah host-host yang valid untuk setiap subnet?
Akan menjadi lebih mudah jika kita gunakan dalam bentuk tabel.

Blok	1	2
Subnet	64	128
Host pertama	65	129
host terakhir	126	190
alamat broadcast	127	191

Tabel 4.4 Analisa Subnetting

Maka didapatkan bahwa host yang valid untuk

- subnet 64 adalah antara 65 - 126, atau lengkapnya 192.168.1.65 – 192.168.126 dengan alamat broadcast 127 (192.168.1.127).
- subnet 128 adalah antara 129-190, atau lengkapnya 192.168.1.129 – 192.168.190 dengan alamat broadcast 191 (192.168.1.191).

3.1.5.1 Contoh Untuk kelas B

Antara kelas B dan kelas C tidak jauh berbeda, masih tetap kita gunakan 5 buah pertanyaan yang telah digunakan pada contoh diatas.
Misal untuk sebuah alamat jaringan 172.16.0.0/18.
18 = 255.255.192.0 = 11111111 . 11111111 . 110000000 . 00000000

- Jumlah subnet? $2^2 – 2 = 2$
- Jumlah host? $2^{14} – 2 = 16.382$ (16 berasal dari 6 oktet ketiga dan 8 oktet keempat)
- Subnet yang valid? 256 – 192 = 64.
  0 + 64 = 64 ←valid
  64 + 64 = 128 ←valid
  128 + 64 = 192 ←tidak valid

- Alamat broadcast tiap subnet?
- Host yang valid?

Tabel berikut akan memperlihatkan kedua subnet yang ada, range host valid dan alamat broadcast masing-masing subnet.

Blok	1	2
Subnet	64.0	128.0
Host pertama	64.1	128.1
host terakhir	127.254	191.254
alamat broadcast	127.255	191.255

Tabel 4.5 Hasil Subnetting

Maka didapatkan bahwa host yang valid untuk

- subnet 172.16.64.0 adalah antara 64.1 – 127.254, atau lengkapnya 172.16.64.1 – 172.16.127.254 dengan alamat broadcast 127.255 (172.16.127.255).
- subnet 172.16.128.0 adalah antara 128.1 – 191.254, atau lengkapnya 172.16.128.1 – 172.16.191.254 dengan alamat broadcast 191.255 (172.16.191.255).

4.5.1.1 untuk kelas A cara yang digunakan tidak jauh berbeda.

5 Router dan Simulator

Overview

Pada bab ini akan dibahas mengenai konsep dasar routing. Akan dibahas juga peralatan jaringan yang berkontribusi besar dalam proses routing, router. Dikenalkan pula aplikasi yang digunakan untuk membantu simulasi jaringan.

Tujuan

1. Memahami konsep router dan routing.
2. Mampu menggunakan simulator untuk mensimulasi kondisi sebenernya.
3. Mampu menggunakan perintah-perintah untuk administrasi router.

5.1 Dasar Teori

Routing, adalah sebuah proses untuk meneruskan paket-paket jaringan dari satu jaringan ke jaringan lainnya melalui sebuah *internetwork*. Routing juga dapat merujuk kepada sebuah metode penggabungan beberapa jaringan sehingga paket-paket data dapat hinggap dari satu jaringan ke jaringan selanjutnya. Untuk melakukan hal ini, digunakanlah sebuah perangkat jaringan yang disebut sebagai *router*. *Router-router* tersebut akan menerima paket-paket yang ditujukan ke jaringan di luar jaringan yang pertama, dan akan meneruskan paket yang ia terima kepada router lainnya hingga sampai kepada tujuannya.

Router memiliki kemampuan melewatkan paket IP dari satu jaringan ke jaringan lain yang mungkin memiliki banyak jalur diantara keduanya. Router-router yang saling terhubung dalam jaringan internet turut serta dalam sebuah algoritma routing terdistribusi untuk menentukan jalur terbaik yang dilalui paket IP dari system ke system lain.

Proses routing dilakukan secara hop by hop. IP tidak megnetahui jalur keseluruhan menuju tujuan setiap paket. IP routing hanya menyediakan IP address dari router berikutnya yang menurutnya lebih dekat ke host tujuan. Router dapat digunakan untuk menghubungkan sejumlah LAN sehingga trafik yang dibangkitkan oleh suatu LAN terisolasikan dengan baik dari trafik yang dibangkitkan oleh LAN yang lain. Jika dua atau lebih LAN terhubung dengan router, setiap LAN dianggap sebagai subnetwork yang berbeda. Merip dengan bridge, router dapat dihubungkan network interface yang berbeda.

Router terletak pada Layer 3 dalam OSI, router hanya perlu mengetahui Net-Id (nomor jaringan) dari data yang diterimanya untuk diteruskan ke jaringan yang dituju. Cara kerjanya setiap paket data yang datang, paket data tersebut dibuka lalu dibaca header paket datanya kemudian mencocokan atau membandingkan ke dalam table yang ada pada routing jaringan dan diteruskan ke jaringan yang dituju melalui suatu interface. Untuk mengetahui network mana yang akan dilewatkan router akan menambahkan (Logical AND) Subnet Mask dengan paket data tersebut.

Algortima routing untuk host Proses routing yang dilakukan oleh host cukup sederhana. Jika host tujuan terletak di jaringan yang sama atau terhubung langsung. IP datagram dikirim langsung ke tujuan. Jika tidak, IP datagram dikirm ke default router. Router ini yang akan mgnatur perngiriman IP selanjutnya, hingga sampai ke tujuannya. Dalam suatu table routing terdapat :

1) IP address tujuan

2) IP address next hop router (gateway)

3) Flag, yang menyatakan jenis routing

4) Spesifikasi network interface tempat datagram dilewatkan.

Dalam proses meneruskan paket ke tujuan, IP router akan melakukan hal-hal berikut;

1) Mencari di table routing, entry yang cocok dengan IP address tujuam. Jika ditemukan, paket akan dikirim ke next hop router atau interface yang terhubunglangsung dengan nya.

2) Mencari di table routing, entry yang cocok dengan alamat network dari network tujuan. Jika ditemukan, paket dikirm ke nxt hop router tersebut.

3) Mencari di table routing, entry data yang bertanda default, jika ditemukan, paket dikirim ke router tersebut. Protokol Routing Protokol routing yang umum digunakan pada jaringan TCP/IP saat ini adalah Routing Information Protokol (RIP), Open Shortest PATH First (OSPF) dan Border Gateway Protocol (BGP)

Dalam sebuah kasus praktikum dimana setiap host yang dihubungkan dengan switch melakukan browsing ke suatu alamat tertentu. Disini penulis menggunakan IP Address 172.24.12.18 yang melakukan permintaan data dari http://www.cisco.com dan melakukan proses FTP ke server puma MTI. Dalam proses tersebut tercata dan tercapture oleh program snifer yang cukup ampuh yaitu Iris Versi 2.0. Pada level aplikasi lewat browser Internet Explorer. Penulis memberikan perintah kepada browser untuk mencari alamat http://www.cisco.com. Dalam TCP/IP terjadi penyampaian data dari protocol yang berada di satu layer ke protocol yang berada pada layer lain. Semua informasi yang diterima protocol diberlakukan sebagai data. Dari layer aplikasi akan diteruskan ke layer transport yang akan mengadakan komunikasi antara dua host kedua protocol yaitu TCP dan UDP. Lalu melalui layer IP yang berfungsi untuk menyampaikan paket data ke alamat yang tepat, protokol yang digunakan yaitu ARP dan ICMP. Sedangkan pada layer berikutnya layer Internet yang bertanggung jawab dalam proses pengiriman paket alamat yang tepat menggunakan protocol IP, ARP, dan ICMP. Pada layer yang paling bawah yaitu layer Network interface, bertanggung jawab mengirim dan menerima data ke dan dari media fisik.
Didalam program Iris mencapture kegiatan penulis yang melakukan kegiatan browsing dengan port 80 dan melakukan transfer data dengan FTP

menggunakan port 21. angka-angka port ini telah distandarkan pada protocol TCP dan dikenal sebagai Well Known Port. ARP bertugas untuk menerjemahkan IP address ke alamat Ethernet. Proses ini dilakukan hanya untuk datagram yang dikirm host karena pada saat inilah host menambahkan header Ethernet pada datagram. Penerjemahan dari IP address ke alamta Ethernet dilakukan dengan melihat table yang disebut sebagai cache ARP.
Jika suatu protocol menerima data dari protocol lain di layer atasnya. Ia akan menambahkan informasi tambahan miliknya kedata tersebut. Setelah itu akan diteruskan ke layer dibawahnya. Hal yang sama juga terjadi jika suatu protocol menerima data dari protocol lain yang berada pada layer di bawahnya. Jika data ini dianggap valid, protocol akan melepas informasi tambahan tersebut, untuk kemudian meneruskan ke protocol lain pada layer diatasnya. Dalam kasus ini dimana host MTI 8 dengan IP address 172.24.12.18 melakukan browsing ke suatu alamat di Internet. ARP akan memcocokkan dengan Network Id dan Host ID addressnya, karena data yang dibawa lain dari subnet mask MTI maka ARP request menuju Router, lalu router akan mencari alamat IP yang terdekat dari rangkaian Routing table yang dibuat dengan router lain. maka pada saat pencarian table routing ini cache ARP akan melakukan :

1. Alamat tujuan datagram dimasking dengan subnet mask host pengirim dan dibandingkan dengan alamat network host pengirim. Jika sama maka ini adalah routing langsung dan frame langsung dikirimkan ke interface jaringan.

2. Jika tujuan datagram tidak terletak dalam satu jaringan. Periksa apakah terdapat entri routing yang berupa host dan bandingkan dengan IP address tujuan datagram. Jika ada entri yang sama, kirim frame ke router menuju host tujuan.

3. Jika tidak terdapat entri host yang cocok ada table routing, gunakan alamat tujuan datagram yang telah dimask pada langkah 1 untuk mencari kesamaan di table routing. Periksa apakah ada network/subnetwork di table routing yang sama dengan alamat network tujuan datagram. Jika ada entri yang sama, kirim frame ke router menuju network/subnetwork tersebut.

4. Jika tidak terdapat entri host ataupun entri netwotk/subnetwork yang sesuai dengan tujuan datagram, host mengirimkan ftrame ke router default dan menyerahkan proses routing selanjutnya ke pada router default.

5. Jika tidak terdapat rute default di table routing, semua host diasumsikan dalam keadaan terhubung langsung. Dengan demikian host pengirim akan mencari alamat fisik host tujuan menggunakan ARP.

5.2 Router

Router adalah perangkat **jaringan** yang bekerja pada *layer* 3 OSI (*network layer*) dan dapat menghubungkan dua atau lebih jaringan yang memiliki *subnet* berbeda. *Router* juga berfungsi sebagai pengatur arus lalu lintas jaringan dan memiliki tugas sangat vital dalam menentukan kondisi sebuah jaringan.

Jadi fungsi router, secara mudah dapat dikatakan, menghubungkan dua buah jaringan yang berbeda, tepatnya mengarahkan rute yang terbaik untuk mencapai network yang diharapkan

Dalam implementasinya, router sering dipakai untuk menghubungkan jaringan antar lembaga atau perusahaan yang masing-masing telah memiliki jaringan dengan network id yang berbeda. Contoh lainnya yang saat ini populer adalah ketika perusahaan anda akan terhubung ke internet. Maka router akan berfungsi mengalirkan paket data dari perusahaan anda ke lembaga lain melalui internet, sudah barang tentu nomor jaringan anda akan bereda dengan perushaaan yang anda tuju.

Jika sekedar menghubungkan 2 buah jaringan, sebenarnya anda juga dapat menggunakan pc berbasis windows NT atau linux. Dengan memberikan 2 buah network card dan sedikit setting, sebenarnya anda telah membuat router praktis. Namun tentunya dengan segala keterbatasannya.

Di pasaran sangat beragam merek router, antara lain baynetworks, 3com dan cisco. Modul kursus kita kali ini akan membahas khusus cisco. Mengapa ? karena cisco merupakan router yang banyak dipakai dan banyak dijadikan standar bagi produk lainnya.

5.3 Simulator Jaringan

Di dalam pembelajaran jaringan komputer,kita akan lebih mudah memahami konsep jaringan melalui rangkaian komponen yang dijalankan dengan mengunakan suatu program pensimulasi atau yang dikenal dengan Network Simulator Software.

Network Simulator adalah suatu program yang dijadikan sebagai simulasi konfigurasi suatu topologi jaringan dengan menganut konsep-konsep jaringan tertentu.

Ada beberapa software simulator yang umum dikalangan masyarakat, seperti Boson NetSim, Packet Tracer, ForceVision, dan sebagainya. Sebagian besar

merupakan pengembangan dari produk vendor-vendor komponen jaringan yang cukup terkenal yang berasal dari Amerika dan Eropa,sebagai contoh : CISCO Corp.
Sama halnya dalam keadaan fisik atau yang ada di lapangan,beberapa software ini berisikan komponen-komponen yang dibutuhkan di dalam konsep jaringan, seperti disediakan router, switch, connector, PC, dan beberapa komponen penunjang lainnya. Tentunya dengan type dan kemampuan yang beraneka ragam.
Komponen-komponen ini dapat dirangkai sedemikian rupa sehingga dapat berfungsi sebagaimana mestinya,menurut keinginan dari user perancang jaringan. Beberapa konsep jaringan dapat diimplementasikan melalui software ini, seperti konfigurasi VLAN, pembuatan access list, penentuan alamat ip suatu device, konfigurasi router dengan RIP atau dengan IGRP, dan sebagainya.
Beberapa software ini cukup handal bila dijalankan di dalam spesifikasi hardware standart, sekalipun berupa software yang bersifat freeware atau gratisan. Untuk pengembangan yang kearah expert, barulah haruslah menggunakan program yang berbayar. User dapat langsung mendownload dan mencoba simulasi jaringan komputer sederhana. Seperti, menghubungkan beberapa komputer client dengan komputer server melalui beberapa switch dan router.
Mekanisme yang sederhana dan hasil konfigurasi yang akurat, jg merupakan kelebihan lain dari software-software ini. Dengan berbekal pengetahuan mengenai konsep ip dan routing,user dapat bereksplorasi dengan komponen-komponen yang tersedia.

5.4 Packet Tracer

Cisco Packet Tracer merupakan program simulasi networking kuat yg memungkinkan siswa utk bereksperimen dgn perilaku jaringan & bertanya pertanyaan "bagaimana jika".
Sebagai bagian integral dari Akademi Jaringan pengalaman belajar yg lengkap, Packet Tracer memberikan simulasi, visualisasi, authoring, penilaian, & kolaborasi kemampuan & memfasilitasi mengajar & belajar dari konsep teknologi yg kompleks.
Packet Tracer suplemen peralatan fisik di kelas dgn memungkinkan siswa utk menciptakan sebuah jaringan dgn jumlah tak terbatas perangkat, mendorong praktik, penemuan, & pemecahan masalah. Simulasi berbasis lingkungan belajar membantu siswa mengembangkan keterampilan abad 21 seperti pengambilan keputusan, kreatif & berpikir kritis, & pemecahan masalah.

Packet Tracer Networking Academy melengkapi kurikulum, sehingga dgn gampang instruktur utk mengajar & menunjukkan konsep-konsep teknis yg rumit & desain sistem jaringan. dgn Packet Tracer, instruktur dapat menyesuaikan kegiatan individu atau multiuser, menyediakan tangan-on pelajaran bagi siswa yg menawarkan nilai & relevansi dalam kelas mereka. Siswa dapat membangun, mengkonfigurasi, & atasi masalah jaringan menggunakan peralatan & simulasi virtual koneksi, sendiri atau bekerja sama dgn siswa lain. Paling penting, Packet Tracer membantu siswa & instruktur menciptakan virtual mereka sendiri "dunia jaringan" utk eksplorasi, eksperimentasi, & penjelasan tentang konsep & teknologi jaringan.
Paket kegiatan Tracer diikutsertakan dalam CCNA Discovery, CCNA Exploration, & Keamanan CCNA kurikulum utk menyediakan teknologi jaringan kaya pengalaman pembelajaran.

Software ini sangat praktis digunakan untuk mendesain topologi jaringan yang kita inginkan, disertai dengan berbagai perangkat - perangakat jaringan dibutuhkan pada suatu area network misal router, switch, hub maupun perangkat lainnya. Dengan dukungan dari banyak perangkat tersebut akan memudahkan kita dalam menentukan jenis perangkat jaringan yang akan kita gunakan pada topologi kita inginkan.

Aplikasi packet tracert memiliki keunggulan dan kemudahan dibandingkan dengan simulator jenis lain. Kita dapat melakukan rancangan suatu topologi jaringan dengan mudah serta penempatan perangkat jaringan dapat diatur dan ditentukan dengan baik. Konfigurasi – konfigurasi juga dapat dilakukan dengan teliti sehingga antara perangkat jaringan dapat dihubungkan dengan baik. Kemudahan yang diberikan packet tracer juga terlihat pada saat penginstallan aplikasi tersebut. Software packet tracer dapat diinstall pada PC maupun laptop dengan spesifikasi rendah sehingga tidak tergantung pada spesifikasi yang baik sekalipun.

Packet tracer sangat mudah digunakan dan diaplikasikan pada suatu desain topologi jaringan/network. Dengan kemudahan tersebut aplikasi telah melakukan peningkatan – peningkatan agar dapat melengkapi aplikasi packet tracer versi sebelumnya. Saya memakai simulator ini versi 4.1, dengan versi kemudahaan sudah sangat kelihatan apalagi sekarang muncul versi terbaru 5.0 keluaran Cisco dengan packet tracer 5.0 akan sangat membantu para administrator jaringan untuk mengimplementasikan topologi jaringan sebelum diterapkan pada suatu area nyata. Untuk mendapatkan aplikasi ini kamu bisa mendownloadnya di internet secara gratis

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 :

Untuk mengkoneksikan peralatan yang berbeda, gunakan kabel Straight-through

Router – Switch
Router – Hub
PC – Switch
PC – Hub

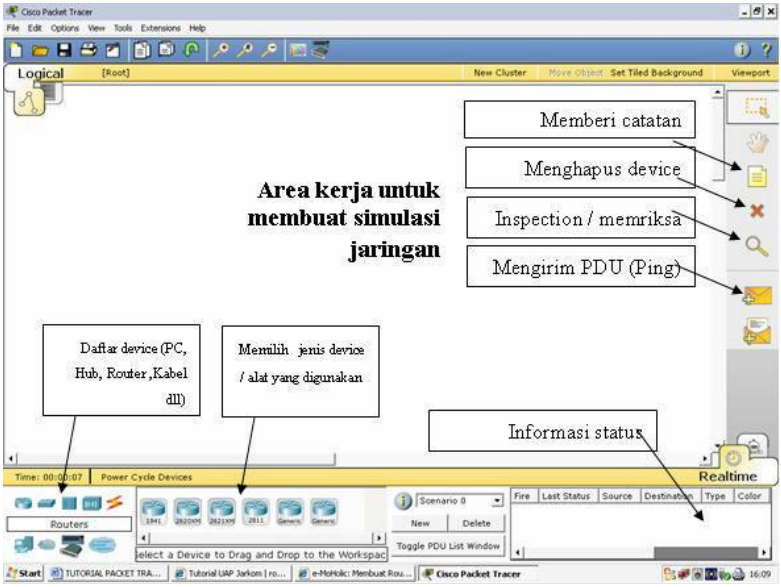
Untuk mengkoneksikan peralatan yang sama, gunakan kabel Cross-Over

Router - Router
Router – PC
Switch - Switch
Switch – Hub

Untuk mengkonfigurasi Router melalui PC gunakan kabel Roll-Over

Pada komfigurasi perangkat – perangkat jaringan sangat menentukan dalam merangcang suatu topologi jaringan . Proses konfigurasi merupakan bagian penting dalam susunan jaringan. 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). Contoh konfigurasi dengan mode GUI Klik device yang akan dikonfigurasi. Pilih menu Config. Klik interface yang diinginkan. Isi IP Address dan subnet mask-nya. Lakukan hal yang sama untuk interface-interface dan device yang lain.
Berikut contoh sederhana penggunaan packet tracer :

1. Buka paket tracer



Gambar 5.1Packet Tracer Main Window

2. Tambahkan device dengan menggunakan panel di bagian bawah.

Gambar 5.2 Panel Device

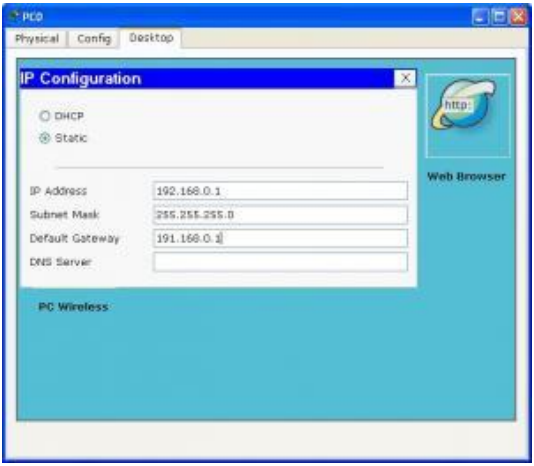
3. Untuk menghubungkan komputer satu dengan yang lain pilihlah connection.

Gambar 5.3 Konektor

4. Susun device seperti gambar berikut.

Gambar 5.4 Skema Jaringan

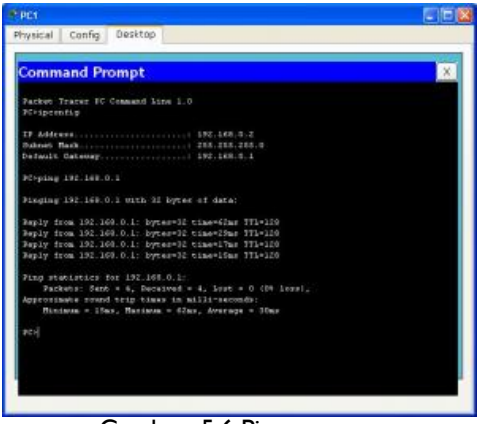
5. Untuk mengatur IP, klik di salah satu komputer kemudian atur IP seperti gambar berikut.



Gambar 5.5 Konfigurasi IP PC

Lakukan hal yang sama dengan komputer lainnya dengan IP berbeda tetapi masih di network yang sama.

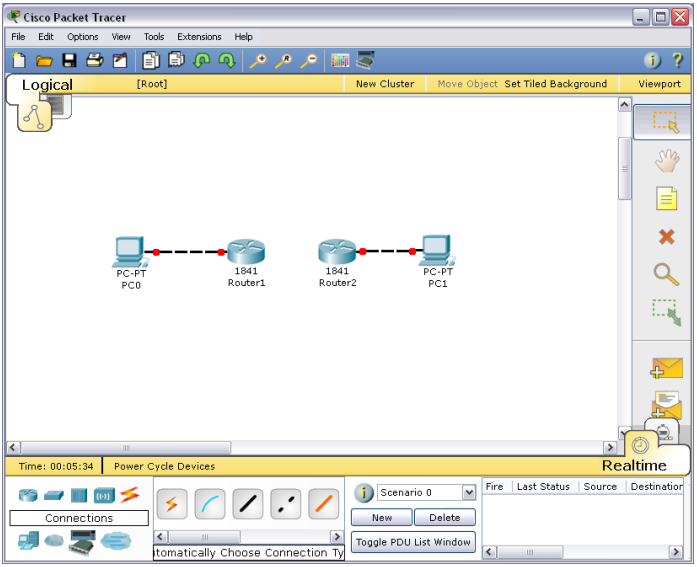
6. Lakukan tes koneksi dengan menggunakan perintah ping.



Gambar 5.6 Ping

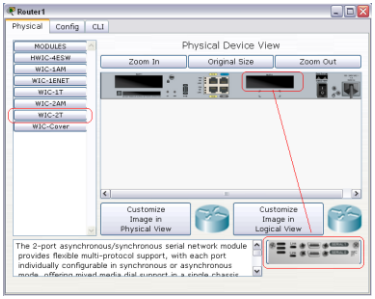
5.5 Administrasi Router Menggunakan Packet Tracer

1. Buatlah skema jaringan seperti berikut



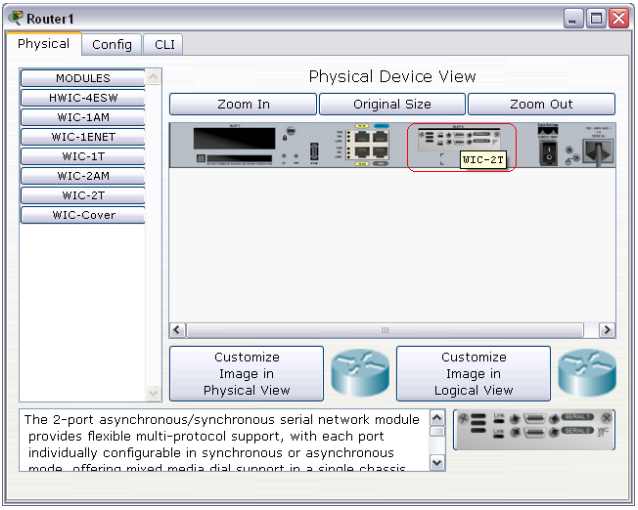
Gambar 5.7 Skema Jaringan Studi Kasus

2. Koneksi dua router di atas belum terbentuk. Untuk menghubungkan dua router tersebut pertama kita harus menambahkan serial port ke router tersebut. Klik salah satu router.



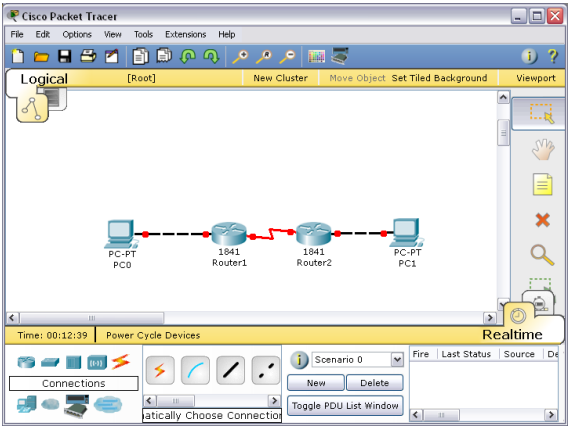
Gambar 5.8 Interface Router

3. Tambahkan modul serial WIC-2T seperti ilustrasi gambar di atas.



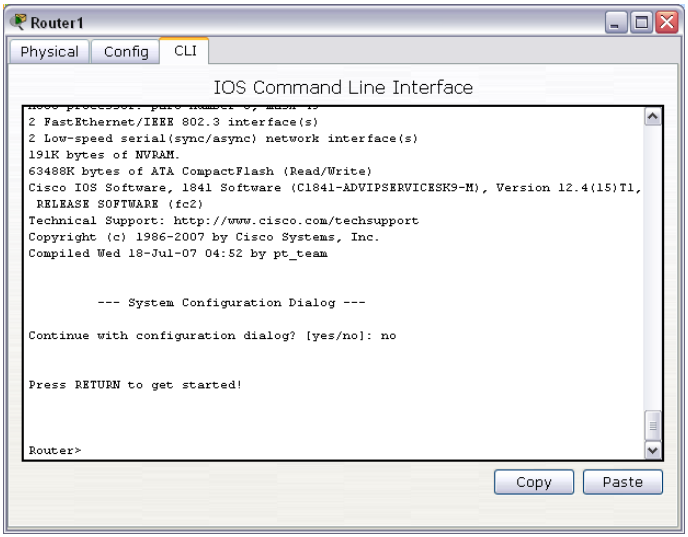
Gambar 5.9 Modul Tambahan

4. Lakukan hal yang sama pada router lainnya.
5. Buatlah koneksi sehingga skema jaringan menjadi seperti berikut.



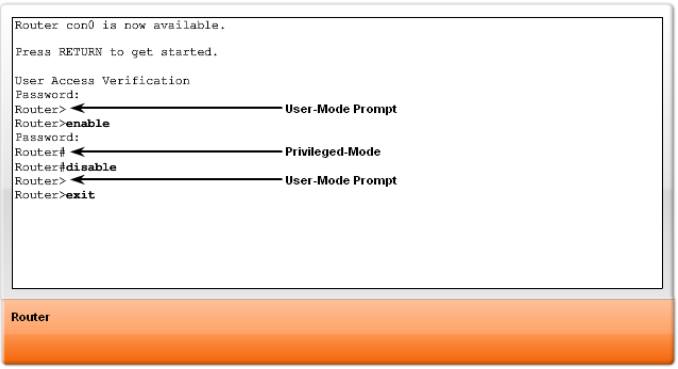
Gambar 5.10 Skema Akhir

6. Klik pada salah satu router dan pilih tab CLI sehingga muncul tampilan berikut.



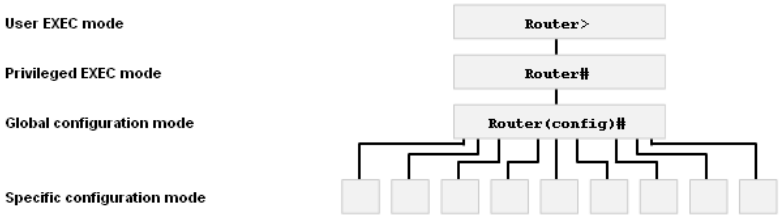
Gambar 5.11 CLI

7. Ada beberapa mode CLI dalam router cisco seperti dibawah ini



Gambar 5.12 Mode CLI

8. Berikut mode konfigurasi dalam Router Cisco CLI



Configuration Mode	Prompt
Interface	Router(config-if)#
Line	Router(config-line)#
Routers	Router(config-router)#

Gambar 5.13 Konfigurasi Interfaces

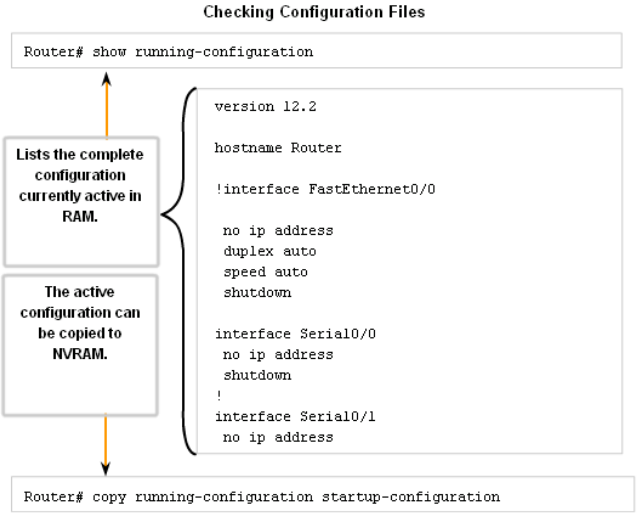
9. Berikut command untuk konfigurasi nama host

Gambar 5.14 Konfigurasi Hostname

10. Konfigurasi password router cisco

Gambar 5.15 Konfigurasi Password

11. Melihat konfigurasi yang sedang berjalan



Gambar 5.16 File Konfigurasi

12. Konfigurasi interface router

```
Router(config)#interface type port
Router(config)#interface type slot/port
Router(config)#interface type slot/subslot/port
```

Gambar 5.17 Konfigurasi Interface

13. Mengaktifkan dan menonaktifkan interface router

```
Router(config-if)#no shutdown
```

Gambar 5.18 Mengaktifkan interface

```
Router(config-if)#shutdown
```

Gambar 5.19 Mematikan Interface

14. Keluar dari konfigurasi interface

```
Router(config-if)#exit
```

Gambar 5.20 Keluar Konfigurasi Interface

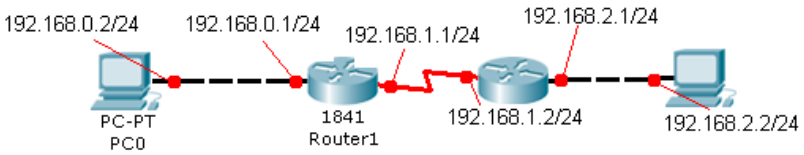
15. Konfigurasi Interface ethernet

```
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

16. Konfigurasi Serial

```
Router(config)#interface Serial 0/0/0
Router(config-if)#ip address 192.168.11.1 255.255.255.252
Router(config-if)#clock rate 56000
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

17. Konfigurasi semua node yang ada di skema jaringan kemudian cobalah melakukan ping.



Gambar 5.21 Skema Jaringan Soal

6 Routing Statis

Overview

Pada modul ini akan dijelaskan mekanisme routing menggunakan routing statis untuk beberapa contoh kasus. Implementasi dari konfigurasi menggunakan simulator.

Tujuan

1. Memahami konsep routing statis
2. Mampu mengkonfigurasi routing statis pada simulator router

6.1 Dasar Teori

Pada suatu jaringan bisnis berskala besar atau enterprise yang terdiri dari banyak lokasi yang tersebar secara remote, maka komunikasi antar site dengan management routing protocol yang bagus adalah suatu keharusan. Baik **static route** ataupun dynamic routing haruslah di design sedemikian rupa agar sangat efficient.

Suatu *static route* adalah suatu mekanisme routing yang tergantung dengan routing table dengan konfigurasi manual. Disisi lain dynamic routing adalah suatu mekanisme routing dimana pertukaran routing table antar router yang ada pada jaringan dilakukan secara dynamic. Lihat juga artikel memahami IP routing protocols.

Dalam skala jaringan yang kecil yang mungkin terdiri dari dua atau tiga router saja, pemakaian **static route** lebih umum dipakai. Static router (yang menggunakan solusi static route) haruslah di configure secara manual dan dimaintain secara terpisah karena tidak melakukan pertukaran informasi routing table secara dinamis dengan router-router lainnya. Lihat juga artikel tentang memahami hardware router.

Suatu static route akan berfungsi sempurna jika routing table berisi suatu route untuk setiap jaringan didalam internetwork yang mana dikonfigure secara manual oleh administrator jaringan. Setiap host pada jaringan harus dikonfigure untuk mengarah kepada default route atau default gateway agar cocok dengan IP address dari interface local router, dimana router memeriksa routing table dan menentukan route yang mana digunakan untuk meneruskan paket. Lihat juga DNS forwarding untuk memahami default gateway.

Konsep dasar dari routing adalah bahwa router meneruskan IP paket berdasarkan pada IP address tujuan yang ada dalam header IP paket. Dia mencocokkan IP address tujuan dengan routing table dengan harapan menemukan kecocokan entry – suatu entry yang menyatakan kepada router kemana paket selanjutnya harus diteruskan. Jika tidak ada kecocokan entry yang ada dalam routing table, dan tidak ada default route, maka router tersebut akan membuang paket tersebut. Untuk itu adalah sangat penting untuk mempunyai isian routing table yang tepat dan benar.

Static route terdiri dari command-command konfigurasi sendiri-sendiri untuk setiap route kepada router. sebuah router hanya akan meneruskan paket hanya kepada subnet-subnet yang ada pada routing table. Sebuah router selalu mengetahui route yang bersentuhan langsung kepada nya – keluar interface dari router yang mempunyai status "up and up" pada line interface dan protocolnya. Dengan menambahkan static route, sebuah router dapat

diberitahukan kemana harus meneruskan paket-paket kepada subnet-subnet yang tidak bersentuhan langsung kepadanya.
Cara kerja routing statis dapat dibagi menjadi 3 bagian:

- Administrator jaringan yang mengkonfigurasi router
- Router melakukan routing berdasarkan informasi dalam tabel routing
- Routing statis digunakan untuk melewatkan paket data

Keuntungan static route:

- Static route lebih aman disbanding dynamic route
- Static route kebal dari segala usaha hacker untuk men-spoof paket dynamic routing protocols dengan maksud melakukan configure router untuk tujuan membajak traffic.

Kerugian:

- Administrasinya adalah cukup rumit disbanding dynamic routing khususnya jika terdiri dari banyak router yang perlu dikonfigure secara manual.
- Rentan terhadap kesalahan saat entry data static route dengan cara manual.

Seorang administrator harus menggunakan perintah **ip route** secara manual untuk mengkonfigurasi router dengan routing statis.

```
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 s0
```

command destination net subnet mask outgoing Interface

Routing statis bias dilakukan dengan dua cara :

1. Berdasarkan outgoing interface

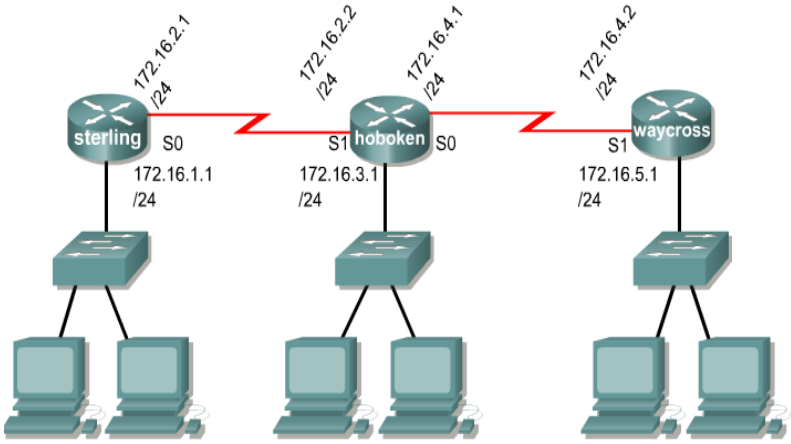
```
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 s1
                  command  destination   sub mask     gateway
                           network
Hoboken(config)#ip route 172.16.5.0 255.255.255.0 s0
                  command  destination   sub mask     gateway
                           network
```

2. Berdasarkan next hop

```
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1
                   command destination   sub mask    gateway
                           network
Hoboken(config)#ip route 172.16.5.0 255.255.255.0 172.16.4.2
                   command destination   sub mask    gateway
                           network
```

6.2 Praktikum

1. Buatlah Jaringan kumputer yang sesuai dengan skema berikut



Gambar 6.1 Skema Jaringan

2. Lakukan konfigurasi berikut agar computer di setiap segmen dapat terhubung satu dengan yang lain.

Configuration for Router1

```
Router> enable
Router# hostname sterling
Sterling#configuration terminal
Sterling(config)# interface eth 0
Sterling(config-if)#ip address 172.16.1.1 255.255.255.0
Sterling(config-if)#no shutdown
Sterling(config-if)#exit
Sterling(config)#interface serial 0
```

```
Sterling(config-if)#ip add 172.16.2.1 255.255.255.0
Sterling(config-if)#clock rate 56000
Sterling(config-if)#no shutdown
Sterling(config-if)#exit
```

Configuration for Router2

```
Router> enable
Router# hostname hoboken
hoboken#configuration terminal
hoboken(config)# interface eth 0
hoboken(config-if)#ip address 172.16.3.1 255.255.255.0
hoboken(config-if)#no shutdown
hoboken(config-if)#exit
hoboken(config)#interface serial 1
hoboken(config-if)#ip add 172.16.2.2 255.255.255.0
hoboken(config-if)#clock rate 56000
hoboken(config-if)#no shutdown
hoboken(config-if)#exit
hoboken(config)#interface serial 0
hoboken(config-if)#ip add 172.16.4.1 255.255.255.0
hoboken(config-if)#clock rate 56000
hoboken(config-if)#no shutdown
```

Configuration for Router3

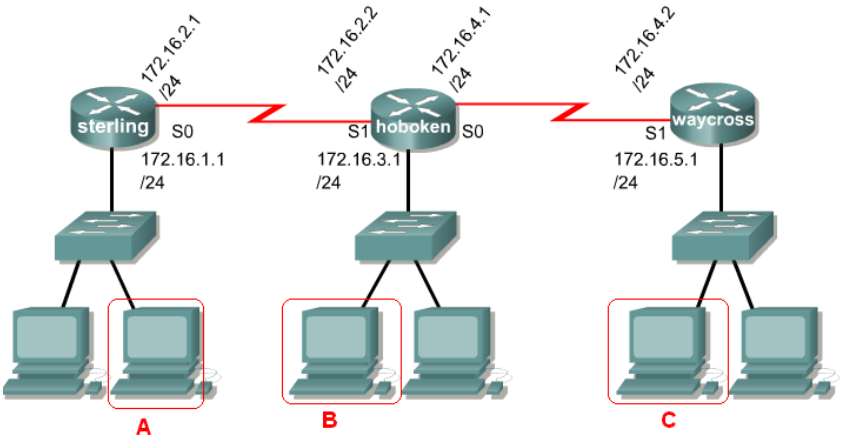
```
Router> enable
Router# hostname Waycross
Waycross#configuration terminal
Waycross(config)# interface eth 0
Waycross(config-if)#ip address 172.16.5.1 255.255.255.0
Waycross(config-if)#no shutdown
Waycross(config-if)#exit
Waycross(config)#interface serial 1
Waycross(config-if)#ip add 172.16.4.2 255.255.255.0
Waycross(config-if)#clock rate 56000
Waycross(config-if)#no shutdown
Waycross(config-if)#exit
```

STATIC ROUTE CONFIGURATION

```
Sterling(config)# ip route 172.16.3.0 255.255.255.0 172.16.2.2
----
hoboken(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1
hoboken(config)#ip route 172.16.5.0 255.255.255.0 172.16.4.2
----
Waycross(config)#ip route 172.16.3.0 255.255.255.0 172.16.4.1
```

3.2 Troubleshooting

Mengecek konfigurasi dari routing static bisa dilakukan dengan cara sebagai berikut :



Gambar 6.2 Skema Testing

Dari PC A :

- Lakukan ping/tracert ke PC B.
- Lakukan ping/tracert ke PC C.

7 Routing Dinamis

Overview

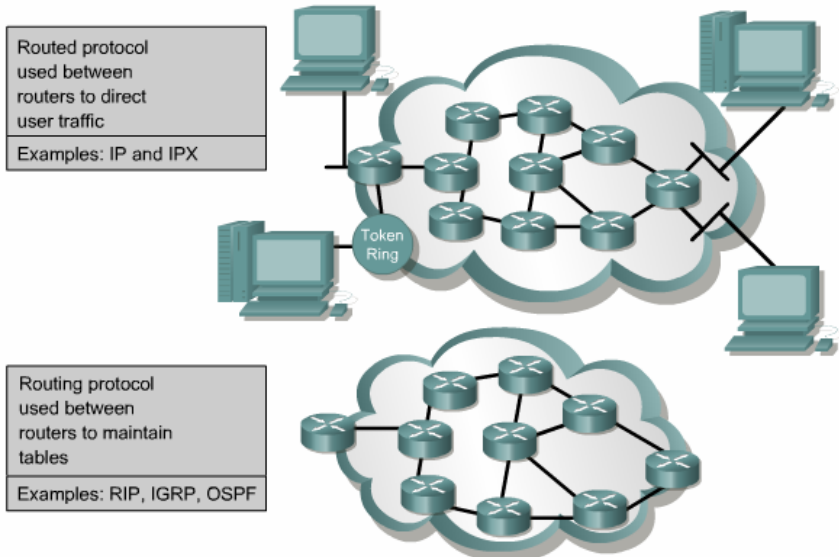
Modul ini berisi tentang routing dinamis. Dibahas beberapa algoritma routing dinamis. Mengimplementasikan routing dinamis dengan menggunakan RIP. Implementasi menggunakan simulator.

Tujuan

1. Memahami konsep routing dinamis
2. Mampu mengkonfigurasi routing dinamis pada router

7.1 Dasar Teori

Routing protocol adalah berbeda dengan routed protocol. Routing protocol adalah komunikasi antara router-router. Routing protocol mengijinkan router-router untuk sharing informasi tentang jaringan dan koneksi antar router. Router menggunakan informasi ini untuk membangun dan memperbaiki table routingnya. Seperti pada gambar di bawah ini.



Gambar 7.1Protokol dalam routing

Contoh routing protokol:

- Routing Information Protocol (RIP)
- Interior Gateway Routing Protocol (IGRP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF)

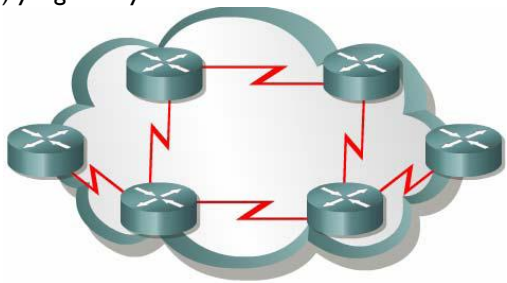
Routed protocol digunakan untuk trafik user langsung. Routed protocol menyediakan informasi yang cukup dalam layer address jaringannya untuk melewatkan paket yang akan diteruskan dari satu host ke host yang lain berdasarkan alamatnya.

Contoh routed protocol:

- Internet Protocol (IP)
- Internetwork Packet Exchange (IPX)

7.2 Autonomous System

AS adalah kumpulan dari jaringan-jaringan yang dalam satu administrasi yang mempunyai strategi routing bersama. AS mungkin dijalankan oleh satu atau lebih operator ketika AS digunakan pada routing ke dunia luar.
American Registry of Internet Numbers (ARIN) adalah suatu service provider atau seorang administrator yang memberikan nomor identitas ke AS sebesar 16-bit. Routing protokol seperti Cisco IGRP membutuhkan nomor AS (AS number) yang sifatnya unik.

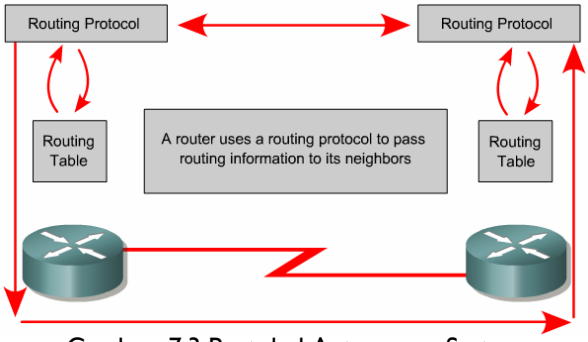


Gambar 7.2 Autonomous System

7.2.1 Tujuan Routing Protocol dan Autonomous System

Tujuan utama dari routing protokol adalah untuk membangun dan memperbaiki table routing. Dimana tabel ini berisi jaringan-jaringan dan interface yang berhubungan dengan jaringan tersebut. Router menggunakan protokol routing ini untuk mengatur informasi yang diterima dari router-router lain dan interfacenya masing-masing, sebagaimana yang terjadi di konfigurasi routing secara manual.
Routing protokol mempelajari semua router yang ada, menempatkan rute yang terbaik ke table routing, dan juga menghapus rute ketika rute tersebut sudah tidak valid lagi. Router menggunakan informasi dalam table routing untuk melewatkan paket-paket routed prokol.

Algoritma routing adalah dasar dari routing dinamis. Kapanpun topologi jaringan berubah karena perkembangan jaringan, konfigurasi ulang atau terdapat masalah di jaringan, maka router akan mengetahui perubahan tersebut. Dasar pengetahuan ini dibutuhkan secara akurat untuk melihat topologi yang baru.
Pada saat semua router dalam jaringan pengetahuannya sudah sama semua berarti dapat dikatakan internetwork dalam keadaan konvergen (converged). Keadaan konvergen yang cepat sangat diharapkan karena dapat menekan waktu pada saat router meneruskan untuk mengambil keputusan routing yang tidak benar.
AS membagi internetwork global menjadi kecil-kecil menjadi banyak jaringan-jaringan yang dapat diatur. Tiap-tiap AS mempunyai seting dan aturan sendiri-sendiri dan nomor AS yang akan membedakannya dari AS yang lain.



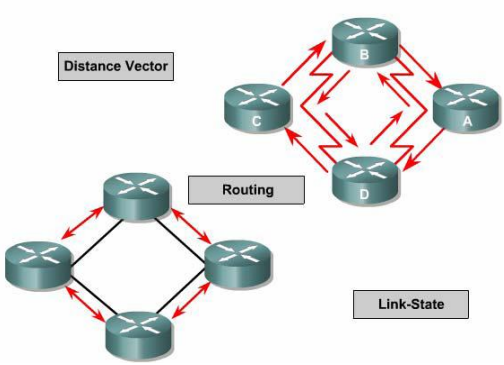
Gambar 7.3 Protokol Autnomous System

7.3 Klasifikasi Routing Protokol

Sebagian besar algoritma routing dapat diklasifikasikan menjadi satu dari dua kategori berikut:

- Distance vector
- Link-state

Routing distance vector bertujuan untuk menentukan arah atau vector dan jarak ke link-link lain dalam suatu internetwork. Sedangkan link-state bertujuan untuk menciptakan kembali topologi yang benar pada suatu internetwork.

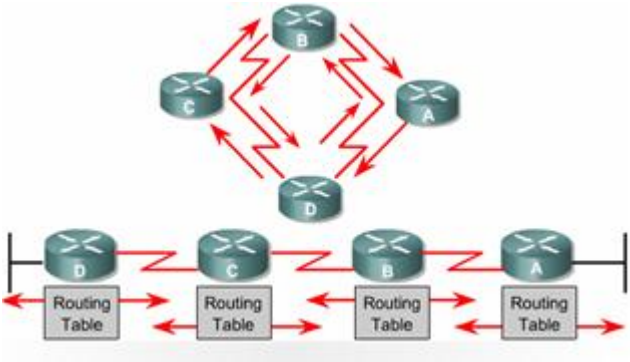


Gambar 7.4 Klasifikasi Routing Protokol

7.3.1 Distance Vector

Algoritma routing distance vector secara periodik menyalin table routing dari router ke router. Perubahan table routing ini di-update antar router yang saling berhubungan pada saat terjadi perubahan topologi. Algoritma distance vector juga disebut dengan algoritma Bellman-Ford.

Setiap router menerima table routing dari router tetangga yang terhubung langsung. Pada gambar di bawah ini digambarkan konsep kerja dari distance vector.



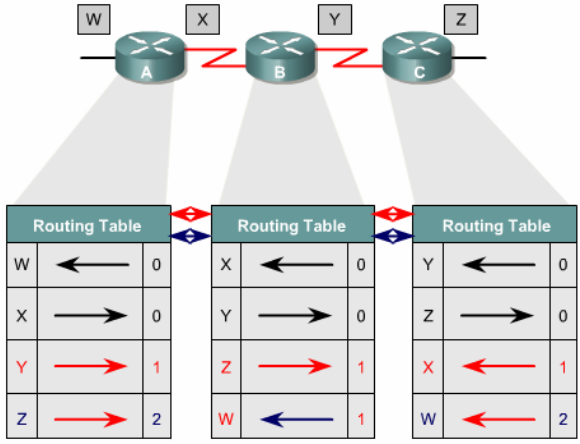
Gambar 7.5 Distance Vector

Router B menerima informasi dari Router A. Router B menambahkan nomor distance vector, seperti jumlah hop. Jumlah ini menambahkan distance vector. Router B melewatkan table routing baru ini ke router-router tetangganya

yang lain, yaitu Router C. Proses ini akan terus berlangsung untuk semua router.

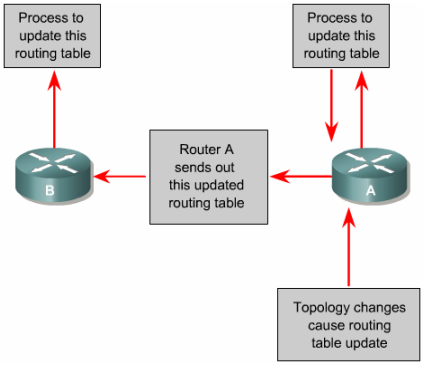
Algoritma ini mengakumulasi jarak jaringan sehingga dapat digunakan untuk memperbaiki database informasi mengenai topologi jaringan. Bagaimanapun, algoritma distance vector tidak mengijinkan router untuk mengetahui secara pasti topologi internetwork karena hanya melihat router-router tetangganya.

Setiap router yang menggunakan distance vector pertama kali mengidentifikasi router-router tetangganya. Interface yang terhubung langsung ke router tetangganya mempunyai distance 0. Router yang menerapkan distance vector dapat menentukan jalur terbaik untuk menuju ke jaringan tujuan berdasarkan informasi yang diterima dari tetangganya. Router A mempelajari jaringan lain berdasarkan informasi yang diterima dari router B. Masing-masing router lain menambahkan dalam table routingnya yang mempunyai akumulasi distance vector untuk melihat sejauh mana jaringan yang akan dituju. Seperti yang dijelakan oleh gambar berikut ini:

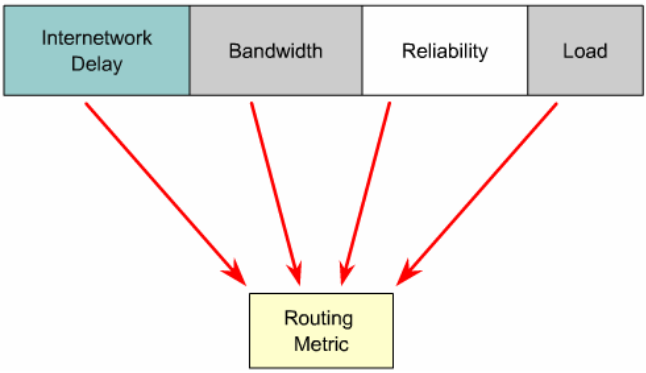


Gambar 7.6 Routing Table

Update table routing terjadi ketika terjadi perubahan toplogi jaringan. Sama dengan proses discovery, proses update perubahan topologi step-by-step dari router ke router. Gambar 9.3 menunjukkan algoritma distance vector memanggil ke semua router untuk mengirim ke isi table routingnya. Table routing berisi informasi tentang total path cost yang ditentukan oleh metric dan alamat logic dari router pertama dalam jaringan yang ada di isi table routing, sperti yang diterangkan oleh gambar 9.4 di bawah ini.



Gambar 7.7 Update Routing Table



Gambar 7.8 Routing Metric

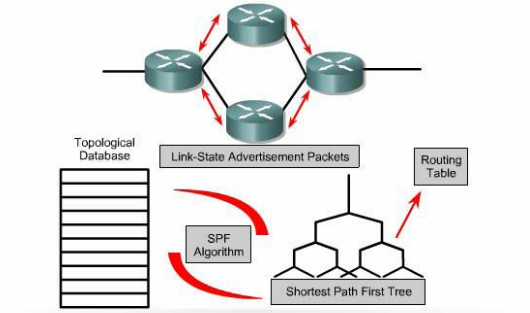
Analogi distance vector dapat digambarkan dengan jalan tol. Tanda yang menunjukkan titik menuju ke tujuan dan menunjukkan jarak ke tujuan. Dengan adanya tanda-tanda seperti itu pengendara dengan mudah mengetahui perkiraan jarak yang akan ditempuh untuk mencapai tujuan. Dalam hal ini jarak terpendek adalah rute yang terbaik.

7.3.2 Link State

Algoritma link-state juga dikenal dengan algoritma Dijkstra atau algoritma shortest path first (SPF). Algoritma ini memperbaiki informasi database dari informasi topologi. Algoritma distance vector memiliki informasi yang tidak spesifik tentang distance network dan tidak mengetahui jarak router.

Sedangkan algortima link-state memperbaiki pengetahuan dari jarak router dan bagaimana mereka inter-koneksi.
Fitur-fitur yang dimiliki oleh routing link-state adalah:

- Link-state advertisement (LSA) – adalah paket kecil dari informasi routing yang dikirim antar router
- Topological database – adalah kumpulan informasi yang dari LSA-LSA
- SPF algorithm – adalah hasil perhitungan pada database sebagai hasil dari pohon SPF
- Routing table – adalah daftar rute dan interface

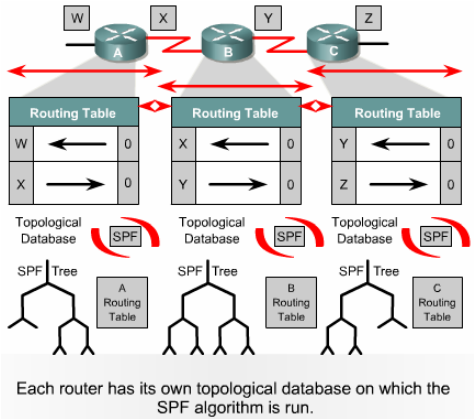


Routers send LSAs to their neighbors. The LSAs are used to build a topological database. The SPF algorithm is used to calculate the shortest path first tree in which the root is the individual router. A routing table is then created.

Gambar 7.9 Link State

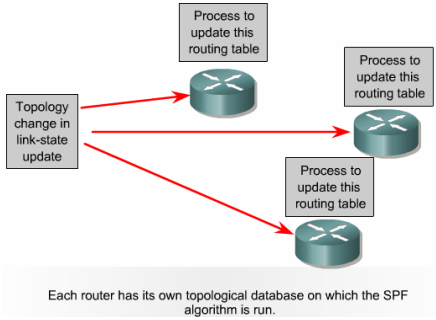
Proses discovery dari routing link-state

Ketika router melakukan pertukaran LSA, dimulai dengan jaringan yang terhubung langsung tentang informasi yang mereka miliki. Masing-masing router membangun database topologi yang berisi pertukaran informasi LSA.
Algoritma SPF menghitung jaringan yang dapat dicapai. Router membangun logical topologi sebagai pohon (tree), dengan router sebagai root. Topologi ini berisi semua rute-rute yang mungkin untuk mencapai jaringan dalam protokol link-state internetwork. Router kemudian menggunakan SPF untuk memperpendek rute. Daftar rute-rute terbaik dan interface ke jaringan yang dituju dalam table routing. Link-state juga memperbaiki database topologi yang lain dari elemen-elemen topologi dan status secara detail.



Gambar 7.10 Link State Routing Table

Router pertama yang mempelajari perubahan topologi link-state melewatkan informasi sehingga semua router dapat menggunakannya untuk proses update. Gambar 10.3 adalah informasi routing dikirim ke semua router dalam internetwork. Untuk mencapai keadaan konvergen, setiap router mempelajari router-router tetangganya. Termasuk nama dari router-router tetangganya, status interface dan cost dari link ke tetangganya. Router membentuk paket LSA yang mendaftar informasi ini dari tetangga-tetangga baru, perubahan cost link dan link-link yang tidak lagi valid. Paket LSA ini kemudian dikirim keluar sehinggan semua router-router lain menerima itu.



Gambar 7.11 Update Routing Table

Pada saat router menerima LSA, ia kemudian meng-update table routing dengan sebagian besar informasi yang terbaru. Data hasil perhitungan digunakan untuk membuat peta internetwork dan lagoritma SPF digunakan

untuk menghitung jalur terpendek ke jaringan lain. Setiap waktu paket LSA menyebabkan perubahan ke database link-state, kemudian SPF melakukan perhitungan ulang untuk jalur terbaik dan meng-update table routing.
Ada beberapa titik berat yang berhubungan dengan protokol link-state:

- Processor overhead
- Kebutuhan memori
- Konsumsi bandwidth

Router-router yang menggunakan protokol link-state membutuhkan memori lebih dan proses data yang lebih daripada router-router yang menggunakan protokol distance vector. Router link-state membutuhkan memori yang cukup untuk menangani semua informasi dari database, pohon topologi dan table routing. Gambar 10.4 menunjukkan inisialisasi paket flooding link-state yang mengkonsumsi bandwidth. Pada proses inisial discovery, semua router yang menggunakan protokol routing link-state mengirimkan paket LSA ke semua router tetangganya. Peristiwa ini menyebabkan pengurangan bandwidth yang tersedia untuk me-routing trafik yang membawa data user. Setelah inisial flooding ini, protokol routing link-state secara umum membutuhkan bandwidth minimal untuk mengirim paket-paket LSA yang menyebabkan perubahan topologi.

7.3.3 Penentuan Jalur

Router menggunakan dua fungsi dasar:

- Fungsi penentuan jalur
- Fungsi switching

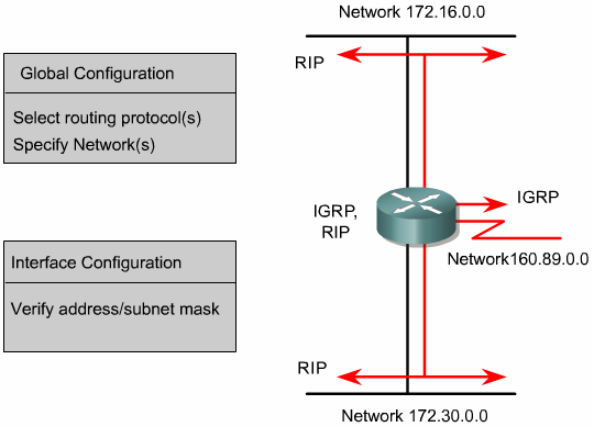
Penentuan jalur terjadi pada layer network. Fungsi penentuan jalur menjadikan router untuk mengevaluasi jalur ke tujuan dan membentuk jalan untuk menangani paket. Router menggunakan table routing untuk menentukan jalur terbaik dan kemudian fungsi switching untuk melewatkan paket.

7.3.4 Konsep Link State

Dasar algoritma routing yang lain adalah algoritma link state. Algoritma link state juga bias disebut sebagai algoritma Dijkstra atau algoritma shortest path first (SPF).

7.3.5 Konfigurasi Routing

Untuk menghidupkan protokol routing pada suatu router, membutuhkan seting parameter global dan routing. Tugas global meliputi pemilihan protokol routing seperti RIP, IGRP, EIGRP atau OSPF. Sedangkan tugas konfigurasi routing untuk menunjukkan jumlah jaringan IP. Routing dinamis menggunakan broadcast dan multicast untuk berkomunikasi dengan router-router lainnya.



Gambar 7.12 Klasifikasi Routing Protokol

Perintah **router** memulai proses routing. Perintah **network** untuk meng-enable-kan proses routing ke interface yang mengirim dan menerima update informasi routing.

Menspesifikasikan routing protocol yang akan digunakan :

Command
`Router(config)#router protocol {options}`

Mendaftarkan network yang terhubung langsung dengan router :

Command
`Router(config-router)#network network-number`

Berikut parameter dariperintah di atas :

router Command	Description
protocol	IGRP, EIGRP, OSPF, or RIP
options	IGRP and EIGRP require an autonomous number. OSPF requires a process ID. RIP does not require either.

network Command	Description
network number	specifies a directly connected network

Contoh konfigurasi Routing adalah sebagai berikut :

```
GAD(config)#router rip
GAD(config-router)#network 172.16.0.0
```

Protokol Routing

Pada layer internet TCP/IP, router dapat menggunakan protokol routing untuk membentuk routing melalui suatu algoritma yang meliputi:

- RIP – menggunakan protokol routing interior dengan algoritma distance vector
- IGRP – menggunakan protokol routing interior dengan algoritma Cisco distance vector
- OSPF – menggunakan protokol routing interior dengan algoritma link-state
- EIGRP – menggunakan protokol routing interior dengan algoritma advanced Cisco distance vector
- BGP – menggunakan protokol routing eksterior dengan algoritma distance vector

Dasar RIP diterangkan dalam RFC 1058, dengan karakteristik sebagai berikut:

- Routing protokol distance vector
- Metric berdasarkan jumlah lompatan (hop count) untuk pemilihan jalur
- Jika hop count lebih dari 15, paket dibuang
- Update routing dilakukan secara broadcast setiap 30 detik

IGRP adalah protokol routing yang dibangun oleh Cisco, dengan karakteristik sebagai berikut:

- Protokol routing distance vector

- Menggunakan composite metric yang terdiri atas bandwidth, load, delay dan reliability
- Update routing dilakukan secara broadcast setiap 90 detik

OSPF menggunakan protokol routing link-state, dengan karakteristik sebagai berikut:

- Protokol routing link-state
- Merupakan open standard protokol routing yang dijelaskan di RFC 2328
- Menggunakan algoritma SPF untuk menghitung cost terendah
- Update routing dilakukan secara floaded saat terjadi perubahan topologi jaringan

EIGRP menggunakan protokol routing enhanced distance vector, dengan karakteristik sebagai berikut:

- Menggunakan protokol routing enhanced distance vector
- Menggunakan cost load balancing yang tidak sama
- Menggunakan algoritma kombinasi antara distance vector dan link-state
- Menggunakan Diffusing Update Algorithm (DUAL) untuk menghitung jalur terpendek
- Update routing dilakukan secara multicast menggunakan alamat 224.0.0.10 yang diakibatkan oleh perubahan topologi jaringan

Border Gateway Protocol (BGP) merupakan routing protokol eksterior, dengan karakteristik sebagai berikut:

- Menggunakan routing protokol distance vector
- Digunakan antara ISP dengan ISP dan client-client
- Digunakan untuk merutekan trafik internet antar autonomous system

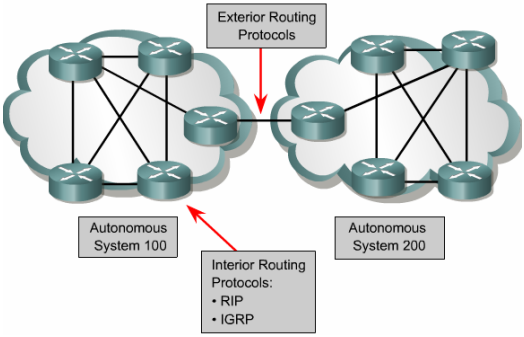
7.3.6 IGP dan EGP

Routing protokol interior didisain untuk jaringan yang dikontrol oleh suatu organisasi. Kriteria disain untuk routing protokol interior untuk mencari jalur terbaik pada jaringan. Dengan kata lain, metric dan bagaimana metric tersebut digunakan merupakan elemen yang sangat penting dalam suatu protokol routing interior.

Sedangkan protokol routing eksterior didisain untuk penggunaan antara dua jaringan yang berbeda yang dikontrol oleh dua organisasi yang berbeda. Umumnya digunakan antara ISP dengan ISP atau antara ISP dengan perusahaan. Contoh, suatu perusahaan menjalankan BGP sebagai protokol routing eksterior antar router perusahaan tersebut dengan router ISP. IP protokol eksterior gateway membutuhkan 3 seting informasi berikut ini sebelum router tersebut bias digunakan:

- Daftar router-router tetangga untuk pertukaran informasi routing
- Daftar jaringan untuk advertise sebagai tanda jaringan dapat dicapai secara langsung
- Nomor autonomous system dari router local

Routing protokol eksterior harus mengisolasi autonomous system. Ingat bahwa, autonomous system diatur oleh administrasi yang berbeda. Jaringan harus mempunyai protokol untuk komunikasi antara sistem-sistem yang berbeda tadi.



Gambar 7.13 IRP dan ERP

7.3.7 RIP

RIP termasuk dalam protokol distance-vector, sebuah protokol yang sangat sederhana.Protokol distance-vector sering juga disebut protokol Bellman-Ford, karena berasal dari algoritma perhitungan jarak terpendek oleh R.E. Bellman, dan dideskripsikan dalam bentuk algoritma-terdistribusi pertama kali oleh Ford dan Fulkerson.

Setiap router dengan protokol distance-vector ketika pertama kali dijalankan hanya mengetahui cara routing ke dirinya sendiri (informasi lokal) dan tidak mengetahui topologi jaringan tempatnya berada. Router kemudia mengirimkan informasi local tersebut dalam bentuk distance-vector ke semua link yang terhubung langsung dengannya. Router yang menerima informasi routing menghitung distance-vector, menambahkan distance-vector dengan metrik link tempat informasi tersebut diterima, dan memasukkannya ke dalam entri forwarding table jika dianggap merupakan jalur terbaik. Informasi routing setelah penambahan metrik kemudian dikirim lagi ke seluruh antarmuka router, dan ini dilakukan setiap selang waktu tertentu. Demikian seterusnya sehingga seluruh router di jaringan mengetahui topologi jaringan tersebut.

Protokol distance-vector memiliki kelemahan yang dapat terlihat apabila dalam jaringan ada link yang terputus. Dua kemungkinan kegagalan yang mungkin terjadi adalah efek bouncing dan menghitung-sampai-tak-hingga (counting to infinity). Efek bouncing dapat terjadi pada jaringan yang menggunakan metrik yang berbeda pada minimal sebuah link. Link yang putus dapat menyebabkan routing loop, sehingga datagram yang melewati link tertentu hanya berputar-putar di antara dua router (bouncing) sampai umur (time to live) datagram tersebut habis.

Menghitung-sampai-tak-hingga terjadi karena router terlambat menginformasikan bahwa suatu link terputus. Keterlambatan ini menyebabkan router harus mengirim dan menerima distance-vector serta menghitung metrik sampai batas maksimum metric distance-vector tercapai. Link tersebut dinyatakan putus setelah distance-vector mencapai batas maksimum metrik. Pada saat menghitung metrik ini juga terjadi routing loop, bahkan untuk waktu yang lebih lama daripada apabila terjadi efek bouncing.

RIP tidak mengadopsi protokol distance-vector begitu saja, melainkan dengan melakukan beberapa penambahan pada algoritmanya agar routing loop yang terjadi dapat diminimalkan. Split horizon digunakan RIP untuk meminimalkan efek bouncing. Prinsip yang digunakan split horizon sederhana: jika node A menyampaikan datagram ke tujuan X melalui node B, maka bagi B tidak

masuk akal untuk mencapai tujuan X melalui A. Jadi, A tidak perlu memberitahu B bahwa X dapat dicapai B melalui A.

Untuk mencegah kasus menghitung-sampai-tak-hingga, RIP menggunakan metode Triggered Update. RIP memiliki timer untuk mengetahui kapan router harus kembali memberikan informasi routing. Jika terjadi perubahan pada jaringan, sementara timer belum habis, router tetap harus mengirimkan informasi routing karena dipicu oleh perubahan tersebut (triggered update). Dengan demikian, router-router di jaringan dapat dengan cepat mengetahui perubahan yang terjadi dan meminimalkan kemungkinan routing loop terjadi.

RIP yang didefinisikan dalam RFC-1058 menggunakan metrik antara 1 dan 15, sedangkan 16 dianggap sebagai tak-hingga. Route dengan distance-vector 16 tidak dimasukkan ke dalam forwarding table. Batas metrik 16 ini mencegah waktu menghitung-sampai-tak-hingga yang terlalu lama. Paket-paket RIP secara normal dikirimkan setiap 30 detik atau lebih cepat jika terdapat triggered updates. Jika dalam 180 detik sebuah route tidak diperbarui, router menghapus entri route tersebut dari forwarding table. RIP tidak memiliki informasi tentang subnet setiap route. Router harus menganggap setiap route yang diterima memiliki subnet yang sama dengan subnet pada router itu. Dengan demikian, RIP tidak mendukung Variable Length Subnet Masking (VLSM).

RIP versi 2 (RIP-2 atau RIPv2) berupaya untuk menghasilkan beberapa perbaikan atas RIP, yaitu dukungan untuk VLSM, menggunakan otentikasi, memberikan informasi hop berikut (next hop), dan multicast. Penambahan informasi subnet mask pada setiap route membuat router tidak harus mengasumsikan bahwa route tersebut memiliki subnet mask yang sama dengan subnet mask yang digunakan padanya.

RIP-2 juga menggunakan otentikasi agar dapat mengetahui informasi routing mana yang dapat dipercaya. Otentikasi diperlukan pada protokol routing untuk membuat protocol tersebut menjadi lebih aman. RIP-1 tidak menggunakan otentikasi sehingga orang dapat memberikan informasi routing palsu. Informasi hop berikut pada RIP-2 digunakan oleh router untuk menginformasikan sebuah route tetapi untuk mencapai route tersebut tidak melewati router yang memberi informasi, melainkan router yang lain. Pemakaian hop berikut biasanya di perbatasan antar-AS.

RIP-1 menggunakan alamat broadcast untuk mengirimkan informasi routing. Akibatnya, paket ini diterima oleh semua host yang berada dalam subnet tersebut dan menambah beban kerja host. RIP-2 dapat mengirimkan paket menggunakan multicast pada IP 224.0.0.9 sehingga tidak semua host perlu menerima dan memproses informasi routing. Hanya router-router yang

menggunakan RIP-2 yang menerima informasi routing tersebut tanpa perlu mengganggu host-host lain dalam subnet.
RIP merupakan protokol routing yang sederhana, dan ini menjadi alasan mengapa RIP paling banyak diimplementasikan dalam jaringan. Mengatur routing menggunakan RIP tidak rumit dan memberikan hasil yang cukup dapat diterima, terlebih jika jarang terjadi kegagalan link jaringan. Walaupun demikian, untuk jaringan yang besar dan kompleks, RIP mungkin tidak cukup. Dalam kondisi demikian, penghitungan routing dalam RIP sering membutuhkan waktu yang lama, dan menyebabkan terjadinya routing loop. Untuk jaringan seperti ini, sebagian besar spesialis jaringan komputer menggunakan protocol yang masuk dalam kelompok link-state.

7.3.8 Cara Kerja RIP

RIP bekerja dengan menginformasikan status network yang dipegang secara langsung kepada router tetangganya.
Karakteristik dari RIP:

- Distance vector routing protocol
- Hop count sebagi metric untuk memilih rute
- Maximum hop count 15, hop ke 16 dianggap *unreachable*
- Secara default routing update 30 detik sekali
- RIPv1 (classfull routing protocol) tidak mengirimkan subnet mask pada update
- RIPv2 (classless routing protocol) mengirimkan subnet mask pada update

Kelemahan RIP
Dalam implementasi RIP memang mudah untuk digunakan, namun RIP mempunyai masalah serius pada Autonomous System yang besar, yaitu :

1) Terbatasnya diameter network

Telah disebutkan sedikit di atas bahwa RIP hanya bisa menerima metrik sampai 15. Lebih dari itu tujuan dianggap tidak terjangkau. Hal ini bisa menjadi masalah pada network yang besar.

2) Konvergensi yang lambat

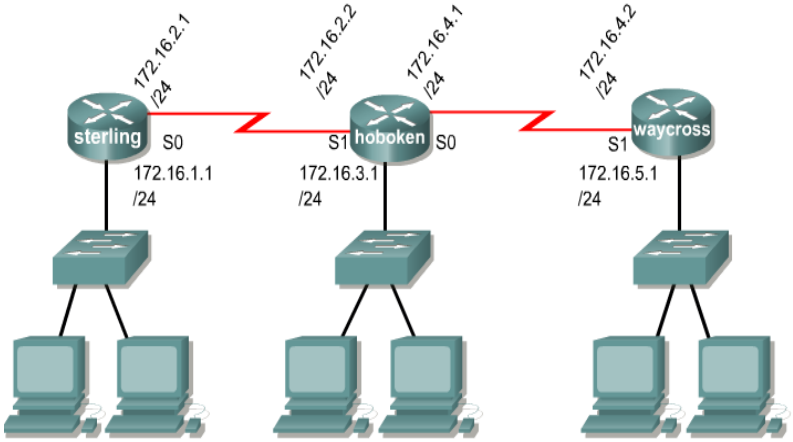
Untuk menghapus entry tabel routing yang bermasalah, RIP mempunyai metode yang tidak efesien. Seperti pada contoh skema network di atas, misalkan subnet 10 bernilai 1hop dari router 2 dan bernilai 2 hop dari router 3. Ini pada kondisi bagus, namun apabila router 1 crash, maka subnet 3 akan dihapus dari table routing kepunyaan router 2 sampai batas waktu 180 detik. Sementara itu, router 3 belum mengetahui bahwa subnet 3 tidak terjangkau, ia masih mempunyai table routing yang lama yang menyatakan subnet 3 sejauh 2 hop (yang melalui router 2). Waktu subnet 3 dihapus dari router 2, router 3 memberikan informasi ini kepada router 2 dan router 2 melihat bahwa subnet 3 bisa dijangkau lewat router 3 dengan 3 hop (2 + 1).Karena ini adalah routing baru maka ia akan memasukkannya ke dalam KRT. Berikutnya, router 2 akan mengupdate routing table dan memberikannya kepada router 3 bahwa subnet 3 bernilai 3 hop. Router 3 menerima dan menambahkan 1 hop lagi menjadi 4. Lalu tabel routing diupdate lagi dan router 2 meneriman informasi jalan menuju subnet 3 menjadi 5 hop. Demikian seterusnya sampai nilainya lebih dari 30. Routing atas terus menerus looping sampai nilainya lebih dari 30 hop.

3) Tidak bisa membedakan network masking lebih dari /24

RIP membaca ip address berdasarkan kepada kelas A, B dan C. Seperti kita ketahui bahwa kelas C mempunyai masking 24 bit. Dan masking ini masih bias diperpanjang menjadi 25 bit, 26 bit dan seterusnya. RIP tidak dapat membacanya bila lebih dari 24 bit. Ini adalah masalah besar, mengingat masking yang lebih dari 24 bit banyak dipakai. Hal ini sudah dapat di atasi pada RIPv2.

7.4 Praktikum

Buatlah jaringan computer sesuai dengan skema berikut :



Gambar 7.14 Skema Jaringan RIP

Konfigurasi router di atas agar semua segment jaringan bisa berhubungan.

Configuration for Router1

```
Router> enable
Router# hostname sterling
Sterling#configuration terminal
Sterling(config)# interface eth 0
Sterling(config-if)#ip address 172.16.1.1 255.255.255.0
Sterling(config-if)#no shutdown
Sterling(config-if)#exit
Sterling(config)#interface serial 0
Sterling(config-if)#ip add 172.16.2.1 255.255.255.0
Sterling(config-if)#clock rate 56000
Sterling(config-if)#no shutdown
Sterling(config-if)#exit
```

Configuration for Router2

```
Router> enable
Router# hostname hoboken
hoboken#configuration terminal
hoboken(config)# interface eth 0
hoboken(config-if)#ip address 172.16.3.1 255.255.255.0
hoboken(config-if)#no shutdown
hoboken(config-if)#exit
hoboken(config)#interface serial 1
```

```
hoboken(config-if)#ip add 172.16.2.2 255.255.255.0
hoboken(config-if)#clock rate 56000
hoboken(config-if)#no shutdown
hoboken(config-if)#exit
hoboken(config)#interface serial 0
hoboken(config-if)#ip add 172.16.4.1 255.255.255.0
hoboken(config-if)#clock rate 56000
hoboken(config-if)#no shutdown
```

Configuration for Router3

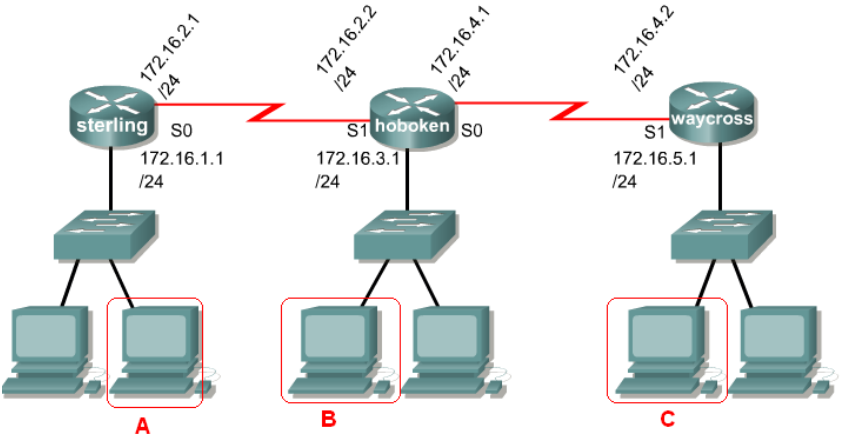
```
Router> enable
Router# hostname Waycross
Waycross#configuration terminal
Waycross(config)# interface eth 0
Waycross(config-if)#ip address 172.16.5.1 255.255.255.0
Waycross(config-if)#no shutdown
Waycross(config-if)#exit
Waycross(config)#interface serial 1
Waycross(config-if)#ip add 172.16.4.2 255.255.255.0
Waycross(config-if)#clock rate 56000
Waycross(config-if)#no shutdown
Waycross(config-if)#exit
```

DYNAMIC ROUTE CONFIGURATION

```
Sterling(config)# router rip
Sterling(config-router)# network 172.16.1.0
Sterling(config-router)# network 172.16.2.0
----
hoboken(config)# router rip
hoboken(config-router)# network 172.16.2.0
hoboken(config-router)# network 172.16.3.0
hoboken(config-router)# network 172.16.4.0
----
Waycross(config)#router rip
Waycross(config-router)#network 172.168.4.0
Waycross(config-router)#network 172.168.5.0
```

7.5 Troubleshooting

Mengecek konfigurasi dari routing static bisa dilakukan dengan cara sebagai berikut :



Gambar 7.15 Skema Testing RIP

Dari PC A :

- Lakukan ping/tracert ke PC B.
- Lakukan ping/tracert ke PC C.

8 Router Fisik

Overview

Modul ini berisi pengenalan router cisco. Dibahas juga bagaimana cara konfigurasi router cisco menggunakan konektor DB9 dan RJ45 melalui port console. Implementasi konfigurasi menggunakan aplikasi hyperterminal pada windows. Implementasi jaringan menggunakan perangkat real.

Tujuan

1. Mengenal hardware router
2. Mampu Mengkonfigurasi Router

8.1 Dasar Teori

Router adalah perangkat **jaringan** yang bekerja pada *layer* 3 OSI (*network layer*) dan dapat menghubungkan dua atau lebih jaringan yang memiliki *subnet* berbeda. *Router* juga berfungsi sebagai pengatur arus lalu lintas jaringan dan memiliki tugas sangat vital dalam menentukan kondisi sebuah jaringan.

Jadi fungsi router, secara mudah dapat dikatakan, menghubungkan dua buah jaringan yang berbeda, tepatnya mengarahkan rute yang terbaik untuk mencapai network yang diharapkan

Dalam implementasinya, router sering dipakai untuk menghubungkan jaringan antar lembaga atau perusahaan yang masing-masing telah memiliki jaringan dengan network id yang berbeda. Contoh lainnya yang saat ini populer adalah ketika perusahaan anda akan terhubung ke internet. Maka router akan berfungsi mengalirkan paket data dari perusahaan anda ke lembaga lain melalui internet, sudah barang tentu nomor jaringan anda akan bereda dengan perushaaan yang anda tuju.

Jika sekedar menghubungkan 2 buah jaringan, sebenarnya anda juga dapat menggunakan pc berbasis windows NT atau linux. Dengan memberikan 2 buah network card dan sedikit setting, sebenarnya anda telah membuat router praktis. Namun tentunya dengan segala keterbatasannya.

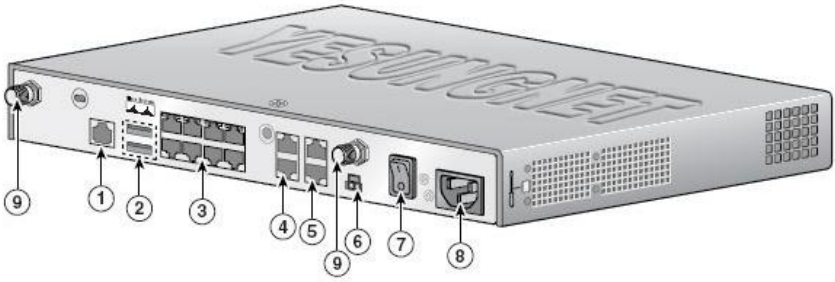
Di pasaran sangat beragam merek router, antara lain baynetworks, 3com dan cisco. Modul kursus kita kali ini akan membahas khusus cisco. Mengapa ? karena cisco merupakan router yang banyak dipakai dan banyak dijadikan standar bagi produk lainnya.

8.2 Cisco Router

Router yang digunakan dalam praktikum kali ini adalah cisco 1801. Interface dari router tersebut seperti gambar berikut :

Gambar 8.1 Interface Router 1801

Sedangkan detail dari interface router cisco 1801 memiliki bermacam-macam interface seperti gambar berikut :



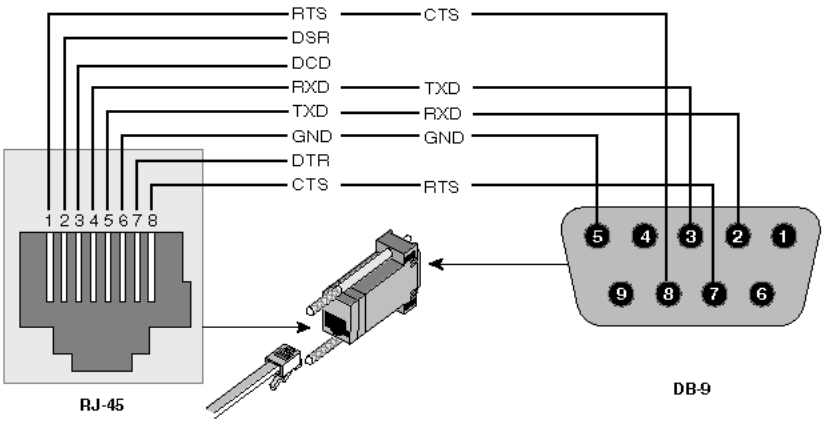
1	ISDN BRI S/T port	5	Console and AUX ports
2	USB 2.0 ports	6	POE connector[1]
3	Managed 8-port FE switch	7	Power switch
4	FE WAN ports	8	Power connector
9	RP-TNC antenna connectors (wireless models only)		

Gambar 8.2 Skema Port Cisco 1801

Untuk melakukan konfigurasi awal router, kita memerlukan kabel DB 9 yang bisa menghubungkan antara serial port pada PC dan console port pada router. Bentuk dari kabel DB9 adalah sebagai berikut :

Gambar 8.3 Konektor RJ45 dan DB9

Skema pembuatan konektor RJ45 dan DB9 secara manual adalah sebagai berikut :



Gambar 8.4 Skema konektor RJ45 dan DB9

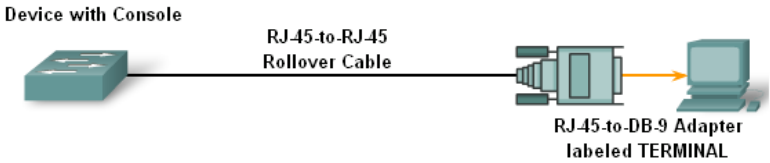
8.3 Praktikum

Alat yang dibutuhkan untuk melakukan praktikum ini adalah :

1) Komputer dengan serial port dan hyperterminal.
2) Cisco Router.
3) Kabel rollover

Langkah-langkah praktikum

1. Hubungkan kabel rollover dengan DB9 ke serial PC dan RJ45 ke port console di router. Seperti skema berikut :

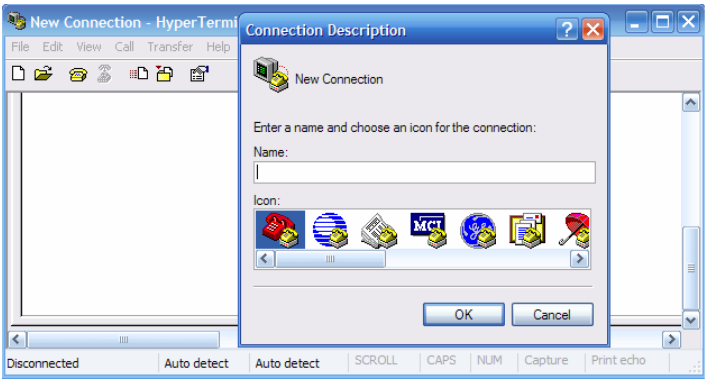


Gambar 8.5 Koneksi menggunakan rollover

2. Nyalakan router dan PC.

3. Jalankan aplikasi hyperterminal pada PC, dengan Start > Programs > Accessories > Communications > HyperTerminal

4. Konfigurasi hyperterminal :

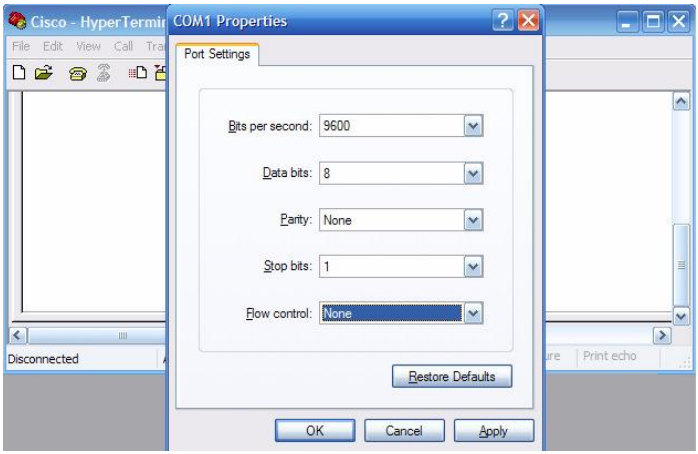


Gambar 8.6 Membuat koneksi

Masukkan nama koneksi di atas dan piih icon yang sesuai.

Gambar 8.7 Konfigurasi Parameter

Pilih COM1 atau koneksi yang sesuai dengan keadaan.

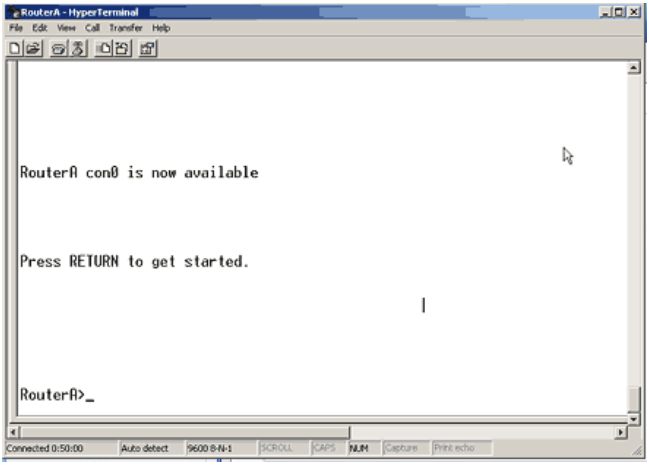


Gambar 8.8 Parameter Koneksi

Masukkan parameter koneksi dengan nilai seperti di bawah ini.

Setting	Value
Bits per Second	9600
Data bits	8
Parity	None
Stop bits	I
Flow control	None

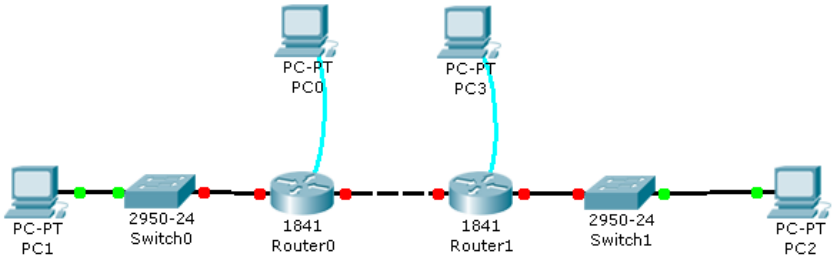
Klik OK. Jika tidak ada error maka akan muncul tampilan seperti gambar berikut.



Gambar 8.9 Hyperterminal Console

3.2.1 Skema praktikum.

Susunlah jaringan computer yang sesuai dengan skema jaringan berikut.



Gambar 8.10 Skema Jaringan Router Fisik

1) Tentukan IP dari setiap segmen jaringan yang ada.
2) Konfigurasi router dengan menggunakan hyperterminal. Dalam hal ini pc yang digunakan untuk konfigurasi adalah PC0 untuk konfigurasi router0 dan PC3 untuk konfigurasi router1.
3) Lakukan testing koneksi dari PC1 ke PC2.

Daftar Pustaka

1. Roger Pressman, "Software Engineering A Practitioner's Approach", 5th Edition, Mc GrawHill
2. Tanembaum, Andrew S.2003.Computer Networks.Prentice Hall
3. Mir, Nader F.2006.Computer and Communication Network.Prentice Hall.
4. Lammle, Todd.2004.CCNA.Sybex.